NUREG -xxxx

Regulatory Structure for New plant Licensing, Part 1: Technology-Neutral Framework

Working Draft Report

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

Revision a
December 2004

FOREWORD

The purpose of this draft NUREG is to discuss an approach, scope, and acceptance criteria that could be used to develop a technology-neutral set of requirements for future plant licensing. At the present time, the material contained in the draft NUREG is preliminary and does not represent final staff positions on the issues discussed. As such, certain sections of this document are incomplete and are planned to be completed following receipt of initial stakeholder feedback.

The work represented in this document is, however, considered sufficiently developed to illustrate one possible way to establish a technology-neutral approach to future plant licensing and to identify the key technical and policy issues to be addressed. In this regard, it can serve as a useful vehicle for engaging stakeholders and facilitating discussion.

Carl J. Paperiello, Director
Office of Nuclear Regulatory Research

ABSTRACT

Table of Contents

List of Figures

List of Tables

PART 1:

TECHNOLOGY-NEUTRAL FRAMEWORK

1. INTRODUCTION

1.1 Background

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. 1-1]

The staff noted in its Advanced Reactor Research Plan [Ref. 1-2] to the Commission, that a risk-informed regulatory structure applied to license and regulate advanced (new) reactors, regardless of their technology, could enhance the effectiveness, efficiency, and predictability (i.e., stability) of new plant licensing. As such, this new process, if implemented, could be available for use later in the decade. The need to develop a risk-informed regulatory structure for new reactors is based on the following considerations:

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

- The regulatory structure for current LWRs has evolved over five decades. Most of this evolution occurred without the benefit of insights from probabilistic risk assessments (PRAs) and severe accident research. It is expected that future applicants will rely on PRAs as an integral part of their license applications. it is further expected that the regulations for these new reactors will be risk-informed. Both deterministic and probabilistic results and insights will be used in the development of the regulations governing these reactors. Consequently, a structured approach for a regulatory structure for new reactors that provides guidance about how to use PRA results and insights will help ensure the safety of these reactors by focusing the regulations on where the risk is most likely while maintaining basic safety principles, such as defense-in-depth and safety margin.

The 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 performance based regulation, as well as ensure a greater degree of coherence among the resulting regulations for new reactors than found among current regulations.

In addition to utilizing the benefits of PRA, the development of a risk-informed technology-neutral structure for new plant licensing has several advantages over continuing to use the 10 CFR Part 50 licensing process for designs substantially different than current generation LWRs. Specifically, the use of a technology-neutral approach can provide more efficiency, stability and predictability then continuing to use the 10 CFR Part 50 process. These points are further discussed below.

- <u>Efficiency</u>: 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 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 technology-neutral licensing process that has acceptance criteria applicable to different reactor designs will reduce the uncertainties in the outcome and duration of the licensing process because acceptance criteria would be stable.

- Predictability: Having a set of technology-neutral requirements 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 technology-neutral regulatory structure will help ensure that a systematic approach is used during the development of the regulations that the design, construction, and operation of new reactors. This will ensure uniformity, consistency, and defensibility in the development of the regulations, particularly when addressing the unique design and operational aspects of new reactors.

1.2 Objectives

1.2.1 Program Objective

The objective of this program is to develop and implement a risk-informed regulatory structure for licensing new reactors that demonstrates that the NRC mission of protecting the public health and safety is met. This regulatory structure will provide the technical basis for the development of a new set of regulations for licensing new reactors. This regulatory structure has four parts :

(1) development of a technology-neutral framework for the regulatory structure,
(2) development of proposed content of technology-neutral requirements,
(3) development of guidance for applying the framework on a technology-specific basis (i.e., technology-specific framework), and
(4) development of technology-specific regulatory guides.

The relationship between the four parts of the regulatory structure is shown figure below:

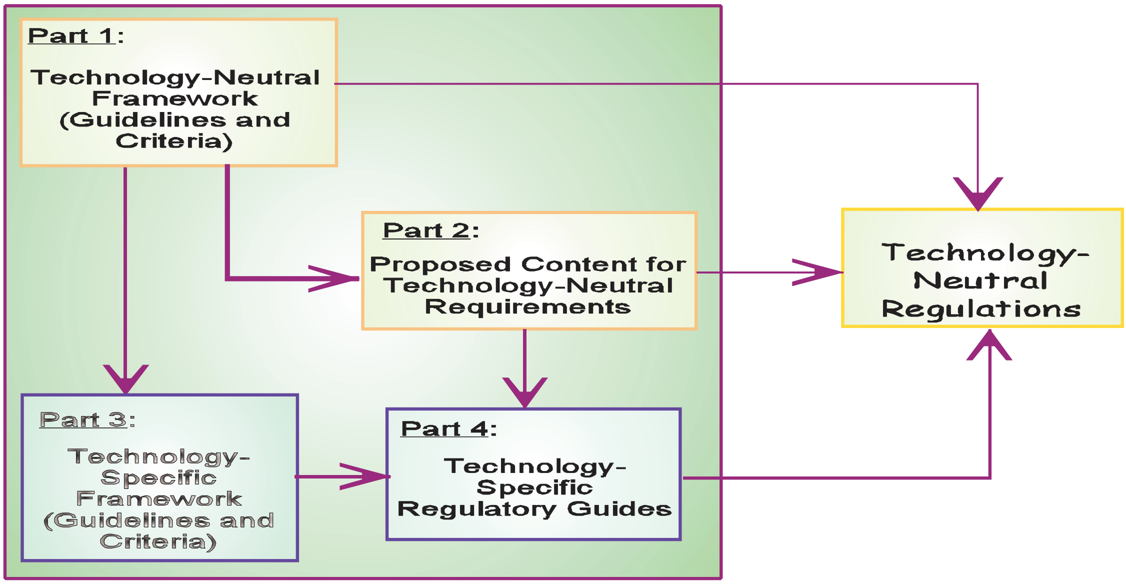

Part 1:
Technology-Neutral Framework (Guidelines and Criteria)
Part 2:
Proposed Content for Technology-Neutral Requirements
Technology-Neutral Regulations
Part 3:
Technology-Specific Framework (Guidelines and Criteria)
Part 4:
Technology-Specific Regulatory Guides

Figure 1-1 Framework for a Regulatory Structure for New Plant Licensing

Part 1 is the development of a technology-neutral framework to anchor the regulatory structure to high-level safety goals. This is a process aligned effort providing guidance for the NRC staff in developing the requirements Part II..

Part II involves the production of a set of high-level, technology-neutral requirements applicable to all reactor designs. These requirements will be based on the framework developed in Part I and will serve as the technical basis for developing technology-neutral regulations for a possible rulemaking.

Part III will develop guidance for the NRC staff on using the technology-neutral framework in conjunction with the technology-neutral requirements on a technology-specific basis. This effort will, therefore, involve development of a technology-specific framework providing technology-specific guidance and criteria.

Part IV is the preparation of technology-specific regulatory guides for specific reactor technologies. This effort will be accomplished by translating the high-level, technology-neutral regulations into technology-specific guidance using the process of Part III.

1.2.2 Technology-Neutral Framework Objective

The objective of the technology-neutral framework is to provide the necessary guidance and criteria for a risk-informed regulatory structure for licensing new reactors. To meet this objective, the guidance and criteria need to address the following:

- safety philosophy
- safety fundamentals
- risk objectives
- design, construction, and operation objectives
- treatment of uncertainties
- process for the identification of requirements

A safety philosophy is defined that establishes the Commission’s expectations for new reactors. Safety fundamentals are defined in terms of protective strategies that are needed to ensure safe nuclear power plant design, construction, and operation.
Quantitative Risk objectives are defined to provide criteria for assessing the risk associated with the design, construction and operation of the plant.

Design, construction, and operation objectives are established to provide criteria for ensuring safe nuclear power plant design, construction, and operation.

The treatment of uncertainties provide the process for ensuring that safety limits are met and the design, construction and operation have enough safety margin to withstand unanticipated events.

1.2.3 Technology-Neutral Requirements Objective

The objective of the technology-neutral requirements is to develop the necessary technical and administrative requirements to ensure safe nuclear power plant design, construction and operation. The requirements should be applicable to any reactor design. These requirements should have the desired characteristics described in Section 1.4 below.

These requirements are to be documented in Part II (Vol. 2) of this NUREG report.

1.2.4 Technology-Specific Framework Objective

The objective of the technology-specific framework is to provide the necessary guidance and criteria for applying the technology-neutral requirements on a technology-specific basis.

1.2.5 Technology-Specific Regulatory Guides Objective

The objective of the technology-specific regulatory guides is to provide the necessary guidance and criteria for meeting the technology-neutral requirements for the specified technology. A technology-specific regulatory guide will be developed to give explicit guidance and criteria for meeting the requirements for that technology.

1.3 Scope

The risk-informed regulatory structure to be developed in this program applies to all new plants. It is expected that the regulations that derive from this structure 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 by having the regulatory requirements specified at a high (technology-neutral) level, supplemented with reactor- technology-specific regulatory guides.

The regulatory structure will address risks from reactor full-power, low-power and shut-down operation, and spent fuel storage and handling and the risks from both internal and external events. Therefore, it includes seismic, fire and (internal and external) flood risks, and risk from high winds and tornados; also included are fuel storage and handling. Issues related to security will also be considered.

The regulatory structure will cover design, construction, and operation. Operation includes both normal operation as well as off-normal events, ranging from anticipated occurrences to rare but credible events, for which accident management as well as emergency response 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, technology-neutral regulations. In effect, the framework provides guidance on key technical issues and the scope of the technology-neutral regulations. Many of the details will only be developed as part of the regulation development.

The structure of the regulations is to be a top down, hierarchal approach that addresses reactor safety, safeguards and security. As discussed in Chapter 4, proper attention to these factors also provides protection to the environment.

The staff intends ultimately to codify the regulatory structure for new plant licensing in a new stand-alone part in 10 CFR. This new part will provide a technology-neutral alternative to the current 10 CFR Part 50. The current 10 CFR Part 50 will also interface 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 Characteristics of the Overall Regulatory Structure

As the regulatory structure is developed and implemented, it should have certain characteristics. These characteristics, essentially define the acceptance criteria of the technology-neutral framework, the technology-neutral requirements, and the technology-specific framework:

- ***Reproducible, traceable, and understandable***. The technical bases for the criteria and guidance developed as part of this approach are clearly articulated, and therefore, each step of the process is identified and clearly described.

- ***Defensible***. The technical bases developed are derived from known technology where the assumptions and approximations and their impacts are known and understood. In particular, the technical bases are consistent with the Commission's Safety Goal Policy.

- ***Flexible***. The technology-neutral and technology-specific frameworks are developed in such manner that they allow, in an efficient and effective manner, for changes and modifications to occur that are based on new information, knowledge, etc., and can be adapted to any technology-specific reactor design.

- ***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.

- ***Completeness.*** The guidance and criteria will identify the topics for a set of safety requirements are needed to meet the mission of protecting the public health and safety, considering that design, construction and operation and that address the public, worker and environment.

- ***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.

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

- ***Consistency.*** The guidance and criteria need to address and implement the policy issues approved by the Commission in its June 26, 2003 SRM. In addition, the guidance and criteria need to be compatible with other applicable parts of 10 CFR (e.g., Part 100, Part 20, etc.).

1.5 Report Organization

This report has three major parts, as shown in Figure 1-2

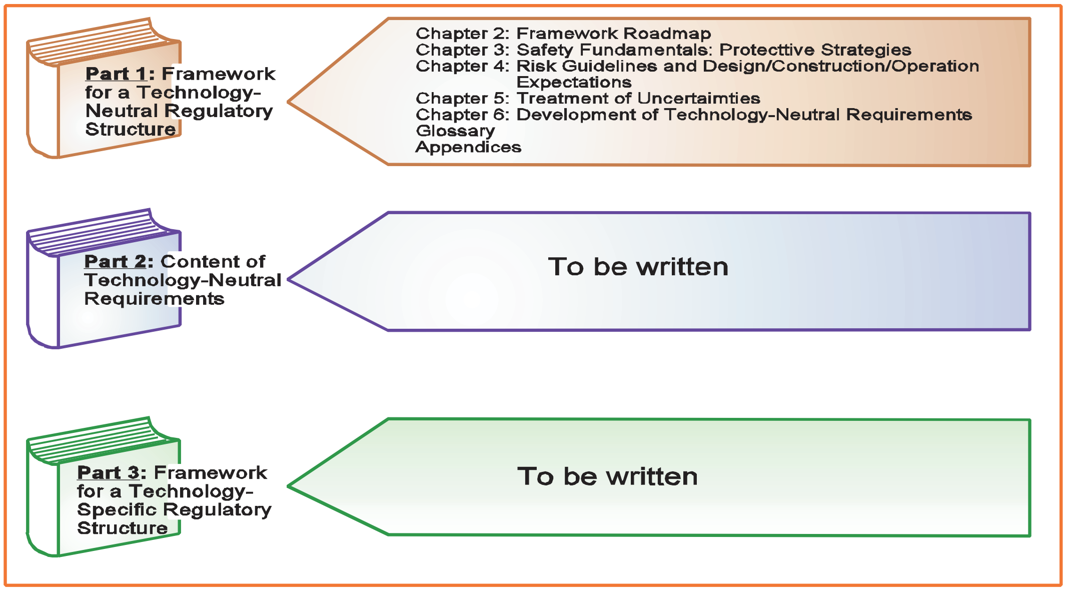

Part 1: Framework for a Technology-Neutral Regulatory Structure
Chapter 2: Framework Roadmap
Chapter 3: Safety Fundamentals: Protecttive Strategies
Chapter 4: Risk Guidelines and Design/Construction/Operation Expectations
Chapter 5: Treatment of Uncertaimties
Chapter 6: Development of Technology-Neutral Requirements
Glossary
Appendices
Part 2: Content of Technology-Neutral Requirements
To be written
Part 3: Framework for a Technology-Specific Regulatory Structure
To be written

Figure 1-2 Report Organization

Part 1 — Framework for a Technology-Neutral Regulatory Structure

This part of the report is divided into six chapters, glossary and six appendices:

- Chapter 1 provides the objectives of the program and the objectives of each part of the program, the scope, desired characteristics, and report organization.

- Chapter 2 provides the framework roadmap, in the form of an hierarchal structure, for how the technology-specific requirements are derived, starting with the Commission's mission of protecting the public health and safety. This discussion includes a description of what level of safety is envisioned for new reactors.

- Chapter 3 describes the safety fundamentals that are needed for safe nuclear power plant design, construction and operation.
- Chapter 4 provides the guidelines and criteria for risk, design, construction and operation objectives. The risk guidelines and criteria, in the form of both high level objectives and surrogates, are developed that meet the Commission's Safety Goals. Further, criteria and guidelines for design basis accidents, safety classification, are also provided.

- Chapter 5 provides a discussion on the treatment of uncertainties via defense-in-depth. This discussion also provides a "working" definition for defense-in-depth.

- Chapter 6 describes the process and identifies the content for proposed technology-neutral requirements using the guidance and criteria established for safety fundamentals, risk guidelines, design, construction and operational objectives, and treatment of uncertainties.

Appendices*, *Glossary, References

- Appendix A: provides guidance and criteria for the formulation of performance-based requirements.

- Appendix B: describes how the surrogates of core damage frequency (1E-4) and large early release frequency (1E-5) are acceptable surrogates for the QHOs for LWRs.

- Appendix C: provides a discussion on the safety characteristics unique to the Generation IV advanced reactors.

- Appendix D: provides a discussion on the PRA quality needs and what "standards" are needed beyond the current PRA standards (e.g., ASME) for new reactors.

- Appendix E: provides a discussion on the assessment of Part 50, which requirements are technology-neutral and which are LWR specific.

- Appendix F: provides a list of requirements against which to check completeness. For example, the IAEA is developing a set of technology-neutral requirements. This reference will serve as one source in checking the requirements developed in Part 2 for completeness.

- Glossary: provides terms and definitions to aid the reader in understanding the specific meaning of each term as used in the report, and to provide a consistent and common understanding to facilitate communication.

- References: provides the references for the sources used in development of the framework.

Part 2 — Proposed Technology-Neutral Requirements

To be written.

Part 3 — Framework for a Technology-Specific Regulatory Structure

To be written

Part 4 — Technology-Specific Regulatory Guides

To be written

2. TECHNOLOGY-NEUTRAL FRAMEWORK ROADMAP

2.1 Safety Overview

This chapter provides a high level discussion of the overall technology-neutral framework. It provides a brief description of the approach, how the technology-neutral requirements will be derived from the Commission Safety Goals, and summarizes the different elements of the framework.

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.

* Emphasis added.

The basis for NRC regulation of reactors originates with the Atomic Energy Act of 1954 and the statutes that amended it, which indicate that the mission of the NRC is to ensure that commercial nuclear power plants (NPPs) 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). The Atomic Energy Act satisfied the overall NRC safety mission to protect public health and safety. The amending statutes and the broad body of NRC regulations implement an underlying safety philosophy for controlling the risk to workers, offsite populations, and surrounding areas(i.e., the environment). This safety philosophy has always included the following elements:

- Preventing
- Mitigating
- Limiting
- Containing
- Responding

To summarize the safety philosophy, regulations address design, construction, and operating practices to prevent accidents, but if a sequence of events that may be to an accident begin, the regulations seek to mitigate the accident, and limit its consequences by containing any release of radioactive material and responding to control the effects of any material remaining from the release.

Two complementary approaches are

combined in the framework for a technology-neutral regulatory structure to ensure that safety is maintained: (1) protective strategies and (2) risk objectives and design/construction/operation objectives. The two approaches continue to provide risk-informed, performance-based approach to the regulation of new reactors. Additional desired characteristics of the overall regulatory structure (listed in Section 1.4) are essential to its proper implementation.

The protective strategies approach is based on a regulatory philosophy that multiple strategies are needed to ensure that gaps in our knowledge have little chance of endangering public health and safety. It is a top-down, hierarchical approach. It starts with a desired outcome, identifies protective strategies (functional requirements) to ensure this outcome is achieved even if some strategies should fail, and then provides a decision model to balance the extent of each strategy that is required to have high confidence of meeting the goal. The protective strategies provide defense-in-depth to protect against uncertainties.

