FRAMEWORK FOR DEVELOPMENT OF A RISK-INFORMED, PERFORMANCE-BASED 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

July 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 May 2006.

This version of the framework is a working draft. It does not represent a staff position and is subject to changes and revisions.

ABSTRACT

Table of Contents

List of Figures

List of Tables

EXECUTIVE SUMMARY

The purpose of this report is to document the technical basis to support the development of a 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 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.

- 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 provide the foundation for technology-specific implementation, through the use of technology-specific implementing guidance in those areas unique to a specific technology.

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.

Defense-in-depth remains a fundamental part of the approach taken and has as its purpose applying determinstic principles to account for uncertainties. The defense-in-depth approach taken, at a high level, calls for:

- the application of a set of defense-in-depth principles that result in certain deterministic criteria; 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:

- consider intentional as well as inadvertent events;
- include accident prevention and mitigation capability;
- ensure key safety functions are not dependent upon a single element of design, construction, maintenance or operation;
- consider uncertainties in equipment and human performance and provide appropriate safety margin;
- provide alternative capability to prevent unacceptable releases of radioactive material; and
- be sited at locations 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 (provides protection against intentional acts);
- maintaining stable operation (provides measures to reduce the likelihood of challenges to safety systems);
- protective systems (provides highly reliable equipment to respond to challenges to safety);
- maintaining barrier integrity (provides isolation features to prevent the release of radioactive material into the environment); and
- protective actions (provides planned activities to mitigate any impacts due to failure of the other strategies).

These protective strategies provide a high-level defense-in-depth structure which new designs would be required to have. In effect, they provide for successive lines of defense, each of which needs to be included in the design.

A set of probabilistic criteria (Chapter 6) have been developed consistent with the Safety Goal QHOs that address:

- allowable consequences of event sequences versus their frequency;
- selection of event sequences which must be considered in the design; and
- safety classification of equipment.

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. This is expressed in the form of a frequency-consequence (F-C) curve as shown in Figure ES-1. The allowable consequences are based upon existing dose limits or doses necessary to meet the QHOs, as described in Chapter 6. Their correlation with event frequency is based upon guidance given in ICRP Publication 64, “Protection

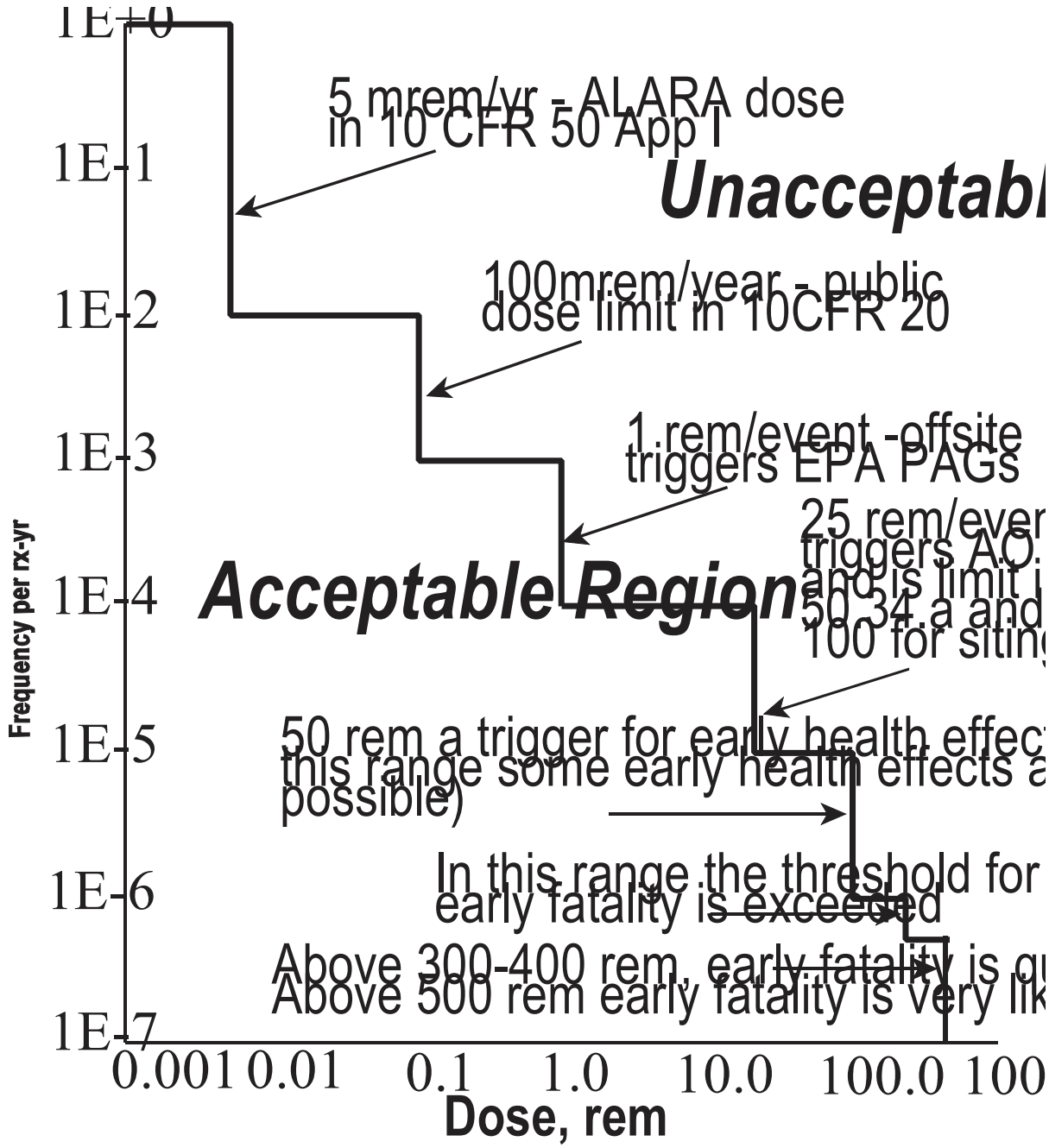


Figure ES-1 Frequency-consequence curve.

from Potential Exposure: A Conceptual Framework." The consequences from each event sequence from the probabilistic risk assessment (PRA) and each event sequence selected as a licensing basis event (LBE - discussed below) must meet the F-C curve.

Frequency categories have been established to guide the selection of events which must be considered in the design. These frequency categories are:

frequent events	$\geq$	10^{-2}/yr			
infrequent events	<	10^{-2}/yr	but	$\geq$	10^{-5}/yr
rare events		< 10^{-5}/yr	but	$\geq$	10^{-7}/yr

In all cases mean frequency values are to be used. These frequency categories define what event sequences must be considered in the licensing process. Within each of these frequency categories certain event sequences are chosen for more conservative deterministic analysis, including comparison to the F-C curve. These events are called LBEs and are generally those with the highest consequences for a given type of accident (e.g., reactivity insertion, loss of coolant, etc.). The purpose of the LBEs is to demonstrate the conservatism of the PRA analysis. In addition, a deterministic event, with a conservative source term is to be used for comparison with siting criteria. Chapter 6 provides additional descriptions of the event categories, the LBE selection and acceptance criteria, the deterministic event and analysis guidelines.

The safety classification of equipment is to follow a probabilistic approach whereby importance measures and other risk metrics are to be used to determine which equipment is safety significant and which is not. Equipment classified as safety significant would be subject to special treatment to ensure it can perform its safety function. Chapter 6 provides additional discussion on the safety classification process.

As discussed above, risk assessment will have a more prominent and fundamental role in the licensing process than it does today under 10 CFR 50, since the risk assessment will be an integral part of the design process and licensing analysis. Therefore, a high level of confidence is needed in the results of the risk assessment used to support licensing. In addition, under the risk-informed licensing approach, the risk assessment will need to be maintained up to date over the life of the plant, since it will be an integral part of decision-making with respect to operations (e.g., maintenance, plant configuration control) and plant modifications. Guidance on the scope and technical acceptability of the risk assessment needed to support this licensing approach is provided in Chapter 7.

In Chapter 8, the protective strategies are examined to identify what needs to be done to ensure the success of each one. Figure ES-2 illustrates the process used for this examination. The process starts with the development of a logic tree for each protective strategy which is used to develop a set of questions, the answers to which identify the topics the requirements must address to ensure the success of the protective strategy. This is supplemented by application of the defense-in-depth principles described above to each protective strategy to address uncertainties and utilization of the risk and design criteria developed in Chapter 6. The topics identified are organized by whether they apply to design, construction or operation and, where guidance related to the topic is provided in the framework, an appropriate reference is given. A similar process was also applied to the identification of topics for administrative requirements. The list of topics resulting from the process in Figure ES-2 is shown Table ES-1. The list of topics 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 (i.e., following the guidelines in NUREG/BR-0303, "Guidance for Performance-Based Regulation") and using existing requirements in 10 CFR 50 where they are already technology-neutral (i.e., building upon existing

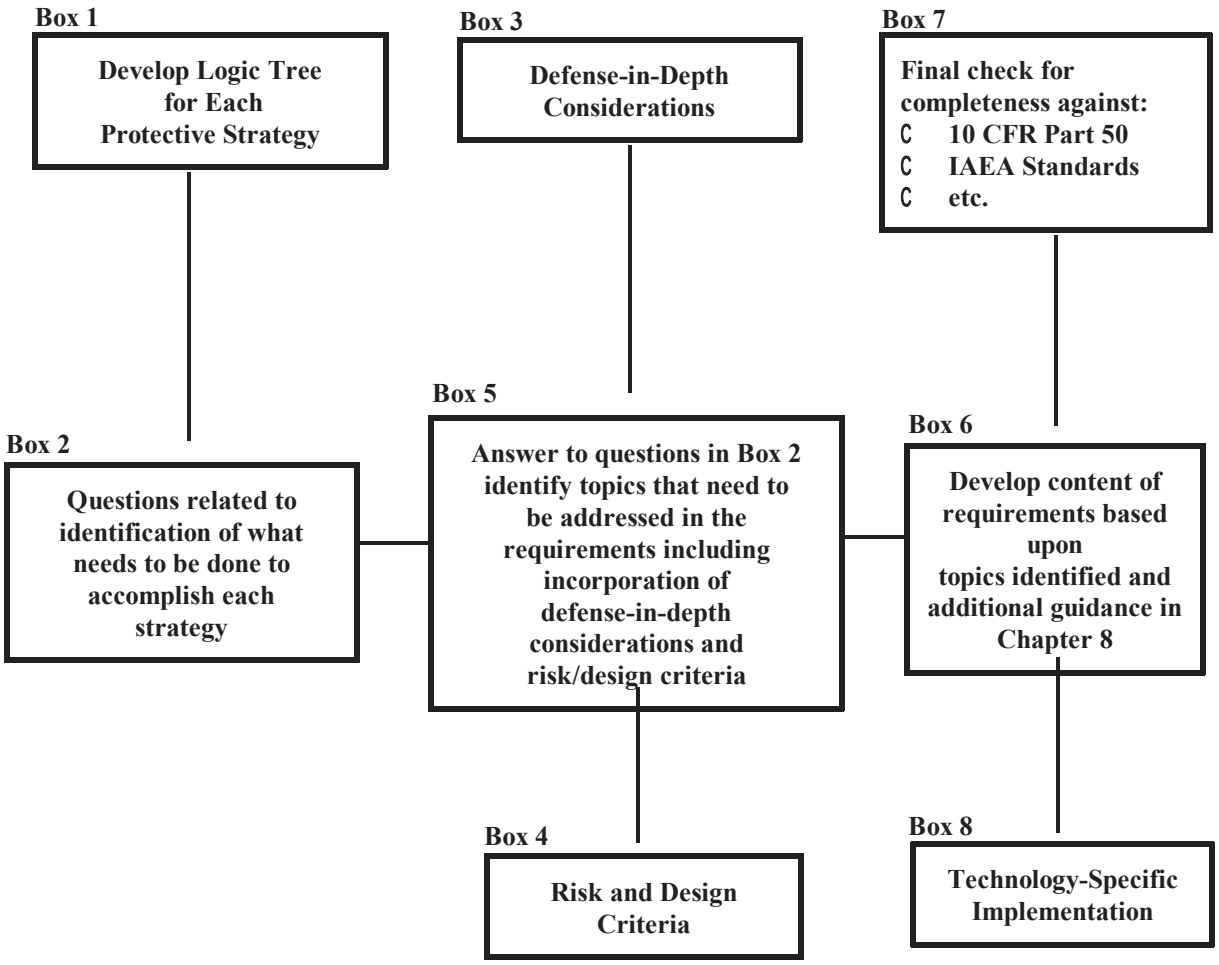


Figure ES-2 Process for identification of requirements topics.

requirements, as much as practical). A completeness check was also made by comparing the topics identified in Chapter 8 to other safety requirements (e.g., IAEA Standards, 10 CFR 50). The results of the completeness check are discussed in Chapter 8, and generally conclude that the topics included in Table ES-1 are reasonably complete. Finally, guidance regarding which of the requirements may need technology-specific guidance to support its implementation is provided in Chapter 8.

Table ES-1 Topics for requirements.

Topic
(A) Topics Common to Design, Construction and Operation
1) QA/QC
2) PRA scope and technical acceptability
(B) Physical Protection
1) General (10 CFR 73)
2) Perform security assessment integral with design
3) Security performance standards
(C) Good Design Practices
1) Plant Risk: - Frequency Consequence curve - QHOs (including integrated risk)
2) Criteria for selection of LBEs
3) LBE acceptance criteria: • frequent events (dose, plant damage) • infrequent events (dose, plant damage) • rare events (dose) • link to siting
4) Keep initiating events with potential to defeat two or more protective strategies $<10^{-7}$/plant year
5) Criteria for safety classification and special treatment
6) Equipment Qualification
7) Analysis guidelines • realistic analysis, including failure assumptions • source term
8) Siting and site-specific considerations
9) Use consensus design codes and standards
10) Materials qualification
11) Provide 2 redundant, diverse, independent means for reactor shutdown and decay heat removal
12) Minimum - 2 barriers to FP release

Table ES-1 Topics for requirements.

Topic
13) Containment functional capability
14) No key safety function dependent upon a single human action or piece of hardware
15) Need to consider degradation and aging mechanisms in design
16) Reactor inherent protection (i.e., no positive power coefficient, limit control rod worth, stability, etc.)
17) Human factors considerations
18) Fire protection
19) Control room design
20) Alternate shutdown location
21) Flow blockage prevention
22) Specify reliability and availability goals consistent with PRA - Establish Reliability Assurance Program - Specify goals on initiating event frequency
23) Use of Prototype Testing
24) Research and Development
25) Combustible gas control
26) Coolant/water/fuel reaction control
27) Prevention of brittle fracture
28) Leak before break
29) I and C Systems • analog • digital • HMI
30) Criticality prevention
31) Protection of operating staff during accidents
32) Qualified analysis tools
(D) Good Construction Practices
1) Use accepted codes, standards, practices
2) Security
3) NDE
4) Inspection

Table ES-1 Topics for requirements.

Topic
5) Testing
(E) Good Operating Practices
1) Radiation protection during routine operation
2) Maintenance program
3) Personnel qualification
4) Training
5) Use of procedures
6) Use of simulators
7) Staffing
8) Aging management program
9) Surveillance, including materials surveillance program
10) ISI
11) Testing
12) Technical specifications, including environmental
13) Develop EOP and AM procedures integral with design
14) Develop EP integral with design
15) Monitoring and feedback
16) Work and configuration control
17) Living PRA
18) Maintain fuel and replacement part quality
19) Security
(F) Administrative
1) Standard format and content of applications
2) Change control process
3) Record keeping
4) Documentation control
5) Reporting
6) Monitoring and feedback:
- plant performance
- environmental releases

Table ES-1 Topics for requirements.

Topic
- testing results
7) Corrective action program
8) Backfitting
9) License amendments
10) Exemptions
11) Other legal and process items from 10CR50

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 framework for licensing future 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.1] The staff noted in its Advanced Reactor Research Plan [Ref.2] to the Commission, that a risk-informed regulatory structure applied to license and regulate advanced (future) reactors, regardless of their technology, could enhance the effectiveness, efficiency, and predictability (i.e., stability) of future 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 framework for establishing requirements, which may be technology-neutral or technology-specific, for future reactors is based on the following considerations:

- 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 the regulations for future 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 future 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. Therefore, 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.

- 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 future reactors. The design and operational issues associated with the future 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 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 future reactors than found among current regulations.

In addition to utilizing the benefits of PRA, the development of a risk-informed performance-based structure for future 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 framework (that can be applied to any reactor design) 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 future 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 future reactors.

1.2 Objectives

The objective of this document is to develop a framework that provides the technical basis, including guidance and criteria, for writing risk-informed, performance-based requirements for licensing future 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 criteria and guidance
- 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 criteria and guidance 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 can be applied to all future 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 (1) having the regulatory requirements specified at a high (technology-neutral) level with accompanying technology-specific regulatory guides, or (2) developing technology-specific requirements for particular designs based on the criteria and guidance offered in the framework.

The framework addresses risks from all sources of radioactivity that are present at the plant except for spent fuel storage and handling. These include: reactor full-power, low-power and shut-down operation, 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 are also 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 covers 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 future plant licensing in a new stand-alone part in 10 CFR. 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. 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:

- ***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.
- ***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.

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 future 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 future 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 future 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.

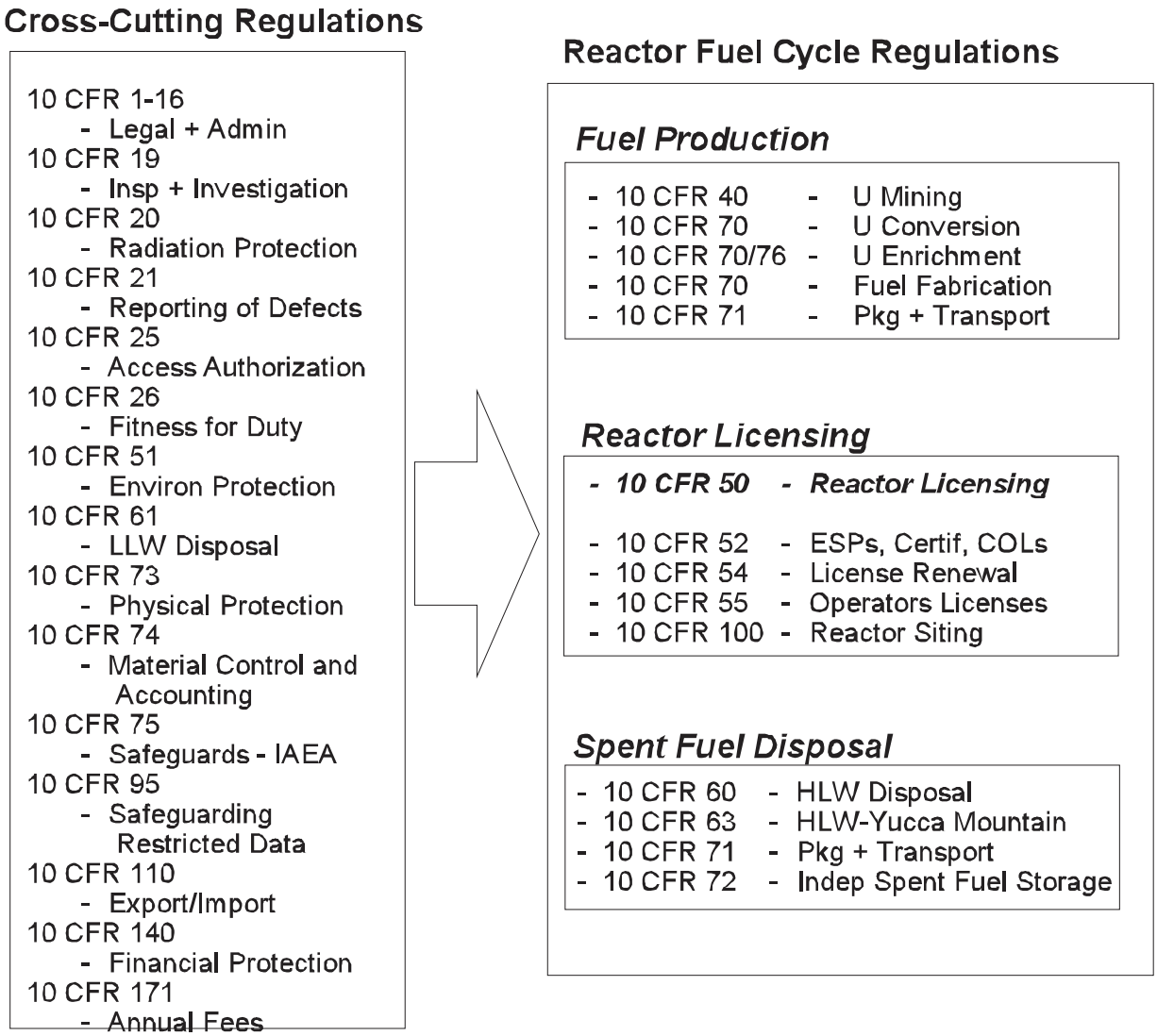
These regulations extend from Part 40 that cover the licensing of source material, through Part 70 that covers the licensing of various operations leading to the fabrication of fuel assemblies, Parts 72 and 63 that cover the licensing of reactor spent fuel storage either at the reactor site or in an 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.

The framework has been developed to provide a structure and technical basis supporting the preparation of a new, stand alone, part for 10 CFR (called 10 CFR 53) which would represent a risk-informed and technology-neutral alternative to licensing NPPs under 10 CFR 50. No changes (other than conforming changes) would be needed in other parts of 10 CFR to implement 10 CFR 53. As such, it is important to recognize where 10 CFR 50 interfaces with the other parts of 10 CFR so that 10 CFR 53 can maintain these same interfaces.

Where 10 CFR 50 interfaces with other parts of 10 CFR is provided in detail in Appendix B. The appendix identifies those interfaces contained in 10 CFR 50 (Table B-1) and those other regulations in 10 CFR that refer to 10 CFR 50 (Table B-2). As can be seen in the tables, there are many interfaces which the new 10 CFR 53 will need to maintain.

Figure 1-1 shows schematically how the framework relates to 10 CFR. As mentioned previously, it is only providing a risk-informed and technology-neutral alternative to 10 CFR 50. All other regulations associated with licensing of NPPs or the nuclear fuel cycle would remain unchanged, except for conforming changes to reference the new Part 53. As can be seen from Figure 1-1, the interfaces are associated with reactor specific regulations, cross-cutting regulations (i.e., those regulations affecting more than reactor licensing) and fuel-cycle regulations. Accordingly, in



developing the framework it is important to ensure that the technical bases, criteria and structure preserve these interfaces such that there will be a seamless transition to other parts of 10 CFR.

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 future 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 OVERVIEW

2.1 Introduction

The purpose of this chapter is to describe the overall approach used in developing the framework for future plant licensing. The approach uses an hierarchal structure to explain 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 criteria, which feed
- A process for development of risk-informed, performance-based requirements.

The basis for nuclear reactor regulation originates with the Atomic Energy Act of 1954[(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.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 future plant licensing provides the guidelines and criteria for developing risk-informed, performance-based requirements for future reactors (that could be either technology-neutral or technology-specific), 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 regulatory structure. [Ref.4] Thus the framework is an evolution of the historical licensing process.