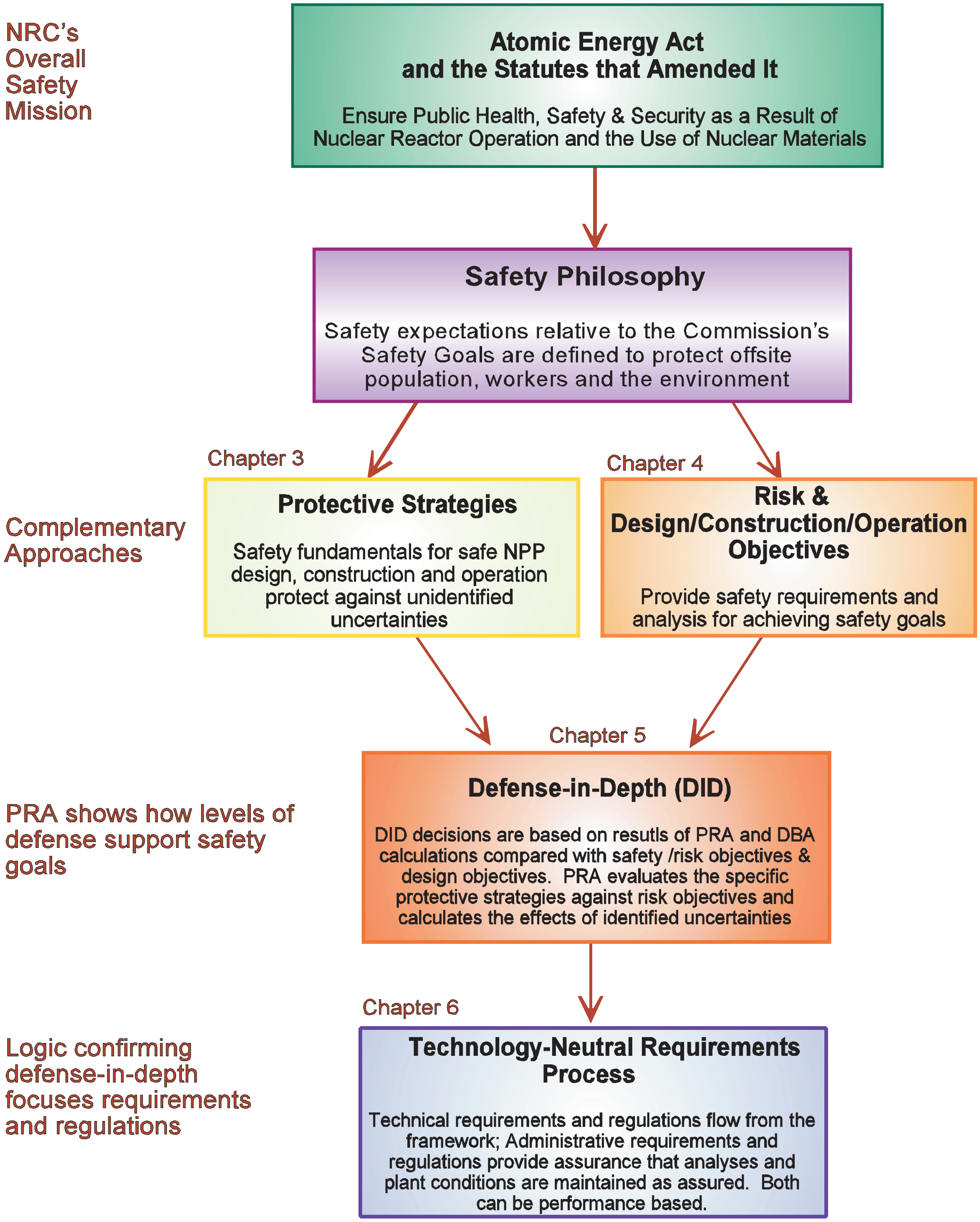
The risk objectives and design/construction/operation objectives approach sets frequency limits on the possible consequences of accidents to ensure that the NRC's safety goals are met. It also provides criteria for accident mitigation (including environmental protection), probabilistic criteria for the selection of events which must be considered in the design and which constitute "design basis accidents," and probabilistic criteria for the safety classification of systems, structures, and components.

Thus the framework uses the reactor quantitative health objectives (QHOs) set forth in the Commission's Reactor Safety Goal Policy to ensure that design, construction, and operations are consistent with the performance goals. The framework is fully a defense-in-depth philosophy to ensure that uncertainties cannot undermine the intended level of safety.

Figure 2-1 gives a high-level view of the technology-neutral framework.

The framework leads to the establishment of technology-neutral technical regulations as shown in Figure 2-2. Administrative regulations[1] are developed to ensure that the bases for the technical regulations (risk calculations, plant conditions, and other assumptions) are sound and do not become invalid.

[1] Note that administrative regulations apply to all aspects of the framework: Protective Strategies, Risk & Design Objectives, Defense-in-Depth, and Technical Regulations in all life cycle phases of design, construction and operation.



NRC's Overall Safety Mission

Atomic Energy Act and the Statutes that Amended It

Ensure Public Health, Safety & Security as a Result of Nuclear Reactor Operation and the Use of Nuclear Materials

Safety Philosophy

Safety expectations relative to the Commission's Safety Goals are defined to protect offsite population, workers and the environment

Complementary Approaches

Chapter 3

Protective Strategies

Safety fundamentals for safe NPP design, construction and operation protect against unidentified uncertainties

Chapter 4

Risk & Design/Construction/Operation Objectives

Provide safety requirements and analysis for achieving safety goals

PRA shows how levels of defense support safety goals

Chapter 5

Defense-in-Depth (DID)

DID decisions are based on resutls of PRA and DBA calculations compared with safety /risk objectives & design objectives. PRA evaluates the specific protective strategies against risk objectives and calculates the effects of identified uncertainties

Logic confirming defense-in-depth focuses requirements and regulations

Chapter 6

Technology-Neutral Requirements Process

Technical requirements and regulations flow from the framework; Administrative requirements and regulations provide assurance that analyses and plant conditions are maintained as assured. Both can be performance based.

Figure 2-1 Technology-Neutral Regulatory Structure Framework.

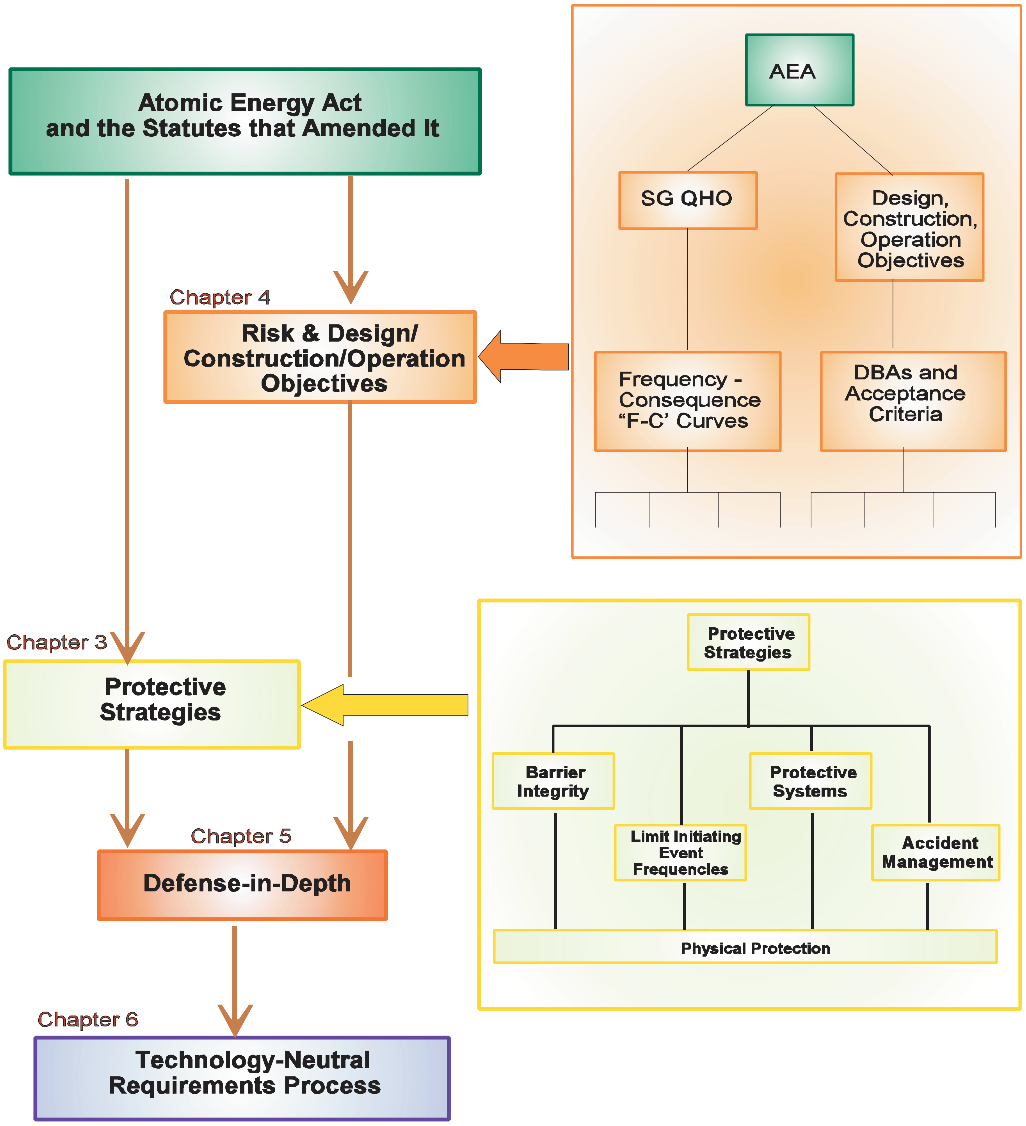


Figure 2-2 Expanded Framework

The "protective strategies and risk & design construction, and operation objectives" are expanded in Figure 2.2. Protective strategies are the safety fundamentals for safe nuclear power plant design, construction, and operation. They are the fundamental building blocks for the developing technology-neutral requirements and regulations. Acceptable performance in these protective strategies provides reasonable assurance that the overall mission of adequate protection of public health and safety is met, as described in Chapter 5. Moreover, the protective strategies go further, implicitly requiring a defense-in-depth approach that will ensure uncertainties in performance do not compromise achieving overall plant safety objectives.[2] "Risk & Design, Construction, and Operation Objectives" develop overall plant risk and deterministic criteria, including criteria for

[2] An important theme Defense-In-Depth is a mean to protect against uncertainties. This is especially important in new technologies where the full range of operating conditions has not been experienced.

selecting DBAs and SSC classification as described in Chapter 4.

2.2 Safety Philosophy

The NRC's safety goals are based on the idea of minimizing additional risk burden to the population for the benefits of nuclear power. These underlying ideas are as appropriate for new reactors (or any new technology) as they are for existing LWRs.

As the Commission notes in the Policy Statement on Regulation of Advanced Nuclear Power Plants:

(1) Advanced reactors will make larger safety margins.

(2) Advanced reactor designs will comply with the Commission's Safety Goal Policy Statement.

The *conceptual sketch* in Figure 2-3 shows the interrelationships of the safety goals in plant licensing. To address the Commission's expectations, a three-region approach to risk acceptance is defined and developed..

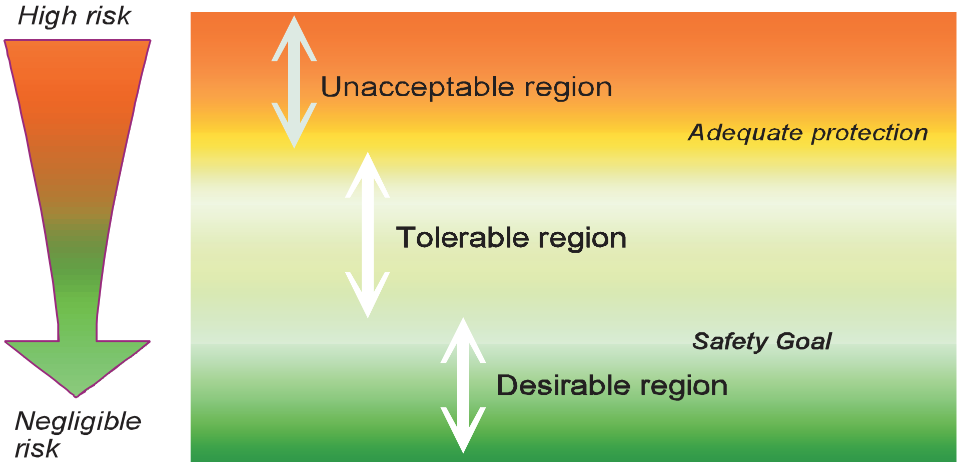


Figure 2-3 Three Region Approach to Risk Tolerability/Acceptance

A three-region approach has been discussed and employed in a number of forums [Ref. 1-3], [Ref. 1-4]. In considering this figure, understand that there is substantial uncertainty (see the following section and Chapter 5 for a discussion of uncertainty) in a plant's risk performance. The lower region represents the value of the risk metric that corresponds to the desired ultimate safety goal and/or objective.; that is, it defines what is "safe enough", i.e., one in which no further regulatory attention is needed.[3]

Some currently operating reactors may fall in the middle region of tolerable risk, a region where regulatory cost-benefit or similar analyses can be carried out for proposed safety enhancements to reduce risks, and risk is reduced as far as reasonably practical. Currently operating reactors have only a small chance of reaching the upper, unacceptable region.

The goal of this framework is to develop requirements for future reactors consistent with the lower, desired region where there is only a small chance that the risk will reach the tolerable region and essentially zero chance that it will reache the upper, unacceptable region.

Accordingly, ***the technology-neutral regulatory requirements for future reactors are expected to keep the risk down in the desirable region. Thus the regulations will be written to achieve the safety goal level of safety.*** This achievement will provide margin for adequate protection to account for uncertainties associated with new designs and technologies as well as help implement the Commission's expectations for safety as expressed in the Advanced Reactor Policy Statement.

In addition, if new plants that meet this level of safety are added to sites with an existing reactor(s) will be little incremental risk to the site. Finally, such an approach is consistent with industry initiatives which are directed at developing designs with enhanced safety over currently operating plants.

It is understood that the consequences from events that may occur one or more times during the lifetime of the plant are no greater than that allowed for normal plant operation under current regulations (i.e., 10 CFR Part 20).

2.3 Protective Strategies

There are five protective strategies: physical protection, barrier integrity, limit initiating event frequencies, protective systems, and accident Management. The five protective strategies introduced here set the design, construction, and operating conditions that will ensure protection of public health and safety, workers, and the environment.

- The **physical protection** objective is to ensure that adequate 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 **barrier integrity**[4] objective is to ensure that there are adequate barriers to protect the

[3] Note that Figure 2-3 is conceptual in nature. The detailed considerations that would be necessary to implement this idea on a quantitative basis are discussed in Chapter 4.

[4] Note that the purpose of barriers, protective systems and accident management 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

public from accidental radionuclide releases. 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 occur. Barriers include only physical barriers but physico-chemical materials that can inhibit the transport of radiation if physical barriers are breeched.

- The **limit initiating event frequency** 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 must be considered that can affect any source of radioactive material on site in any chemical and physical form.

- The **protective system** objective is to ensure that the systems that mitigate[5] initiating events are adequately designed, and perform adequately, with respect to reliability and capability, to satisfy the design assumptions regarding accident prevention and mitigation during all states of reactor operation. The protective systems include human actions to assist the systems protect the barriers.

- The **accident management** objective is to ensure that the public health and safety can be adequately protected. Accident management measures can include emergency evacuation plans, drills, and training.

How these protective strategies are implemented is discussed in Chapter 3. Note that the physical protection protective strategy is somewhat unique. Security considerations affect all aspects of design (including the other strategies), construction, and operation. Changes to any other protective strategy must consider the impact on physical protection. This is not to say that there are no interactions with the other protective strategies. A top-down analysis of each protective strategy confirms the validity of the set of strategies and leads directly to a categorization of the kinds of regulations needed to ensure that the protective strategies are carried out. It is important to identify the failures and human actions that can defeat the barriers and their protective systems.

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

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

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

[5] 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 lead to an accident involving protective systems failures.

studies help in the evaluation of the necessary defense-in-depth in a risk-informed structure.

2.4 Risk Objectives and Design, Construction, and Operational Objectives

Returning to the framework of Figure 2-1, the risk objectives and the design, construction, and operational objectives complement the protective strategies. The risk and design objectives lay out a parallel safety approach for meeting safety and risk goals for all facilities. This approach keeps worker risk and land contamination to acceptable levels, and sets specific design expectations that amount to defense-in-depth requirements at the design level. The safety and risk objectives are derived from the quantitative health objectives (QHOs) of the NRC's safety goals. Chapter 4 explains how risk goals and design expectations are to be used to ensure that the safety goal QHOs are met.

In SECY-03-0047 the staff proposed and in a June 26, 2003 SRM the Commission endorsed a process for future non-LWR plant licensing similar process used in the certification of the two evolutionary and one advanced LWRs (i.e., ABWR, System 80+, and AP-600). The evolutionary and ALWR design certification process used CDF and CCFP to measure overall plant risk and compared them to the CDF and CCFP surrogates described above. In addition, uncertainties related to evolutionary and ALWR plant performance, particularly with respect to the prevention or mitigation of severe accidents, were addressed on a case-by-case basis with any additional proposed requirements being subject to Commission review and approval. The development of this framework and a risk-informed licensing approach is based upon implementing the process employed in the ALWR reviews in a more structured fashion. This would include better defining the level of safety desired in new plant designs and the process to be used to address uncertainties (i.e., defense-in-depth). The level of safety desired is that associated with the Commission's Reactor Safety Goals and has been used as the basis for the risk objectives. This approach is considered consistent with the Commission's expectation (as expressed in the Advanced Reactor Policy Statement) that advanced reactor designs are "expected to comply with the Commission's Safety Goal Policy Statement" and "provide enhanced margins of safety." By having the framework identify the criteria consistent with this expectation, the need for case-by-case determinations is reduced. However, the process still allows for case-by-case determinations on additional features, subject to Commissions review and approval, if such a need arises.

From the conceptual structure of Figure 2-3, frequency-consequence curves are developed in Chapter 4 that are consistent with the overall safety goal objective and are applicable to all reactor concepts. The approach combines probabilistic risk criteria and "design-basis" criteria. The risk criteria include accident prevention and accident mitigation criteria. Probabilistic criteria are used for the selection of design basis accidents and safety classification of systems, structures and components. Design basis criteria set fixed acceptance criteria for events that are used for comparison to siting requirements.

Returning to the framework of Figure 2-1, following development of the two complementary approaches, defense-in-depth decisions based on the PRA and judgment lead to the development of specific regulations. In particular, the PRA provides a means for risk-informing the selection of any specific implementation of the protective strategies. The PRA identifies the most important elements in protective strategy. PRA calculates the risk and compares it with the frequency-consequence limit curves.

Reactor (and other facility) safety is achieved by considering the combination of initiating events, performance of barriers, performance of protective systems and accident management with respect to an appropriate set of reactor-specific safety functions, human actions, and integrated system response.[6]

2.5 Defense-in-Depth: Treatment of Uncertainty

Future reactor designs may use passive systems and inherent physical characteristics (confirmed by sensitive nonlinear dynamical calculations) to ensure safety, rather than relying on the 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 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, 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. A facility can operate outside its design assumptions in other scenarios:

- The operators and maintenance personnel place the facility in unexpected conditions.

- Gradual degradation has led to unobserved corrosion or fatigue or some other physical condition not considered in the design.

- Passive system behavior (e.g., physical, chemical, and material properties) is incorrectly modeled.

Much of the work of PRA for future reactors will be to identify and evaluate initially unexpected scenarios.[7] 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, as discussed in Chapter 5.

In general, uncertainties associated with new plants will tend to be larger than uncertainties associated with existing plants due to new technologies being used, the lack of operating experience or, in the case of some proposed LWRs, new design features (e.g., increased use of passive systems). Any licensing approach for new plants must account for the treatment of these uncertainties. The aim is to develop an approach for future reactors which can be reconciled with 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.

A range of uncertainties in future reactor performance should be considered including:

- 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

[6] Note that the radiation health risk of routine operations can represent a simple scenario with unit probability in the PRA structure.

[7] Weick has pointed out that the real key to safe operations in any activity is a focus on managing the "unexpected." [ref] Note that searching for the unexpected is exactly what PRA originally did. With repeated application to current plants, the original creativity of PRA has given way to its routine application.

data for the situation being modeled

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

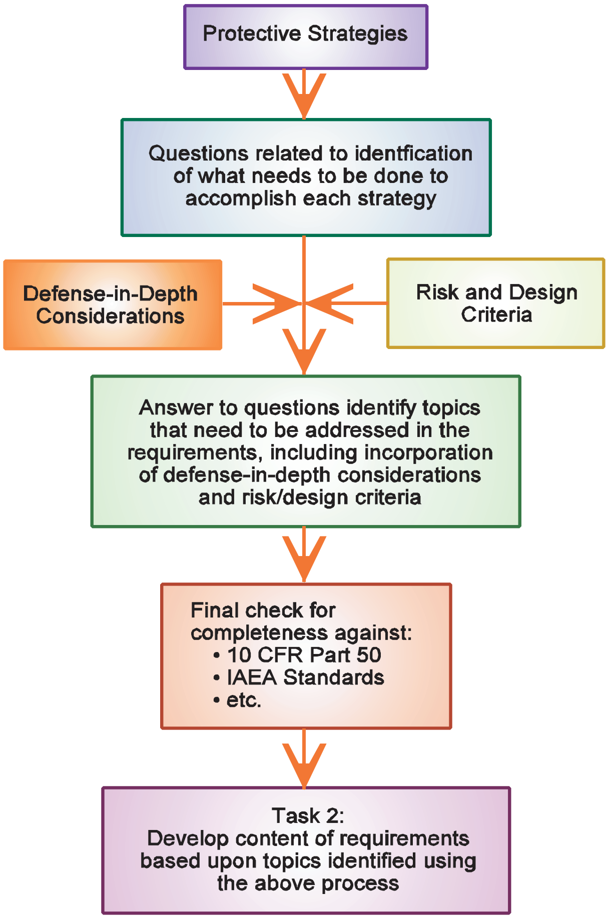
All identified and quantified uncertainties (aleatory and epistemic) can be included in PRA that supports development of regulation (evaluation of design, construction and operation risks; comparison with risk objectives; evaluation of the effectiveness of Protective Strategies). The PRA directly uses the results of parameter estimation in the data uncertainty distributions 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. Finally, it will be important to qualitatively describe and catalog all aspects of uncertainty, even those difficult to quantify, for consideration in balancing structuralist and rationalist aspects of regulation.

2.6 Process for Development of Technology-Neutral Requirements

The risk information and safety goals should be linked to the protective strategies to develop technology-neutral requirements for new reactor concepts. This is carried out in Chapter 6. These regulations, being technology-neutral, should be compatible with acceptable safety performance for existing LWRs. Technical (intrinsic) regulations and administrative (extrinsic) regulations, organized by design, construction, and operation, will be developed in order to anticipate and neutralize potential challenges that could prevent the risk objective from being achieved. Of course, the concern during design and construction is to control those aspects of each that could have positive or negative impacts on the risk during operations. Traditionally, NRC regulations and practices have ensured public health and safety is not compromised by commercial nuclear power plant operation by requiring the use of good design, construction and operational practices.

NRC's role has been to specify requirements associated with each of these three elements of "good practice," and through review, approval, and oversight, to monitor and judge a licensee's compliance with these requirements. Regulations for new plant licensing would also embody these good practices. In addition, they would enjoy the simplifying advantage of having the process structured to use risk insights throughout the process. The emphasis given to each aspect will be developed according to how they address the threats that challenge one or more of the protective strategies and how they ensure meeting the safety/risk objectives and design/construction/operation expectations.

Chapters 3, 4, and 5 feed naturally into the identification of technology-neutral technical and administrative requirements in Chapter 6. The protective strategies of Chapter 3 establish the systems and functions to be protected by the requirements. The most important functionality during design, construction and operation can be established at this level. Chapter 4 identifies the objectives that must be met. Chapter 5 identifies the uncertainty issues that must be recognized and addressed, as well as the tools that can be used to ensure that uncertainty in performance and operating conditions are addressed in a way to promote proper balance between protective strategies and risk, between technical requirements and administrative requirements. Together these lead to a set of questions to ask about the design to ensure all goals are met. Chapter 6 then seeks performance-based measures to satisfactorily answer all the questions.


Protective Strategies
Questions related to identfication of what needs to be done to accomplish each strategy
Defense-in-Depth Considerations
Risk and Design Criteria
Answer to questions identify topics that need to be addressed in the requirements, including incorporation of defense-in-depth considerations and risk/design criteria
Final check for completeness against:
• 10 CFR Part 50
• IAEA Standards
• etc.
Task 2:
Develop content of requirements based upon topics identified using the above process

The process for developing technical and administrative requirements from the protective strategies is outlined in Figure 2-4 and explained fully in Chapter 6. It begins with the protective strategies themselves, described in Chapter 3. Then a deductive analysis of the logic of events that can defeat each protective strategy is performed as discussed in Chapter 3 and elaborated in Chapter 6. These logic trees lead directly to the questions staff must ask to ensure each protective strategy is accomplished. The answers to these questions must be balanced among the strategies based on information from the risk and design criteria and considerations of defense in depth. 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. (Note that some of these LWR requirements may not be applicable to the new reactor design and that these LWR standards cannot be assumed complete for new reactors.) Finally, the answers to the questions are formulated as performance-based requirements.

Figure 2-4 Process for Identifying Topics to Be Included in the Requirements.

3. SAFETY FUNDAMENTALS: PROTECTIVE STRATEGIES

3.1 Introduction

This chapter describes how the safety/risk objectives, (generalized in Chapter 4 from the QHOs described in the Commission's Reactor Safety Goal Policy) are complementary with the protective strategies discussed in Chapter 2 (Figure 3-1). The five protective strategies (Physical Protection, Barrier Integrity, Limit Initiating Event Frequency, Protective Systems, and Accident Management) introduced in Chapter 2 establish the high level structure that, if followed, can systematically result in requirements for safe nuclear power plant design, construction, and operation. This chapter explains why the set is sufficient and how regulations can flow from the process.

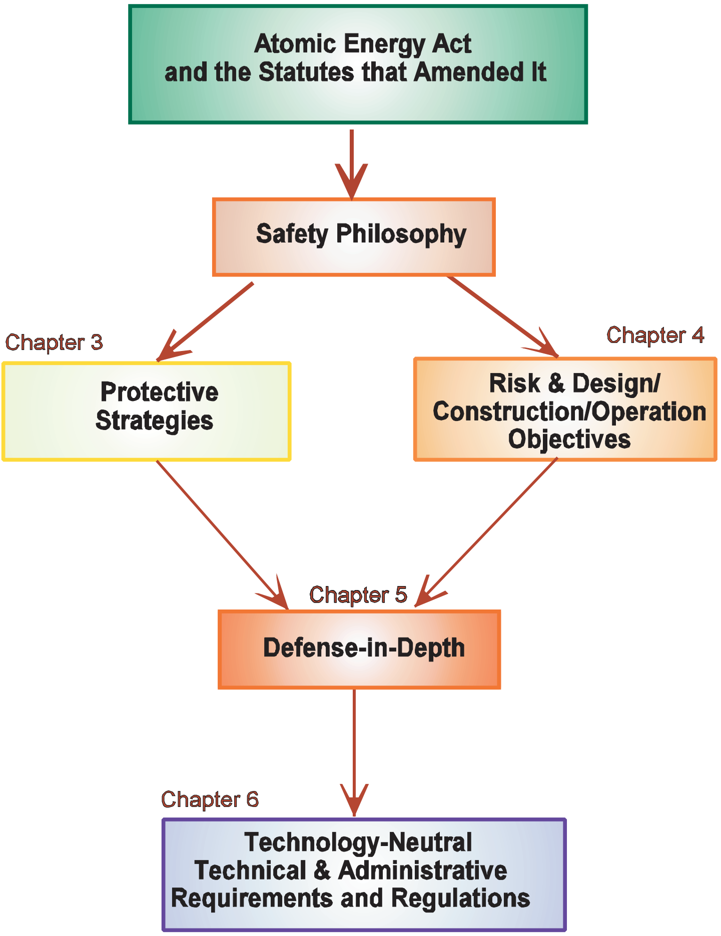

Atomic Energy Act
and the Statutes that Amended It
Safety Philosophy
Chapter 3
Protective Strategies
Chapter 4
Risk & Design/ Construction/Operation Objectives
Chapter 5
Defense-in-Depth
Chapter 6
Technology-Neutral Technical & Administrative Requirements and Regulations

Figure 3-1 Summary View: Framework for Technology-Neutral Regulation

These five protective strategies form an adequate set for two reasons–they meet a set of minimal needs from an engineering perspective and they map to all elements modeled in a nuclear power plant PRA (i.e., if they succeed, no PRA accident sequence can lead to a release of radionuclides dangerous to the population surrounding the site). As described in Chapter 2, the protective strategies were selected based on engineering judgment, as a minimal set to provide a layer of protection with respect to all key safety functions. The relevance of this set is supported by its similarity to the seven[8] "cornerstones" of the Reactor Oversight Process [Ref. 1-5], a process that has the benefit of several years of operational experience. However, the viewpoint taken in this framework is that of design and construction, as well as operation.

[8] Note that the ROP safety cornerstones – Initiating Events, Mitigating Systems, Integrity of Barriers to Release of Radioactivity, Emergency Preparedness, Occupational Radiation Safety, Public Radiation Safety, and Physical Protection – were developed to address operational risk, while the focus of the current document is on licensing a design to provide protection during operations from causes that arise during design, construction, or operation. The ROP performance indicators were selected to support an inspection process; the framework for technology-neutral regulation lays out a process to develop technical and administrative requirements and associated performance indicators to support licensing. The protective strategies ensure that defense in depth will provide protection, even if state of knowledge uncertainties mean that the plant may respond in unexpected ways. Note also, that the two radiation safety cornerstones do not translate to protective strategies. As explained in conjunction with Figure 3-2, they affect doses that can occur in case of an accident and factor into the PRA consequences calculations.

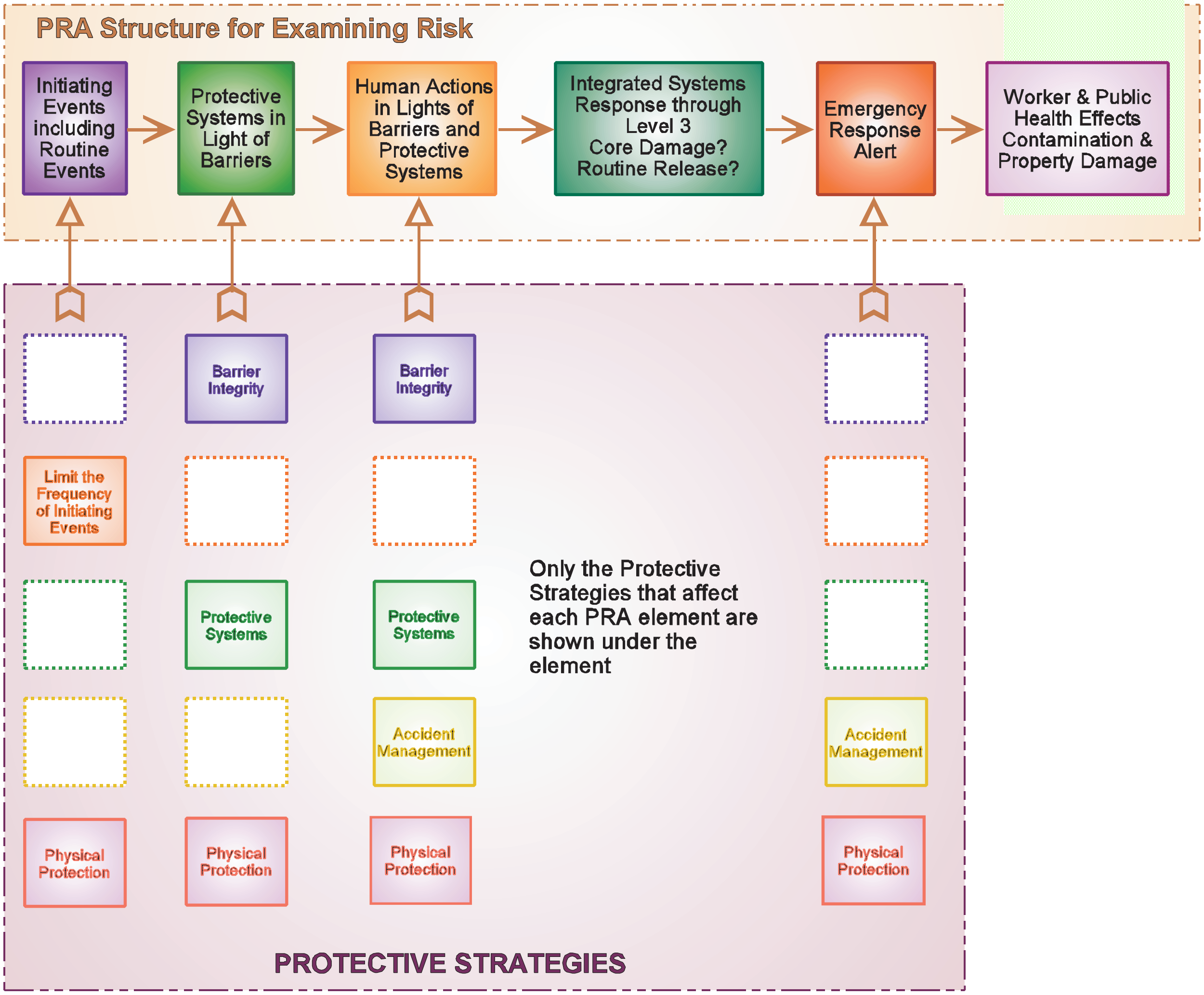

PRA Structure for Examining Risk
Initiating Events including Routine Events
Protective Systems in Light of Barriers
Human Actions in Lights of Barriers and Protective Systems
Integrated Systems Response through Level 3 Core Damage? Routine Release?
Emergency Response Alert
Worker & Public Health Effects Contamination & Property Damage
Barrier Integrity
Barrier Integrity
Limit the Frequency of Initiating Events
Protective Systems
Protective Systems
Only the Protective Strategies that affect each PRA element are shown under the element
Accident Management
Accident Management
Physical Protection
Physical Protection
Physical Protection
Physical Protection
PROTECTIVE STRATEGIES

Figure 3-2 The Relationship between the Protective strategies and Elements of the PRA

The second case for these protective strategies is based on the alignment of the protective strategies with the analysis elements of PRA, as outlined in Figure 3-2. The first element of PRA is the identification and modeling of the possible initiating events. The response of plant systems that can terminate the event sequence before barrier damage occurs is then modeled. Success criteria are based on the functional performance required to limit damage or control radionuclide release. Human actions that can control or exacerbate protective systems and barrier performance are modeled next. Finally, given the calculated performance of protective systems, the physical response of the plant is calculated. For event sequences leading to radionuclide release, doses to surrounding populations (in light of accident management and protective measures) and land contamination are calculated.[9] The five protective strategies directly affect the PRA's initiating events, human performance, protective systems, barrier performance, and physical protection, as shown in Figure 3-2. Because these are the driving factors in determining the risk, the five protective strategies form a complementary and diverse (defense-in-depth) set of defenses for controlling the risk.

For every source of radioactive hazard on site, all initiating event are considered in the PRA. Thus the PRA examines the ways in which multiple barriers[10] can be breeched; it models:

- initiating events
- successes and failures in the protection systems that are designed to protect barriers
- human actions that can offset or defeat the protective systems or barriers themselves
- the physical response of the integrated plant to event sequences, including radiological dispersion pathways
- the emergency response system developed to protect the public and workers in case barriers fail
- dose response (calculating the probable 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 evolving design and implementation, which are 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 6. Furthermore, this layer of defense-in-depth provides a measure of

Are There Better Protective Strategies?