[(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.

The framework for future 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 risk-informed, performance-based requirements are developed that 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.

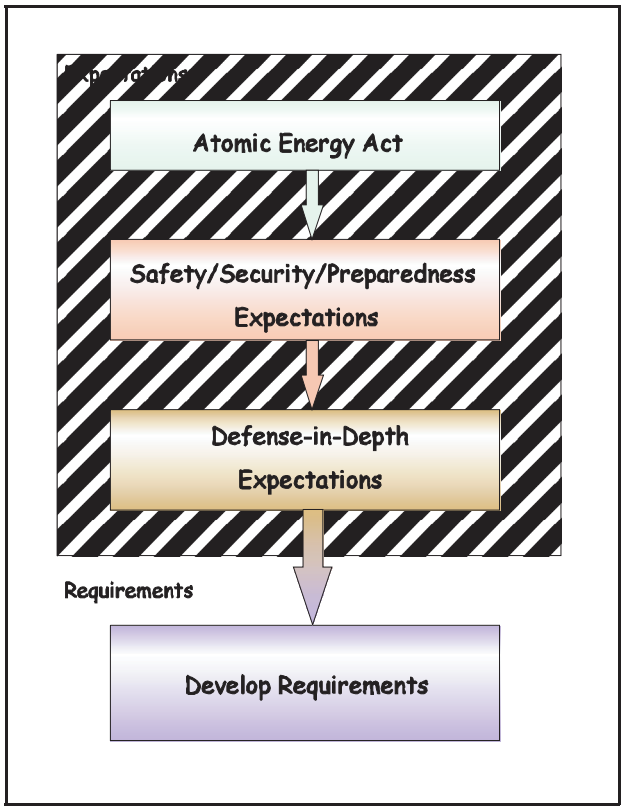


Figure 2-1 Structure of the Risk-Informed, Performance-Based, Technology-Neutral Framework

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. The approach requires that safety and security assessments be done in an integral fashion and realistically model plant and preparedness response. The entire process ensures that safety and security design issues and preparedness requirements are addressed early in the design and that the interface among safety, security and preparedness be considered in decisions regarding plant design, operations and security.

The NRC's ***safety expectations*** are anchored in the Commission's safety goals [Ref. 3.5], 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 future reactors as they are for existing LWRs.

The Commission in their Policy Statement on "Regulation of Advanced Nuclear Power Plants," [Ref. 3.6] noted two expectations:

- that advanced reactors will provide enhanced margins of safety
- 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.

NRC's ***security expectations*** are that new reactors are expected to have the same level of protection as established by 10 CFR 73 and the post 9/11 orders. However, a more robust and risk-informed approach is proposed. Accordingly, a statement that defines security expectations for new plants has been developed. These security expectations describe, in qualitative terms, what security at nuclear power plants is to achieve. As such, they address the level of safety and security to be achieved, the scope of what must be protected and considered, and key aspects of the approach to be followed. They also provide guidance regarding the scope and purpose of the security performance standards to be developed.

Specifically, the security expectations for new plants encompass the following:

- Protection of public health and safety with high assurance is the goal of security.
- The overall level of safety to be provided for security related events should be consistent with the Commission's expectations for safety from non-security related events.
- Security is to be considered integral with (i.e., in conjunction with) design and preparedness.
- A defined set of beyond DBTs (BDBT) are to be considered, as well as the DBT, to identify vulnerabilities, assess margin and help compensate for uncertainties.
- Defense-in-depth is to be provided against the DBT and each BDBT considered, to help compensate for uncertainties.
- Security is to be accomplished by design, as much as practical.

The NRC's ***preparedness expectations*** include the necessity for emergency preparedness capability, regardless of reactor technology or design or level of safety. On-site and off-site preparedness is expected to be able to support the response to the full range of accidents and security threats. The objective of emergency preparedness is to simplify decisionmaking during emergencies. The emergency preparedness process incorporates the means to rapidly identify, evaluate and react to a wide spectrum of emergency conditions. Actions, such as planning and coordination meetings, procedure writing, team training, emergency drills and exercises, and prepositioning of emergency equipment, all are part of "emergency preparedness." Emergency plans are expected to be dynamic and routinely reviewed and updated to reflect an ever changing environment. The NRC expects that an acceptable, integrated emergency plan will be in place that provides reasonable assurance that adequate protective measures can, and will, be taken in the event of a radiological emergency.

The requirements for emergency planning established in 10 CFR Part 50 and associated guidance will be applicable to new reactors. Making emergency preparedness more risk-informed and performance based is a possibility. A performance-based and risk-informed emergency preparedness regulatory structure would be more efficient and would free up resources. With a performance-based approach, licensees and communities would have the flexibility to address their own challenges and develop their own unique solutions – as long as they met the ultimate performance measures.

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, security, and preparedness 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.5] 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 future 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 future plants will tend to be larger than uncertainties associated with existing plants. In laying the groundwork for defense-in-depth for future 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 future 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).

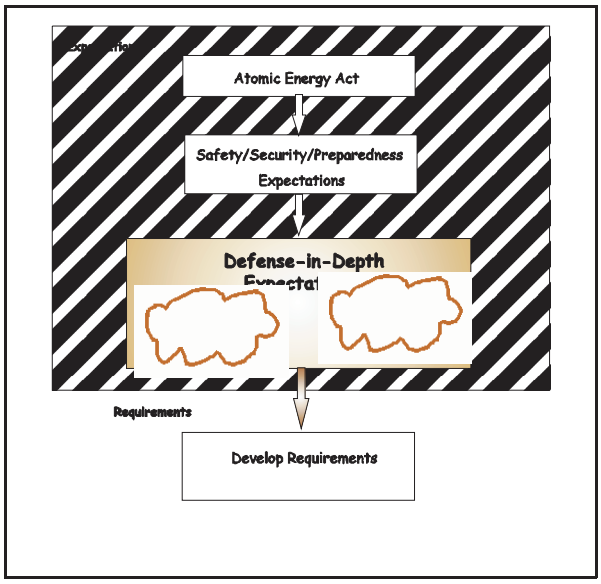


Figure 2-2 Framework Approach to Defense-in-Depth

The deterministic elements of the framework ensure that a set of defense-in-depth principles are followed. These principles[(2)] 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, characteristics of this approach are that

- the high level lines of defense are maintained,
- accident prevention alone cannot be relied on to reach an acceptable level of safety, and
- the capability to mitigate accidents is also needed.

This approach to defense-in-depth has been used in the past to achieve adequate protection and primarily to address completeness uncertainties. A major guarantor of this approach is the maintenance of the five protective strategies[(3)] described in Section 2.4 below.

The probabilistic elements of defense-in-depth are the aggregate of provisions made to

(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.

(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.

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, and

(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 defense-in-depth 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.

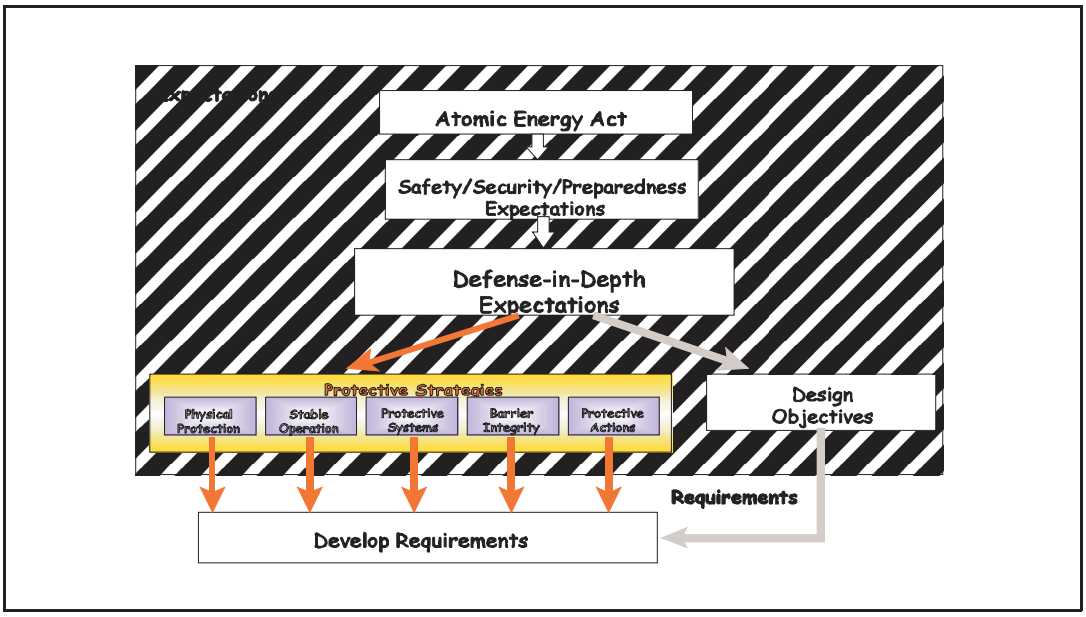


Figure 2-3 Protective Strategies as Elements of Defense-in-Depth

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.

- The **Protective Systems** objective is to ensure that the systems that mitigate[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.

- The **Barrier Integrity**[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 the requirements, as introduced in Section 2.7.

2.5 Design Criteria and Guidance

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 criteria and guidance 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

---

[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.

[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 future reactor designs and prevention/mitigation definitions change as the object under discussion changes - core damage, release from the primary system, release off-site, etc.

that the protective strategies are intended to meet. The design criteria 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.

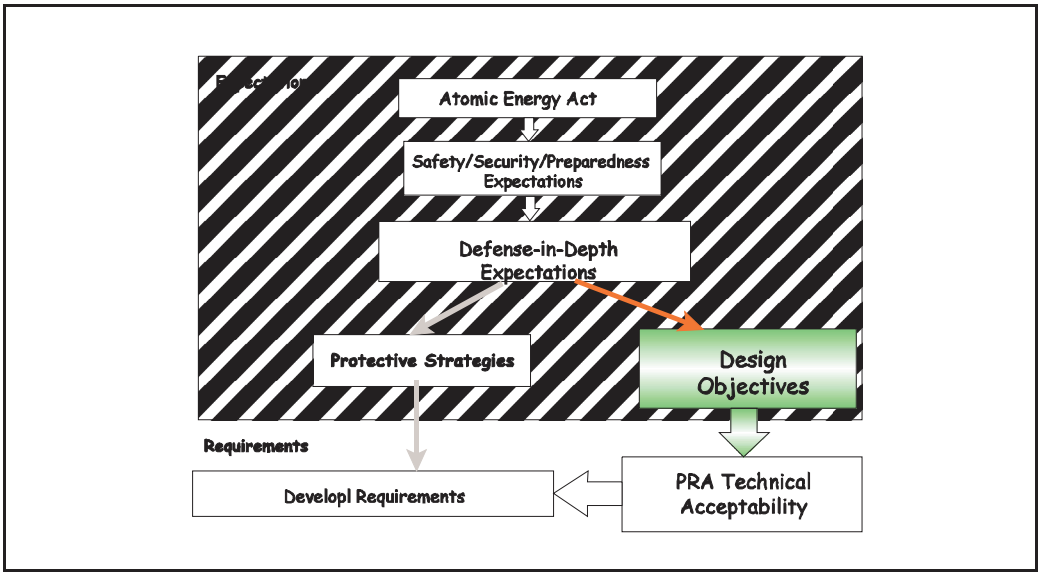


Figure 2-4 How Design Objectives Support Defense-in-Depth

The framework establishes safety related design objectives to ensure that:

(1) the plant risk is acceptable, i.e., meets the QHOs and the frequency consequence (F-C) curve established in Chapter 6.

(2) the selection of those events that are used in the design to establish the licensing basis (licensing basis events or LBEs) is carried out in a risk-informed manner, and LBEs meet the F-C curve with margin, and

(3) the safety classification of systems, structures, and components (SSCs) reflects their importance in reducing plant risk.

In both the LBE selection and the SSC selection, defense-in-depth measures are incorporated, but, in addition, the risk information from the PRA is used 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. As explained in Chapter 6, the LBEs also provide a detailed check on whether the PRA analysis meets the necessary risk guidelines, and are also used in assessment of site suitability.

2.6 PRA Scope and Technical Acceptability

Probabilistic risk assessment (PRA) will play a greater role in the licensing of future reactors. Since the quality of the PRA used in making licensing decisions is commensurate with the significance of the regulatory decision, the expectations of the quality of future PRAs is greater than for currently operations plants. The framework requires a 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 and during plant operation. The PRA is used in the framework to help in:

- establishment of the LBEs,
- identification of safety-significant SSCs and their corresponding special treatment requirements,
- identification of 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.

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 (HLR) are provided for evaluating both internal and external events during all modes of operation. In meeting these HLRs, many of the current PRA methods, techniques, and data used for LWRs are applicable. However modeling future reactors may necessitate extensions of current PRA methods.

For example, future 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.6] 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.

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 future reactors will require that PRAs be living documents.

2.7 Process for Development of Technology-Neutral Requirements

The design criteria and guidance are linked to the protective strategies to develop requirements for future reactor concepts. These requirements 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.

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 future plant licensing would also embody these good practices along with risk insights. 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 taking into account defense-in-depth and design criteria. 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.

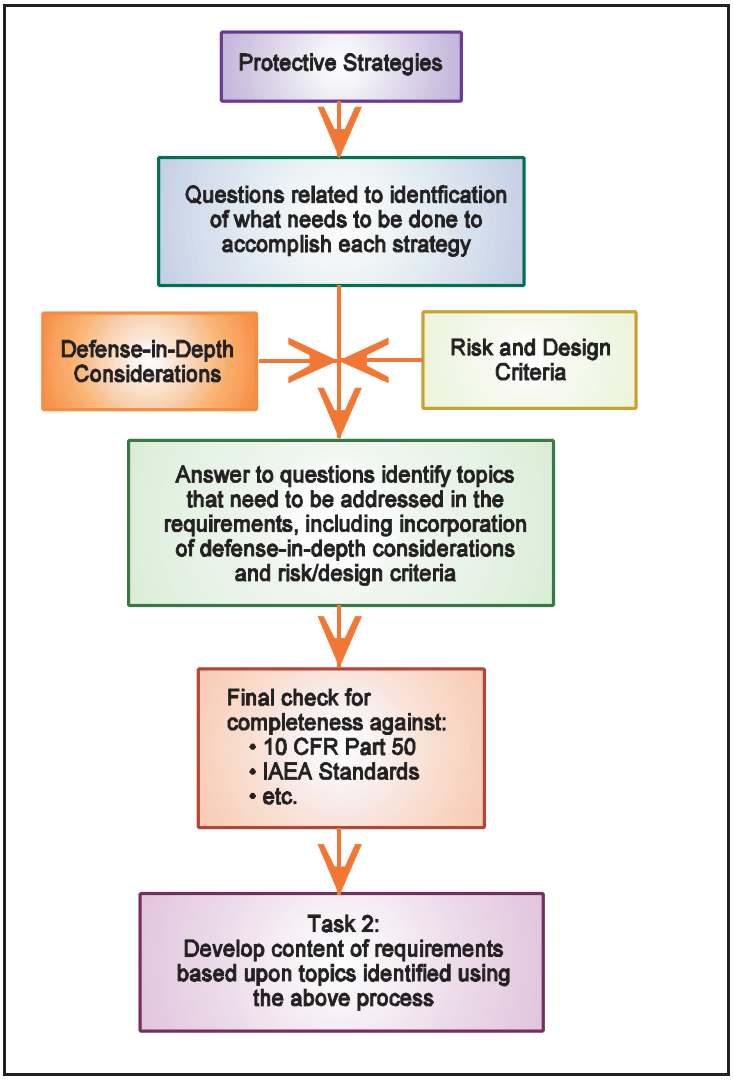


Figure 2-5 Process for Developing Technical and Administrative Requirements from the Protective Strategies

2.8 Summary of Approach

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.

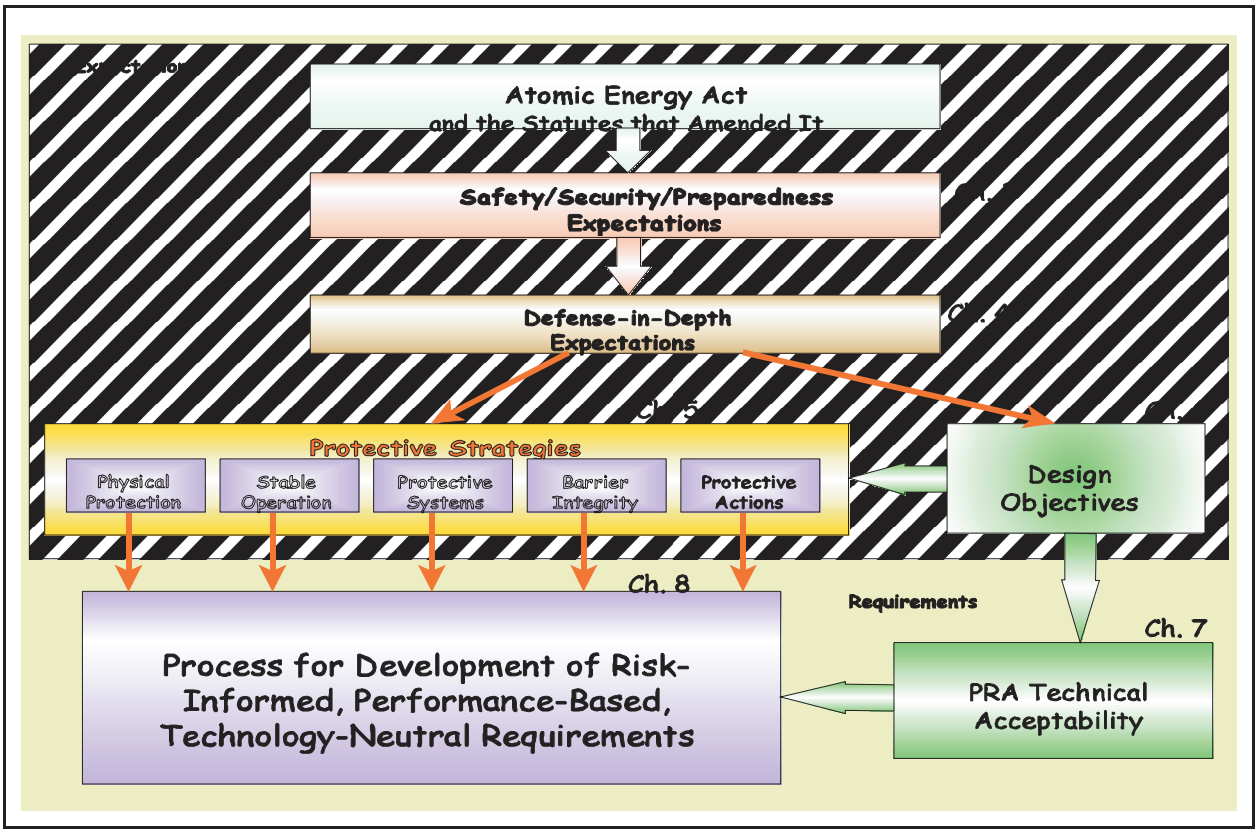


Figure 2-6 The Risk-Informed, Performance-Based, Technology-Neutral Framework Roadmap

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

- The Design Criteria 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 the 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 criteria and PRA technical acceptability lead to the establishment of technical requirements. Administrative requirements[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

[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.

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 the 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.

3. SAFETY, SECURITY AND PREPAREDNESS EXPECTATIONS

3.1 Introduction

The purpose of this chapter is to define the expectations for safety, security, and preparedness required at future plants licensed by the NRC. The chapter's place in the structure of the risk-informed, performance-based, technology-neutral framework (the framework) 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 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.

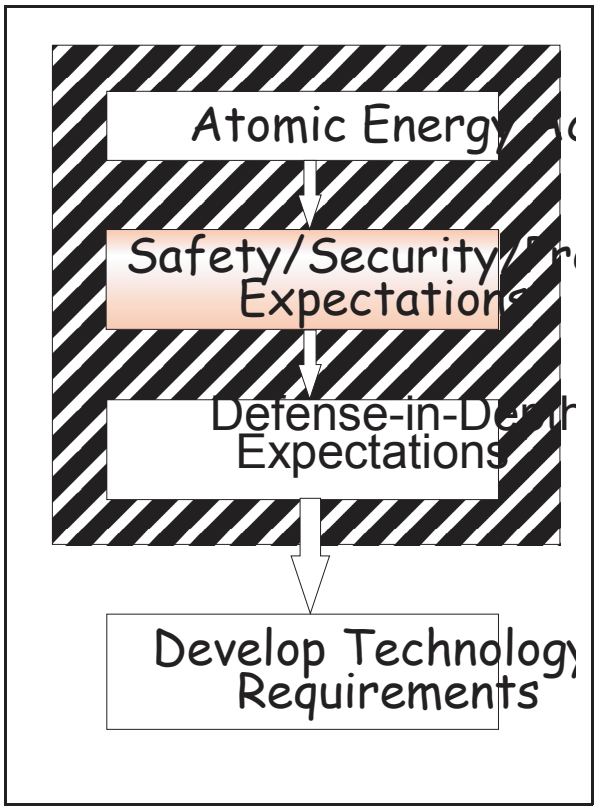


Figure 3-1 Structure of the Framework

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 clarified in "Security Design Expectations for New Reactor Licensing Activities" [Ref.7]. 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.[7] The NRC's ***preparedness expectations*** include the necessity for an emergency planning and preparedness capability, regardless of reactor technology or design.

[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:

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

(14) 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.8] 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. .[8]

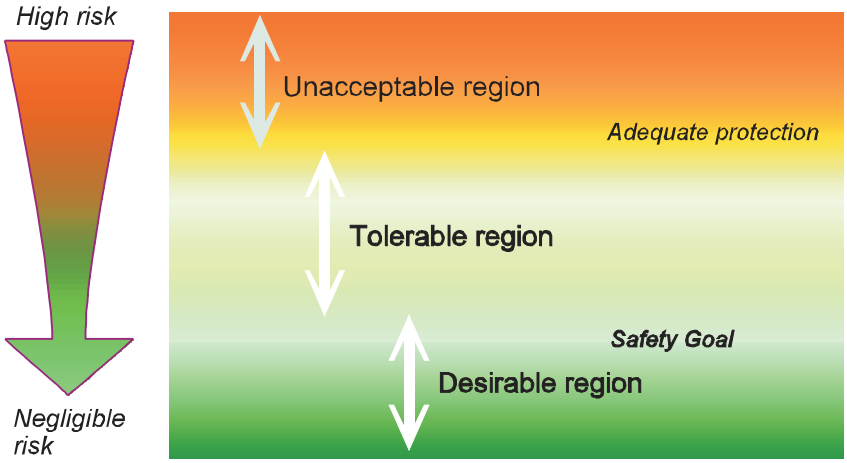


Figure 3-2 Three Region Approach to Risk Tolerability/Acceptance

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 there is only a small chance that the risk will extend into the tolerable region and negligible chance

[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.

that it reaches the upper, unacceptable region. Accordingly, ***the 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.

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.

The NRC's expectations for safety include protection of the environment, as well as direct public health. Appendix C describes how the environment is being protected to the same degree as the public, by the approach described above.

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 can 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.

For current LWRs, the risk examined is almost always expressed in terms of the surrogate 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[(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

[(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.

quantitative values for CDF and LERF be no longer applicable, CDF itself may no longer be a useful risk metric.

Risk metrics that would be applicable to a variety of different reactor designs, 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) 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 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.

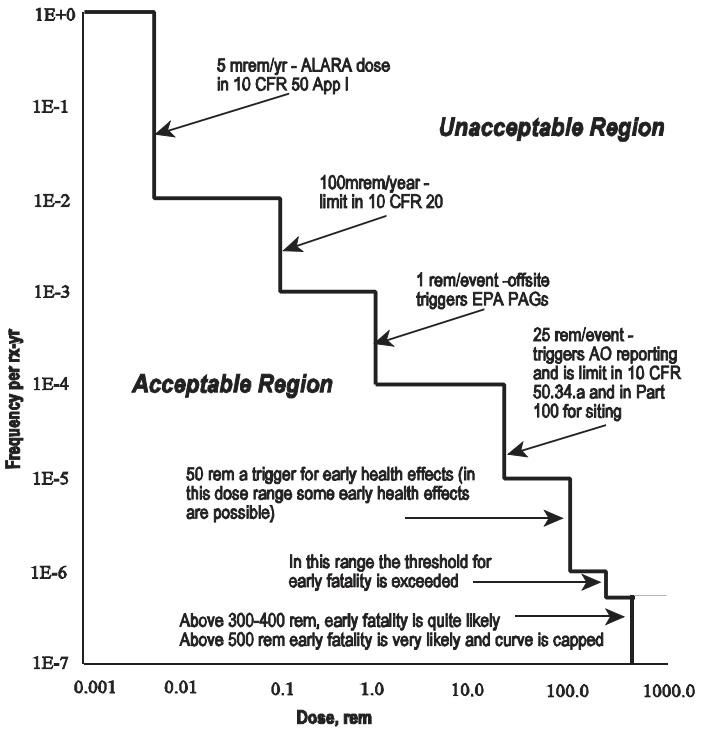


Figure 3-3 Frequency-Consequence Curve

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 their totality. The risk in the safety goals and the QHOs is the total plant risk incurred over a reactor year. This means the PRA results must demonstrate that the total plant risk, i.e., the risk summed 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 per reactor year. 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.

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.

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 Surrogate 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, surrogate 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., 2×10^{-6}/ry individual risk for latent fatalities and 5×10^{-7}/ry individual risk for early fatalities). These surrogate 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 surrogate 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 D 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 surrogate 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 surrogate 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 surrogate objectives should also focus more directly on plant design, thus simplifying the analysis needed.

Surrogate 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 surrogate 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).

CDF and LERF can be demonstrated to be acceptable surrogate risk objectives for current LWRs. Such a demonstration depends on the characteristics of LWR technology, in particular, the ways in which severe accidents can occur and the source terms related to these accidents. Given these characteristics, one can show that restricting CDF below 1E-4/ry and LERF below 1E-5/ry will ensure that the consequence limits embodied in the latent cancer and early fatality safety goals can be met. It is expected that surrogate 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 10 CFR 73 and the post 9/11 NRC requirements. [Ref. 3.2] [Ref. 3.3] However, the framework proposes a major difference in approach, for new plants, where a risk-informed approach is to be taken and security will be evaluated integral with the design, rather than post-design compensatory measures. As discussed in Section 6.4, the security expectations for new plants encompass the following:

- Protection of public health and safety with high assurance is the goal of security.
- The overall level of safety to be provided for security related events should be consistent with the Commission's expectations for safety from non-security related events.
- Security is to be considered integral with (i.e., in conjunction with) design and preparedness.
- A defined set of beyond DBTs (BDBT) are to be considered, as well as the DBT, to identify vulnerabilities, assess margin and help compensate for uncertainties.
- Defense-in-depth is to be provided against the DBT and each BDBT considered, to help compensate for uncertainties.
- Security is to be accomplished by design, as much as practical.

The above security expectations define the elements which must be addressed in the security performance standards (described in Section 6.4). These security expectations are intended to promote enhanced security, emphasize design solutions to security issues, provide means to ensure integration of security, safety and preparedness and provide guidance for qualitative and quantitative measures for assessing security. 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.

A security assessment will be required to ensure performance is adequate. The security assessment will involve characterization of the potential threat, the potential targets, and the potential consequences. The frequency of the threat depends on some factors only known to the adversary, so it is expected to be outside the scope of evaluations. Nevertheless, the types, objectives, and capabilities, as well as the strategies, of the potential adversaries will need to be taken into account. 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.

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.

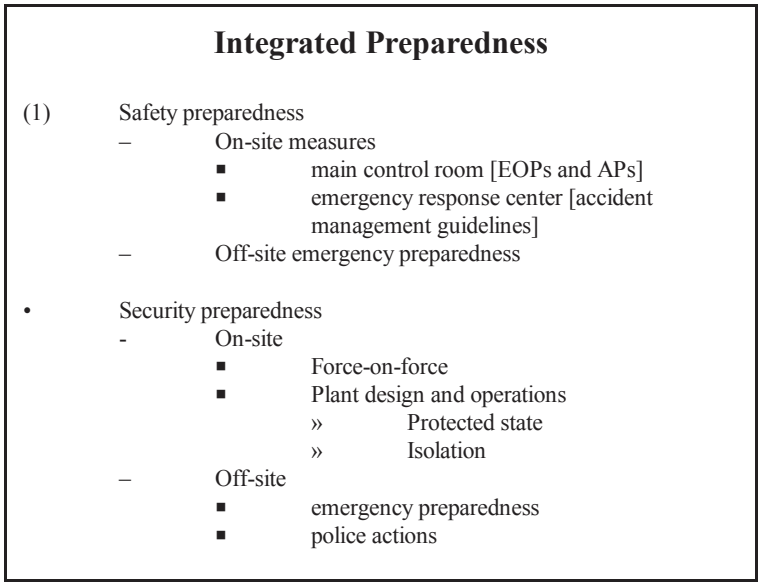


Figure 3-4 Generalized Preparedness as Part of the Protective Actions Protective Strategy

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 expected to function in a unified and coordinated manner. The expectations for the level of safety and protection, implemented through an integrated process, lead to a plant that is safe and robust against all internal and external hazards, and inadvertent and advertent threats, and meet the NRC objectives of protecting the public health and safety, and the common defense and security.

The plant's safety and security features are to be designed to minimize adverse interactions and optimize their integrated benefit. This includes potential SSC interactions that are the result of the design process, and expected operational and maintenance practices that could change the required response by operation or security personnel. An example of a design interaction is restricting the number of access points for a given location which may be beneficial to security, but could result in longer response times for operators during plant emergencies. An example of a operational interaction could be the removal from service of a key plant component for maintenance that could impact the plant's security response. Therefore, it is expected that during the development of the safety and security requirements that their impact on each other and on preparedness be examined. It is also expected that changes in design, operation and maintenance that have the potential for adverse effects on safety and security, including the site emergency plan, will be assessed and managed before implementing changes to plant configurations, facility conditions, or security. This assessment could be accomplished using PRA methods and security vulnerability assessment techniques in order to provide a rational bases for decision-making by infusing safety objectives with security concerns.

In addition to the integration of safety and security, the on-site and off-site preparedness is expected to be able to support the response to the full range of accidents and security threats. This results in the security and preparedness implications of design decisions being fully integrated with more traditional safety decisions. This integration needs to be exercised in such a way to ensure that security requirements do not place undue limits on the ability for preparedness in protecting plant safety, and the health and safety of nearby populations.

Another important element associated with integration is the expectation that there will be an increased reliance on design enhancements over operational solutions. These design enhancements should increase the margins associated with key elements of emergency response including the required times and complexities of actions associated with operation, security and emergency responders.

The net impact of the integration of safety, security, and preparedness is an increase in the overall effectiveness of the integrated response to any plant challenge.

4. DEFENSE-IN-DEPTH: TREATMEN

4.1 Introduction

The purpose of this chapter is to describe the approach u in-depth for future reactors. The core of the NRCs safety ept of defense-in-depth, and defense-in-depth remains bas ns of the risk-informed, performance-based, framework. T pth is to compensate for uncertainty. This includes uncertain es to safety, as well as in the measures taken to assure safe he relationship of defense-in-depth to the rest of the struc

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."

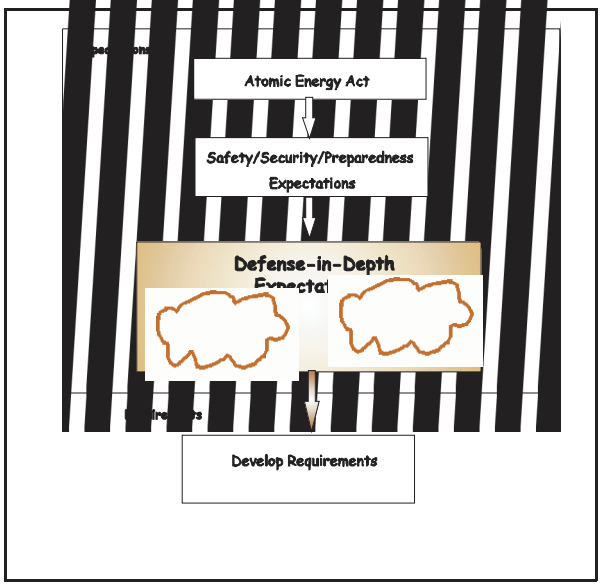


Figure 4-1 Framework Approach to Defense-in-Depth

Regulatory Guide 1.174, which deals with risk-informed decisionmaking regarding changes to the licensing basis of plants, states that "... the staff expects that:.....appropriate consideration of uncertainty is given in analyses and interpretation of findings, including using a program of monitoring, feedback, and corrective action to address significant uncertainties." It further states that "Defense-in-depth... has been and continues to be an effective way to account for uncertainties in equipment and human performance. If a comprehensive risk analysis is done, it can be used to help determine the appropriate extent of defense in depth (e.g., balance among core damage prevention, containment failure, and consequence mitigation) to ensure protection of public health and safety."

While Reg Guide 1.174 and other references always link defense-in-depth and safety margin [10] the terms are often discussed separately. The framework definition of defense-in-depth includes safety margin as an integral part: *Defense-in-depth is an element of NRC's safety philosophy that is used to address uncertainty by employing successive measures including safety margins to prevent and mitigate damage if a malfunction, accident or naturally caused event occurs at a nuclear facility.*

In a broad sense, the objective of defense-in-depth is to ensure that safety will not be wholly

[10] For example, Reg Guide 1.174 lists among key principles to be met that: (1) the proposed change is consistent with the defense-in-depth philosophy, and (2) the proposed change maintains sufficient safety margins.

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 future reactors and is based upon the following principles, which address the scope and approach taken for defense-in-depth:

5. both intentional acts and inadvertent events should be considered

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

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

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

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

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

This chapter also addresses the most common defense-in-depth measures arising from these principles. These are providing redundancy, diversity, and safety margins, both in the equipment and the human actions that are important for the safe operation of the plant. Redundancy enhances the reliability of independent means to accomplish a needed function; diversity (and separation) generally provide protection against dependent (common cause) failures of multiple means. Allowances in excess of minimum requirements for physical parameters such as the capacities of hydraulic, electrical and structural components contribute to safety margins that ensure unanticipated increases in demand can be met. Allowances in excess of minimum requirements for temporal parameters, such as time needed for operator actions and preventive systems to correct for deviations, contribute to safety margins that ensure deviations can be remedied even after some initial lapses.

Safety analysts [Ref.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 future 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 future 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 future 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 future reactors the challenge is somewhat different: Establishing what constitutes an adequate level of defense-in-depth in the future reactor designs. In laying the groundwork for

defense-in-depth for future 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. Much of the work of PRA for future 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 future 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 [Ref.10] 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. 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, and

(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 framework approach to defense-in-depth incorporates both deterministic and probabilistic elements.

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). 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.

(2) ensuring that the defense-in-depth principles, discussed in Section 4.4, are followed to develop licensing requirements. 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

(1) using the PRA, to the extent possible, to search for and identify unexpected scenarios, including their associated uncertainties.

(2) 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 future 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 hazards that are known to be extremely small 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., initiating eventss 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 future 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 initiating events 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 excess capacities in the equipment, structure and procedures used here to provide safety margins 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. Sufficient allowances in temporal parameters to ensure safety 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 and appropriate safety margins are provided.***

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 future reactor designs without always having the benefit of reviewing past performance.

Ensuring adequate safety margins is important here in achieving a robust design. (Safety margins are further discussed in Section 4.6.) Excess capacity in physical and temporal

parameters are incorporated in the plant equipment and procedures. Allowances in excess of minimum requirements for physical parameters such as the capacities of hydraulic, electrical and structural components contribute to safety margins that ensure unanticipated increases in demand can be met. Allowances in excess of minimum requirements for temporal parameters, such as time needed for operator actions and preventive systems to correct for deviations, contribute to safety margins that ensure deviations can be remedied 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 future 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 future 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 future 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. (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, 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 intent of the General Design Criteria in Appendix A to 10 CFR Part 50 is maintained.

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.

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.

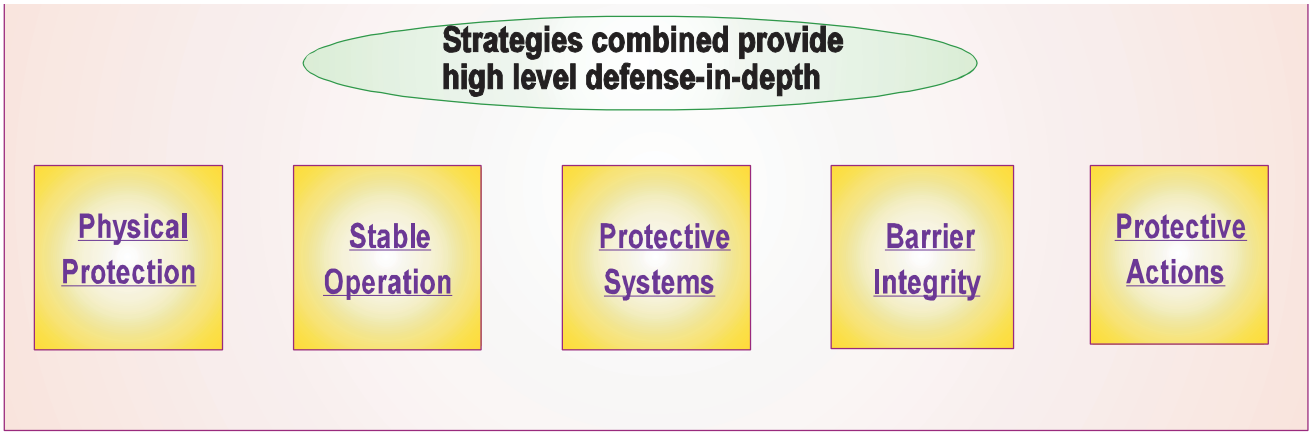


Figure 4-2 Protective Strategies as high level defense-in-depth

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.

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. The application of the defense-in-depth principles to the protective strategies to develop requirements is discussed in detail in Chapter 8. A brief summary of the application of the principles to each strategy is presented here.

Physical protection

- Physical protection obviously needs to consider intentional acts.
- Physical protection needs to address prevention as well as mitigation. 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
- Physical protection must not be dependent upon a single element of design, construction or operation.
- Physical protection needs to account for uncertainties.
- Since physical protection needs to be directed toward preventing an unacceptable release of radioactive material to the environment, 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

Stable operation

- Intentional acts to disrupt operation need to be considered, and such disruptions should be considered under physical protection.

- Designing the plant to prevent accidents is the main emphasis of the stable operation protective strategy. Chapter 6 of this document provides some measures to ensure that the assumptions in the PRA on initiating events are preserved.

- 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.

- 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 defeat barrier integrity and protective actions strategies need to have a very low frequencies, as discussed in Chapter 6.

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

Protective Systems

- At least some of the protective systems need to have the ability to respond to intentional acts as well as inadvertent events.

- Protective systems are needed that prevent events from leading to major plant damage (prevention) as well as preventing the uncontrolled release of radioactive material to the environment should major plant damage occur (mitigation).

- Key plant safety functions (i.e., reactor shutdown and decay heat removal) should not be 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.

- 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 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.

- Plant siting can affect the types and performance of safety systems since site specific hazards may be different.

Barrier integrity

- The number of barriers and their design need to be based upon consideration of both intentional as well as inadvertent events.

- 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. Accident mitigation will be achieved by ensuring the barriers perform their function of containing radioactive material.

- 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.

- 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 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).

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

- 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.

Protective Actions

- The development of protective actions needs to consider intentional acts as well as inadvertent events, and be included in the physical protection protective strategy.

- 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 accomplishment of protective actions must not rely on a single element of design, construction, maintenance or operation.

- Protective actions need to be developed in consideration of uncertainties. 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 protective action program.

- Plant siting will affect protective actions, and needs to be considered in developing plans.

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 the framework view of defense-in-depth a probabilistic approach to defense-in-depth is combined with a deterministic one.

4.5 Safety Margin

Throughout this chapter safety margin has been described as an integral part of defense-in-depth, since the basic purpose of safety margins is to cope with uncertainty. In addition, the compensatory measures that are also part of defense-in-depth must have some margins embedded in them to deal with the accident, malfunction, etc. Compensatory measures that lack margin are not very practical.

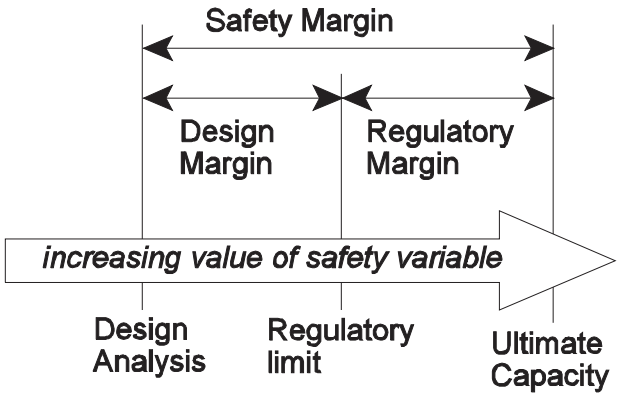


Figure 4-4 Safey Margin Definition

Although the term safety margin is frequently used in engineering design, There are different interpretations of the term “safety margin.” The term is frequently found in regulatory documents that contain phrases such as “maintain adequate safety margin,” or “provide sufficient safety margin,” without a quantitative definition of safety margin. While this use of the term as a qualitative descriptor is useful in many contexts, for the framework a more quantitative description is needed.

Safe operating conditions can be characterized by maintaining limits on one or more safety variables. As stated in Reference 4.x, safety margins are linked to safety limits—limiting values imposed on safety variables (e.g., peak clad temperature (PCT) and containment pressure in current LWRs). Thus, when operating conditions stay within safety limits, the safety barrier or system continues to function, and an adequate safety margin exists. The intent is to allow margin for phenomena and processes that are inadequately considered or neglected in the analysis predicting the behavior of the given system or physical barrier.

For the framework definition of safety margin the safety variable is assumed to have an ultimate capacity, beyond which the safety system or barrier fails, e.g., the ultimate strength of a critical barrier. A regulatory limit is set on the safety variable, well below this capacity, to ensure that the ultimate capacity is not reached during normal operation as well as excursions from normal operation. The difference between the ultimate capacity and the regulatory limit is termed the “regulatory margin” in the framework. The designer can incorporate an additional margin, called the “design margin” in the framework, by designing the system so it operates well below the regulatory limit for normal operations and excursions. Together the regulatory margin and the design margin constitute the safety margin. This definition is schematically illustrated in Figure 4-4.

The schematic of Figure 4-4 provides the background to a quantitative basis for safety margin, but is very simplified. In practice the capacity and the design range of a plant safety variable are not single valued quantities but have probability distributions associated with them. Questions immediately arise, such as what measure of capacity should be used, what excursions from normal operation should be included, what inadequately considered processes need to be compensated for, etc. Defining margin in light of the probabilistic nature of the safety variables and the questions asked above are further pursued in Chapter 6.

From the above discussion it is clear that providing adequate safety margin puts responsibility (1) on the regulator to place the regulatory limit with proper consideration of loads and capacities, and (2) on the designer to adequately set design limits to meet regulatory limits with 'margin.'

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 requirements in Chapter 8.

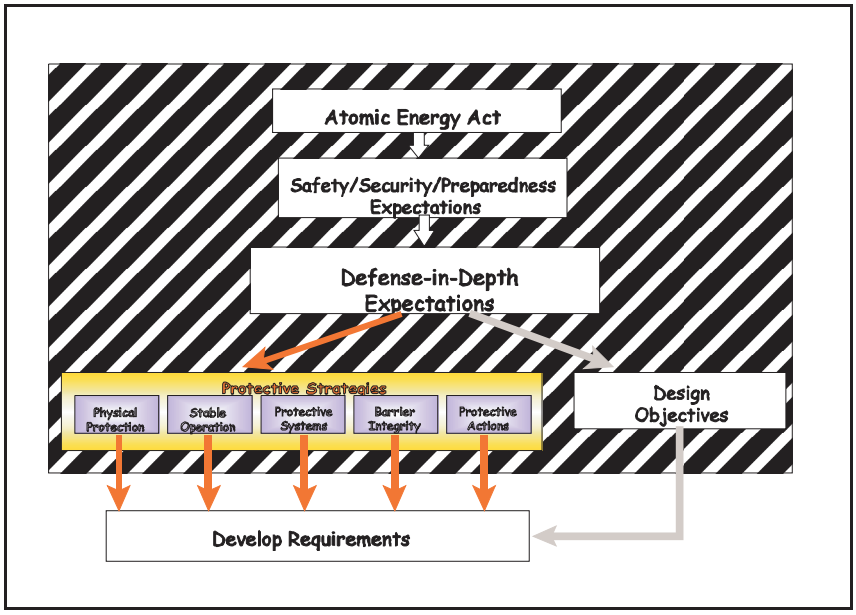


Figure 5-1 Role of Protective Strategies as Elements of Defense-in-Depth

The five protective strategies introduced in Chapter 2 – *Physical Protection, Stable Operation, Protective Systems, Barrier Integrity, and Protective Actions* – satisfy the deterministic (structuralist[11]) [Ref.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.