A number of additional/alternative protective strategies have been suggested in discussions with staff, licenses, vendors and other interested parties; these have included "inherent design features," radiation protection, and others. Because the protective strategies are intended as structuralist *requirements*, they must be limited to those functional issues that provide and protect barriers to release.

In evaluating the effectiveness and reliability of the protective strategies, designers and regulators must consider all factors affecting each strategy. Inherent design features are part of every design; they may directly provide some of the protective strategy functions and, when they do, this should be included in the risk analysis. Likewise, radiation protection

[9] Note that the status of protective systems and radiation protection systems enters into this calculation of consequences.

[10] Barriers include physical barriers and the physical-chemical form of the material, if that can inhibit radioactive material transport should physical barriers be breeched.

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 is established by examining the necessary elements of each strategy. The protective strategies are discussed below.

3.2 Protective Strategies

3.2.1 Physical Protection

The physical protection strategy ensures that adequate measures are in place to protect workers and the public against intentional acts (e.g., sabotage, theft) that could compromise the safety of the plant or lead to radiological release. Physical protection is provided by design and by extrinsic measures (“guns, guards, and gates”) to provide defense-in-depth against attack. This requires that design makes it unlikely that outsiders (or, even single insiders) can reach sufficient sensitive areas of the plant to accomplish their goals. Further, the extrinsic features provide delay and opposing force. Adequate physical protection requires a integrated view of the plant and the opposing forces.

3.2.2 Barrier Integrity

Functional barriers to radionuclide release must be 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-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 will be used to demonstrate that the frequency of radionuclide release is within the desirable range, with adequate consideration of uncertainty. Uncertainties associated with barrier degradation, e.g., corrosion, erosion, aging, and other materials issues, will need to be considered. For some systems, chemical interactions will be important.

Additional barriers, beside those identified from the risk analysis, may be needed to address credible scenarios not amenable to risk analysis and covered by design basis accidents (DBAs), (Chapter 4). They may be needed to provide assurance against uncertainties in modeling completeness as well.

3.2.3 Limit the Frequency of Initiating Events

To ensure adequate limitation of accident initiators, a thorough examination of potential initiating events should be conducted as part of the risk analysis of the design. The initiators should be identified, along with their mean frequency of occurrence. Uncertainty in their frequency should also be considered and quantified as a probability of frequency distribution. Initiators should 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 should be considered.

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

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

For the future reactor technologies, initiating event consideration may be substantially different from those for current US LWRs. Examples are events associated with on-line refueling, recriticality due to more highly enriched fuels and fuels with higher burnup, and chemical interactions with some reactor coolants or structures. In particular, initiators that can confuse operators and lead them to take actions that could defeat important safety features in advanced plants, e.g., passive cooling and events that cause conditions outside the designers' expectations, could be important.

3.2.4 Protective Systems

Plant features should be provided to mitigate the consequences of initiating events by protecting the barriers identified in the first 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 must be carried out for the future designs. These PRAs are expected not only to determine the needed features, but also their required reliability and capability. The PRAs will be used to demonstrate that the safety/risk objectives are within the desirable range, with adequate consideration of uncertainty.

For some scenarios which appear credible but have very broad uncertainty (due to insufficient data, not well understood phenomena, etc.), additional protective features may need to be incorporated. If DBAs are needed to address such scenarios, as described in Chapter 4, then the protective features necessary to cope with the DBAs need to be identified and incorporated.

For the future reactor technologies, some mitigative considerations will be substantially different from those for current US LWRs. Examples are performance and monitoring of passive safety systems (including passive decay heat removal), the performance and testing as well as the PRA modeling of digital systems, qualification and testing of new materials including fuel, non-traditional emergency core heat removal systems, limited operator intervention, and, for LMRs, potential energetic interactions of the working fluid when exposed to the environment.

3.2.5 Accident Management

Accident management includes management of all accident scenarios, whether release has occurred or not. Therefore, plant abnormal and emergency procedures are part of accident management, as well as severe accident management guidelines and on-site and off-site emergency plans. If functional barriers fail to adequately limit the radionuclide release, accident management must be provided to control the accident progression and ultimately to limit the public health effects of accidents. The plant PRA will help 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.

3.3 Analysis to Identify Requirements

The five protective strategies are analyzed deductively in Chapter 6. The approach is to develop a fault 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 often begins by partitioning the functional failure into two or more classes of failure. It usually proceeds by identifying specific causes of failure.

Next, these failures causes are examined for their relevance during design, construction, and operations. Questions are developed for regulators that, when answered, will identify the topics that must 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 should be used wherever practical. The use of such an approach is consistent with Commission direction as expressed in a 1999 White Paper on risk-informed and performance based regulation. In that white paper a performance-based approach was defined as one that establishes performance and results as the primary basis for regulatory decision-making, and incorporates the following attributes: (1) measurable (or calculable) parameters (i.e., direct measurement of the physical parameter of interest or of related parameters that can be used to calculate the parameter of interest) exist to monitor system, including facility and licensee, performance, (2) objective criteria to assess performance are established based on risk insights, deterministic analyses and/or performance history, (3) licensees have flexibility to determine how to meet the established performance criteria in ways that will encourage and reward improved outcomes; and (4) a framework exists in which the failure to meet a performance criterion, while undesirable, will not in and of itself constitute or result in an immediate safety concern.

Further, the White Paper also defines a risk-informed and performance-based approach as one in which 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.

The features included in the integrated risk-informed and performance-based approach as compared with just the performance-based approach are noteworthy. Taken together, the Commission's views a performance-based approach as bringing about a focus on results as the primary basis for regulatory decision making, whether PRA information is available or not.

The performance-based approach is characterized and recognized by the occurrence of the following four attributes and sub-attributes:

- A framework exists or can be developed to show that performance by identified elements will serve to accomplish desired goals and objectives. Margins of performance exist such that if performance criteria are not met, an immediate safety concern will not result.
    - An adequate safety margin exists.
    - Time is available for taking corrective action to avoid safety concerns.
    - The licensee is capable of detecting and correcting performance degradation.
- Measurable, calculable, or constructable parameters to monitor acceptable plant and licensee performance exist or can be developed.

  - Directly measured parameters related to the safety objective are preferred and will typically satisfy this guideline.

  - Calculated or constructed parameters may also be acceptable if there is a clear relationship to the safety objective.

  - Parameters that licensees can readily access, or are currently accessing, in real time are preferred and will typically satisfy this guideline. Parameters monitored periodically to address postulated, design basis, or other conditions of regulatory significance may also be acceptable.

  - Acceptable parameters will be consistent with defense-in-depth and uncertainty considerations.

- Objective criteria to assess performance exist or can be developed.

  - Objective criteria consistent with the desired outcome are established based on risk insights, deterministic analyses, and/or performance history.

- Licensee flexibility in meeting the established performance criteria exists or can be developed.

  - Programs and processes used to achieve the established performance criteria will be at the licensee's discretion.

  - A consideration in incorporating flexibility to meet established performance criteria will be to encourage and reward improved outcomes, provided inappropriate incentives can be avoided.

Appendix A provides additional guidance on the application of these attributes in developing performance-based requirements.

4. RISK AND DESIGN, CONSTRUCTION, AND OPERATIONAL OBJECTIVES

4.1 Introduction

This chapter provides guidance and criteria for developing the overall risk objectives for new plants, and establishes the safety objectives for their design, construction and operation. The overall risk objectives, in terms of both high level objectives and surrogates, are developed for the public and the worker, but also address the environment. The focus of Chapter 4 is on those objectives, criteria and elements necessary for a risk-informed licensing approach.

Design objectives are provided which involve both probabilistic and deterministic criteria. Probabilistic criteria are developed to categorize events to be considered in the design. Deterministic acceptance criteria are established for events expected to occur one or more times in the life of the plant and for probabilistically selected "design basis accidents" that must be considered for siting purposes. A risk-informed approach to determine the safety classification of structures, systems, and components is also discussed.

Construction objectives issues regarding modular fabrication in factories, fabrication outside the U.S. and issues of fuel quality are discussed.

Operational objectives for staffing, accident management, protection of operating staff during accidents, and offsite emergency preparedness, all of which may differ for new plants, are provided.

Uncertainties are addressed in Chapter 5.

4.2 Risk Objectives

4.2.1 High Level Risk Objectives

This section discusses the risk objectives for the public, the workers, and the environment. The public risk objective is defined by the Safety Goal Policy Statement of the U.S. NRC in terms of the two quantitative health objectives (QHOs):

- "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 percent) of the sum of prompt fatality risks resulting from other accidents to which members of the U.S. population are generally exposed". The Commission defined "vicinity" in this case as the area within one mile of the plant site boundary, and the average individual risk is determined by the mean of the frequency-weighted early fatality distribution summed over all accidents and divided by the total population within 1 mile.

- "The risk to the population in the area near a nuclear power plant of cancer fatalities that might result from nuclear power plant operation should not exceed one-tenth of one percent (0.1 percent) of the sum of cancer fatality risks resulting from all other causes." The Commission defined the "area near a nuclear power plant" for this objective to be the area within 10 miles of the site boundary and the risk to the population was again stated in terms of average individual risk of latent cancer determined by the mean of the frequency-weighted latent cancer fatality distribution summed over all accidents and divided by the total population within 10 miles.

Based on the rates of accidental death and cancer fatality in the U.S., the prompt (or early) fatality QHO has a value of # 5E-7 per year and the latent cancer fatality QHO has a value of # 2E-6 per year.

On an individual plant basis, a site-specific Level 3 PRA (which incorporates a probabilistic treatment of site weather along with other factors such as population) has to be performed to evaluate whether the plants meets the QHOs defined above. For operating plants, surrogate (or subsidiary) risk objectives have been defined in terms of large early release frequency (LERF) and core damage frequency (CDF). The risk objectives are consistent with the level of risk (or safety) implied by the prompt fatality and latent cancer fatality QHOs ,respectively. Surrogate risk objectives for new plants are discussed below in Section 4.3.

An approximate visualization of the level of safety needed for advanced plants on a technology-neutral basis can be provided by a frequency-consequence curve (shown in Figure 4-1 and described in Section 4.2.1.1 below) that is based upon ensuring the overall risk to the public from plant operation is no greater than that defined by the Commission's Reactor Safety Goal Policy Statement. This curve spans a range of frequencies from events that may occur during the life of a plant to rare events (less than 1E-6 per year). It is understood that the consequences from events which may occur one or more times during the life of the plant are no greater than that allowed for normal plant operation under current regulations (i.e., 10 CFR Part 20).

The worker risk objective is based on current regulations (10 CFR Parts 50 and 20) and the environmental risk objective is also developed from the current regulation in 10 CFR Part 140. Surrogate risk objectives are developed in a manner similar to the way the subsidiary risk objectives (core damage frequency and large early release frequency) for operating reactors are derived from the quantitative health objectives of the reactor safety goal policy Statement.

4.2.1.1 Public Risk Objectives

Radiation protection of the public from normal operation of nuclear facilities, including power reactors, is provided by the dose limits in 10 CFR Part 20. Under normal operation of a licensed nuclear facility, the total effective dose equivalent to individual members of the public is limited to 100 mrem per year above background. This limit is supplemented by the requirement that the doses be "as low as reasonably achievable" (ALARA). This limit is consistent with the recommendations of the International Commission on Radiation Protection (in ICRP-60) that effective dose for the public should be limited to 1 mSv per year (100 mrem per year) averaged over any 5 consecutive years. The National Commission on Radiological Protection (NCRP-116) also recommended that the public dose limit should be 100 mrem per year; in addition, NCRP recommended a limit of 5 mSv per year (500 mrem per year) for "infrequent" exposures. Part 20 allows a licensed facility to operate for specified periods of time with a public dose limit of 500 mrem per year provided justification is given and authorization is received.

Dose limits to the public apply to routine exposure during normal operation of licensed facilities, i.e., doses received with essentially unit probability. Doses due to accidents (called "potential exposures" by the IRCP) were addressed qualitatively in ICRP- 60 as follows: "Dose limits do not apply directly to potential exposures. Ideally, they should be supplemented by risk limits, which take account of both the probability of incurring a dose and the detriment associated with that dose if it were received."

ICRP-64 developed a conceptual approach for limiting the risks of doses from accidents, i.e., potential exposures. This approach can be summarized as a range of recommended annual probabilities of accident sequences (from which constraints may be selected) leading to different severities of radiation exposure. The ICRP recommendations for limits on frequency of accidental doses are as follows:

Dose ranges	Frequency ranges
• Doses treated as part of normal exposures	1E-1 to 1E-2 per year
• Stochastic effects only but above dose limits:	1E-2 to 1E-5 per year
• Doses where some radiation effects are deterministic:	1E-5 to 1E-6 per year
• Doses where death is the likely result:	< 1E-6 per year

The recommendations of ICRP 64 are consistent with the generally accepted principle that the larger the potential consequence of an accident the smaller its frequency of occurrence. The following considerations are relevant to translating the ICRP recommended dose categories into numerical estimates that apply to an individual member of the public (assumed to be located at or in the immediate vicinity of the exclusion area boundary).

Doses in the range of 1 mrem to 100 mrem fall in the first category of doses that can be treated as normal exposures (i.e., within dose limits). The second category, doses that are above limits but only involve stochastic effects, ranges from 100 mrem to about 20-25 rem. (NCRP 64 [Ref. 1-6], for example, change the latent cancer fatality risk coefficient from 5E-4 per rem to 1E-3 per rem for doses above 20 rem). Doses above 50 rem fall in the third category where some radiation effects are deterministic (ICRP 41 [2] 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). Doses where death, i.e., early fatality, is the likely result 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 [3] and 2-3 Sv [4] for a population receiving good medical care. In the NRC-sponsored MACCS probabilistic consequence analysis code, 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 [5] based on the early health effects models developed in NUREG/CR-4214 [4].

Based on the above considerations, a table of values of accident frequency versus dose is proposed as shown in Table 4-1.

Table 4-1 Proposed dose/frequency ranges for public accidental exposures

Dose Range	Frequency (per year)	Comment
1 mrem - 100 mrem	1E-2	Doses treated as normal exposures
100 mrem - 1 rem (1)	1E-3	1 rem off site triggers EPA PAGs
1 rem - 25 rem (1)	1E-4	25 rem triggers AO reporting

Table 4-1 Proposed dose/frequency ranges for public accidental exposures

Dose Range	Frequency (per year)	Comment
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	5E-7	Above 300 - 400 rem, early fatality is quite likely

(1) Doses that are stochastic and in the range of 100 mrem to 25 rem are subdivided into two ranges: those below the EPA protective action guideline of 1 rem off site are assigned a frequency of 1E-3/year. Doses in the next higher 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) which defines substantial radiation levels to imply a whole body dose of 25 rem to one or more persons.

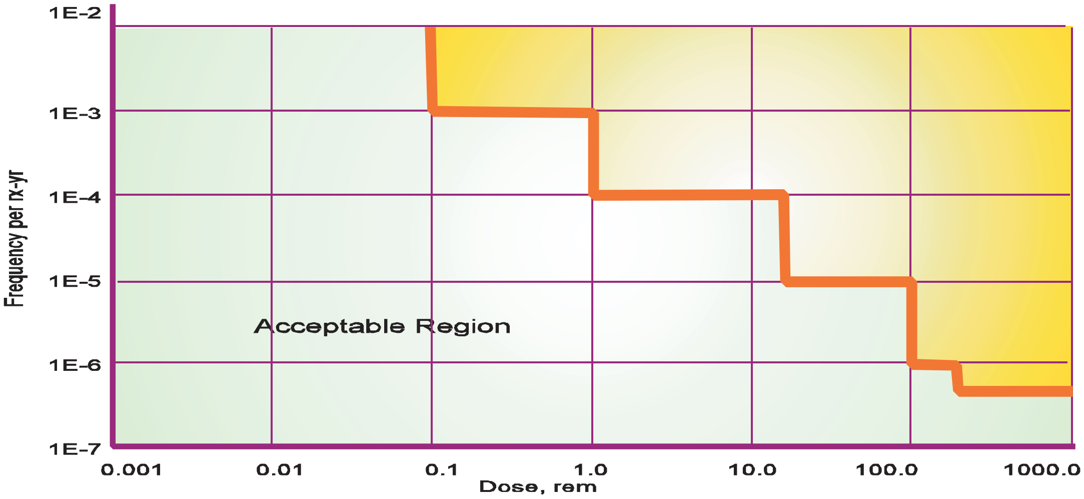


Figure 4-1 Frequency/consequence curve for public health and safety

Based on Table 4-1, Figure 4-1 gives a representation of a frequency-consequence plot (annual frequency vs. dose in rem) for doses incurred in accidents. The breakpoints for the dose ranges in Figure 4-1 are described in Table 4-1. The curve as a whole is meant to provide guidance on the frequency and consequence of accidents and to be reasonably consistent with the quantitative health objectives (QHOs) of the Commission's Safety Goal Policy Statement. The QHOs limit the total risk of all accidents to the "average" individual within specified distances of the exclusion area boundary.

Figure 4-1, the ordinate represents the frequency of accidents leading to a particular dose at/near the site boundary. Since each airborne accidental release, by virtue of inherent plume transport characteristics, is expected to affect only a small fraction of the offsite population around the plant, the average individual risk of early fatality (averaged over the population within 1 mile of the site boundary) or the average individual risk of latent cancer (averaged over the population within 10 miles of the site boundary) should be conservatively met by the curve shown in Figure 4.1. Of course, the line shown in Figure 4.1 should not be treated as a strict acceptance criterion; it is only an indicative guide to the event frequencies and consequences that meet the criteria for public risk embodied in the QHOs.

Figure 4-1 can also be utilized for the deterministic event frequency - consequence accidents under the AOOs and DBAs discussed in Section 4.3.1.3 below. In this case, a curve such as shown in Figure 4-1 could be used as part of an acceptance criterion by selecting the event with the highest possible consequence from the frequency categories (as discussed in detail in Section 4.4.2.3 shown in Table 4-2) and then demonstrating that the curve is met at a 95% confidence level.

4.2.1.2 Protection of Operating Staff and Environment

In developing the framework the NRC staff considered protection of the operating staff and the environment. The staff considered separate risk goals for protecting the operating staff but judged unnecessary at this time, as explained below.