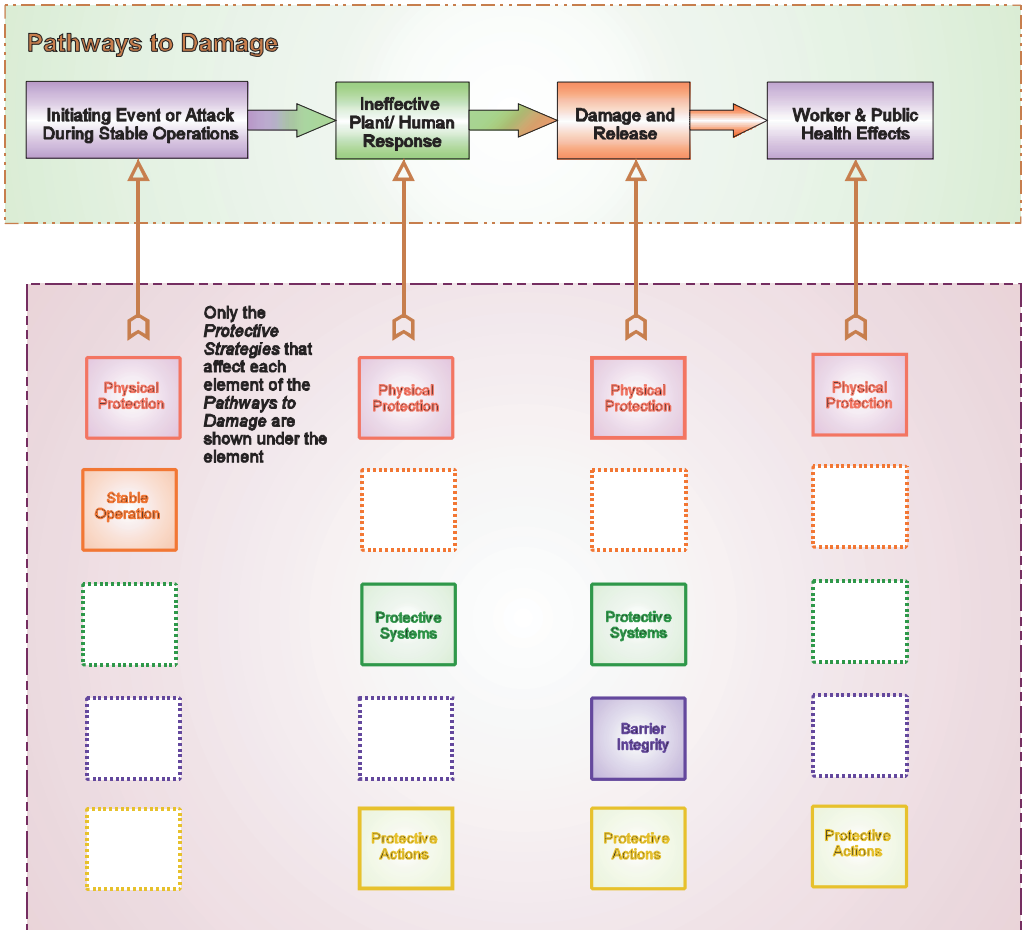
There is another direct way to consider the protective strategies. Look at the pathways to damage

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

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[12] can be breeched; it models:

- initiating events
- successes and failures in the protection systems that are designed to protect barriers
- human actions that can perform or defeat the protective systems or barriers themselves

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

- 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.

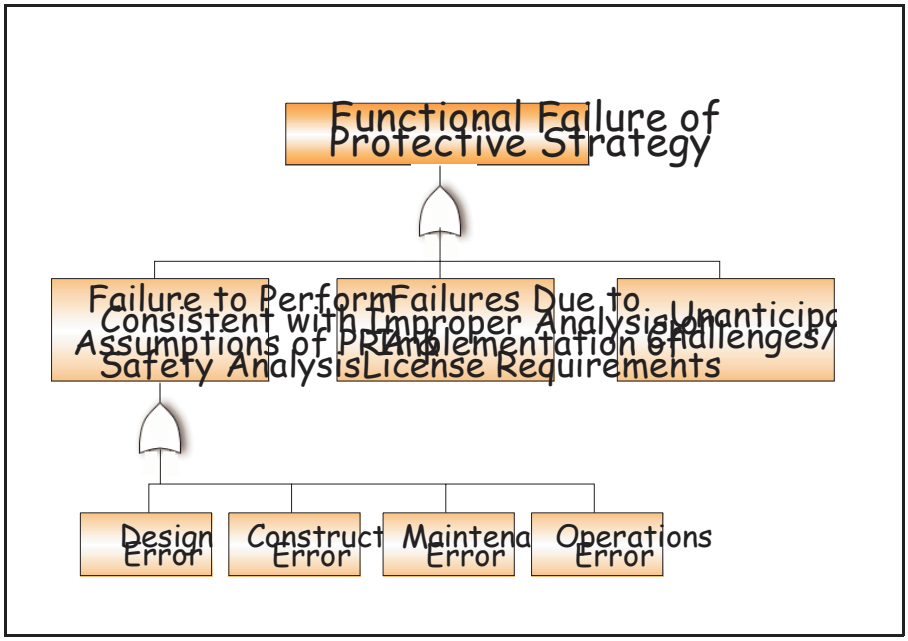


Figure 5-4 Logic Tree Developing Requirements for Each Protective Strategy

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] 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.3] against the range of threats to understand the possible scenarios. [Ref.4]

It is a goal of the risk-informed, performance-based, technology-neutral 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 initiating events are identified, along with their mean frequency of occurrence. Uncertainty in their frequency is also considered and quantified as a probability of frequency distribution. Initiating events 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 initiating events 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 initiating events by their risk significance.

It may also be advantageous to group the initiating events 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 initiating events group, so as to limit the frequency of fuel damage accidents to acceptable levels.

For the future 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 future 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 AND GUIDELINES

6.1 Introduction

The purpose of this chapter is to provide design criteria and associated guidance for the risk-informed licensing process that is part of the risk-informed, performance-based framework approach that is applicable to all reactor designs. 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:

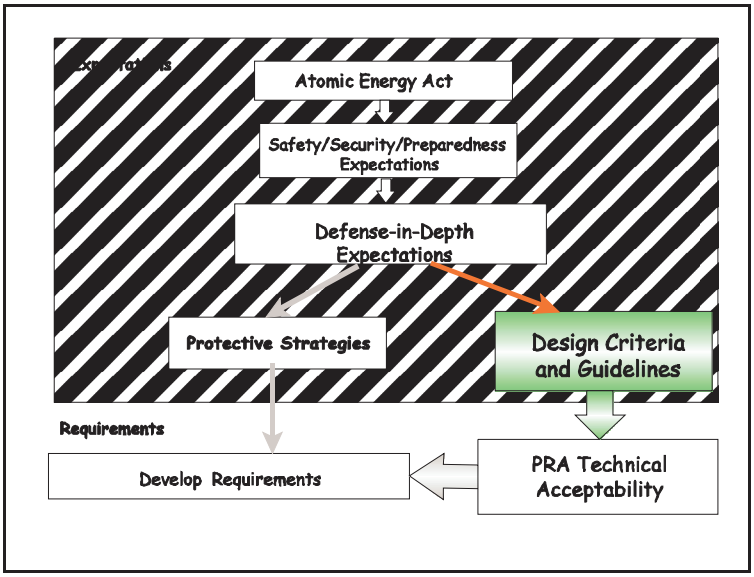


Figure 6-1 How Design Objectives Support Defense-in-Depth

- To demonstrate the acceptability of the estimated plant risk (Section 6.2),
- To demonstrate compliance with the Quantitative Health Objectives (QHOs) of the Commission's safety goal policy statement and (QHOs) [Ref.5] (Section 6.3),
- To develop a process, i.e., criteria and guidance, 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 (Section 6.4),
- 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 (Section 6.5),
- To ensure that adequate regulatory margin exists and to encourage the use of additional design margin (Section 6.6), and
- To integrate security into the design process at least at the same level of protection as established by the post 9/11 NRC requirements (Section 6.7).

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 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 however, does provide a risk-informed link between the PRA and the SSC selection for safety classification by the use of importance measures to identify SSCs for special treatment.)

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 which 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 still relies on deterministic 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.

6.2 Acceptability of Plant Risk

In the framework approach a probabilistic risk assessment (PRA) is used as part of the licensing of plants to generate a sufficiently complete set of accident scenarios whose frequencies and consequences, individually and cumulatively, provide an estimate of the overall risk profile of the plant. The question is what constitutes an acceptable plant risk as estimated with the PRA.

The scope of a PRA used in the framework approach is broader than the scope of PRAs that have been conducted for the current generation of plants. Since the safety and licensing basis for the current fleet of plants was established without the benefit of PRA, and due to the nature of the LWR risk profile, the scope of PRAs for LWRs has been mostly confined to the analysis of beyond design basis core damage accidents. For a future reactor PRA, the framework approach expects that the PRA will provide important input to the selection of licensing basis events (see Section 6.4), so the scope is larger and is not necessarily limited to very low frequency event sequences. This means that the scope of the future reactor PRA must include frequent, infrequent as well as rare events and event sequences, and this expands the scope in comparison with the traditional severe core damage accident type of PRA.

In addition, although risk can be generally expressed in terms of consequences resulting from exposures, in LWR PRAs the risk is often expressed in terms of surrogate measures such as core damage frequency (CDF) or large early release frequency (LERF). These surrogate measures and the criteria associated with them (such as CDF < 1.E-4/yr or LERF <1.E-5/yr for some applications) are LWR specific and not suited for all reactor designs. Finally, since frequent, infrequent, as well as rare events are included in the PRA, a single limiting criterion on consequence or its surrogate (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.

6.2.1 Frequency - Consequence Curve

A criterion that specifies limiting frequencies for a spectrum of consequences, from none to very severe can be denoted via a frequency consequence (F-C) curve. On the F-C plane, the F-C curve provides an acceptable limit in terms of the frequency of potential accidents and their associated consequences. The consequences of the F-C curve can be expressed in terms of radiation dose at the plant site boundary, since dose is an example of a metric that can be directly linked to consequences.

An F-C curve, shown in Figure 6-2, has been developed that 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. This principle, and the whole F-C curve, is broadly consistent with the approach of ICRP 64. Recommendations on the annual frequencies and doses to individual members of the public from accidental exposures are provided IN ICRP 64. The doses cover a wide range of severity, from small exposures that are within regulatory limits to very high exposures that can lead to an early fatality. [Ref.6]

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.7] 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.8]) 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.9] 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.10], 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.11]. 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 6-2.

Note that Appendix I of 10 CFR Part 50 and 10 CFR Part 20 are used above to justify the dose limits at the higher frequencies, i.e., greater than 1E-3 per year, of the F-C curve. These dose limits specified by Appendix I of Part 50 and by Part 20 are cumulative (over one year) dose limits for normal operation, while the other dose references used for the F-C curve are per event doses. Since the F-C curve is meant to provide criteria for unplanned exposures, i.e., exposures on a per event basis, the use of Appendix I and Part 20 may seem questionable for the F-C curve, in that it blurs the distinction between normal and unplanned exposures, but no per event criteria for unplanned exposures exist at low doses. The cumulative nature of the criteria in Appendix I and Part 20 will also play a role in the criteria imposed by the framework on LBEs, as discussed in Section 6.4.

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

6.2.2 Meeting the Frequency - Consequence Curve

The sequences of the PRA will populate the space under the F-C curve. Some sequences 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.

The framework approach specifies that the F-C curve is met with the dose calculated at distances which depend on the sequence frequency:

- For each PRA sequence with frequency greater or equal to 1E-5/yr, the mean value of the dose at the Exclusion Area Boundary (EAB) of the plant, as calculated with a probabilistic consequence code like MACCS, has to meet the F-C curve.

- For each PRA sequence with frequency less that 1E-5/yr, the mean value of the dose at one mile from the Exclusion Area Boundary (EAB) of the plant, as calculated with a probabilistic consequence code like MACCS, has to meet the F-C curve.

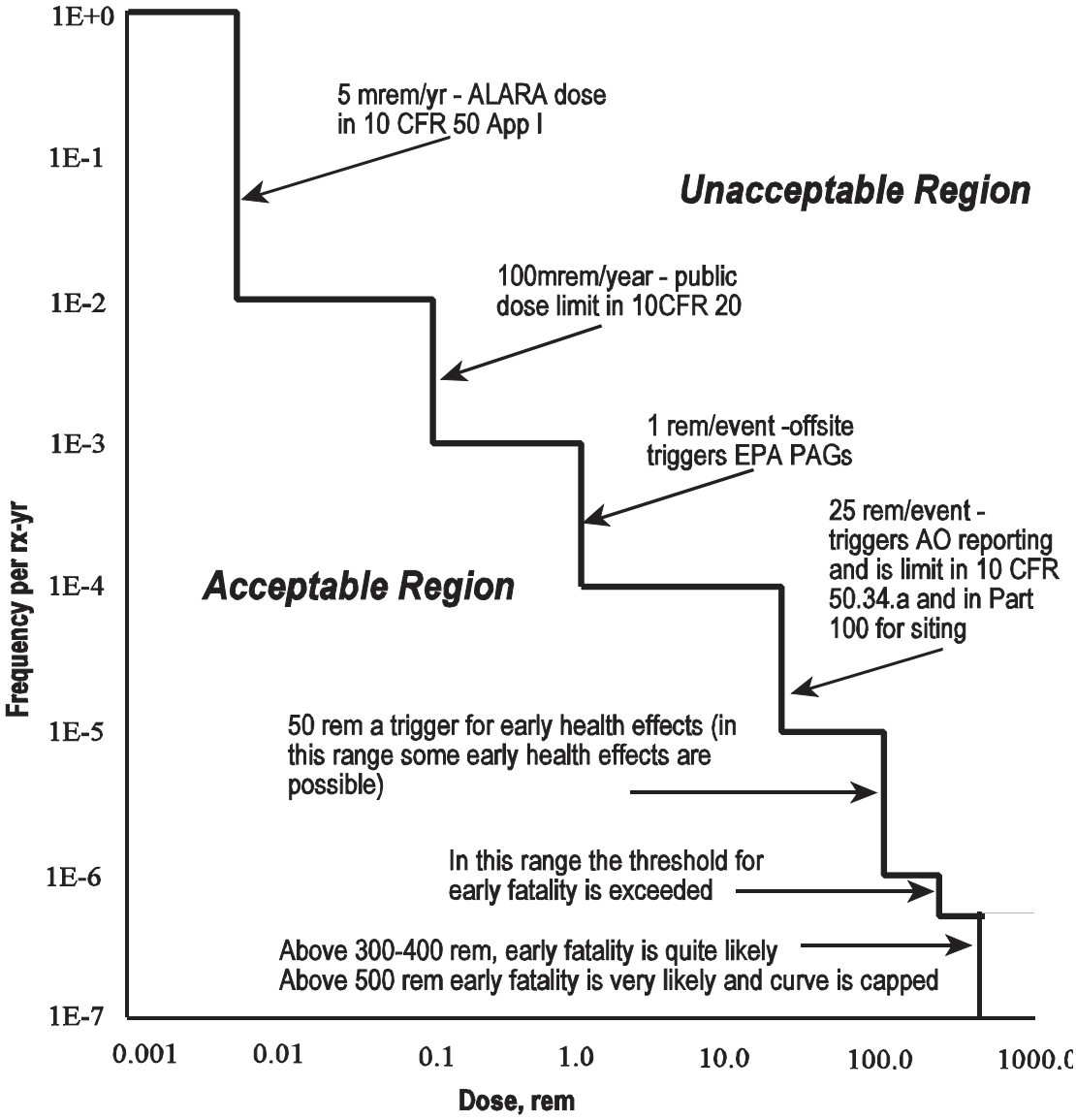


Figure 6-2 Frequency-consequence curve.

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, i.e., CDF or LERF, associated with high consequence event sequences, is an acceptance criterion. For the PRAs required by the framework, whose scope covers all types of off-normal event sequences, the criterion is a series of limiting frequencies whose permitted value depends on the magnitude of their associated consequences. As illustrated in Figure 6-2, event sequences with high frequencies must lead to no consequences or very minor ones; event sequences that are rather infrequent can have somewhat higher doses associated with them, and rare (very low frequency) event sequences 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.

6.3 Compliance with Quantitative Health Objectives

The following are definitions of the Quantitative Health Objectives (QHOs) taken directly from the Safety Goal Policy Statement [Ref. 6.1]:

(57) "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."

(58) "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 and the QHOs is the total plant risk incurred over a reactor year. This means the PRA results must demonstrate that the total plant risk, i.e., the risk summed 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 per reactor year. 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.

Therefore 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 summation of the risk from all the PRA sequences is carried out using the mean value of each sequence dose and frequencies.

With the curve of Figure 6-2, 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.

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 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 all of the new reactors at one site, 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.12]," 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.

6.4 LBE Selection Process and LBE Criteria

The purpose of the LBEs is similar to the purpose of the DBAs in the current licensing process:

57. to provide assurance that the design meets the design criteria for various accident challenges with adequate defense-in-depth (including safety margin) to account for uncertainties, and

58. to evaluate the design from the standpoint of the dose guidelines in the siting criteria of 10 CFR Part 100.

The framework includes probabilistic selected LBEs that address the first requirement and a deterministic selected LBE that addresses the second requirement. For the future reactors addressed by the framework, the LBEs also are used to demonstrate that the Commission's safety expectations for new reactors are met.

As described below, the PRA is used to select most of the LBEs, but the LBEs have to meet additional criteria, besides satisfying the F-C curve.

The LBEs selection process and the acceptance criteria the LBEs must meet are described in the Subsections below.

6.4.1 Probabilistic LBE Selection

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 EAB and (for sequences with frequencies less than 1E-7/yr) 1 mile from the EAB.[13] 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.

The probabilistic selected LBEs provide a means to ensure that the design meets the design criteria for various accident challenges with adequate defense-in-depth (including safety margin). These sequences are derived from a design-specific PRA through a process described later in this chapter. The probabilistic selection process helps to ensure that the LBEs represent all potentially 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. Probabilistic selected LBEs must also meet some deterministic criteria in addition to meeting the frequency-consequence curve.

The probabilistic selected LBEs are event sequences which represent challenges to plant safety. They encompass a whole spectrum of off-normal events including frequent, infrequent and rare

[13] 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."

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.

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.). It would also include design basis accidents as described in Part 50.34 or Part 100.11. (These are accidents 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.) Finally it includes large releases (These are accidents where a significant quantity of fission products is released from containment into the environment with a potential for causing early health effects to the offsite population).

Before describing the LBE selection process it is well to note the fact that SSCs credited in the LBEs will be considered safety significant in the framework approach. All functions included in the PRA have the potential to influence the frequency of LBE sequences and many influence the consequences. Therefore, any function and the associated SSCs included in the PRA used to develop the set of LBEs is safety significant unless it has been set to 1.0 or guaranteed failure. As stated above, the designer can remove mitigation functions from the PRA in order to reduce the set of safety significant SSCs. However, the resulting PRA must meet the F-C curve and the defense-in-depth deterministic requirements, discussed later. 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.

It is the designer's decision as to what SSCs will be considered safety-significant as long as the framework's acceptance criteria are met. This determination could be accomplished through an iterative approach, where the impact on the selection of LBEs is evaluated with a proposed set of safety significant SSCs, then re-assessed with another set of safety significant SSCs, until the desire set of LBEs and other design objectives are achieved.

The goal of the probabilistic selection process is to identify a set of bounding event sequences that demonstrate adequate defense-in-depth and safety margin from the standpoint of public health and safety. The process is shown in Figure 6-3 with each step described below.

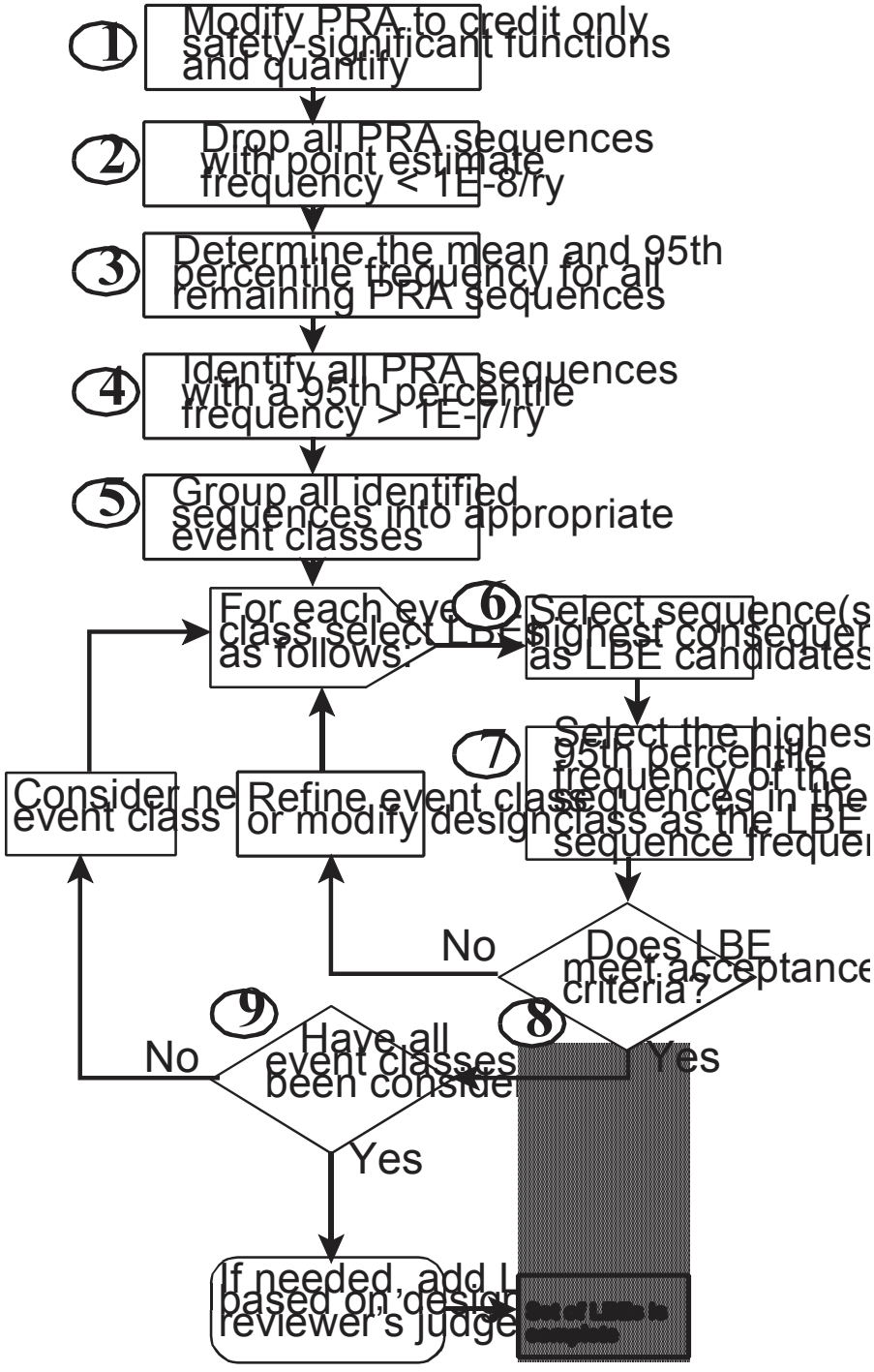


Figure 6-3 LBE Selection

Step 1

M
o
d
i

fy the PRA to only credit those mitigating functions that are to be considered safety significant.

As stated above, those SSCs whose functionality plays a role in meeting the acceptance criteria imposed on the LBEs define the set of safety significant SSCs. The SSCs of interest are those that influence the frequency or consequence of the LBEs, or both. All functions included in the PRA have the potential to influence the frequency of LBE sequences and many influence the consequences. Therefore, any function and the associated SSCs included in the PRA used to develop the set of LBEs is safety significant unless it has been set to 1.0 or guaranteed failure. The designer can remove mitigation functions from the PRA in order to reduce the set of safety significant SSCs. However, the resulting PRA must meet the F-C curve and the defense-in-depth deterministic requirements.

Step 2 Determine the point estimate frequency for each resulting event sequence from the quantification of the modified PRA.

Drop all PRA sequences with point estimate frequency < 1.E-8/yr. This step establishes the complete set of event sequences that will be processed to determine the LBEs.

Step 3 For sequences with point estimate frequencies equal to or greater than 1E-8, determine the mean and 95th percentile frequency.

The frequency used to determine whether an event sequence remains within scope of the LBE selection process is based the 95th percentile. Therefore, the mean and 95th percentile are determined in this step.

Step 4 Identify all PRA event sequences with a 95th percentile frequency > 1E-7 per year.

This step identifies those sequences that are to be included in the event class grouping process. Sequences less than 1E-7 per year are screened from the process.

Step 5 Group the PRA event sequences with a 95th percentile frequency > 1E-7 per year into event classes.

In this approach, the LBEs are chosen by grouping similar accident sequences into an event class. Similar accident sequences are those that have a similar initiating events 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 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 goal of the grouping process is to account for all the event classes with 95th percentile frequency greater than 1E-7 per year, 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 PRA 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. 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.

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).

Step 6 Select an event sequence from the event class that represents the bounding consequence.

The selected event sequence defines the accident behavior and consequences for the LBE that represent this event class. If several events within the event class have similar consequences, then a bounding event is selected. If there is not a clear bounding event, then the event with the lowest frequency is selected. Note that the frequency of the event class is determined separately from the bounding consequence event. See Step 7.

Step 7 Establish the LBE's frequency for a given event class.

The frequency of an event class is determined by setting the LBE's mean frequency to the highest mean frequency of the event sequences in the event class and its 95th percentile frequency to the highest 95th percentile frequency of the event sequences in the event class. Note that the mean and 95th percentile frequencies can come from different event sequences.

Step 8 Verify that each LBE meets the acceptance criteria.

The LBEs have to meet the F-C curve plus the defense-in-depth requirements that are a function of the LBE frequency range, as described below. If criteria are not met, either the event class is refined or modifications are made to the design.

Step 9 Repeat these steps for all event classes.

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.

Note that, 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.

For the LBE selection 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.

A schematic example of how a particular set of event classes that start out with similar failures may be broken down into 3 different classes and related LBEs and compared against the F-C curve is shown in Figure 6-4 below.

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 6-4, which belong to the same event class, will contribute in terms of frequency to the LBE frequency of that class.

A detailed example application of the selection process described above can be found in

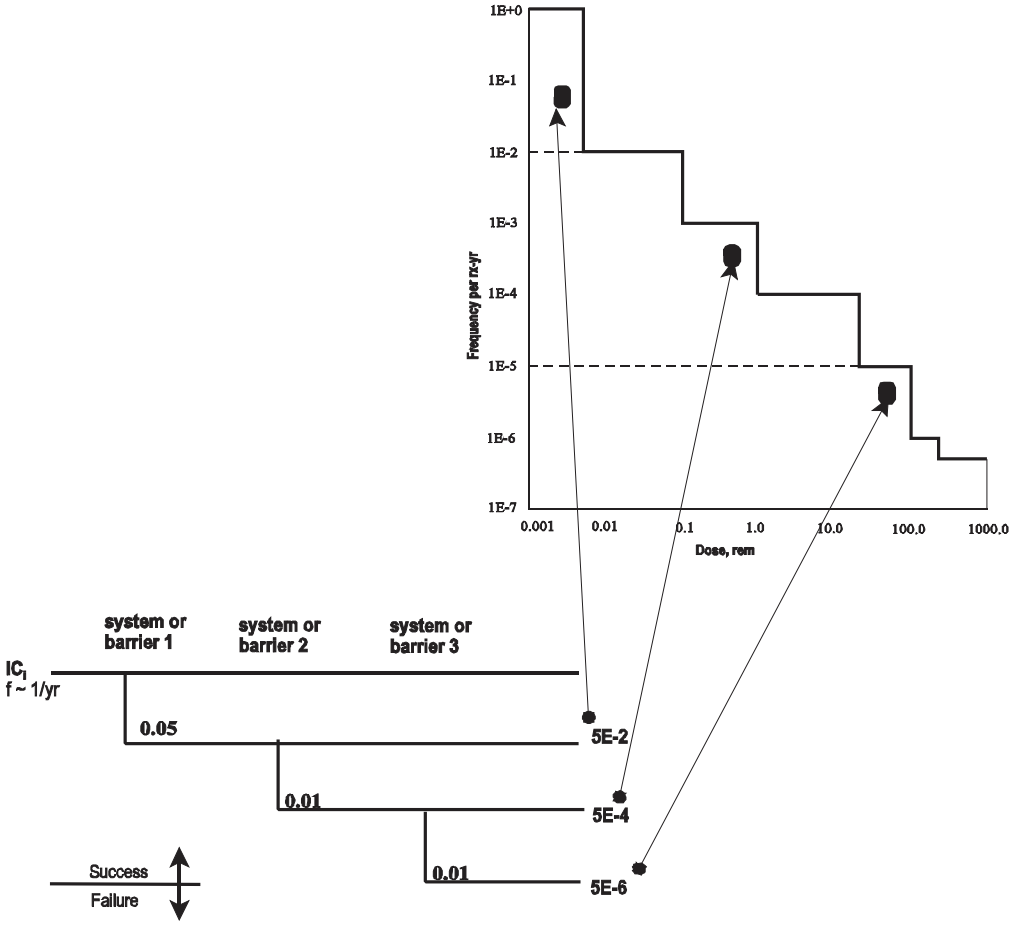


Figure6-4 LBE selection schematic example

Appendix E.

6.4.2 Additional Criteria to be met by Probabilistic LBEs

6.4.2.1 Binning Probabilistic LBEs by Frequency

The LBEs selected by the process have to meet some additional criteria, depending on the frequency range they fall into. Consequently, 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

The frequencies in Table 6-2 apply to the entire event sequences not the initiating event (IE) frequencies.

6.4.2.2 Additional Deterministic Criteria

For defense-in-depth purposes additional deterministic criteria are imposed on the LBEs. These additional criteria reflect some of the considerations that are found in the General Design Criteria of Appendix A to 10 CFR 50 for the current reactors. The criteria vary with the frequency range the LBE falls in:

In the frequent range, LBE frequency greater than or equal to 1E-2 per year:

- no impact on the safety analysis assumptions occurs
- no barrier failure occurs
- redundant means of reactor shutdown remain functional
- redundant means of decay heat removal remain functional

In the infrequent range, LBE frequency greater than or equal to 1E-5 per year, but less than 1E-2 per year:

- a coolable geometry is maintained
- at least one barrier remains
- at least one means of reactor shutdown remains functional
- at least one means of decay heat removal remains functional

For the rare range, LBE frequency less than 1E-5 per year, no additional deterministic criteria apply.

6.4.2.3 Additional Dose Criteria

The frequency ranges of the LBEs also affect some additional dose criteria the LBEs have to meet. As noted in the F-C curve discussion of Section 6.2.1, the dose limits specified by Appendix I of Part 50 and by Part 20 are cumulative (over one year) dose limits. Therefore, an additional requirement for the LBEs with frequencies greater than 1E-3 per year is that they meet the cumulative dose requirements. This means a frequency weighted summing of the doses of all the LBEs in the range, as identified below. In addition, some further dose criteria are also imposed on LBEs with lower frequencies. All these criteria are summarized below:

In the frequent range, LBE frequency greater than or equal to 1E-2 per year:

- the cumulative dose meets the 5 mrem dose specification of Appendix I of 10 CFR 50

.

In the infrequent range, LBE frequency greater than or equal to 1E-5 per year, but less than 1E-2 per year:

- the cumulative dose of LBEs with frequencies greater than or equal to 1E-3 per year, has to meet the 100 mrem specification of 10 CFR Part 20.

- for LBEs with frequencies less than 1E-3 per year the worst (maximum based on meteorological conditions) two hour dose at the EAB meets the F-C curve

For the rare range, LBE frequency less than 1E-5 per year:

- the 24 hour dose at one mile from the EAB meets the F-C curve

To carry out the dose calculations, sequence specific source terms are used for the consequences analysis associated with the probabilistic LBE sequences, based on the following criteria:

- They are selected from the design specific PRA with due consideration for uncertainty,

- They are based on analytical tools that have been verified with sufficient experimental data to cover the range of conditions expected and to determine uncertainties,
- They reflect the sequence specific timing, energy, 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

- The radionuclide release fractions used to characterize the source term are the 95% value of the probability distribution[14]

For the accident sequence established on the basis of experimental data or analytical considerations, where uncertainties cannot be quantified, engineering judgement is used. These criteria provide a flexible, performance-based approach for establishing sequence 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 sequence 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 burn up levels

[14] The upper value of the 95% Bayesian probability interval

that the fuel can experience and the physical and chemical conditions associated with various accident sequences 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.

6.4.2.4 Criteria on Initiating Events

In the framework approach there are also limits on the initiating event (IE) frequencies themselves in the various frequency categories. 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.

6.4.3 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 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.

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 low population zone (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.

6.4.4 Comparison of Plant Risk (PRA) Criteria and LBE Criteria

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 with the 95% probability value 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

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 and the discussions above indicate, 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 probability range for the amount of radionuclides released for both the PRA and the LBE calculations.

The statistic with which the dose levels of the F-C curve are met are the mean value for the PRA, but the 95% probability value for the event sequences selected as the LBEs[15]. LBEs also meet the additional deterministic and dose criteria, depending on their frequency category, as discussed above. As stated above, for the frequent and infrequent category the doses are calculated at the EAB. 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 statistic between the standard PRA sequences and the LBE sequences with which the F-C dose criteria are met (mean versus 95% probability value) 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.

Table 6-3 PRA and LBE Criteria

Category (Mean Event Frequency Per ry)	Statistic for meeting F-C curve		Additional acceptance criteria for LBEs (demonstrated with calculations at the 95% probability value* with success criteria that meet adequate regulatory margin)
	PRA	*LBE*	
frequent (10^{-2})	mean	95% probability value*	-no barrier failure -no impact on safety analysis assumptions -redundant means for reactor shutdown and decay heat removal remain functional -annual dose to a receptor at the EAB #5mrem TEDE

[15] Further guidance will be provided on how to calculate source terms at the 95% probability value.

infrequent (< 10^{-2} to \$$10^{-5}$)	mean	95% probability value*	-at least one barrier remains -a coolable geometry is maintained -at least one means of reactor shutdown and decay heat removal remains functional -for LBEs with frequency > 1E-3 annual dose to a receptor at the EAB # 100mrem TEDE -for LBEs with frequency < 1E-3 the worst two-hour dose at the EAB meets the F-C curve
rare (<10^{-5} to \$$10^{-7}$)	mean	95% probability value*	- 24 hour dose at 1 mile from EAB meets the F-C curve
Note: 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% probability value* of the amount of radionuclides released, obtained from a mechanistic calculation, and use RG 1.145 or the equivalent for calculating atmospheric dispersion(16)			
EAB - exclusion area boundary TEDE - total effective dose equivalent * The upper value of the 95% Bayesian probability interval [Ref.13]			

6.5 Safety Significant SSCs and Special Treatment

In the framework, 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 SSCs need special treatment or not(17). As discussed under the LBE selection process, the term 'safety significant' is assigned to those SSCs whose functionality plays a role in meeting the acceptance criteria imposed on the LBEs. These SSCs require special treatment

The term 'special treatment' is used to designate requirements imposed on SSCs that go beyond industry-established requirements for equipment classified as "commercial grade." These requirements provide additional confidence that the equipment is capable of meeting its functional requirements under PRA analyzed conditions. The type of special treatment varies dependent on the function and importance of the SSC. The treatment helps to ensure that the SSCs will perform reliably (as postulated in the PRA) under the conditions (temperature, pressure, radiation, etc.) assumed to prevail in the event sequences for which the SSC's successful function is credited in the risk analysis.

(16) Further guidance will be provided on how to calculate source terms at the 95% probability value.

(17) 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.

A basic special treatment requirement for all safety-significant SSCs will be the establishment and monitoring of reliability and availability goals. All safety-significant SSCs will have reliability and availability consistent with the values assumed in the PRA. 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 this special treatment requirement. 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. 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.

Other special treatment requirements may be required dependent on the function and importance of the SSC. Risk importance calculations could be used to focus the types of special treatments that would be applied to a SSC. However, these importance calculations 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 sequences where it is needed. Verification of the functionality of the SSC under the required conditions is demonstrated via a reliability assurance program.

6.6 Safety Margin

Safety margin is incorporated in the framework as an element of defense-in-depth through the use of requirements containing regulatory margin and by encouraging the designer to include design margin as an element of the design. Regulatory and design margin were introduced in Section 4.6. The purpose of this section is to describe how these two types of safety margins are addressed within the framework.

In keeping with the treatment of a draft NUREG on the subject of safety margins[18], it is assumed that the operation of a safety system or barrier can be characterized by one or more safety variables, e.g., pressure, temperature, ductility, etc. and that the safety variables can demarcate the transition from "intact" to "lost function." If the safety variable remains in an acceptable range the system or barrier remains functional. If the variable exceeds that range loss of function occurs. These safety variables must be directly or indirectly measurable, and their values must be predictable for plant conditions during normal and emergency operation.

As was indicated in Figure 4-4, for purposes of the framework, the safety margin is the sum of (1) the regulatory margin which is the difference between the ultimate capacity of the safety variable and the regulatory limit of the safety variable, and (2) the design margin, added at the option of the designer, which is the difference between the regulatory limit of the safety variable and the value of the safety variable at which the system or barrier is expected to perform, according to the design. In the words of the draft NUREG on safety margins [2.8], "Adequate safety margins" are inextricably linked to safety limits—limiting values imposed on safety variables (e.g., peak clad temperature (PCT) and containment pressure in current LWRs). Thus, when operating conditions stay within safety limits, the barrier or system has a negligible probability of loss of function, and an adequate safety margin exists.

In practice, the design value and the ultimate capacity of a safety variable are not particular single values but probabilistically distributed quantities. Therefore, one has to specify (1) from where on the capacity distribution the regulatory limit should be measured from, and (2) what part of the design analysis distribution should be used to show compliance with the regulatory limit, and (if pertinent) show additional margin beyond that provided by the regulatory limit.[19] This question is further complicated by the fact that accurate distributions, especially for the ultimate capacity of the safety variable are often not available. Such information may be beyond the current state of the art or very costly.

This lack of detailed information about the capacity distribution is often addressed by picking a safety variable capacity value that reflects judgement as to where the onset of damage of the system or barrier being analyzed occurs. This value reflects the judgement of what is a reasonable bound on the lower limit of the capacity distribution, given its assumed uncertainty. Further judgement then is used to set the safety limit below this onset of damage value by an amount that is commensurate with the lack of data, and the importance of the safety variable, and the system or barrier whose functionality it determines. This judgement reflects an allowance for unknowns that are part of the incompleteness uncertainty.

The design analysis distribution of the safety variable is usually less costly to obtain and better known. The framework advocates using the 95% probability value (The upper value of the 95% Bayesian probability interval) of the design distribution to show that the regulatory limit is met. These concepts are illustrated in Figure 6-5.

---

[18] Draft NUREG-XXXXX, "A Framework for Integrating Risk and Safety Margins," to be published

[19] If the probability distributions of both design analysis and capacity were perfectly known and included both random and state-of-knowledge uncertainties, the distributions could be convoluted and the probability of failure (i.e., design value exceeds capacity) obtained directly from the convolution. If this probability was not low enough, the design could be adjusted until it was and there would be no need for safety margin. However, in reality the distributions are not perfectly known.

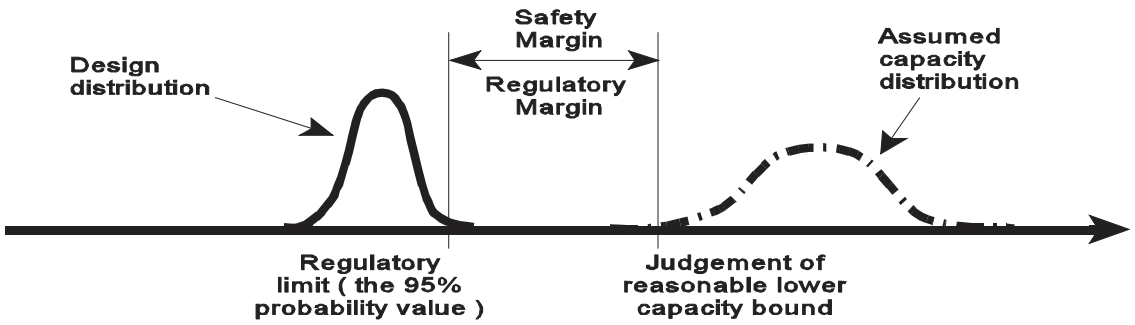


Figure 6-5 Safety Margin

In Figure 6-5, the capacity distribution, which is not well defined, is indicated by a dashed line. Judgement is used to pick a capacity value, below which the probability of failure of the system or barrier whose operation is characterized by the safety variable is considered negligible. This represents a lower bound on the needed capacity. If the safety variable exceeds this value, loss of function is assumed. The regulatory margin is then the distance between this lower bound capacity value and a point on the upper tail of the design distribution of the safety variable. A point corresponding to the 95% probability value on the tail of the design distribution is suggested as a credible point on the distribution if the distribution is reasonably well established. As noted above, the judgement in setting the regulatory margin will be influenced by (1) the availability of data about the safety variable distributions, (2) the importance of the safety variable in characterizing the safe operation of the system or barrier, and (3) the importance of the system or barrier itself. The intent is to allow margin for phenomena and processes that may have been inadequately considered in generating models to simulate the behavior of the given system or barrier. The margin thus provides an allowance for unknowns that are part of the incompleteness uncertainty.

In Figure 6-5 the safety margin and regulatory margin are identical, i.e., no additional design margin is deliberately provided. Figure 6-6 illustrates the situation when additional margin has been added by the designer to further increase the safety margin.

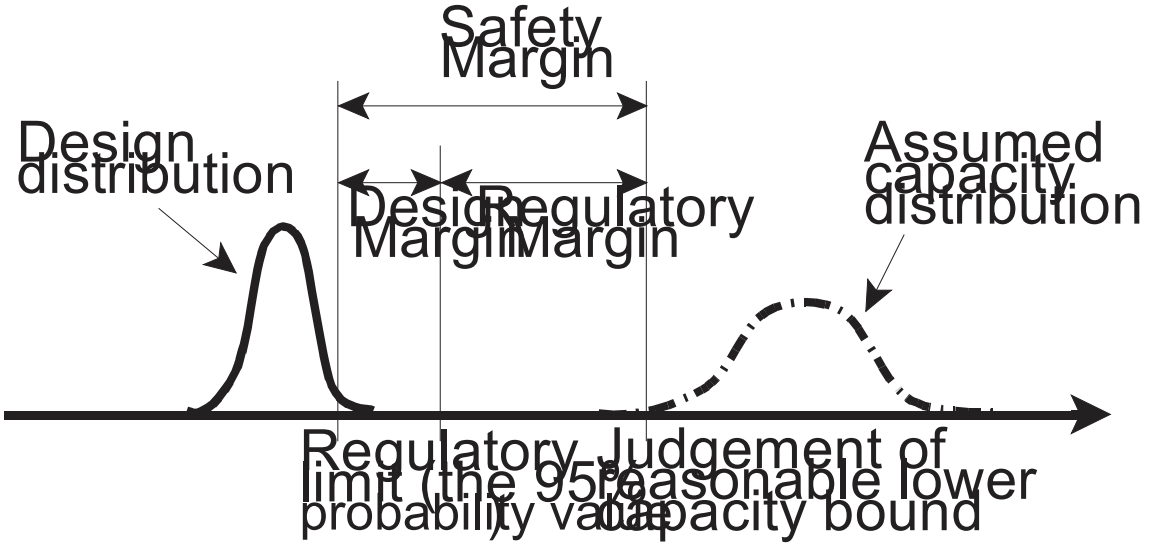


Figure 6-6 Safety Margin with Design I

In the terminology of the Chapter 4 discussion, the operational range of the safety variable, represented here by the design distribution, has been moved to lower values to provide a design margin to add to the safety margin. This may be included by the designer to assure regulatory limits are easily met even if the operational range of the safety variable is found to change in the future, for example.

Based on either Figure 6-5 or 6-6, the safety margin for the safety variable can be taken to be the distance between the bounding prediction of the design analysis probability distribution of the safety variable and the point at which failure becomes non-negligible on the capacity probability distribution of the safety variable. The phrases “sufficient margin” and “adequate margin”can be taken to mean that regulatory margin is preserved.

6.6.1 Regulatory Safety Margin in the Framework

Safety margin is incorporated into the framework as an element of defense-in-depth. Since the framework is performance-based, it does not prescribe specific margins at the various levels of a safety analysis.

6.6.1.1 Frequency-Consequence Curve

At the highest level of the safety analysis, involving the results of the PRA and the LBE calculations, the framework establishes the regulatory limits of the frequency-consequence curve consistent with the discussion above. The F-C curve limits are defined at the different frequencies by dose levels which reflect the regulatory limits on dose at the frequencies specified. These limits are based on conservative decision-making rooted in current practices and reflect judgement as to the acceptable risk for a given likelihood and consequence. The F-C curve is an example of a regulatory limit where the capacity distribution is not well understood and where judgement was used to set the safety limit below the onset of unacceptable risk.

The margin associated with the F-C curve results in both a consequence margin and a 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.

As indicated in the earlier discussions, these LBEs have to meet the F-C curve at the 95% probability level in both frequency and consequence. The use of the 95th percentile is consistent with the margin discussion above.

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 of using the 95th percentile values and regulatory margin associated with the F-C curve increases the evaluated frequency of the LBE and tightens the acceptance criteria, 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 their success criteria and by the selection of reliability and availability goals, for which margins are discussed below. For reliability and availability goals, the designer may choose to include design margin within these goals which will be reflected in the overall frequency of each event sequence.

6.6.1.2 Safety Variable Limits

In addition to the margin included in the F-C curve, regulatory margin will be specified for selected key variables on a design-specific basis. This includes key variables used in the determination of PRA success criteria.

With in the PRA, 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 such that issues of manufacturer or construction variability, code limitations and other uncertainties are unlikely to result in a failure path being considered a success path. Ensuring that success paths are truly success paths will be supported by requiring regulatory margin for selected key variables and by encouraging the incorporation of design margin.

6.6.1.3 Code and Standards

The framework does assume that appropriate codes and standards are used for the analyses of systems, structures and components for the determination of the plant's level of safety, and that the margins in these analyses follow the general guidelines presented here. Specific guidance is not provided for codes and standards within the framework for it is expected that most codes and standards will be associated with a design-specific features.

6.6.1.4 Completeness

The framework includes a process for identifying a complete set of probabilistic LBEs that bounds all PRA event sequences having a 95th percentile frequency greater than 1E-7 per year.

The identification of a complete set of LBEs is key to ensuring that adequate safety margin is

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

The scope of the PRA used for the framework 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).

The framework also includes a deterministic LBE that addresses the limiting challenge to the final radiological barrier to address uncertainties that are not fully known.

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. The use of a deterministic LBE is one of the defense-in-depth measures that the framework requires to address incompleteness uncertainty.