Protection of Operating Staff

Protection of individual members of the public and the workers during normal operation is provided by the system of dose limits contained in 10 CFR Part 20. Subpart B of Part 20 establishes radiation protection program, including the ALARA requirement, for each licensee. Subpart C of Part 20 provides occupational dose limits for adult workers, including limits for planned special exposures, occupational dose limits for minors, and dose limits for the embryo/fetus due to occupational exposure of a declared pregnant woman worker.

Operating personnel are vital to plant safety and are called on to perform safety related actions during design basis and beyond-design-basis events (e.g., accident management actions). Accordingly, protection of the operating staff during accidents should be considered in the design and operation of future reactors.

General Design Criteria (GDC) 19 of 10 CFR Part 50 Appendix A currently requires main control rooms to be designed to ensure habitability under a variety of conditions, including design basis accident conditions. The conditions which must be considered include a postulated source term representative of a core melt accident (or an alternate source term) and chemical releases. As a result, LWR main control rooms are provided with shielding and habitability systems that ensure the safety of the operators during the postulated conditions. However, no corresponding requirements exist in 10 CFR 50 for protection of operating staff outside the main control room, who may be called upon to perform accident management actions and communicate with other staff during accident situations.

In the development of accident management programs for existing LWRs (which were developed on the basis of a voluntary industry initiative), it was recognized that access by the operating staff to certain portions of the plant was essential to carry out the planned actions. Accordingly, NEI, in its “Severe Accident Issue Closure Guidelines” document (NEI-91-04, Rev. 1, dated December 1994) on the development of accident management programs, identified operational and phenomenological conditions as factors which must be assessed in planning and implementing operator accident management actions.

For new plants the NRC staff proposed similarly require that the main control room be designed to protect the operating staff during all events which must be considered in the design and that the procedures and accident management programs consider the environment (e.g., temperature, radiation) in which local operator actions take place and ensure that the design and procedures sufficiently protect all the operators so that the actions can be safely accomplished without serious injury. For radiation exposure the limits in 10 CFR Part 20.1206, “Planned Special Exposures” should be used as the measure to prevent serious injury for personnel outside the control room. For personnel inside the control room, limits similar to those in GDC-19 could be used. Scenario specific source terms may be used in the assessment, consistent with those used in other accident analyses. Other accepted limits should be applied for other hazards (temperature, chemicals, etc.).

Utilizing the above approach, new risk goals are not necessary at this time for protection of the operating staff during accidents.

Protection of the Environment

Protection of the environment during normal operation is required by 10 CFR Part 50.34a, which sets forth design objectives for equipment to control releases of radioactive material in effluents to the environment and by 10 CFR Part 50.36a, which provides technical specifications for effluents during operation. 10 CFR Part 50.34a specifies that the design objectives for keeping releases contained in effluents during normal operation and expected operational occurrences should be ALARA (as low as reasonably achievable considering technology, cost-benefit to society and other related socio-economic considerations). 10 CFR Part 50.36a provides technical specifications for releases of liquid and gaseous effluents to unrestricted areas that, in addition to meeting the requirements of Part 20, should be as low as reasonably achievable. Numerical guidance on design objectives and limiting conditions of operation for releases to meet the ALARA criterion is provided in Part 50, Appendix I. This guidance states :

(1) “The calculated annual total quantity of all radioactive material above background to be released from each light-water-cooled nuclear power reactor to unrestricted areas will not result in an estimated annual dose or dose commitment from liquid effluents for any individual in an unrestricted area from all pathways of exposure in excess of 3 millirems to the total body or 10 millirems to any organ.”

(2) “The calculated annual total quantity of all radioactive material above background to be released from each light-water-cooled nuclear power reactor to the atmosphere will not result in an estimated annual air dose from gaseous effluents at any location near ground level which could be occupied by individuals in unrestricted areas in excess of 10 millirads for gamma radiation or 20 millirads for beta radiation.”

(3) “The Commission may specify, as guidance on design objectives, a lower quantity of radioactive material above background to be released to the atmosphere if it appears that the use of the design objectives in paragraph (2) is likely to result in an estimated annual

external dose from gaseous effluents to any individual in an unrestricted area in excess of 5 millirems to the total body; and

(4) Design objectives based upon a higher quantity of radioactive material above background to be released to the atmosphere than the quantity specified in paragraph (2) will be deemed to meet the requirements for keeping levels of radioactive material in gaseous effluents as low as is reasonably achievable if the applicant provides reasonable assurance that the proposed higher quantity will not result in an estimated annual external dose from gaseous effluents to any individual in unrestricted areas in excess of 5 millirems to the total body or 15 millirems to the skin."

(5) "The calculated annual total quantity of all radioactive iodine and radioactive material in particulate form above background to be released from each light-water-cooled nuclear power reactor in effluents to the atmosphere will not result in an estimated annual dose or dose commitment from such radioactive iodine and radioactive material in particulate form for any individual in an unrestricted area from all pathways of exposure in excess of 15 millirems to any organ."

Protection of the environment is also provided by 10 CFR Part 51 which contains the environmental protection regulations applicable to NRC's domestic licensing and related regulatory functions. Part 51 implements the relevant portions of the provisions of the National Environmental Policy Act (NEPA) of 1969, as amended, in a manner consistent with the NRC's domestic licensing and related regulatory authority under the Atomic Energy Act of 1954, as amended. Section 51.20 specifies the criteria for and identification of licensing and regulatory actions requiring environmental impact statements (EIS) ; for example, a permit to construct or operate a nuclear power reactor, and Section 51.29 provides the scope of the EIS. Section 51.45 specifies the requirements of the environmental report, Sections 51.50, 51.51, and 51.52 specify the data required to comply with requirements to obtain a construction permit, and Section 51.53 provides requirements for the postconstruction environmental reports, including the reports on the operating license stage, the license renewal stage, and postoperating license (i.e., decommissioning) stage.

Currently, there are no requirements for protection of the environment from accidents at NPPs. It has been generally accepted that the current low risk to members of the public also provide for low risk to the environment. Many new plant designs will have long response times under accident conditions, allowing licensees to meet the Commission's safety goals by greater reliance on evacuation of the public, a situation where the public can be protected, even though the land may be contaminated, could be the result.

In consideration of the above, the need for a separate goal related to protection of the environment was evaluated. This evaluation consisted of assessing how well the frequency-consequence curve (discussed in Section 4.2.1) and the accident mitigation risk criteria of 10^{-6}/ry large release frequency (discussed in Section 4.3 below) provides protection for the environment. The adequacy of the environmental protection provided by the frequency-consequence curve (Figure 4-1) and 10^{-6}/ry large release frequency (LRF) was assessed using the criteria for an extraordinary nuclear occurrence (ENO) contained in 10 CFR Part 140. The ENO criteria represent levels of individual dose and land contamination or offsite cleanup costs resulting from an accident below which there should be minimal societal impact since the cost of any remedy would be born by the licensee. Accordingly, both the ENO dose, land contamination criteria and cleanup cost criteria were used in this assessment as discussed below. In both cases the objective is to show that the environment is being protected at least as well as the public.

Dose/Land Contamination Assessment

This assessment is based upon showing that the frequency-consequence curve discussed in Section 4.1 is sufficient to ensure an individual risk to the public is approximately equal to that expressed by the Commission safety goal QHOs. Therefore, using Equation 1, the individual risk to a member of the public is estimated using the frequency-consequence curve.

$$R_I = D*F*C \qquad \textit{Equation 1}$$

where:

D = Equivalent dose in rem

Section 140.84 Equivalent Criterion I provides two criteria for determining whether there has been a substantial discharge of radioactive material or substantial radiation levels offsite to cause contamination.

The first criterion is stated in terms of actual or projected doses to one or more persons offsite as a result of the release. A whole body dose of 20 rem, a bone marrow dose of 20 rem, a thyroid dose of 30 rem, a skin dose of 60 rem, and another organ dose of 30 rem provide the basis for making the determination there has been sufficient doses to cause contamination.

The second criterion is stated in terms of surface contamination levels of at least a total of 100 square meters of any offsite property. These levels are presented two ways: the first is for property that is contiguous to the licensee's site and is owned or leased by a person with whom an indemnity agreement has been executed and the second is for any offsite property. The second set of levels are as follows:

Contamination Source	Contamination Level
Alpha emission from transuranic:	0.35 microcuries per square meter
Alpha emission from non-transuranic:	3.5 microcuries per square meter
Beta/gamma emissions:	4 millirads per hour

These levels result in an equivalent dose of 20 rem [reference x].

F = Frequency (per year)

To anchor a frequency to these contamination levels, consider that the projected dose and the surface contamination levels of Criterion I in Section 140.84 are essentially equivalent, i.e., contamination levels of 0.35 microcuries per square meter of alpha emitting non-transuranic of and beta gamma emitters of 4 millirads per hour, are both equivalent to a dose level of 20 rem per year.

Using the frequency vs. consequence levels of contamination shown above it can be seen that a dose level of 25 rem is associated with a frequency of 10^{-5}/yr. Accordingly, the levels of contamination stated above in 10 CFR §140.84 are approximately related to this frequency.

C = Risk Coefficient

The standard risk coefficient for members of the public, where an individual exposed to 1 rem/yr has a $5*10^{-4}$ likelihood of contracting a fatal cancer over their lifetime.

This results in an individual risk to a member of the public of (10^{-5}/yr) (20rem) ($5x10^{-4}$/rem) =10^{-7}/yr. 10-7 per year.
This value is below the latent fatality QHO value of $2*10^{-6}$/yr. Thus, it can be concluded that a plant meeting the frequency-consequence curve shown in Section 4.2.1 would protect the environment as well as the public.

This same analysis approach can also be applied to the effluent limit that corresponds to an abnormal occurrence as defined in NUREG-0090. These limits are used to define the desired outcome of the Commission's strategic goal for safety in the FY2004-FY2009 Strategic Plan as it pertains to releases of radioactive materials that cause significant adverse environmental impacts.

Cleanup Cost Assessment

This assessment is based upon showing that the 10^{-6}/ry large release frequency (LRF) criterion provides protection of the environment equivalent to protection of the public on a value-impact basis, using dollars as the common figure of merit. The rationale as to why a 10^{-6}/ry LRF provides for at least equivalent protection of the environment using the ENO criteria related to cleanup costs is as follows.

First, it is assumed that a large release must occur to result in substantial offsite contamination. Therefore, LRF is chosen as the design parameter for the assessment. Second, it is assumed that the ENO criteria represent the measure of environmental protection desired and, therefore, a goal of future designs ensure that offsite cleanup costs do not exceed the criteria in 10 CFR Section 140.85:

- $2,500,000 to an individual or
- $5,000,000 cumulative

Using a LRF of 10^{-6}/ry, the cleanup cost criteria equate to annualized values of:

- $2.50/ry (individual risk)
- $5.00/ry (cumulative risk)

These values corresponds to a range of 1-10 dollars/reactor year.

annualized value = cleanup cost * LRF

Using the frequencies for early and latent fatalities associated with the reactor safety goal QHOs:

early fatality frequency	=	$5*10^{-7}$/ry
latent fatality frequency	=	$2*10^{-6}$/ry

Using the values of a life assumed in regulatory analysis (NUREG/CR-6212):

value for early fatality	=	$2.1*10^6 per life saved
value for latent fatality	=	$2000/person-rem

Early and latent fatality, based on dollars, can be estimated:

Fatality = (cost per life saved)*(fatality frequency) Equation 2

early fatality = $(2.1*10^6$ dollars) $(5*10^{-7}$/ry)
= 1 dollar/ry

latent fatality = [(2000 dollars/person-rem)/$(5*10^{-4}$/person-rem)]$*(2*10^{-6}$/ry)
= 8 dollars/ry

These comparisons, using dollars, show an equivalent level (1-10 dollars/reactor year range) of value-impact for the environment and the public when a 10^{-6}/ry LRF is used. Thus an approach has been taken to define a frequency-consequence curve and a risk goal for accident mitigation (independent of the timing of the release) that ensure protection of the environment at least equivalent to that provided to the public. Therefore, no separate goals on environmental protection are proposed.

4.2.2 Risk Objective Surrogates

Although a designer could propose to use the frequency-consequence curve directly (using Level 3 PRA), implementation of the frequency-consequence curve described in Section 4.2 can also be accomplished through establishment of a series of surrogate risk criteria. These surrogate risk criteria would more directly focus on plant design and avoid the additional complexity and uncertainty introduced by the use of Level 3 PRA. These surrogates are described in this section.

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 (LWR and non-LWR) achieve a level of safety at least equivalent to that expressed by the Safety Goal Policy Statement. Accordingly, the overall safety objective (i.e., frequency-consequence curve) is based upon meeting the Commission's Safety Goal Policy Statement. For currently operating LWRs, subsidiary objectives related to accident prevention and 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.

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. However, there is an expectation that new plants will be substantially safer than current plants and the conceptual discussion above makes that expectation more explicit. For currently operating plants, subsidiary objectives related to accident prevention and mitigation i.e. CDF and LERF or CCFP have been developed and used as surrogates for the QHOs expressed in the Safety Goal Policy. The QHOs specify goals for individual risk to members of the public corresponding to 2 x 10^{-6}/yr for latent fatalities and 5 x 10^{-7}/yr for early fatalities. The surrogates were developed so as to be consistent with the level of safety specified in the Safety Goal Policy and not impose a more stringent level of safety. They 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). In effect the 10^{-4}/ry CDF serves as a surrogate for the latent fatality QHO as well as a measure of accident prevention, and the 10^{-5}/ry LERF or 0.1 CCFP serves as a surrogate for the early fatality QHO for currently operating reactors. (See Appendix A for detailed discussion on derivation of surrogates.)

These subsidiary objectives and surrogates developed for current LWRs were summarized in Chapter 2 and are based upon specific LWR characteristics. However, for new plants, power level (i.e., megawatt thermal size of reactor), performance, source terms, emergency preparedness) may be different than for current generation plants. The question then becomes are there generic surrogate risk criteria that could be applied that address accident prevention and mitigation while remaining consistent with the level of safety implied by the Commissions Safety Goal Policy Statement.

To develop such generic surrogates, one must eliminate any dependency on power level, performance, source term characteristics, emergency preparedness, etc., and consider only the effects of atmospheric dispersion. Atmospheric dispersion generally limits exposure to approximately a 30 degree sector radiating out from the plant in the direction of the prevailing wind at the time of the accident. Accordingly, only about one-tenth of the population around the plant would be exposed to the release, thus allowing the surrogates for the early and latent fatality QHOs to be a factor of 10 higher than the QHOs themselves. With only this consideration, reasonable generic surrogates for accident prevention and accident mitigation become 10^{5}/ry (surrogate for latent fatality QHO) and 10^{6}/ry (surrogate for early fatality QHO). In general, accident prevention will involve avoiding a major fission product release from the core, such as could occur from loss of coolable geometry and resulting significant fuel damage. However, the specific definition of accident prevention will be technology dependent and will need to be defined in the technology-specific regulatory guides, considering factors such as:

- the type of fuel,
- the type of coolant, and
- reactor core design.

For LWRs it is expected that core damage frequency will continue to be used. For other technologies, appropriate definitions for accident prevention will need to be developed. LERF is considered a reasonable accident mitigation metric and has been substituted for LERF (which is used for current LWRs) so as not to distinguish between early and late period releases. LERF is a technology-neutral surrogate for the early fatality QHO. The magnitude of a large release may be technology-specific, but can generically be the magnitude which has the potential to cause one or more early fatalities offsite.

It should be noted that these generic criteria are approximately an order of magnitude more conservative than the values used for current LWRs. In a June 15, 1990, SRM the Commission approved the use of a 10^{-4}/ry CDF guideline. It is recognized that recommending the use of a 10^{-5}/ry accident prevention guideline goes beyond the June 15, 1990, SRM; however, the 10^{-4}/ry CDF value was developed in consideration of LWR technology and characteristics (including EP) and needs to be reassessed for non-LWRs. Accordingly, for designs where traditional offsite EP may not be proposed, a 10^{-5}/RY value for accident prevention is proposed to ensure the latent fatality QHO is met. In addition, the Commission recognized that some conservatism may be necessary in the use of surrogate values and, in its June 15, 1990, SRM, accepted an order of magnitude conservatism when requesting the staff to evaluate the 10^{-6}/RY general plant performance guideline for a large release of radioactive material to the environment. The staff, in SECY-93-138, provided its evaluation and recommended against defining a large release. However, this evaluation was based upon the characteristics associated with current LWRs. Given the generic nature of the framework, a 10^{-6}/ry large release frequency is necessary to ensure the early fatality QHO is met, is consistent with the Commission's Safety Goal Policy Statement and is proposed for use. It should also be noted that a new plant designer who wants to take credit for EP and/or certain plant-specific characteristics, he would be free to propose alternatives to the generic values. Specifically, an applicant could propose an accident prevention risk criterion applicable to this design using the following guidelines.

The definition of accident prevention should be based upon limiting fission product release from the fuel to a value less than or equal to that calculated for design basis accidents. The frequency for the accident prevention criteria should be consistent with the frequency of design basis accidents. Specific success criteria that can be used in a risk assessment will be technology specific and should also be propose.

The above risk criteria are intended to be compared to the mean value of risk information from the PRA. They are also intended for application on an individual reactor basis, except for modular reactor [11]designs, where a number of small reactors are used to equal the power output from one large reactor. For modular reactors, the integrated risk from multiple reactors needs to account for the situation when the use of multiple reactors is equal the output of one large reactor.

In accounting for the integrated risk from modular reactors, both accident prevention and accident mitigation risk need to be considered.

It is recognized that accident prevention is important, regardless of reactor power level, whereas, in many cases accident mitigation has a relation to reactor power level (i.e., the lower the reactor power the fewer fission products available for release to the environment and thus the more difficult it is to have a large release). Given the non-linear response of early fatality health effects to dose, accounting for reactor power level, can make a large difference in the early fatality results. Accordingly, the integrate risk associated with accident mitigation risk criteria should take into consideration reactor module size. The goal of considering the integrated risk from modular reactors is to ensure that the integrated risk from multiple reactor modules is at least as low as the risk from an equivalent large rector design. Therefore, the following guidelines should be applied:

[11] As described in SECY-02-0180 "Legal and Financial Policy Issues Associated With Licensing New Nuclear Power Plants", dated October 7, 2002, for the purposes of financial protection the proposed Energy Bill has defined modular reactors as combination of two or more reactors (each rated 100-300 Mwe) with a combined rated capacity of not more than 1300 Mwe.