6.6.2 Design Margin

The designer can incorporate an additional margin, called the “design margin” in the framework, by designing a system so it operates below the regulatory limit for normal operations and excursions. The framework encourages the use of margin beyond that required, 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. This design margin can be applied to the LBE consequence analysis to create margin between these results and the limits of the F-C curve, to safety variables used in success criteria and, codes and standards, and to the reliability and availability goals established for the SSCs within the PRA.

For example, the design margin incorporated in the reliability and availability goals could vary depending on the SSC’s function, performance uncertainty and/or importance. These goals should be designed such that variations in SSC performance are unlikely to change the selection and characteristics of the LBEs.

The incorporation of design margin into the various elements of the framework should help to provide added insurance that plant operation and event response will not deviate from the inputs and assumptions and the associated analysis used to demonstrate compliance with the Commission’s safety goals.

6.7 Security Performance Standards

The purpose of this section is to define risk-informed and technology-neutral security expectations and performance standards for new plants.

Requirements related to security for current NPPs are contained in 10 CFR 73 and in post 9/11 orders. For new reactors, current security expectations are that they shall have the same level of protection as established by 10 CFR 73 requirements and the post 9/11 NRC orders. These requirements are primarily prescriptive and require plant specific features and measures related to protection against the design basis threat (DBT). These requirements cover a number of subjects, including:

- guard force and training
- protection of vital areas
- personnel screening
- security fences and detection devices
- mitigation strategies

These requirements provide a baseline of preventive and mitigative features directed toward protecting public health and safety from the DBT related to sabotage, armed intrusion, external attack, and theft or diversion of nuclear material. They generally require measures to detect, delay, assess and respond to security related threats up to and including the DBT.

6.4.1Security Expectations

New reactors are expected to have the same level of protection as established by 10 CFR 73 and the post 9/11 orders. However, a more robust and risk-informed approach is proposed. Accordingly, a statement that defines security expectations for new plants has been developed. These security expectations describe, in qualitative terms, what security at nuclear power plants is to achieve. As such, they address the level of safety and security to be achieved, the scope of what must be protected and considered, and key aspects of the approach to be followed. They also provide guidance regarding the scope and purpose of the security performance standards to be developed.

Specifically, the security expectations for new plants encompass the following:

- Protection of public health and safety with high assurance is the goal of security.

- The overall level of safety to be provided for security related events should be consistent with the Commission's expectations for safety from non-security related events.

- Security is to be considered integral with (i.e., in conjunction with) design and preparedness.

- A defined set of beyond DBTs (BDBT) are to be considered, as well as the DBT, to identify vulnerabilities, assess margin and help compensate for uncertainties.

- Defense-in-depth is to be provided against the DBT and each BDBT considered, to help compensate for uncertainties.

- Security is to be accomplished by design, as much as practical.

The above security expectations define the elements which must be addressed in the security performance standards and the safety and security assessment. These security expectations are intended to promote enhanced security, emphasize design solutions to security issues, provide means to ensure integration of security, safety and preparedness and provide guidance for qualitative and quantitative measures for assessing security. They are intended to be consistent with existing measures of safety (e.g., public health and safety) wherever possible and relevant aspects of NRC's safety philosophy (e.g., defense-in-depth). Also, it was assumed in developing these expectations, that the design would be in compliance with 10 CFR 73 requirements and the post 9/11 orders. The security performance standards and their basis are described in the next section.

6.4.2Security Performance Standards

The goal of the security performance standards discussed in this section is to define quantitative

and qualitative criteria that can be used to determine whether or not the security expectations discussed above are met. The focus of the security standards is to be on performance of the system, rather than on prescriptive requirements. As such, the performance standards need to be developed consistent with the guidance in NUREG/BR-0303 "Guidance for Performance-Based Regulation." The guidance in this NUREG identifies the characteristics which must present to have performance-based requirements, which includes:

- can observable characteristics, together with objective criteria, provide measures of safety performance,
- what is the performance level desired,
- can corrective action be taken if the level of performance is not met, and
- is flexibility for NRC and licensees provided?

Accordingly, the security performance standards must conform with this guidance.

To assess performance, each new plant will be required to conduct a safety and security assessment and evaluate the results of that assessment against the performance standards described in this section. This safety and security assessment is intended to:

- consider safety and security integral with design, rather than as post-design compensatory measures,
- consider safety and security in the development of preparedness measures, and
- ensure that the relationship and impact among security, safety and preparedness is considered in decision making.

The safety and security assessment will involve characterization of the potential threat, the potential targets and the potential consequences. The adequacy of the methodology used will also need to be established. However, the likelihood of the threat depends on some factors only known to the adversary, so it is expected to be outside the scope of the assessments. Nevertheless, the types, objectives, and capabilities, as well as the strategies, of the potential adversaries need to be taken into account in the assessment.[20] The scope and guidelines for performing the safety and security assessment will be provided in a separate document.

Security needs to be considered during the design stage and design, security and preparedness decisions made in an integral fashion. During design, reasonable assumptions about the threats that need to be considered over the full life of the facility can be made, together with a spectrum of threats the facility is likely to encounter. It is important that these threat assumptions include the broad categories of potential physical protection challenges. These broad categories include:

- sabotage
- armed intrusion
- external attack
- cyber security
- theft or diversion of nuclear materials

[20] 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.

The theft or diversion of radioactive materials, namely fuel, is included in the broad category for potential physical protection challenges only for reactor designs that use MOX or HEU fuel. Theft or diversion is not considered for reactor designs that use LEU fuel. With respect to fresh LEU fuel that has not been irradiated, subsequent dispersal would not create a significant hazard for public health and safety and is not suitable for a weapon. With respect to spent LEU fuel, its nature generally makes it self-protecting and difficult to steal. Therefore, theft or diversion of LEU nuclear fuel is not anticipated to be a significant contributor to risk at commercial nuclear power plants.

The threats to be considered in the evaluation are the DBT and a defined set of BDBTs selected and categorized consistent with NRC safety and security assessment guidance with respect to threat level severity (see Table 1). The BDBTs selected for evaluation should be sufficient to demonstrate that the design has margin to withstand security related events beyond the DBT and to identify any significant vulnerabilities or consequence thresholds. This will then help to compensate for uncertainties and also help provide high assurance of protection of public health and safety.

A risk-informed and performance-based approach has been taken in the development of security performance standards. This approach utilizes a combination of risk criteria to define the level of safety desired and deterministic criteria to complement the risk criteria to help account for uncertainties. An integrated decision process is then used to assess the various elements of the standards and the need for any additional action.

Risk information is useful in helping to make decisions regarding the level of protection provided against various events and the relative importance of plant equipment, actions or modifications in responding to those events. As such, having some probabilistic elements as part of the security performance standards will provide a means to judge the importance of various threats and potential solutions. However, since the probability of the threat itself has considerable uncertainty, any probabilistic performance standards will be most practical and useful if they are expressed as conditional (conditional upon the initiating event) probabilistic values and used in an integrated decision-making process that considers all factors.

The security performance standards proposed for new plants are as follows:

a) Probabilistic Performance Standard:
   - Assess and take action on vulnerabilities to high, medium and low level threats in accordance with Figure 1.

b) Deterministic Performance Standards:
   - Ensure that the plant design, operation and security provide multiple lines of defense against each security related threat that could endanger public health and safety.

   - Ensure that the plant design, operation and security provide both prevention and mitigation measures for each security related threat that could endanger public health and safety.

c) Theft or Diversion Performance Standards:
   - For plant designs using MOX or HEU fuel, ensure that detection and surveillance are provided sufficient to detect the theft or diversion of material that could result in an Extraordinary Nuclear Occurrence, as defined in 10 CFR 140.

d) Design Solution Performance Standard:
   - The resolution of security related issues should utilize design solutions, whatever practical.

The technical basis for each of these standards is discussed below.

Probabilistic Performance Standard

The purpose of the probabilistic performance standard is to define the level of safety desired and, based upon this definition, identify potential vulnerabilities and the effectiveness of potential solutions to reduce those vulnerabilities. Since safety corresponds to the protection of public health and safety, the risk metrics used must also be related to public health and safety as well as be technology-neutral. Accordingly, for consistency with previous Commission expectations for safety, the quantitative health objectives (QHOs) from the Commission's 1986 Safety Goal Policy Statement have been selected as the risk metrics to be used. These QHOs are expressed in terms of individual risk of a latent fatality (2×10^{-6}/yr) and an early fatality (5×10^{-7}/yr) and are applicable out to 10 miles and 1 mile, respectively, from the exclusion area boundary of the plant. The use of the QHOs also provides margin for uncertainties, since the level of safety represented by the QHOs is in excess of the minimum required for licensing, sometimes referred to as "adequate protection".

To use the QHOs as an element of the security performance standards, the conditional risk (latent fatality and early fatality individual risk, assuming a probability of one for the initiating event) from each postulated security threat should be calculated and compared to a qualitative assessment of the severity of the threat level (see Table 1). Those threats judged high, medium or low should be evaluated as potential vulnerabilities in accordance with Figure 1. The basis for the conditional risk values shown in Figure 1 comes from trying to maintain a level of safety equivalent to the QHOs. Since the probability of the threats is not known, estimates of the range of probability for each threat level were assigned as follows to support establishing the conditional risk values for early and latent fatalities shown in Figure 1, consistent with the QHOs:

High - 0.01 to 0.001

Medium - 0.001 to 0.0001

Low - 0.0001 to 0.00001

The starting point of 0.01 was chosen considering that there are approximately 100 plants operating in the country and, therefore, the likelihood of any one being a target is 1/100. If, in the future, there are more than 100 plants operating, the 0.01 probability will represent a conservative value. In addition, for the purposes of this report, the QHOs themselves were reduced by a factor of 10 to account for the fact that more than one threat is being considered and, therefore, the cumulative risk from all threats is the measure of interest. Modifications which could reduce the conditional risk of the potential vulnerabilities should then be evaluated as shown in Figure 1. The regions shown in Figure 1 are intended to help ensure that the safety goal level of safety is achieved, when the cumulative effect of security related threats is considered. Specifically, region 1 represents an area where the conditional risk is high enough to warrant action, region 2 represents an area where additional justification for action is needed and, thus, cost-benefit should be considered and region 3 represents an area where the QHOs will likely be met and, therefore, no action is warranted. Accordingly, ensuring that vulnerabilities to threats that could result in high conditional risk are assessed in accordance with Figure 1 represents a probabilistic element of the security performance standards.

It should be noted that in a technology-specific application of this performance standard, a technology-specific set of risk metrics may be substituted for the QHOs (e.g., CDF and LERF for LWRs).

Deterministic Performance Standards

It is recognized that any analysis of security related events carries with it considerable uncertainty, mainly due to the uncertainty in likelihood and consequences associated with the potential threats. Accordingly, to help compensate for this uncertainty, a defense-in-depth deterministic approach is proposed, such that the design should have multiple lines of defense against a range of postulated threats (i.e., defense-in-depth). These lines of defense can consist of preventive or mitigative measures, but should be consistent with the following principles:

- Plant security should not be dependent upon a single element of design, operation, maintenance or security, and

- the plant design, operation and security measures should address both prevention and mitigation of the threats considered.

The intent of these principles is to ensure that the plant design, operation and security provides multiple ways to defend against security related threats. This can be accomplished by (1) having a plant that is not susceptible to a single action by an individual or group of individuals that threatens public health and safety and (2) addressing both threat prevention and mitigation. In addition, these principles integrate security with the basic concept of defense-in-depth used in reactor safety and preparedness, namely designing in up front measures to protect against accidents and ensuring mitigation is available if the accident happens. Each of these principles is discussed below along with its related performance standard.

Regarding the first principle, the plant design, operation and security needs to include multiple ways of providing protection (e.g., multiple systems, barriers, response plans, etc.) in the event of a security related event. This is consistent with the fundamental approach and principles of defense-in-depth which helps ensure that the plant design, operation and security is not vulnerable to a single security related threat adversely impacting public health and safety. Accordingly, providing multiple lines of defense against each of the postulated threats represents an element of the security performance standards.

Regarding the second principle, the design should include measures to both prevent and mitigate security related events from being a threat to public health and safety. As such, the design, operation, preparedness and security measures need to include at least one preventive and one mitigative response for each security related threat. In this regard, prevention means preventing the security related threats from causing the intended plant damage and mitigation means, assuming the intended damage occurs, what can be done to reduce its consequences and protect public health and safety. Accordingly, ensuring preventive and mitigative measures are provided for each threat represents an element of the security performance standards.

Theft or Diversion Performance Standard

For theft or diversion of MOX or HEU fuel, the risk to public heath and safety could be substantial. However, this risk would not likely be to the population surrounding the plant, but rather could be to an area far from the plant. Accordingly, the use of the Commission's Safety Goals to define the level of safety desired may not be appropriate. Therefore, a different measure is being proposed as the desired level of safety. This measure is the dose, contamination and cleanup cost criteria associated with an extraordinary nuclear occurrence (ENO) as defined in 10 CFR 140. The ENO criteria represent dose, contamination and cleanup cost levels below which there would be a small societal impact (i.e., Price-Anderson would not apply).

To develop a security performance standard that relates to the ENO criteria, it is necessary to focus on preventing the theft or diversion of an amount of fuel that could be used in a fashion (i.e., dispersal or weapon) that would exceed the ENO criteria. Accordingly, detection and inventory tracking are key to prevention. Thus, ensuring new plant designs includes sufficient

detection capability and a surveillance program capable of rapidly detecting the loss of material (before large quantities can be lost) is an element of the security performance standards.

Design Solutions Performance Standard

Consistent with Commission direction in its SRM of September 9, 2005, design solutions to security concerns are preferred over operational controls. Accordingly, when alternative solutions to the resolution of security issues are possible, those alternatives that can resolve the issue by design should be used, whenever practical. Design solutions represent the first line of defense with the least uncertainty and will remain in effect over the life of the plant.

Summary

The proposed security performance standards can be used to (1) describe the protection against security related threats desired in new plants and (2) assess whether or not changes should be made to plant design, operation, preparedness or security to provide high assurance of protection of public health and safety.

The security performance standards provide specific criteria to implement the security expectations. They focus on protection of public health and safety and build upon and are consistent with existing safety philosophy (e.g., defense-in-depth) and expectations (e.g., safety goals), thus helping to integrate safety, security and preparedness. They are risk-informed and written in a performance-oriented fashion expressed either in a qualitative fashion or a quantitative fashion. However, the way in which these standards are used in decision making will require an integrated decision-making process, which is described in the next section.

6.4.3Integrated Decision-Making Process

The results of the safety and security assessment will need to be reviewed with respect to the security performance standards and other considerations important to making a decision on the adequacy of security. This will require an integrated decision-making process that takes into account a number of factors that could influence the decision. These factors and their relevance to the decision are discussed below.

(a) The Security Performance Standards

The security performance standards listed above provide factors to be considered in the decision that can be related to performance of the plant. This performance can be calculated in a quantitative fashion or qualitatively determined. Each of these factors should be considered in the decision as follows:

- The guidelines of Figure 1 should be met for each threat considered, for both early and latent fatality risk. The cost benefit associated with region 2 of Figure 1 should be done in accordance with NUREG/BR-0058, “Revision 4, “Regulatory Analysis Guidelines of the USNRC.”

- The defense-in-depth provisions (i.e., multiple lines of defense and prevention and mitigation) should be met for each threat considered.

- Theft or diversion should not result in the loss of nuclear material sufficient to exceed the ENO criteria of 10 CFR 140 for each threat considered.

- Design solutions to security related issues are preferred, particularly when they eliminate the

need for operational controls (e.g., operational security actions).

(b) Other Factors

Other factors not related to performance standards also need to be considered in the decision. These factors are:

- The requirements in 10 CFR 73 and the post 9/11 orders should be complied with, unless an exemption is obtained.
- The scope and quality of the analysis used in the assessment should be consistent with the scope of the threat being assessed and with accepted methods and data.
- The impact of security related actions (e.g., design changes, operational changes) should not detract from overall plant safety or preparedness or worker safety.
- Unquantified uncertainties should be considered with respect to whether or not they could have a major influence on the decision.

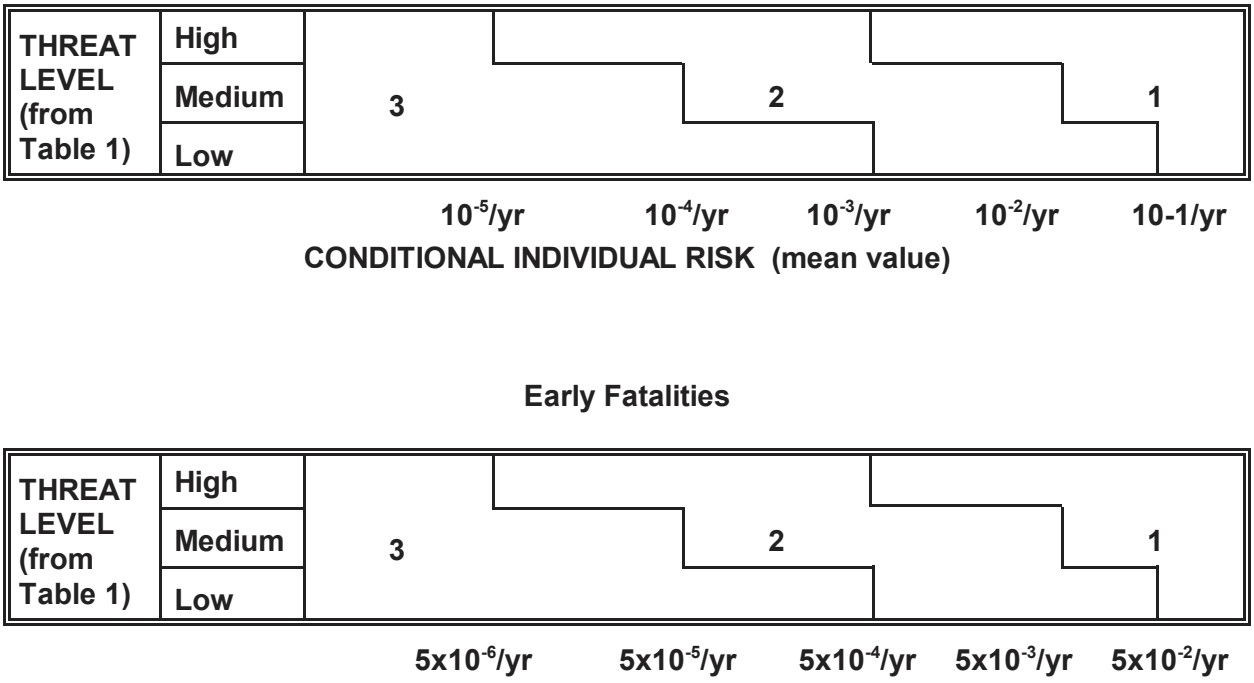
The decision process used in evaluating whether or not to make change in plant design, operation or security as a result of the safety and security assessment needs to consider all of the above factors. Considering all of these factors will help to ensure integration of safety, security and preparedness. Ideally, all factors should be met before deciding to take an action. However, this may not always be possible, in which case the factors for and against a change will need to be weighed and the decision justified on a relative basis.

Finally, it should be noted that over the lifetime of the plant design, operational and security changes are likely to be proposed. Such changes should be evaluated with respect to their impact on security using the same security performance standards and integrated decision making process described above.

Table 1 - Threat Level Severity

Level	Threat Description
High	Capability exists, intentions stated and history make this a credible threat.
Medium	Capability and history exist, but no stated intentions make this a possible threat.
Low	Capability exists, but no stated intentions or history make this an unlikely threat.
Negligible	Neither capability, intentions or history exists and the threat is not considered credible.

Latent Fatalities



Early Fatalities

1 = action warranted, regardless of cost
2 = cost-benefit region
3 = no action warranted

Figure 6.7 Conditional Risk

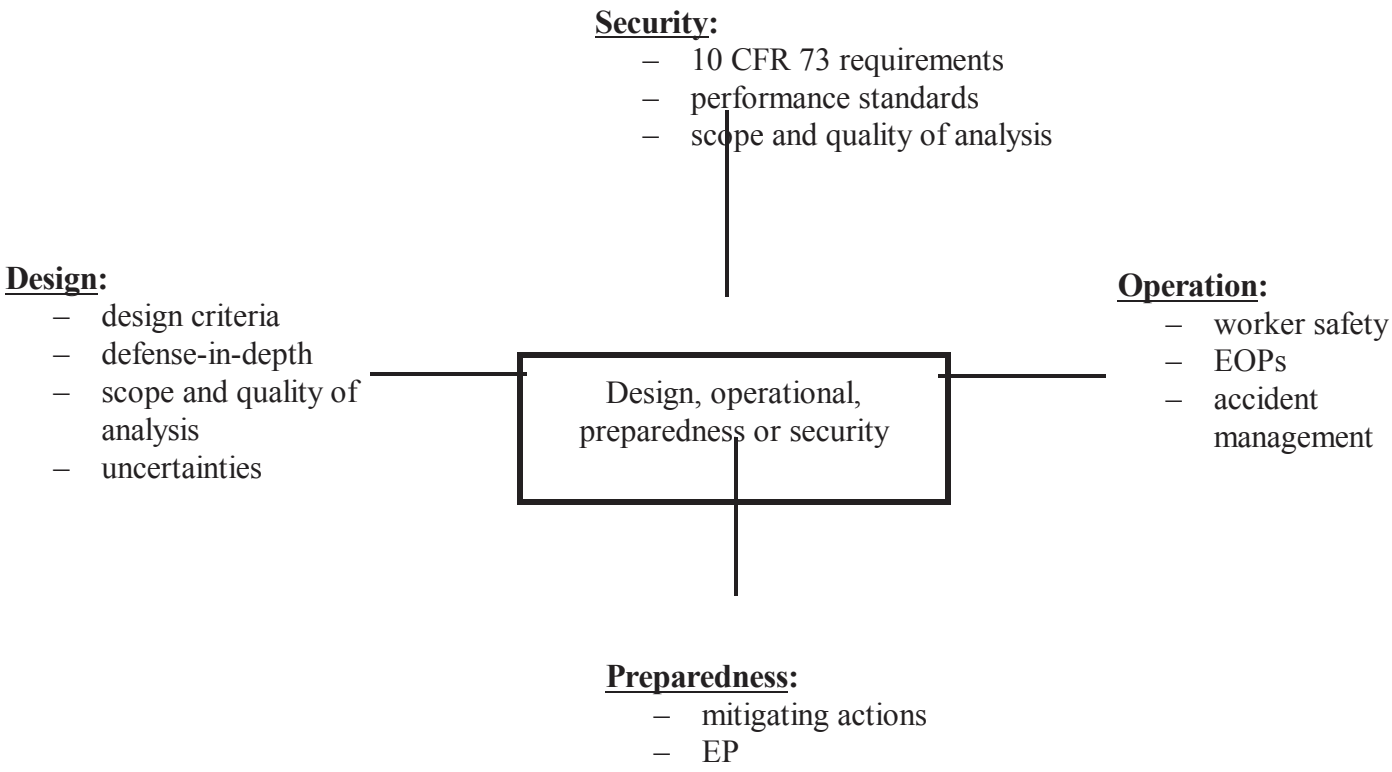


Figure 6.8 Integrated Decision Making

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 risk-informed, performance-based, technology-neutral framework (the framework). These requirements were developed in recognition of the increased role that PRA will play in the establishment of the licensing framework for future 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 framework is to develop a basis for a regulatory structure 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 framework.