- taking into consideration the integrated effect of risk when assessing accident prevention for modular reactor designs, independent of reactor power level, and

- taking into consideration the integrated effect of risk when assessing accident mitigation for modular reactor designs in a fashion that allows for consideration of the effect of reactor power level.

A parallel issue is whether or not the Commission intended the safety goals to apply t the risk from the entire site or from an individual reactor on a site. This issue remains “to be determined” at this time.

4.3 Design Objectives

The overall risk-informed approach to specifying design expectations consists of defining a set of probabilistic and deterministic criteria that, if met, will ensure the overall risk profile of the plant meets or exceeds the goal defined by the frequency-consequence curve for risk to the public, described in Section 4.1. This approach will also eliminate the need for performing a Level 3 PRA (thus eliminating uncertainties and site assumptions associated with Level 3 PRA analysis), although an applicant would be free to propose an alternative approach using a Level 3 PRA and the frequency-consequence curve described above. As a complement to the probabilistic criteria, described in Section 4.2, a set of anticipated operational occurrences and design basis accidents will also be defined (using the results of the plant specific PRA) and analyzed against a set of deterministic acceptance criteria. These anticipated operational occurrences and design basis accidents are the deterministic element of a risk-informed approach and will also serve as reference points for interfacing with other parts of the regulations (e.g., 10 CFR 100) and for evaluating the effectiveness of certain plant engineered safety features (ESFs). In addition, the anticipated operational occurrences will help ensure that for high probability events, the consequences are low. Design basis accidents will not be defined for low probability events that traditionally would be considered only for EP or overall plant risk.

Implementation of the risk-informed approach will require a living PRA over the plant lifetime. As operating experience and reliability information is collected and fed back into the PRA, the plant risk profile and important sequences may change. This may affect the anticipated operational occurrences and design basis accidents initially selected as well as how the plant compares to the acceptance criteria. In addition, it could affect the safety classification of SSCs as described in Section 4.3.2. Accordingly, a process will need to be developed that recognizes this potential for change and defines a way to accommodate it without undue burden or delay (e.g., 50.59 type process), while ensuring changes with high safety significance receive NRC review and approval. In addition, such a change process will need to be integrated with the design certification process (10 CFR §52) which certifies designs by rule making. This is discussed further in Section 6.3.1.5. Discussed below are various elements of the risk-informed approach to specifying design expectations.

4.3.1 Design Basis Event Criteria

4.3.1.1 Event Categorization

It is not proposed that the events which must be considered be pre-defined for future reactors. To do so would presume that these events would provide the acceptable design basis for any future reactor concept, which would limit innovative and unique concepts, and could also result in the selection of events that do not provide the necessary safety. Therefore, it is proposed to develop technology-neutral, risk-informed criteria for the selection of events that could be applied to any future reactor design, on a plant specific basis. Guidance regarding the development, uses and implementation of these criteria are given below. This guidance can be used to support development of generic requirements or can be applied on a plant specific basis.

The use of a probabilistic approach in selecting events begins with categorizing initiating events and event sequences by the frequency of their expected occurrence, based upon the initiating events and event sequences considered in the plant specific PRA. In performing this categorization, initiating events and event sequences shall be grouped by type. The event categories were chosen to correspond to anticipated operational occurrences (frequent), design basis accidents (infrequent) and beyond design basis accidents (rare). Generic, technology-neutral criteria for the categorization of event sequences (which include the initiating event) are given below:

Event Category	Frequency of Initiating Event/Event Sequences
Frequent events	$\$10^{-2}$/ry (mean value)
Infrequent events	$<10^{-2}$/ry to $\$10^{-5}$/ry (mean value)
Rare events	$<10^{-5}$/ry to $\$10^{-7}$/ry (mean value)

The above criteria for categorizing event sequences would apply to all internal events and external events for the purposes of risk assessment. Event sequences with a probability $<10^{-7}$/ry (mean value) are considered extremely rare and do not have to be considered in the design for licensing purposes. The frequency ranges associated with the above event categories were chosen to ensure that, when the frequencies for event sequences are summed, cumulative frequencies associated with the event categories meet the following:

- capture all event sequences expected to occur one or more times during the life of an individual reactor (frequent category). These sequences have traditionally been called anticipated operational occurrences (AOOs). Assuming a plant lifetime of 60 years, this equates to a frequency of approximately 10^{-2}/year.

- capture all events and event sequences that could occur in the population of reactors of that design over their lifetime (infrequent category). These sequences have traditionally been called design basis accidents (DBAs). Assuming a population of 1000 reactors, this equates to a frequency of approximately 10^{-5}/year.

- capture all events and event sequences necessary to ensure the assessment covers low frequency events, and event sequences needed to assess the Commission's safety goals (rare category). Since the early fatality QHO is $5\text{x}10^{-2}$/year, a frequency of 10^{-7}/year is chosen as the cutoff.

4.3.1.2 Design Basis Event Selection

Once event sequences are categorized by frequency, the event sequences associated with the frequent and infrequent event categories in the plant PRA are examined. This examination is for the purpose of selection of AOOs and design basis accidents.

For each of the frequent and infrequent event sequence categories the worst event scenarios from each accident type (e.g., reactivity insertion, fuel handling, shutdown, loss of coolant, etc.) are identified and used for AOOs and DBAs. Since it is desired that none of the event scenarios in the frequent or infrequent categories exceed the accident prevention criteria, the worst event scenarios shall be those that cause the largest release of radioactive material internal to the plant and/or to the environment.

All event sequences with a frequency of 10^{-2}/year or greater (for AOOs) and those between 10^{-2}/year and 10^{-5}/year (for DBAs) shall be examined and, as mentioned above, those that lead to the largest release of radioactive material (for each accident type) shall be identified as AOOs and DBAs. These AOOs and DBAs should then be assessed against the deterministic criteria discussed in Section 4.3.1.3.

Engineering judgement may also be used to supplement the selection of DBAs where uncertainties may not be adequately addressed in the PRA. It should be noted that the use of probabilistic selection criteria, such as these described above, will likely result in AOOs, and DBAs different than those traditionally used in safety analysis. [Initiating events related to security to be addressed.]

4.3.1.3 Event Acceptance Criteria

The event sequences selected as AOOs and DBAs shall then be compared to the following deterministic acceptance criteria summarized below in Table 4-2.

Table 4-2 Event acceptance criteria

Event Category	Acceptance Criteria
Frequent Event sequences (AOOs)	• 100 mrem TEDE (At the EAB) for exposure to the public • no loss of core cooling[*] or fuel damage • at least 2 barriers to the uncontrolled release of radioactive material remain intact
Infrequent Event Sequences (DBAs)	• Doses from Figure 4-1 corresponding to event frequency (At the EAB-worst 2 hr dose) (at the LPZ duration of the accident) for exposure to the public • no sustained loss of core cooling or fuel melting[*] • at least one barrier to the uncontrolled release of radioactive material remains intact.

Deterministic analysis of the AOOs and DBAs would be by best estimate methods, including an

[*] The technology-specific regulatory guides will provide appropriate definitions for these terms.

uncertainty analysis. Further discussion on best-estimate analysis is provided in Chapter 6. The results of the best estimate analysis would then be compared to the deterministic acceptance criteria and shown to meet it with a 95% confidence. In performing the best estimate analysis the number of failures of SSCs and human errors that should be assumed would be the same as that contained in the PRA sequence from which the DBA was derived. In other words, the single failure criterion would be replaced by a probabilistic approach based upon the PRA. This approach would apply to assumptions in the analysis as well be reflected in the plant design. Other guidelines for performing the deterministic analysis (e.g., atmospheric dispersion) will also be developed.

Other surrogate acceptance criteria may also be established for AOOs and DBAs. These may be in the form of deterministic engineering parameters (e.g., temperature) or related to equipment performance. Performance-based acceptance criteria are preferred and guidance on how to establish such criteria is provided in Appendix A. In either case the acceptance criteria should be set conservatively. Usually this means that the acceptable value of an important temperature, pressure, stress, etc. is set below the best-estimate of the critical value of such an important parameter (where critical refers to a value where unacceptable changes or phenomena begin)

For future reactors, establishing adequate acceptance criteria involves two immediate questions. What are the important parameters, direct or surrogate, that need to be used to adequately capture the safety performance of the plant, and at what values should these important parameters be set to ensure safe operation of the plant under normal and accident conditions. The answer to the first question is design dependent. As to how to set the acceptable values of the important parameters, the optimum solution would be one where the best-estimate of the critical value of the important parameter, along with the uncertainty surrounding the critical value has been established. Then the uncertainty in the critical value can be used to quantify the degree of conservatism. This would allow using a uniform level of confidence for the critical values for which sufficient information (best-estimate value and uncertainty) is established. If the best-estimate and associated uncertainty of the critical value(s) cannot be established, then the setting of acceptable criteria for the important parameter(s) will have to be done using less quantified methods, relying on engineering judgement and other more qualitative considerations, and the methods applied will have to be established on a case by case basis.

Rare events do not have associated deterministic acceptance criteria since they are beyond traditional design basis accidents. Rather they shall be used in the assessment of overall plant risk (i.e., comparison to the accident prevention and accident mitigation risk criteria) and to assess the extent of EP required as described in Chapter 5. In general, when evaluating whether or not the risk criteria are met, the mean value of the risk information shall be used to compare to the risk criteria. External initiating events that fall in the rare category shall be treated in the PRA in a realistic fashion.

4.3.1.4 Scenario Specific Source Term

Scenario specific source terms may be used for licensing purposes (e.g., siting) providing the following are met:

- the scenarios to be used for the source term evaluation should be selected from a design specific probabilistic risk assessment, with due consideration of uncertainties.

- the source term calculation, using the selected scenarios, should be based upon analytical tools that have been verified with sufficient experimental data to cover the range of conditions expected and to determine uncertainties.

- the source terms used for licensing decisions should reflect the scenario specific timing, form and magnitude of radioactive material released from the fuel and coolant. Credit may be taken for natural and/or engineered attenuation mechanisms in estimating the release to the environment, provided there is adequate technical basis to support their use.

- The source terms used for assessing compliance with dose related siting requirements should be 95% confidence level values based upon best estimate calculations with quantified uncertainties. Where uncertainties cannot be quantified, engineering judgement shall be used.

- the source terms used in assessing emergency preparedness should be mean values based upon best estimate calculations with quantified uncertainties.

The above guidance is intended to provide a flexible, performance-based approach for establishing scenario specific licensing source terms. However, it puts the burden on the applicant to develop the technical bases (including experimental data) to support their proposed source terms. Applicants could, however, propose to use a conservative source term for licensing purposes (in order to reduce research and development costs and schedule), provided the use of such a source term does not result in design features or operational limits that could detract from safety. Finally, it should be noted that the use of scenario specific source terms may result in smaller source terms being used for siting purposes then traditionally used for LWR siting.

In developing technology-specific regulatory guides, the staff may propose acceptable conservative source terms(s), if it is feasible to do so.

4.3.2 Physical Protection Event Criteria

In general, protection against sabotage and external threats will follow current requirements (e.g., 10CFR 73). Applicable current requirements will be determined, as appropriate.

Since risk assessments do not model events caused by sabotage, armed intruders or acts of terrorism, design bases threats may be selected by other means. The selection of design basis threats will follow Commission guidance for new plants.

The role of risk assessment in assessing physical protection or vulnerabilities to security related events is currently under development. If a role of risk information in the physical protection area is developed, it will be incorporated into the technology-neutral regulatory structure.

4.3.3 Risk-Informed Safety Classification

The use of a risk-informed approach to the classification of systems, structures and components (SSCs) as safety related was approved by the Commission in its June 26, 2003, SRM.

The risk-informed approach consists of two steps: (1) a screening evaluation at the system level and, if desired, (2) a more detailed evaluation at the component/structure level of those systems which pass the initial screen. The basic approach used in each step is essentially the same, as described below and is to be applied to all plant SSCs, regardless of the initiating event or event sequence category they are associated with.

4.3.3.1 Approach

The approach consists of a systematic assessment of the safety significance of the system being assessed using risk measures based upon the plant PRA and a complementary deterministic assessment based upon defense-in-depth considerations (thus ensuring a risk-informed, not a risk-based approach). The risk information to be used will be mean values from the full scope, PRA for each mode of operation. The risk measure to be used will take into consideration the importance of the system, structures or component with respect to its availability, reliability, common cause failure contribution and initiating event contribution. For LWRs, the approach, risk metrics and lessons learned in the development of a risk-informed process for special treatment for application to existing LWRs (i.e., 10 CFR 50.69) will be considered in developing a risk-informed approach to future LWRs. For other technologies, different risk metrics may apply. The specific risk metrics may be technology specific and, accordingly, be addressed in the technology-specific regulatory guides.

All systems will also be assessed with respect to their defense-in-depth role. If the system being assessed has been included in the design to fulfill a defense-in-depth role (i.e., is necessary to meet one or more of the DID principles), then it will also be considered as safety significant. The risk-informed safety classification assessment will be applied to all systems in the plant, regardless of whether or not they are necessary to respond to frequent, infrequent or rare events, as defined in Section 4.3.1.1.

4.3.3.2 Implementation

As mentioned above, the safety classification approach will be applied in two steps. The first step is a screening step to be applied at the system level. If an entire system can be shown to be not safety significant, then it can be removed from further consideration. If, however, a system is shown to be safety significant, then an applicant can choose to do a more detailed assessment at the component/structure level to further screen out sub-system components/structures. Finally, after all systems/components/structures are classified as either safety significant or not safety significant, a check on the cumulative effect of not taking credit for all non-safety significant SSCs to will be made. An acceptance criteria will be developed for this final check.

All SSCs not screened out are candidates for special treatment requirements that could involve one or more of the following:

- QA
- seismic qualification
- environmental qualification
- reliability assurance

The scope and nature of the special treatment requirements should be applied in a graded fashion in consideration of the safety functions performed by the SSCs and the environment and reliability with which they must function to be consistent with the PRA.

4.3.4 Spent Fuel Storage (On-Site)

The protective strategies, risk goals, design-construction-operation objectives, and defense-in-depth principles are intended for application to SSCs related to the safe on-sight storage of spent fuel, as well as to the reactor itself. Accordingly, in designing, construction and operating on-site spent fuel storage, SSCs, it should be shown that those SSCs meet the same acceptance criteria as the reactor as described in Chapters 4, 5 and 6 of this framework. In doing this assessment, accident scenarios, source term, etc. specific to the on-site fuel storage SSCs should be used.

4.4 Construction Objectives

Regulatory requirements related to the construction of new plants are expected to be similar in many ways to those employed in the past (e.g., QA, inspection). Where existing requirements are applicable, they will be incorporated into the new licensing structure.

The construction of new plants, however, is expected to differ in several ways from the construction approach and issues associated with currently operating plants. Specifically, it is expected that the construction of new plants will:

- rely more on factory fabrication to produce modules that can be installed in the field, thus reducing the amount of field fabrication,

- utilize components fabricated outside the U.S. and possibly to non-U.S. codes and standards, and

- in the case of HTGRs, have safety highly dependent upon the quality of the fuel fabrication and inspection process

Field fabrication will also be important and need to conform with accepted practice and building codes and standards. It is expected that NRC’s role in field construction will be similar to that employed previously involving QA and on-site inspections. A framework regarding such inspections is contained in NUREG-1789, “10 CFR Part 52 Construction Inspection Program Framework Document” and will be used as guidance in preparing construction inspection requirements. However, regarding the expected differences mentioned above, the requirements that will need to be considered are briefly discussed below.

Factory Fabrication

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

Fabrication Outside the U.S.

The role of NRC in inspecting and regulating components fabricated outside the U.S. needs to be established. The preferred approach would be to establish requirements on the applicant to provide controls and inspections on non-U.S. vendors that ensure quality, thus putting the burden on the applicant, not NRC. NRC would then specify what documentation is to be submitted by the applicant to confirm the appropriate quality has been achieved. In addition, the use of non-U.S.

codes and standards for design and fabrication will require staff review and acceptance. As directed by the Commission in its SRM of June 26, 2003, staff review of international codes and standards is to be done on a case-by-case basis, in the review of applications or pre-application submittals.

Fuel Quality

How to ensure fuel quality over the life of the plant is an issue of concern (this is particularly applicable to HTGRs, whose fuel quality is key to plant safety and needs to be controlled at the fuel fabrication facility). To address fuel quality over the life of the plant, the requirements need to cover what documentation, controls and testing a licensee must provide to ensure the fuel that is put into the reactor is satisfactory (this approach would put the burden on the licensee versus NRC to ensure fuel quality).

4.5 Operational Objectives

The operation of a NPP can have a large impact on safety and risk. Accordingly, it is important that the requirements for future NPPs address the key aspects of operation that are important to safety. Many issues associated with operation are expected to be similar to those for currently operating plants. For these areas, requirements for new plants can build upon and utilize much of the existing regulatory infrastructure. These areas would include:

- operating staff training
- use of procedures
- radiation protection from routine operation (e.g., ALARA)
- maintenance
- human factors considerations
- work control
- configuration control

Other areas may be different and are discussed below.

Staffing

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

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

This issue was discussed in SECY-02-0180, “Legal and Financial Policy Issues Associated with Licensing New Nuclear Power Plants.” In that paper it was acknowledged that staffing for new plants need to be addressed.

Therefore, the requirements will need to include criteria for the review and acceptance of proposed staffing for new plants.

Accident Management

Each reactor design should develop and maintain an accident management program which provides plans and procedures for managing accident sequences, as defined in Section 4.3.1.

Protection of Operating Staff During Accidents

Plant procedures, including those for accident management, shall be developed to ensure the operating staff do not receive exposures in excess of 10 CFR 20.1201 for accidents in the frequent and infrequent range, and comply with 10 CFR 20.1206 for accidents in the rare category. Also, the control room shall be designed to protect the operating staff and remain habitable during accidents external to the control room.

Offsite Emergency Preparedness

Offsite emergency preparedness is a key element of defense-in-depth and is discussed in Chapter 5.

5. TREATMENT OF UNCERTAINTIES: DEFENSE-IN-DEPTH

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. Uncertainties have always been a factor to contend with in any safety assessment and have traditionally been dealt with through research, the application of safety margins, the application of defense-in-depth, periodic surveillance, inspection and testing. As operating experience has been gained, uncertainties have tended to be reduced.

In general uncertainties associated with new plants will tend to be larger than uncertainties associated with existing plants due to new technologies being used, the lack of operating experience or, in the case of some proposed LWRs, new design features (e.g., increased use of passive systems). Any licensing approach for new plants must account for the treatment of these uncertainties. The aim is to develop an approach for future reactors which can be reconciled with 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.

5.1 Approach to Treatment of Uncertainty

The approach recommended for dealing with uncertainties when ensuring the safety of new plants is the concept of multiple successive layers of barriers and lines of defense against undesirable consequences. This approach is usually referred to as defense-in-depth. The concept of defense-in-depth is fundamental to the treatment of uncertainties.

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."*

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."

As in the Strategic Plan quoted above, discussion of defense-in-depth has almost always referred to successive measures taken to prevent or mitigate the consequences of malfunctions or accidents. In more recent discussions of defense-in-depth the reason for the malfunctions and accidents, i.e., uncertainty in equipment and human performance, are also directly mentioned. Involving uncertainty directly in the discussion is made practical by the development of the ability to quantify risk and estimate uncertainty using PRA techniques. Quantifying uncertainty, where possible, and taking credit for defense-in-depth measures in risk analyses also allows a better answer to the question of how much defense-in-depth is enough.

As an example of the significance of uncertainty, one can consider the common question: Will the capacity of a structure, system, or component (SSC) be exceeded during an accident? If there is no uncertainty in the imposed challenge and no uncertainty in the capability of the SSC, there is no uncertainty in the answer. If a particular SSC had a capacity that exceeded the challenge by a very small margin, there would be no benefit, in probabilistic terms, of replacing the SSC with one twice as strong. In both cases the failure probability would be zero. Generally, of course, there is uncertainty in the imposed challenge, the capacity, or both, and the greater the uncertainties, the greater the need for added levels of defense, such as adequate safety margin (where adequate means the margin is sufficient to assure a predefined high probability that the capacity will be sufficient to meet the challenge, taking the uncertainties into account).

5.2 Types of Uncertainty

Uncertainties have generally been categorized into aleatory, i.e., random, or stochastic uncertainty and epistemic, or state-of-knowledge, uncertainty (Ref. 1 and 2). Aleatory 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. Aleatory 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 aleatory uncertainty. Aleatory 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.

Epistemic 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. Epistemic uncertainty can be reduced, at least in principle, by additional study (theoretical research, experiments) or improved study techniques. Aleatory and epistemic uncertainties are often intertwined and may be difficult to distinguish: measurement uncertainty usually has an aleatory component; some apparent randomness may prove to be epistemic after closer examination. The epistemic 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. Model uncertainties are maximized 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 either because of deliberate limitations of scope or because of lack of knowledge. This includes: (1) risk contributors (e.g., initiators and accident scenarios) that have not been conceived, (2) considerations for which adequate methods of analysis have not been developed, for example, heroic acts and influences of organizational performance, and, finally, (3) risk contributors that can be modeled but are often excluded, such as external events and accidents at low power and shutdown.

5.3 Defense-in-Depth Approach

Defense-in-depth is the philosophy and process that will be used to deal with uncertainties and it is described below. The defense-in-depth philosophy and process will be embedded in the regulations so as to provide for multiple lines of defense, and additional confidence where necessary (via increased safety margins for example), to address the treatment of uncertainties.

The term defense-in-depth has evolved historically from a narrow application of the multiple barrier concept to the application of an overall safety strategy [3]. Currently the term is used in two different but related senses. It is used to characterize a safety philosophy of high level protective strategies, as alluded to in Chapter 2, such as providing physical protection, preventing accident initiators from occurring, terminating or mitigating accidents adequately, preventing degradation or failure of barriers designed to contain radionuclides, and accident management plans to protect the offsite public in case radionuclides penetrate the barriers. The term is also used to denote the multiple physical barrier approach, exemplified in current reactors by the fuel elements and cladding, primary system pressure boundary and containment structure (Implicitly included in the term are the redundant and diverse active and passive systems which protect the integrity of these barriers). In both cases the term conveys the concept of successive barriers or levels, either in terms of physical barriers or in terms of high level protective strategies.

Defense-in-depth measures can be embodied in systems, structures, and components (SSCs), in procedures (including accident management plans to protect the offsite public), or in the chemical and physical properties used during the fission process and the transfer of its energy (for example the volatility of the chemical form of the radionuclides produced). The Commission has stated that the concept of defense-in-depth has always been and will continue to be a fundamental tenet of regulatory practice in the nuclear field. Risk insights can make the value of elements of defense-in-depth more clear by quantifying their impact on risk to the extent practicable. Decisions on the adequacy of or the necessity for elements of defense should reflect risk insights gained through identification of the individual performance of each defense system in relation to overall performance.

Defense-in-depth can be applied in various ways. Inherent reactor features can be selected to minimize the potential for radionuclide release and eliminate barrier failure modes. Redundant or diverse means may be used to accomplish key safety functions, such as safe shutdown or removal of decay heat. The classic example is the use of multiple, independent and diverse barriers (fuel cladding, reactor coolant pressure boundary, and containment) to prevent the release of significant quantities of radionuclides to the environment. In some advanced 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. Redundancy enhances the reliability of independent means; diversity provides protection against dependent (common cause) failures of multiple means, and therefore some assurance that safety functions can be met successfully despite the uncertainty in the mechanism of dependent failures.

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 must also include protection against intentional acts directed at nuclear plants that would threaten public health and safety.

5.3.1 Defense-in-Depth Principles

A summary of the objectives of defense-in-depth can be stated as the ability to:

- compensate for potential adverse human actions (this includes commission as well as omission) and component failures,
- maintain the effectiveness of barriers by averting damage to the plant and the barriers themselves, and
- protect the public and environment from harm in the event that these barriers are not fully effective.

To achieve these objectives, and therefore assure public safety despite uncertainties in our knowledge or rigor, the first principle of defense-in-depth is that

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

The protective strategies discussed in Chapter 3 comprise these measures at a high level. The use of these multiple strategies ensures that there are successive measures in place to protect public health and safety even if some of the strategies fail.

Intentional acts against nuclear power plants that could threaten the plant personnel and/or the public are mainly countered by the strategy of physical protection. As mentioned in Chapter 3, this strategy is still being developed in other programs and will be discussed more fully in the next draft of the framework. Physical protection will involve both design and operational aspects that will be a part of, and affect, the other four protective strategies, as indicated in Chapter 2. In addition, physical protection will include administrative types of requirements that will address the size, nature and training of protective forces that may be used at the plant site.

From this first principle of defense-in-depth, four additional defense-in-depth principles have evolved, and are defined as follows:

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

Accident prevention and mitigation capability should be provided such that there is no undue emphasis on either accident prevention measures or mitigation measures (at the expense of the other) for maintaining the plant in a safe condition given various challenges. However, accident prevention and mitigation can, in general, be defined at various levels in terms of events or event sequences. Reducing the frequency of initiating events is generally viewed as a preventive measure; if the initiator occurs, then helping to cope with its consequences is seen as a mitigative measure. But 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. Specific measures are sometimes seen as either preventive or mitigative depending on the point in the event sequence and the point of view of the observer. 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.

The principle that both accident prevention and mitigation features should be provided is embodied in the protective strategies of Chapter 3. 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 do not have to be ‘equal’ in terms of their quantitative risk reduction, for example, but none should be completely absent from the design and operation of the plant.

For both commercial and safety reasons, there is likely to be a great deal of emphasis on the first protective strategy of limiting initiating events. 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, either by preventing the acts in the first place, or by prevent the intentional acts from progressing to the point where plant safety is impaired.

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 can also be thought of as playing both a preventive and mitigative role, with the barrier associated with the fuel seen as a preventive feature whose integrity prevents an off-normal event from escalating, while 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 prevent accident progression, and by mitigation of the consequences of selected severe accidents. Adequate safety margins in the equipment, structure and procedures used here are an important part of the strategy. The physical protection strategy may also introduce barriers against external missiles that could compromise plant safety systems.

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

The protective strategy of 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 accident management 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. Temporal margins are key here. Physical protection aspects may introduce additional considerations into both on-site and off-site accident management.

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

Redundancy, diversity, and independence in structures, systems, and components (SSCs) and actions will ensure 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: control of reactivity, removal of decay heat, and the functionality of physical barriers to contain the release of radioactive materials[**]. In addition, hazards such as fire, flooding, and seismic events which have the potential to defeat redundancy, diversity, and independence, need to be considered.

Although no universal quantitative targets can be expressed for the individual reliability requirements for each protective strategy, the greatest emphasis is likely be placed on the preventive aspects of the strategies, i.e., limiting initiating events, whether inadvertent or intentional, and using the protective systems in a preventive mode. This would be also consistent with the licensee's objective of high availability of the plant for commercial reasons. In some cases maximum unavailability limits for certain safety systems may be established in the regulations to ensure the necessary reliability for the performance of

[**] Physical barriers would include containments in current LWRs. For new plants, the role of containments is under consideration. A low leakage, pressure retaining building has been the traditional design feature provided on most existing plants to serve as the final barrier to the release of large quantities of radioactive material following an accident. However, some plants, most notably HTGRs, have been designed with non-pressure retaining buildings based on the inherent safety functions of those designs, including the performance of the fuel barrier over the spectrum of frequent, infrequent, and rare events. In the development of the framework, it has been a goal to define the performance desired (using risk-informed criteria) so as to provide flexibility to the designer.

safety functions.

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. 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 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, saturation of signals, 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 carrying it out. For the purposes of redundancy, identical or diverse components may be used.

The reliability of some systems can be further 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 should examine some of the more subtle aspects of the equipment employed. For example, to reduce the potential for common cause failures the designer should examine 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 should be 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 and physical separation to achieve independence among plant 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.

Physical separation includes:

- separation by geometry (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 or humidity, etc. 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 may be containment penetrations, motor control centers, cable spreading rooms, equipment rooms, the control room and the plant process computers. These locations should be particularly scrutinized and appropriate measures should be taken to avoid common cause 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, i.e. they would fall into the rare events category discussed in Chapter 4. Examples of such events are pressurized thermal shock in current reactors, or a graphite fire in a graphite moderated reactor design.

(4) ***Uncertainties in SSCs and human performance should be accounted for such that reliability and risk goals can be met.***

The designer should allocate goals that meet the overall risk criteria including uncertainty. 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 should be set, and the calculations that show they have been met should be 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 reactors without the benefit of reviewing past performance. The role of safety margins is important here in achieving a robust design. Both physical and temporal margins should be incorporated in the plant equipment and procedures. Physical margins ensure that capacities of hydraulic, electrical and structural components are well in excess of minimum requirements, so unanticipated increases in demand can easily be met. Temporal margins ensure preventive systems can correct deviations even after some initial lapses. Therefore, careful attention is paid to the selection of appropriate design codes and materials, and to the control of fabrication of components and of plant construction. In addition, performance monitoring and feedback should be 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 may focus on the use of passive systems and inherent physical characteristics (confirmed by sensitive non-linear dynamical calculations) 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 . 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. Other ways that the facility can operate outside its design assumptions could 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.

(5) ***Plants should be sited in areas that meet the intent of Part 100 and are consistent with the principles for siting established in Reg Guide 4.7.***

The location of regulated facilities should be chosen so as to serve the protection of public health and safety. Consideration of population densities and the proximity of natural and man-made hazards in the siting of plants can provide further assurance that hazards to the public are minimized. Physical protection aspects associated with security concerns are obvious additional considerations in the siting selection.

For reactors, this principle is also intended to ensure that accident management including emergency preparedness remains a fundamental element of defense-in-depth. However, to ensure a level of protection of the public commensurate with the Commission’s safety goals, it is recognized that the scope and nature of offsite emergency preparedness activities could be different for future reactors. These differences could arise from factors such as reactor size (i.e., power level), location, level of safety (i.e., likelihood of release), magnitude and chemical form of the radionuclide release, and timing of releases (i.e., long term response).

> Accordingly, criteria for determining the scope and nature of required offsite emergency preparedness measures are needed that consider the above factors.
>
> Current requirements associated with emergency preparedness (i.e.,10 CFR 50.47, and 10 CFR 50, Appendix E) have been developed primarily in consideration of the risks from currently operating LWRs. However, 10 CFR 50.47 does recognize that for gas-cooled nuclear reactors and for reactors with an authorized power level less than 250 Mwt, the size of the emergency planning zones (EPZs) may be determined on a case-by-case basis. This situation was the case for the Fort Saint Vrain reactor, which had a 5-mile EPZ, instead of the 10-mile EPZ that is applied to currently operating LWRs.
>
> In the past, there have been proposals to modify current emergency preparedness requirements to give credit for reactor designs with enhanced safety characteristics. Staff reviews and response to these proposals were provided. In general, these responses indicated that for new reactor designs, it is too early to identify specific conditions that would allow a reduction in the 10-mile plume exposure pathway EPZ. Until sufficient experience is gained on any prototype reactor, a case-by-case basis should be used to evaluate whether a requested reduction in the size of the 10-mile EPZ can be allowed. This criteria would also apply to the 50-mile ingestion control pathway EPZ. Some conditions that would have particular importance would include, but not be limited to, the following:
>
> (1) consideration of the full range of accidents
> (2) use of the defense-in-depth philosophy
> (3) prototype operating experience is gained
> (4) acceptance by federal, state, and local agencies
> (5) acceptance by the public
>
> Finally, all sixteen Planning Standards and Evaluation Criteria (A through P) in NUREG-0654/FEMA-REP-1, Rev. 1, should be addressed for any size EPZ. The specific requirements under each applicable standard could be scaled down, as appropriate, in order to account for any reduction in EPZ size. Modification of the rules or guidance documents should not occur until sufficient experience is gained in dealing with reduced EPZs.
>
> In its SRM of June 26, 2003, the Commission approved the staff recommendation in SECY-03-0047, "Policy Issues Related to Licensing Non-Light-Water Reactor Designs," dated March 28, 2003, related to offsite emergency preparedness. Specifically, the staff recommended that, in the near term, no changes to current emergency preparedness requirements be made. In the longer term, the role of emergency preparedness in defense-in-depth would be addressed as part of the staff's work to develop a policy or description of defense-in-depth, which is part of the framework development.

These defense-in-depth principles are based upon and consistent with the Commission's Strategic Plan, 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 will not be wholly dependent on any single element of the design, construction, maintenance, or operation of a nuclear facility. The net effect of incorporating defense-in-depth into design, construction, maintenance, and operation is that the facility or system in question tends to be more tolerant of failures and external challenges. The principles are also consistent with Regulatory Guide 1.174

where it is stated that consistency with the defense-in-depth philosophy is maintained if:

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

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

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

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

- Independence of barriers is not degraded.

- Defenses against human errors are preserved.

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

5.3.2 Coordination of Defense-in-Depth with Containment Functional Performance Requirements and Criteria

For current plants a low leakage, pressure retaining containment building has always been an essential part of defense-in-depth, and it is a vital part of the Barrier Integrity protective strategy, as applied to current LWRs. Analyses have shown that these containment buildings also provide physical protection against natural as well as man made events such as airplane crashes.

In considering the five defense-in-depth principles of the previous section, it is clear that containment buildings, like the ones currently in use, can play a role with respect to at least four of the five principles. A containment provides: (1) a measure against some intentional as well as inadvertent events, (2) accident mitigation capability, (3) assurance for some safety functions that they are not dependent on a single element of design, construction , maintenance or operation, and (4) some protection against uncertainties in SSC and human performance.

For new plants the proposed regulatory structure, discussed in this report, is being coordinated with an effort to establish non-LWR containment functional performance requirements and criteria. This effort arose from SECY-03-0047 and the subsequent June 23, 2003 SRM. The Commission asked the staff to develop functional performance requirements and criteria working closely with industry experts (e.g., designers, EPRI, etc.) and other stakeholders regarding options in this area, taking into account such features as core, fuel, and cooling systems design.

The staff evaluated the functional performance requirements and criteria for containment on a technology-neutral basis utilizing applicable Commission technical policies, NRC and industry documents, foreign and domestic technical information, and stakeholder input. Since there was no consensus among stakeholders on a single descriptive term such as “containment,” “confinement,” “vented low pressure confinement,” “reactor building” or “containment structure,” the term "third-level barrier" or "TLB" was adopted and will be used here. From its evaluation, the staff has concluded that the function of TLB designs, includes a direct or support functional role for the following accident prevention and mitigation safety functions:

- Protection from Internal and External Events -The TLB must be adequate to protect risk-significant SSCs from environmental events (e.g., tornado, flooding, seismic), from external events (e.g., design-basis air crashes, fires), high energy breaks, and internal missiles such that those that are relied upon to mitigate these events are not prevented from performing their required safety functions.

- Physical Support of Risk-Significant SSCs -The TLB must be adequate to physically support risk-significant SSCs such that those that are relied upon to mitigate the events in the event categories do not exceed the established design and safety limits.

- Protect Onsite Workers from Radiation - The TLB must be adequate to protect plant personnel from onsite radiation sources during normal operation and accidents such that 10 CFR Parts 20 requirements are met.

- Physical Protection - The staff will coordinate TLB physical protection requirements consistent with Commission policy decisions associated with another SECY paper, currently being prepared by the staff on security design requirements for new plant licensing.

- Heat Removal to Protect Risk-Significant SSCs - The TLB must be adequate to allow reactor fuel, core and TLB heat removal systems to perform their functions such that the SSCs relied upon to mitigate the events in the event categories do not exceed the established design and safety limits.

- Reduce Radionuclide Releases to the Environs (Including Limit Core Damage) - The TLB must be adequate to reduce radionuclide releases to the environs to ensure that doses do not exceed the dose criteria for the selected events in the event categories.