The consideration of uncertainties is a vital part of understanding the extent of the risk. Uncertainties need to be addressed in the calculation of both frequencies and consequences of the event sequences and the understanding of uncertainties is necessary for the evaluation of these event sequences against the requirements of the frequency-consequence curve. 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 Development of the Environmental Impact Statement (EIS) and the Severe Accident Mitigation Design Alternative (SAMDA) Analysis

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 per 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 future reactors, 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 cannot 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 is 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 needs 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 or at one mile. 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

It is expected that each future reactor will be required to perform a security assessment integral with the design and that PRA techniques will be used to identify combinations of equipment functions and operator actions that, if failed, could generate radiological releases. 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.

7.2.6 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 is 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 needs to be given to conditions that could shape the action's failure probability such as: its 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 of 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 future 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 future 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 future reactor. 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.

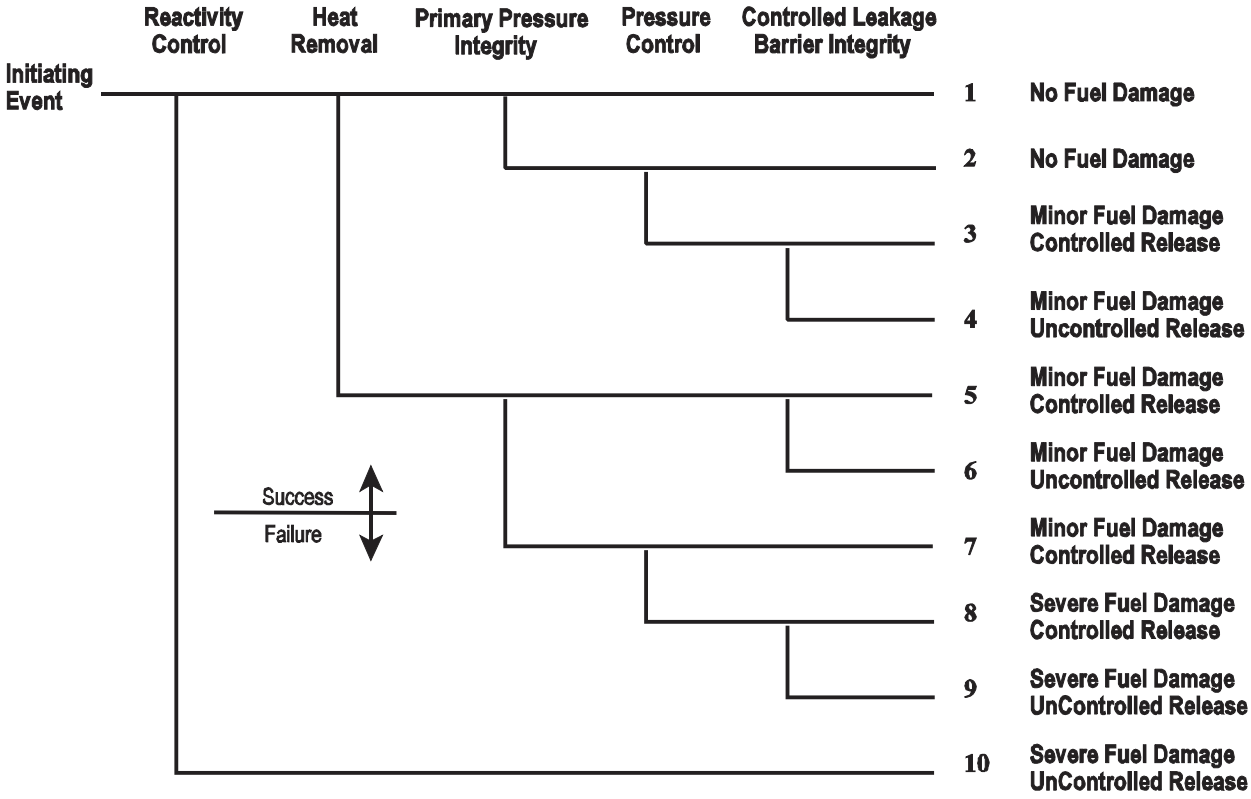


Figure 7-1 Event Sequence Example

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.14] and [Ref.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 needs 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 needs 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, needs 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.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 needs 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 needs 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 future reactor 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 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.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.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. 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 regulatory 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 requirements and to summarize the application of the process to identify the topics which the requirements must cover to ensure the success of the protective strategies. Only the topics which the requirements must address (and reference to the appropriate framework section for guidance regarding the scope and nature of those requirements) are included in this chapter.

As discussed in Chapter 1, the 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 10 CFR part that would be an alternative to the 10 CFR 50 requirements for licensing of future NPPs.

Since a stand-alone new 10 CFR part is envisioned, it must be complete with respect to administrative, as well as technical requirements and interface with the other parts of 10 CFR similar to 10 CFR 50. To accomplish the above, the approach taken is to ensure that all necessary provisions of 10 CFR 50 (e.g., technical, process, administrative, etc.) must also appear in the requirements. Accordingly, since 10 CFR 50 has some requirements that are already applicable to all reactor technologies (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 10 CFR 50 requirements as is reasonable based upon their technology-neutral characteristics. Appendix H of the framework identifies those 10 CFR 50 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), including a summary of the results of the application of that process to the technical and administrative areas, guidelines to be followed in developing the actual requirements (Section 8.3), technology specific considerations (Section 8.4), and how the results of applying the process were checked for completeness (Section 8.5). Appendix G contains the detailed discussion of the application of the process to the technical and administrative areas which led to the summary contained in Section 8.2.

8.2 Process for Identification of Requirements Topics

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. Each of the boxes shown in Figure 8-1 is discussed in the subsections below.

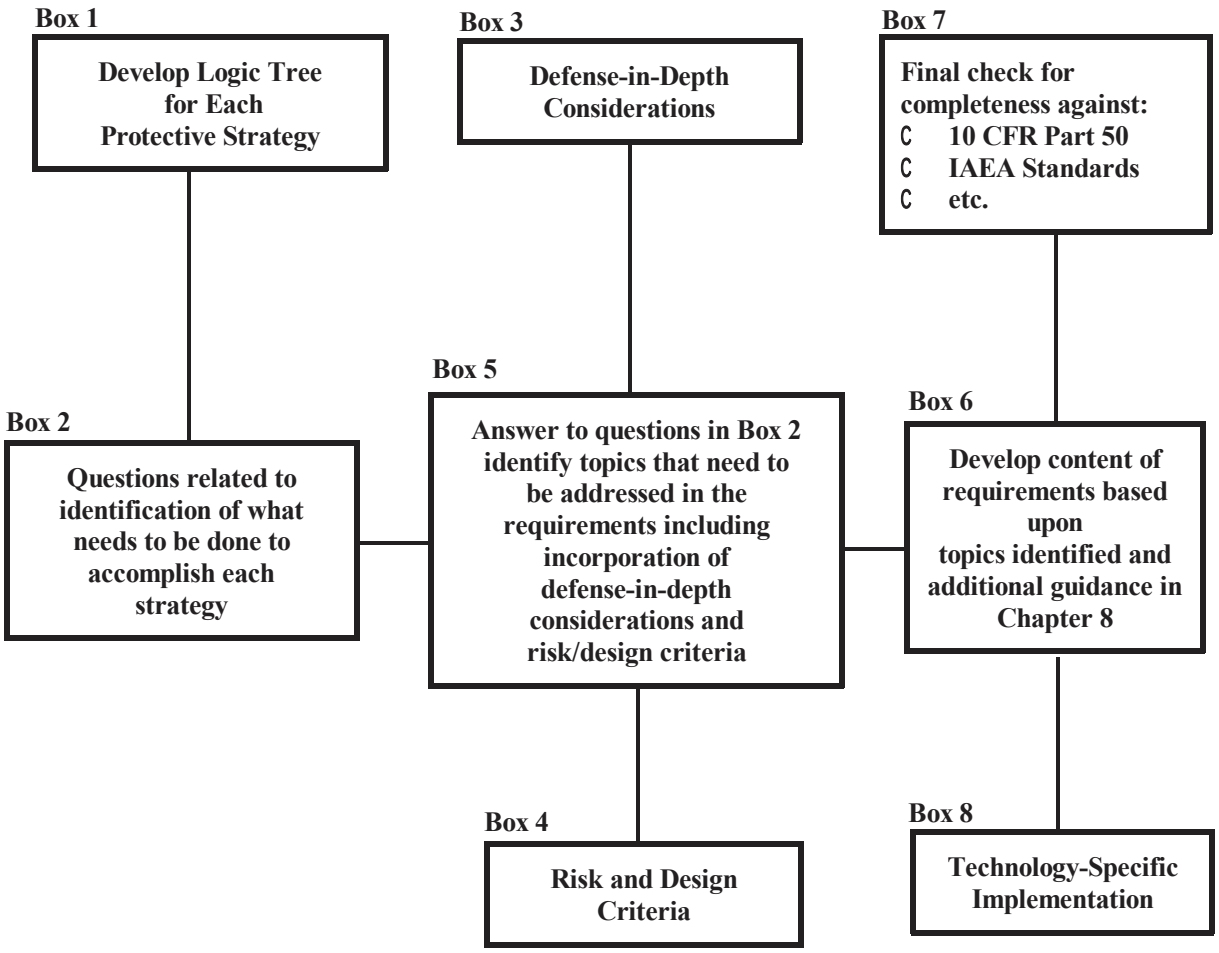


Figure 8-1 Process for identification of requirements topics.

8.2.1 Box 1 - Logic Trees

For each protective strategy, a logic tree is developed that identifies what would need to occur to fail the protective strategy (Box 1 of Figure 8-1). 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. An example logic tree is shown in Figure 8-2. 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.

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. The "Functional Failure of a Protective Strategy," as shown in Figure 8-2, can occur in one of the following three ways:

1) **"Failure of Plant 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. Even though the licensing analysis may be correct, 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 perform its anticipated function. For example:

   - 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.

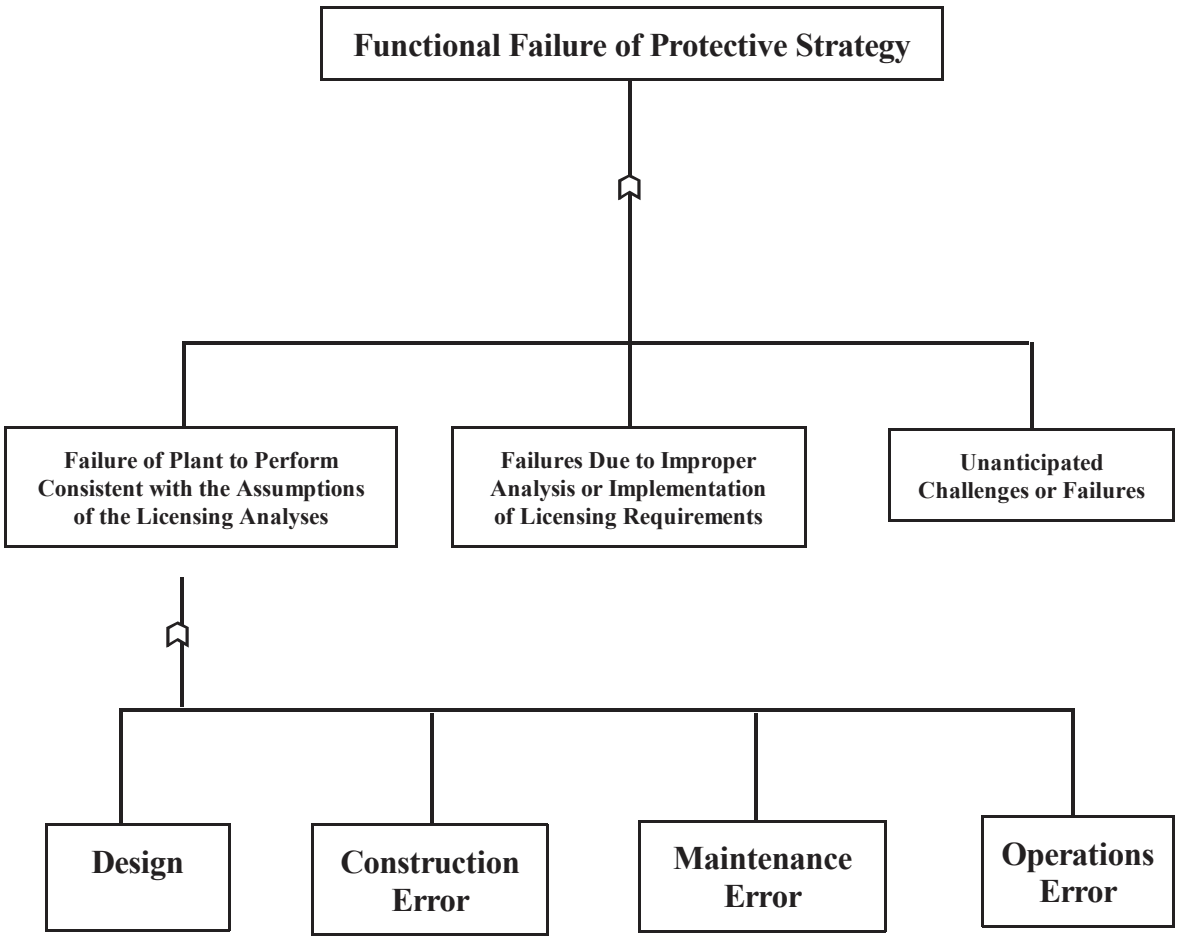


Figure 8-2 Example logic tree.

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. The licensing analysis is the basis for confidence that the design is implemented and maintained in accordance with the requirements. Failure to properly implement these requirements (due to errors in the analysis or interpretation of requirements) means that the risk could become greater than expected. Such errors can obscure or mask the risk and lead to unanalyzed events.

3) "Unanticipated Challenges / Failures"

This pathway acknowledges completeness uncertainty. There may be initiating events and scenarios not identified in the PRA. 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 the protective strategies and 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.

8.2.2 Box 2 - Questions

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 of Figure 8-1) were developed, the answers to which identify the actions that need to be taken to ensure the protective strategy is successful. These answers may be related to design construction, maintenance, or operation. 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). Table 8-1 provides an example of the questions and answers for the Barrier Integrity Protective Strategy.

Table 8-1 Example questions - barrier integrity.

Protective Strategy Questions	Topics to be Addressed in the Requirements		
	Design	**Construction**	**Operation**
Failure to Perform Consistent with Assumptions - Operations Error			
• What needs to be done to prevent operational errors? (BI-4)	• Use good HF and HMI engineering • Use fault tolerant designs	• N/A	• verified procedures • 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 • provisions to establish a containment functional capability independent of fuel and RCS for the reactor.	• N/A • N/A	• technical specifications • technical specifications

8.2.3 Box 3 - Defense-In-Depth

In developing the answers to each question, other issues also need to be considered (Boxes 3 and 4 of Figure 8-1). Box 3 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 and appropriate safety margins are provided.

- 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 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 that could cause an adverse impact on the health and safety of workers or the environment.

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 (i.e., protective strategy), as well as in a broad sense across the entire design. Table 8-2 shows the results of applying the defense-in-depth principles to each of the protective strategies. Each of the items identified in Table 8-2 results in a topic for which a requirement is needed.

Table 8-2 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	Security 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	Security Assessment	Ensure events that can fail multiple PS are $<10^{-7}$/plant year.	Provide 2 independent, redundant diverse means for: reactor shutdown and DHR.	Provide at least 2 barriers:	No key safety function dependent upon a single human action or piece of hardware
4) Account for uncertainties in performance and provide safety margins	Security Assessment and Consideration of Beyond DBTs	Reliability Assurance Program (RAP). Provide safety margins in performance limits.	Applicant to propose reliability and availability goals and RAP. Provide safety margin in regulatory limits.	Provide containment functional capability independent from fuel and RCS. Provide safety margin in regulatory limits.	EP Use 95% ST in calculations for safety margin.

Table 8-2 Defense-in-Depth (DID) provisions.

DID Principle	Physical Protection	Stable Operation	Protective Systems	Barrier Integrity	Protective Actions
5) Prevent unacceptable release of radioactive material	Security Assessment	Ensure events that can fail (stable oper, PS and BI) PS are $<10^{-7}$/plant year.	N/A	Provide containment functional capability independent from fuel and RCS	AM
6) Siting	Security Assessment	Applicant should propose limits on ext. event cumulative frequencies.	N/A	N/A	EP

N/A = Not applicable

8.2.4 Box 4 - Risk and Design Criteria

Chapter 6 identifies a number of risk and design criteria that are key to ensuring a risk-informed licensing process consistent with the Commission's safety goals. This includes:

- a frequency-consequence curve
- probabilistic event selection criteria
- criteria for the selection of licensing basis events (LBEs)
- LBE acceptance criteria
- risk-informed safety classification criteria

Box 4 of Figure 8-1 is intended to ensure that the answers to the questions identified in Box 2 incorporate the risk and design criteria contained in Chapter 6 of the framework and the PRA requirements contained in Chapter 7.

8.2.5 Box 5 - Topics

The answers to the questions for each protective strategy (Box 5 of Figure 8-1) 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.

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 identification of the topics (i.e., implementation of Boxes 1 through 5) is described in Appendix G. This subsection summarizes the results of that application, as documented in Appendix G. Table 8-3 summarizes the topics identified in Appendix G for which requirements need to be written. These topics are organized by:

- Topics common to design, construction, operation
- Physical protection
- Design
- Construction
- Operation
- Administrative

Also shown in Table 8-3 is the location in the framework where additional discussion related to each topic is provided.

Table 8-3 Topics for requirements.

Topic	Framework Technical Description
(A) Topics Common to Design, Construction and Operation	
1) QA/QC	Appendix G - Section G.2.2
2) PRA scope and technical acceptability	Chapter 7 and Appendix F
(B) Physical Protection	
1) General (10 CFR 73)	Appendix G - Section G.2.1
2) Perform security assessment integral with design	Appendix G - Section G.2.1
3) Security performance standards	Section 6.4
(C) Good Design Practices	
1) Plant Risk: - Frequency-Consequence curve - QHOs (including integrated risk)	Chapter 6
2) Criteria for selection of LBEs	Chapter 6
3) LBE acceptance criteria: • frequent events (dose, plant damage) • infrequent events (dose, plant damage) • rare events (dose) • link to siting	Chapter 6
4) Keep initiating events with potential to defeat two or more protective strategies $<10^{-7}$/plant year	Appendix G - Section G.2.2
5) Criteria for safety classification and special treatment	Chapter 6
6) Equipment Qualification	Appendix G - Section G.2.2
7) Analysis guidelines • realistic analysis, including failure assumptions • source term	Chapter 6
8) Siting and site-specific considerations	Appendix G - Section G.2.2
9) Use consensus design codes and standards	Appendix G - Section G.2.2
10) Materials and equipment qualification	Appendix G - Section G.2.2
11) Provide 2 redundant, diverse, independent means for reactor shutdown and decay heat removal	Appendix G - Section G.2.3
12) Minimum - 2 barriers to FP release	Appendix G - Section G.2.3
13) Containment functional capability	Appendix G - Section G.2.4
14) No key safety function dependent upon a single human action or piece of hardware	Appendix G - Section G.2.5

Table 8-3 Topics for requirements.

Topic	Framework Technical Description
15) Need to consider degradation and aging mechanisms in design	Appendix G - Section G.2.2
16) Reactor inherent protection (i.e., no positive power coefficient, limit control rod worth, stability, etc.)	Appendix G - Section G.2.2
17) Human factors considerations	Appendix G - Section G.2.2
18) Fire protection	Appendix G - Section G.2.2
19) Control room design	Appendix G - Section G.2.5
20) Alternate shutdown location	Appendix G - Section G.2.5
21) Flow blockage prevention	Appendix G - Section G.2.2
22) Specify reliability and availability goals consistent with PRA: - establish Reliability Assurance Program - specify goals on initiating event frequency	Appendix G - Section G.2.2
23) Use of prototype testing	Appendix G - Section G.2.2
24) Research and Development	Appendix G - Section G.2.2
25) Combustible gas control	Appendix G - Section G.2.3
26) Coolant/water/fuel reaction control	Appendix G - Section G.2.3
27) Prevention of brittle fracture	Appendix G - Section G.2.2
28) Leak before break	Appendix G - Section G.2.2
29) I and C System • analog • digital • HMI	Appendix G - Section G.2.2
30) Criticality prevention	Appendix G - Section G.2.2
31) Protection of operating staff during accidents	Appendix G - Section G.2.5
32) Qualified analysis tools	Chapter 6
(D) Good Construction Practices	
1) Use accepted codes, standards, practices	Appendix G - Section G.2.2
2) Security	Appendix G - Section G.2.1
3) NDE	Appendix G - Section G.2.2
4) Inspection	Appendix G - Section G.2.2
5) Testing	Appendix G - Section G.2.2
(E) Good Operating Practices	

Table 8-3 Topics for requirements.

Topic	Framework Technical Description
1) Radiation protection during routine operation	Appendix G - Section G.2.2
2) Maintenance program	Appendix G - Section G.2.2
3) Personnel qualification	Appendix G - Section G.2.2
4) Training	Appendix G - Section G.2.2
5) Use of Procedures	Appendix G - Section G.2.2
6) Use of simulators	Appendix G - Section G.2.2
7) Staffing	Appendix G - Section G.2.2
8) Aging management program	Appendix G - Section G.2.2
9) Surveillance (including materials surveillance program)	Appendix G - Section G.2.2
10) ISI	Appendix G - Section G.2.2
11) Testing	Appendix G - Section G.2.2
12) Technical specifications, including environmental	Appendix G - Section G.2.2
13) Develop EOP and AM procedures integral with design	Appendix G - Section G.2.5
14) Develop EP integral with design	Appendix G - Section G.2.5
15) Monitoring and feedback	Appendix G - Section G.2.2
16) Work and configuration control	Appendix G - Section G.2.2
17) Living PRA	Chapter 7
18) Maintain fuel and replacement part quality	Appendix G - Section G.2.2
19) Security	Appendix G - Section G.2.1
(F) Administrative	
1) Standard format and content of applications	Appendix G - Section G.3
2) Change control process	Appendix G - Section G.3
3) Record keeping	Appendix G - Section G.3
4) Documentation control	Appendix G - Section G.3
5) Reporting	Appendix G - Section G.3
6) Monitoring and Feedback: - plant performance - environmental releases - testing results	Appendix G - Section G.3
7) Corrective action program	Appendix G - Section G.3
8) Backfitting	Appendix G - Section G.3

Table 8-3 Topics for requirements.

Topic	Framework Technical Description
9) License amendments	Appendix G - Section G.3
10) Exemptions	Appendix G - Section G.3
11) Other legal and process items from 10CR50	Appendix G - Section G.3

8.2.6 Box 6 - Development of Requirements

The next step of the process is the actual development of the technology-neutral requirements (Box 6 of Figure 8-1).

Section 8.3 provides guidance on how to take the topics identified in Section 8 and develop requirements. As described in Section 8.3, the guidance covers five factors which need to be considered. These factors are:

- use of 10 CFR 50 requirements and their supporting regulator guides where practical (i.e., technology-neutral, risk-informed and performance-based);
- ensure requirements consider lessons learned from the past;
- use of a risk-informed and performance-based approach;
- development of a stand-alone set of requirements; and
- need for technology-specific guidance.

8.2.7 Box 7 - Completeness Check

Before finalizing the requirements, a check for completeness was made (Box 7 of Figure 8-1). This check was performed by comparing the list of topics against other documents containing reactor design or licensing requirements. The details of this completeness check are described in Appendix K and summarized in Section 8.5.

8.2.8 Box 8 - Technology-Specific Implementation

Many of the requirements will likely require some technology-specific guidance for implementation. Section 8.4 provides a preliminary assessment as to which requirements will likely require technology-specific guidance for implementation and why.

8.3 Guidelines for Developing Requirements

Section 8.2.5 identifies 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;
- ensure requirements consider lessons learned from the past;
- use of a risk-informed and performance-based approach;
- development of a stand-alone set of requirements;
- need for technology-specific guidance.

Each of these guidelines is discussed in the sections that follow and their relationship to the requirements development process is shown in Figure 8-3. 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.

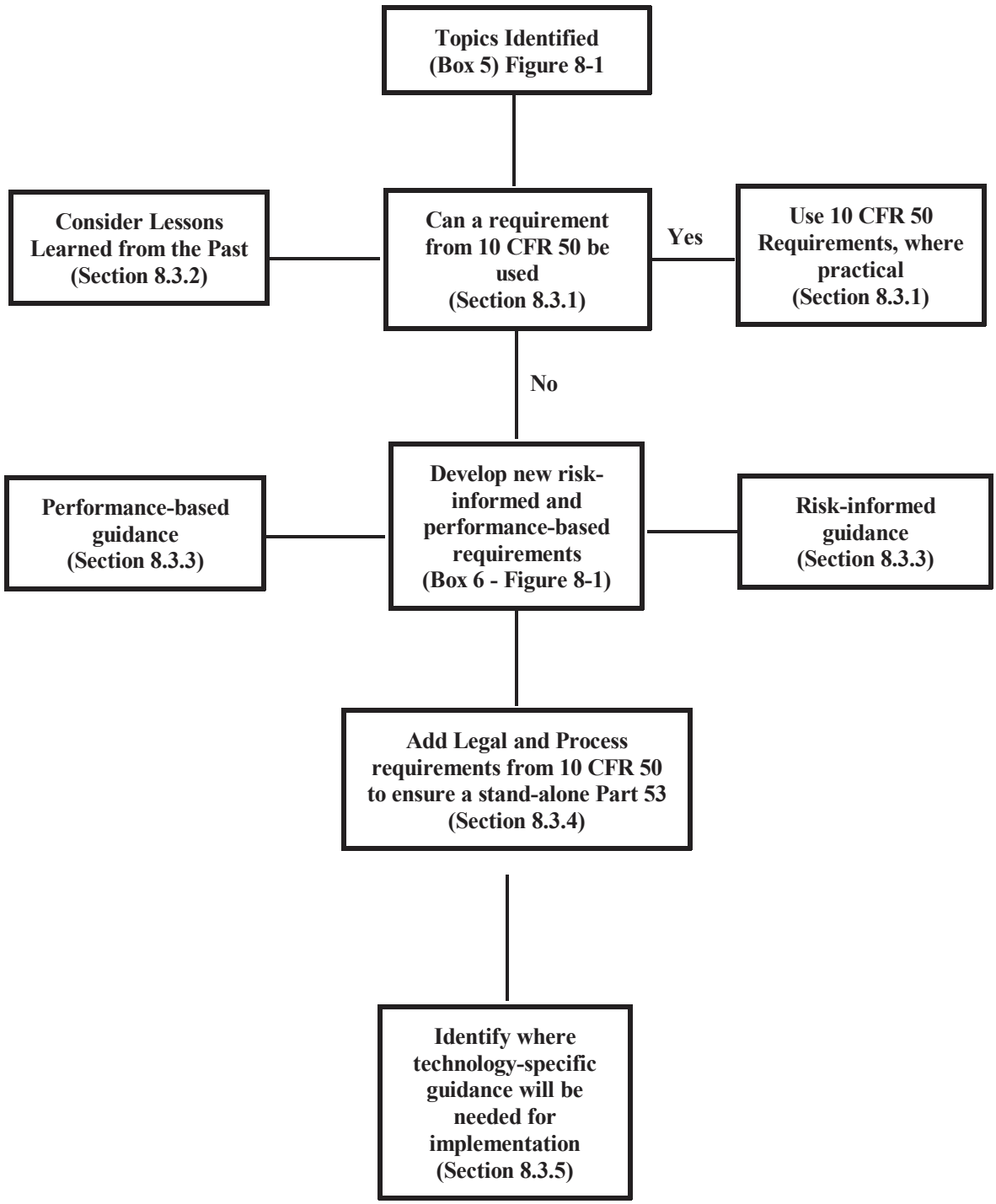


Figure 8-3 Requirements development.

8.3.1 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 H to identify which requirements are technology-neutral and are candidates for use in the technology-neutral requirements. Where they can be used they should be used, 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.

8.3.2 Lessons Learned from the Past

Lessons learned from the past should be applied in writing the requirements. Requirements or gaps in the regulations from the past should not be repeated where they have lead to problems or safety concerns. Examples of areas that should be addressed in the new requirements include:

- preventing flow blockage

- no positive power coefficient;

- limiting control rod worth, and

- preventing direct impingement of molten core material on the containment shell

- items identified by the NRC generic safety issues program as documented in NUREG-0933

- items identified by EPRI in their ALWR Utility Requirement Document.

8.3.3 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, 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. Chapter 6 and 7 contain guidance and criteria related to risk-informing the licensing approach which the requirements need to address. 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 I 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 success criteria from the PRA can provide insights as to the parameters that need to be monitored. 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.

8.3.4 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 8.4.1, 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. Appendix H provides a preliminary identification of where 10 CFR 50 wording can be used.

8.3.5 Technology-Specific Implementation

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. Table 8-4 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.

8.4 Requirements

Applying the guidelines above to the topics identified in Section 8.3 will result in a set of 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. However, Appendix J contains some example requirements to illustrate the format and level of detail envisioned in the requirements.

One of these example requirements is discussed below with respect to the five factors discussed

in Section 8.3.1 through 8.3.5 to illustrate application of the guidance.

Example Requirement - Plant Risk

Each application to construct and operate a NPP shall include a probabilistic risk assessment that:

(1) includes the risk from full power and low power operation, shutdown, refueling and spent fuel storage (except that from dry cask storage)

(2) includes assessment of internal and external events and uncertainties

(3) shows each accident sequence in the PRA meets the appropriate does limit on the F-C curve at its mean value

(4) shows overall risk from the NPP (or if more than one NPP from all NPPs on site) meets the QHOs expressed in the Commission's 1986 Safety Goal Policy using mean risk values.

Application of Factors

- Use 10 CFR 50 Requirements - no equivalent requirements on plant risk exist in 10 CFR 50; therefore a new requirement is needed
- Lessons Learned from the Past - address all modes of operation and internal and external events
- Risk-Informed/Performance-Based - uses risk criteria and calculations can show plant performance with respect to the criteria
- Stand-alone Requirement - is needed to ensure a complete set of regulations
- Technology-Specific Considerations - will likely not be needed due to technology-neutral nature of criteria.

Table 8-4 Topics needing technology-specific implementation guidance.

Topic	Technology-Specific Guidance Required?	Comment
(A) Topics Common to Design, Construction and Operation		
1) QA/QC	No	
2) PRA scope and technical acceptability	Yes	risk metrics and methods may be technology dependent
(B) Physical Protection		
1) General (10 CFR 73)	No	
2) Perform security assessment integral with design	No	
3) Security performance standards	No	
(C) Good Design Practices		
1) Plant Risk: - Frequency-Consequence curve - QHOs (including integrated risk)	No	
2) Criteria for selection of LBEs	No	
3) LBE deterministic acceptance criteria: • frequent events (dose, plant damage) • infrequent events (dose, plant damage) • rare events (dose) • link to siting	Yes	plant damage definitions are tech dependent
4) Keep initiating events with potential to defeat two or more protective strategies $<10^{-7}$/plant year	Yes	example events should be stated
5) Criteria for safety classification and special treatment	Yes	different risk metrics for each technology
6) Equipment Qualification	No	
7) Analysis guidelines • realistic analysis, including failure assumptions • source term	No	
8) Siting and site-specific considerations	No	
9) Use consensus design codes and standards	Yes	will need to identify acceptable codes and standards

Table 8-4 Topics needing technology-specific implementation guidance.

Topic	Technology-Specific Guidance Required?	Comment
10) Materials qualification	Yes	different technologies have different materials
11) Provide 2 redundant, diverse, independent means for reactor shutdown and decay heat removal	No	
12) Minimum - 2 barriers to FP release	Yes	barrier definition
13) Containment functional capability	Yes	design conditions are technology dependent
14) No key safety function dependent upon a single operator action	No	
15) Need to consider degradation and aging mechanisms in design	No	
16) Reactor inherent protection (i.e., no positive power coefficient, limit control rod worth, stability, etc.)	No	
17) Human factors considerations	No	
18) Fire protection	Yes	different technologies have different fire hazards
19) Control room design	No	
20) Alternate shutdown location	No	
21) Flow blockage prevention	No	
22) Specify reliability and availability goals consistent with PRA: - establish Reliability Assurance Program - specify goals on initial event frequency	No	
23) Use of prototype testing	No	
24) Research and Development	No	
25) Combustible gas control	No	
26) Coolant/water/fuel reaction control	Yes	different technologies have different hazards

Table 8-4 Topics needing technology-specific implementation guidance.

Topic	Technology-Specific Guidance Required?	Comment
27) Prevention of brittle fracture	Yes	different materials and fluence will require different limits
28) Leak before break	Yes	different materials and technologies will require different leak detection and limits
29) I and C Systems: • analog • digital • HMI	No	
30) Criticality prevention	No	
31) Protection of operating staff during accidents	No	
32) Qualified analysis tools	No	*
(D) Good Construction Practices		
1) Use accepted codes, standards, practices	Yes	will need to identify acceptable codes and standards
2) Security	No	
3) NDE	Yes	different techniques will apply to different materials
4) Inspection	Yes	different techniques
5) Testing	No	
(E) Good Operating Practices		
1) Radiation protection during routine operation	No	
2) Maintenance program	No	
3) Personnel qualification	No	

Table 8-4 Topics needing technology-specific implementation guidance.

Topic	Technology-Specific Guidance Required?	Comment
4) Training	No	
5) Use of Procedures	No	
6) Use of simulators	No	
7) Staffing	Yes	different needs will be design and technology dependent
8) Aging management program	No	
9) Surveillance (including materials surveillance program)	Yes	different technologies require different programs
10) ISI	Yes	will need to identify acceptable ISI methods or standards
11) Testing	Yes	different needs for different technologies
12) Technical specifications, including environmental	No	
13) Develop EOP and AM procedures integral with design	No	
14) Develop EP integral with design	No	
15) Monitoring and feedback	No	
16) Work and configuration control	No	
17) Living PRA	No	
19) Maintain fuel and replacement part quality	No	
19) Security	No	
(F) Administrative		
1) Standard format and content of applications	No	
2) Change control process	No	
3) Record keeping	No	
4) Documentation control	No	

Table 8-4 Topics needing technology-specific implementation guidance.

Topic	Technology-Specific Guidance Required?	Comment
5) Reporting	No	
6) Monitoring and Feedback: - plant performance - environmental releases - testing results	No	
7) Corrective action program	No	
8) Backfitting	No	
9) License amendments	No	
10) Exemptions	No	
11) Other legal and process items from 10 CR 50	No	

8.5 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 Table 8-1. 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 K 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 failure 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.

GLOSSARY

Term	Definition
Abnormal Occurrence	an unscheduled incident or event which the Commission determines is significant from the standpoint of public health and safety
Acceptance Criteria	criteria established by NRC regulation or other regulatory document that licensee must demonstrate by calculation or experiment is satisfied in order to obtain NRC approval to operate a nuclear facility
Accident Mitigation	a strategy to reduce the severity of an accident
Accident Prevention	a strategy to prevent an accident from occurring that could result in releases from the fuel
Accident Progression Analysis	Evaluates the type and severity of challenges to the integrity of the available barriers that may arise during accident sequences. Includes characterization of the source term to the environment.
Accident Sequence	a representation of an accident in terms of an initiating event followed by a combination of system, function and operator failures or successes that lead to a specified end state.
Adequate Protection	that level of protection that results in no undue risk to public health and safety

Term	Definition
Aleatory Uncertainty	the uncertainty inherent in a nondeterministic (stochastic, random) event or phenomenon.
Anticipated Operational Occurrence	A condition of normal operation that is expected to occur one or more times during the life of the power plant.
Average Individual Risk	"Found by accumulating the estimated individual risks and dividing by the number of individuals residing in the vicinity of the plant" (e.g. the average individual risk of early fatality is calculated by estimating the total risk of early fatalities per year to the population within 1 mile of plant and dividing by the population within 1 mile)
Barrier Integrity	one of five protective strategies with intent to prevent release of radionuclides across a preventive or mitigative barrier (e.g., barriers may include fuel cladding, reactor vessel, containment building)
Best Estimate	the point estimate of a parameter used in a computation that is not biased by conservatism or optimism
Common Cause Failure (CCF)	a failure of two or more components during a short period of time as a result of a single shared cause
Completeness Uncertainty	uncertainty in the PRA model related to lack of knowledge or intentional exclusion from scope
Conditional Probability	probability of an event given that a second event has occurred

Term	Definition
Consequence Analysis	Evaluates the offsite consequences of an accidental release of radionuclides to the environment expressed in terms of human health, environmental, and economic measures
Defense In Depth	an element of NRC's safety philosophy that is used to address uncertainty by employing successive measures, including safety margins, to prevent accidents or mitigate damage if a malfunction or accident occurs at a nuclear facility
Design Basis Accident	a postulated accident that a nuclear facility must be designed and built to withstand without loss to the systems, structures, and components necessary to assure public health and safety;
Deterministic	descriptor of a phenomenon, function, parameter or model that defines it as being causal rather than random
Deterministic Acceptance Criteria	criteria based upon causal (non-probabilistic) analysis for acceptance of safety analysis based on a set of accident sequences
Early Fatality	A fatality that occurs within one year (or less) from radiation doses accumulated during exposure to radionuclides released to the environment in an accident
Emergency Plan	a plan to mitigate the consequences of a release of radioactivity from the fuel elements, that includes actions by the utility and governmental agencies to shelter or evacuate people in the community in the event of a severe accident

Term	Definition
Emergency Planning Zone	the areas around a nuclear power plant for which planning is needed to assure that prompt and effective actions can be taken to protect the public in the event of an accident at a nuclear power plant or the areas around a nuclear power plant for which there exists a preplanned strategy for protective actions during an emergency
Emergency Preparedness	"Emergency preparedness means taking action to be ready for emergencies before they happen. The objective of emergency preparedness is to simplify decision making during emergencies... The emergency preparedness process incorporates the means to rapidly identify, evaluate and react to a wide spectrum of emergency conditions."
Environmental Qualification	A process for ensuring that equipment will be capable of withstanding the ambient conditions that could exist when the specific function to be performed by the equipment is actually called upon to be performed under accident conditions
Epistemic Uncertainty	the uncertainty attributable to incomplete knowledge about a phenomenon or event that affects the ability to model it •
Equipment Qualification	the generation and maintenance of data and documentation to ensure that the equipment will operate on demand to meet system performance requirements
Event Class	a grouping of event (accident) sequences that are similar in terms of initiating events and accident behavior, leading to similar source terms

Term	Definition
Event Sequence	the sequence of events that characterize the response of a plant to an upset condition, beginning with a given initiating event, including the safety system responses and the human actions, to the defined end state of the sequence
Exclusion Area Boundary	boundary of "the area surrounding the reactor where the reactor licensee has the authority to determine all activities, including exclusion or removal of personnel and property."
Failure Mechanism	any of the processes that results in failure modes, including chemical, electrical, mechanical, physical, thermal, and human error
Failure Mode	a specific functional manifestation of a failure (i.e., the means by which an observer can determine that a failure has occurred) precluding the successful operation of a piece of equipment, a component, or a system.
Failure Probability	the likelihood that a system, structure, or component will fail to operate upon demand or fail to operate for a specific mission time
Failure Rate	expected number of failures per unit of time, evaluated, for example, by the ratio of the number of failures in a population of components to the total time observed for that population
Fault Tree	a deductive logic diagram that depicts how a particular undesired event can occur as a logical combination of other undesired events
Human Error (HE)	any human action, including inaction, that exceeds some limit of acceptability where required, excluding malevolent behavior
Inherent Design Feature	a design feature that has been engineered into the plant, or that is a result of the physics of plant performance

Term	Definition
Initiating Event	any event, either internal or external to the plant, that perturbs the steady state operation of the plant (if operating) thereby initiating an abnormal event such as a transient or LOCA within the plant.
Initiating Event Frequency	frequency of occurrence (e.g., per year) of an Initiator (or Initiating Event)
Intentional Acts	Adverse actions taken by an individual or group against a plant
Internal Initiating Event (or Initiator)	an initiating event originating within a nuclear power plant that, in combination with safety system failiures and/or operator errors, can affect the operability of plant systems and may lead to fuel damage and radionuclide release
Large Early Release Frequency (LERF)	expected number of large early releases per unit of time
Large Early Release	the rapid, unmitigated release of airborne fission products from the plant to the environment occurring before the effective implementation of off-site emergency response and protective actions such that there is a potential for early health effects
Latent Fatality	a cancer fatality due to radiation doses that may occur many years after exposure to radionuclides released to the environment in an accident
Licensing Basis Event	Event sequences 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.
Living PRA	a PRA that is maintained and upgraded to reflect the as built and as operated plant
Passive Systems	safety systems that rely on basic physical material properties or natural physical phenomena to perform essential safety functions

Term	Definition
Passive Safety Features	safety features of a plant that rely on basic physical material properties or natural physical phenomena to perform essential safety functions
Performance Based	descriptor of processes that can be monitored by quantitative measures of performance.
Performance Based Regulation	Performance-based regulation is defined as " Required results or outcome of performance rather than a prescriptive process, technique, or procedure."
Probabilistic Risk Assessment (PRA)	a quantitative assessment of the risk associated with plant operation and maintenance that is measured in terms of frequency of occurrence of risk metrics, such as core damage or a radioactive material release and its effects on the health of the public
Quantitative Health Objectives (QHO)	numerical measures of acceptable risk to the population in the vicinity of a plant expressed in terms of risk of public health effects - early fatalities and latent cancer fatalities
Random	descriptor of a phenomenon, function, parameter or model that defines it as being subject to chance
Rationalist	approach to safety that views defense-in-depth in terms of provisions to compensate for uncertainty and incomplete knowledge of accident initiation and progression, and seeks to evaluate the uncertainties to determine what steps should be taken to compensate
Reliability	the probability that a system or component will performs its specified function under given conditions upon demand or for a prescribed time

Term	Definition
Risk	probability and consequences of an event, as expressed by the "risk triplet" that is the answer to the following three questions: (I) What can go wrong? (ii) How likely is it? and (iii) What are the consequences if it occurs?
Risk Achievement Worth (RAW)	for a specified basic event, risk achievement worth reflects the increase in a selected figure of merit for risk when an SSC is assumed to be unable to perform its function due to testing, maintenance or failure
Risk Based	an approach to regulatory decision-making in which a safety decision is solely based upon the numerical results of a risk assessment.
Risk-Inform(ed)	a characteristic of regulatory decision-making that includes results and findings that derive from risk assessments and other factors that are designed to better focus licensee and regulatory attention on design and operation issues commensurate with their importance to health and safety.
Risk Measure	a quantitative basis for measurement of risk
Safety Classification	the designation of a plant system as safety-related or non-safety related, and (more recently) safety-significant or non-safety significant (RISC scheme)
Safety Function	the safety-related purpose of a structure, system or component, or human action

Term	Definition
Safety Margin	an element of defense-in-depth that is the sum of (1) the regulatory margin which is the difference between the ultimate capacity of the safety variable and the regulatory limit of the safety variable, and (2) the design margin, added at the option of the designer, which is the difference between the regulatory limit of the safety variable and the value of the safety variable at which the system or barrier is expected to perform, according to the design.
Safety Significance	usually refers to a quantitative measure of the importance to safety of an SSC or operator action
Severe Accident	an accident that involves extensive fuel damage and fission product release into the reactor vessel and surrounding plant structure, with potential release to the environment
Source Term	"...the magnitude and mix of the radionuclides released from the fuel, expressed as fractions of the fission product inventory in the fuel, as well as their physical and chemical form, and the timing (and energy) of the release."
Stable Operation	Controlled operation of a nuclear plant under full power, shutdown and transitional states.
Standard Design Certification under 10 CFR Part 52,	NUREG/BR-0298, Rev 2 (derived), independent of the review of the specific site
Stochastic	involving chance or probability
Structuralist	approach to safety that views defense-in-depth requirements as resulting from repeatedly asking 'what if this barrier or safety system fails?' without a quantitative estimate of the likelihood of such a failure
Success Criteria	criteria for establishing the minimum number or combinations of systems or components required to operate, or minimum levels of performance per component during a specific period of time, to ensure that the safety functions are satisfied.

Term	Definition
Surrogate Risk Objective	a risk objective that is derived from (and is essentially equivalent to) the Quantitative Health Objective of the Commission Safety Goal Policy Statement but is dependent on plant design and features modeled in the plant PRA

7.1 Appendix B to Part 50 – Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants.

7.2 ANSI N45.2.11, “Quality Assurance Requirements for the Design of Nuclear Power Plants.”

7.3 ANSI/ANS-10.4-1987, “American National Standard Guidelines for the Verification and Validation of Scientific and Engineering Computer Programs for the Nuclear Industry.”

7.4 ASME RA-S-2002, “Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications.”

7.5 NUMARC 93-01, “Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants”, Revision 3, July 2000.

[7]Vietti-Cook, A.L., ”Staff Requirements - SECY 05-0120 - Security Design Expectations For New Reactor Licensing Activities,” USNRC Memorandum, September 9, 2005.

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 International Commission on Radiation Protection, ICRP Publication 64: Protection from Potential Exposure: A Conceptual Framework, Annals of the ICRP Volume 23/1, Elsevier, May 1993.

6.3 U. S. Environmental Protection Agency, Office of Radiation and Indoor Air Radiation Protection Division, Protective Action Guides (PAG) Manual.

6.4 U. S. Nuclear Regulatory Commission, “Abnormal Occurrence Reports: Implementation of Section 208 Energy Reorganization Act of 1974,” 62 FR 18820, 1997.

6.5 International Commission on Radiation Protection, ICRP 41: Non-stochastic effects in ionizing radiation, 1984.

6.6 U. S. Nuclear Regulatory Commission, “Code manual for MACCS2,” NUREG/CR-6613, 1998.

6.7 U. S. Nuclear Regulatory Commission, “Health Effects Models for Nuclear Power Plant Consequence Analysis: Low LET Radiation,” NUREG/CR-4214, 1989.

6.8 Commission Policy Statement on the Regulation of Advanced Nuclear Power Plants, 59 FR 35461, 1994.