While none of the above functions is exclusively a TLB function, the first four may be viewed as preventive functions, while the latter two may be viewed as mitigative functions.

These TLB functional performance requirement have been developed to be consistent with the regulatory structure for new plant licensing as follows:

- The TLB supports meeting the overall plant risk criteria, which includes accident prevention criteria and accident mitigation criteria.

- A probabilistic approach may be used to identify events which must be considered in the design. Frequency-based categories are established for: normal operation and anticipated operational occurrences; design-basis events; and events beyond the design-basis. Design-specific PRA information, including consideration of uncertainty, is used to categorize the event sequences. This approach requires that the probabilistic information that supports event categorization is adequate and acceptable. Additionally, in categorizing events, deterministic engineering judgement may be used to ensure that uncertainties associated with event probabilities are adequately treated. A set of events from the design-basis accident category is selected on a deterministic basis as scenarios that most severely challenge the TLB to meet the dose criteria and are used for assessing site suitability. The actual events selected for the design-basis are determined at the time of the staff review of a particular plant design.

- An event frequency versus event dose consequence limit curve is used. For the events selected for the design-basis category, the dose consequence limit curve provides that the offsite dose does not exceed the limits specified in 10 CFR100 and 10 CFR50.34 (a) (1).

- For each of the selected events in each of the event categories, the source terms used to assess radionuclide releases into and out of the TLB may be calculated on a mechanistic basis. That is, the radionuclides released into TLB, and radionuclide release out of the TLB to the environs, takes credit for the reactor, fuel and core characteristics (i.e., accident response), including radionuclide retention and attenuation characteristics of each of the multiple mechanistic barriers and obstacles to radionuclide transport. The use of a mechanistic approach requires sufficient quantitative understanding and assurance of both design-specific plant system performance (including radionuclide transport behavior) and fuel system performance (including radionuclide transport behavior) to adequately model all pathways, barriers and obstacles to the environs. 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. This quantitative basis must utilize either existing applicable data or a suitable technology development program. Deterministic engineering judgement is applied to ensure that the (technology-specific) calculated source term for each event selected is bounded.

- Events selected for deterministic analysis from the TLB design-basis category are analyzed using best estimate methods, including uncertainty analysis. The results of the best estimate analysis are compared with the dose acceptance criteria and must be shown to meet it at the 95% confidence level. Bounding calculations may also be performed. Events beyond the design-basis are analyzed in the PRA, including uncertainty analysis, and the mean value is compared with the overall plant risk acceptance criteria.

- Defense-in-depth is applied to ensure that compensatory measures are in place to prevent and mitigate accidents and to address both random (stochastic) uncertainties and state of knowledge (i.e., completeness) uncertainties. The application of defense-in-depth for developing the performance requirement and criteria of the TLB for radioactive releases to the environs is based on the following principles and model:

  – The design should provide for the prevention and mitigation of accidents

  – Safety functions (e.g., control of fission product release, control of chemical attack on core components) should not depend on a single element of design, construction or operation

  – Uncertainties in the performance of risk-significant structures, systems and components and the performance of humans should be accounted for

  – Defense-on-depth should be a combination of : (1) a rationalist element to account model and parameter uncertainties; (2) a structuralist element to account for completeness uncertainties (unknowns).

All of the six safety functions listed above for the TLB can have an impact on defense-in-depth and on the protective strategies. However, the most direct impact will result from the requirements for number 4, physical protection, and for number 6, reduce radionuclide releases to the environs.

With respect to physical protection the staff will coordinate TLB requirements with Commission policy decisions associated with security design requirements for new plant licensing, the subject of another SECY paper currently being prepared. Clearly, security requirements can have a critical influence on TLB design requirements.

With respect to Function 6, reduce radionuclide releases to the environs, the proposed TLB technology-neutral performance requirement for reducing radionuclide releases to the environs states that the TLB must:

- adequately reduce radionuclide release to the environs to meet the onsite and offsite radionuclide dose acceptance criteria for the events selected for the event categories,

- have the capability for low leakage and controlled release of the delayed accident source term radionuclides, and,
- include within the design-basis category, selected low probability, but credible events, with the potential for a large source term and a significant radionuclide release to the environs.

These requirements are consistent with the defense-in-depth principles enunciated in the previous section, and with the protective strategies.

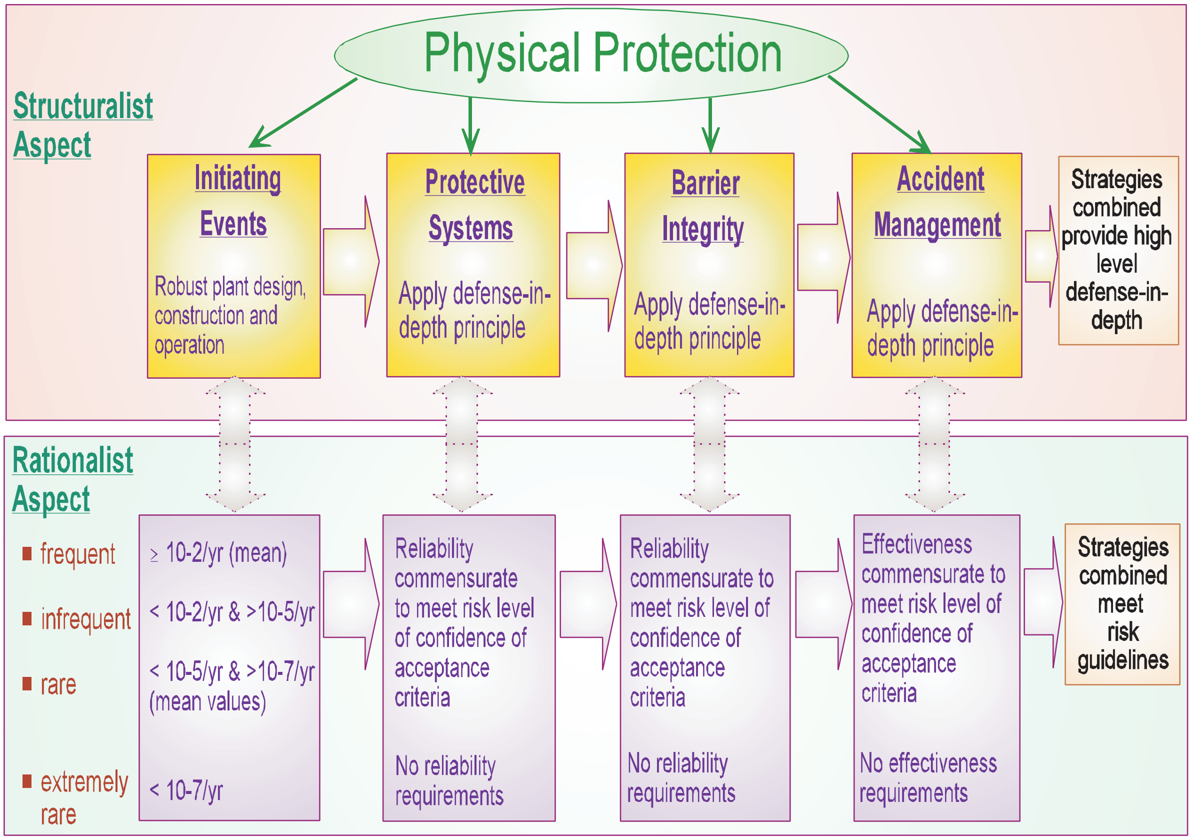
5.3.3 Defense-in-Depth Model

To meet the above defense-in-depth principles, two basic approaches to dealing with uncertainty have been defined, the structuralist approach and the rationalist approach [3]. According to the structuralist 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?” This question is asked without a quantitative estimate of the likelihood of such a failure. Therefore, a characteristic of this approach is that a balance among the high level lines of defense must be 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 been used in the past to achieve adequate protection. In summary, the elements of the structuralist approach are:

- specific qualitative requirements should be included in the regulations to ensure the accomplishment of key safety functions are not dependent upon a single element of plant design or operation, and

- structuralist elements address primarily completeness uncertainties.

In the rationalist 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 rationalist approach seeks to evaluate the uncertainties in the analysis and to determine what steps should be taken to compensate for those uncertainties. In the rationalist approach the probability of accidents is kept acceptably low by providing appropriate defense-in-depth measures in the design, construction, and operation of the plant. The adequacy of the defense-in-depth measures can be assessed in the rationalist approach via quantitative criteria that appear in safety goals or more general frequency/consequence curves. Therefore the essential elements of the rationalist approach are:


Physical Protection
Structuralist Aspect
Initiating Events
Robust plant design, construction and operation
Protective Systems
Apply defense-in-depth principle
Barrier Integrity
Apply defense-in-depth principle
Accident Management
Apply defense-in-depth principle
Strategies combined provide high level defense-in-depth
Rationalist Aspect
frequent
infrequent
rare
extremely rare
≥ 10-2/yr (mean)
< 10-2/yr & >10-5/yr
< 10-5/yr & >10-7/yr (mean values)
< 10-7/yr
Reliability commensurate to meet risk level of confidence of acceptance criteria
No reliability requirements
Reliability commensurate to meet risk level of confidence of acceptance criteria
No reliability requirements
Effectiveness commensurate to meet risk level of confidence of acceptance criteria
No effectiveness requirements
Strategies combined meet risk guidelines

- specific performance goals are included in the regulations to define the balance between prevention and mitigation. Examples include:
  - large release goal
  - equipment reliability goals

- specific requirements are included in the regulations to ensure uncertainties are properly accounted for in meeting the goals. Examples include:
  - safety margins
  - level of confidence
  - monitoring and feedback

- rationalist elements address primarily modeling and parameter uncertainties and allow an estimate of how much defense-in-depth is needed in these areas.

Figure 5-1 shows a defense-in-depth model that incorporates both the structuralist and rationalist approaches.

Figure 5-1 Defense-in-Depth Model

At the high level of the protective strategies the structuralist model is used. The figure shows the protective strategies not in the order of the safety philosophy (as described in Chapter 2), but 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. By requiring the achievement of each protective strategy with a certain confidence, the structuralist aim of assuring several layers of defense, no matter how well any one layer may work, is preserved. Within each protective strategy a rationalist approach is used to determine how much defense-in-depth is needed to achieve the desired quantitative goals on initiating event frequency and safety system reliability, including uncertainty. This is the model of defense-in-depth recommended for application to future reactors.

Depending on the inherent characteristics of various innovative 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.

5.4 Application of Defense-in-Depth

The approach advocated here for application of defense-in-depth in the regulation of future reactors is a combination of the structuralist and rationalist approach.

As pointed out in Chapter 2, the protective strategies dealing with Physical Protection, Barrier Integrity, Initiating Events, Mitigating Systems and Accident Management, are the fundamentals for safe nuclear power plant design, construction, and operation. If these protective strategies are "successfully" met, the adequate protection of public health and safety is achieved. Conversely, the "success criteria" or the acceptable performance of these levels-of-defense can be defined as performance which demonstrates that the design, construction, and operation meets the safety goals. This also requires assurance that uncertainties in performance are taken into account and do not adversely impact the safety goals. This means that each protective strategy requires sufficient defense-in-depth measures to assure the aggregate performance of the protective strategies, including uncertainties, is acceptable.

Before discussing the defense-in-depth needed to support each protective strategy, it is important to point out that, taken together, the protective strategies already constitute a high level defense-in-depth approach of a structuralist nature. The barrier integrity objective is the embodiment of the fundamental reactor safety function of confinement of radioactive material during normal operation as well as during off-normal and accident events. Ensuring that there are adequate barriers to protect the public, the plant personnel and the environment from radioactive releases is the designers primary and ultimate safety objective (Note that barriers here are the generalized barriers specified in Chapter 2). All other safety functions, such as reactivity control and core heat removal in LWRs, for example, can be thought of as supporting this ultimate objective. This confinement of radioactive material is accomplished by providing rugged, well designed barriers and systems to maintain them, as well as by addressing potential challenges to the barriers. The objective of limiting the frequency of initiating events supports the barrier objective by limiting the possible challenges to barrier integrity that potential accident initiators could give rise to. Similarly, the objective of ensuring the reliability of mitigating systems further supports the objective of maintaining barrier integrity by providing systems which can meet the challenges and either terminate or mitigate the challenge. The protective strategy of accident management has as its objective the mitigation of consequences should barrier integrity be compromised. The physical protection strategy supports all the other strategies since it ensures that initiating events from intentional acts are prevented, and that intentional acts do not compromise the ability of mitigating systems, or compromise barrier integrity, or compromise the ability to carry out accident management actions. It should also be reiterated here, that an important part of all the protective strategies is the incorporation of both physical and temporal safety margins, as emphasized in the discussion of the defense in depth principles.

Taken together the protective strategies are a classic example of the structuralist defense-in-depth approach: What if initiating events cannot be avoided, from either intentional or inadvertent acts? Mitigating systems will restore the plant to normal operation or limit the accident consequences. What if mitigating systems fail? Barriers will confine the radioactive material. What if barriers are degraded and allow fission products to escape? Accident management will mitigate the consequences.

Within each of the protective strategies, a rationalist defense-in-depth philosophy is applied to ensure adequate performance in meeting the objective of the defense level. The systems, barriers and actions used in the performance of the safety functions associated with the protective strategy are examined in terms of structuralist and rationalist principles of defense-in-depth. The whole process of applying defense-in-depth is outlined in Figure 5-2, which depicts the application as a series of iterative steps.

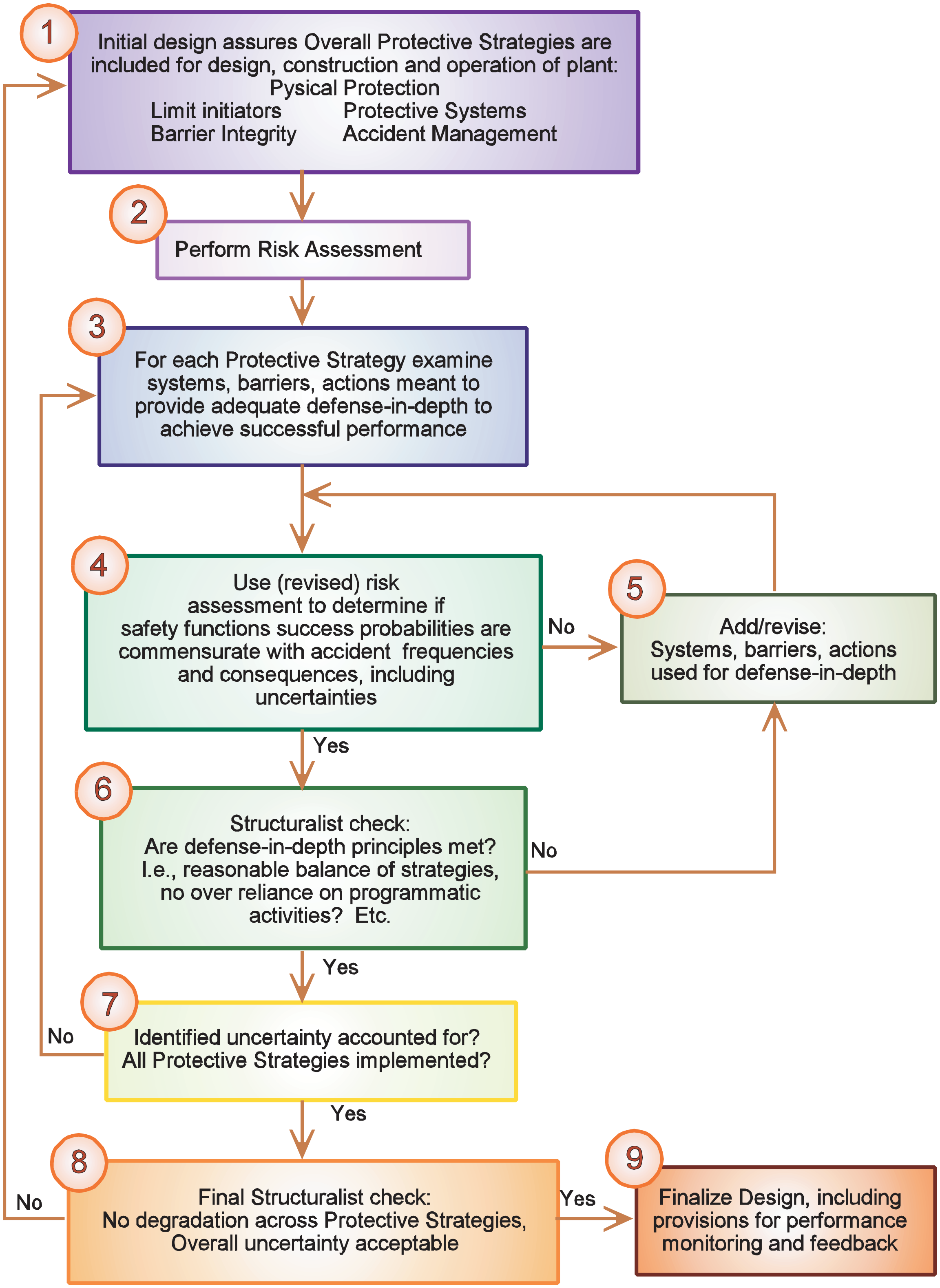

1
Initial design assures Overall Protective Strategies are included for design, construction and operation of plant:
Pysical Protection
Limit initiators
Protective Systems
Barrier Integrity
Accident Management
2
Perform Risk Assessment
3
For each Protective Strategy examine systems, barriers, actions meant to provide adequate defense-in-depth to achieve successful performance
4
Use (revised) risk assessment to determine if safety functions success probabilities are commensurate with accident frequencies and consequences, including uncertainties
No
5
Add/revise:
Systems, barriers, actions used for defense-in-depth
Yes
6
Structuralist check:
Are defense-in-depth principles met?
I.e., reasonable balance of strategies, no over reliance on programmatic activities? Etc.
No
Yes
7
No
Identified uncertainty accounted for?
All Protective Strategies implemented?
Yes
8
No
Final Structuralist check:
No degradation across Protective Strategies, Overall uncertainty acceptable
Yes
9
Finalize Design, including provisions for performance monitoring and feedback

Figure 5-2 Defense-in-Depth Approach

The iterative process described below, for the development of acceptable defense in depth for innovative reactors, is expected to be used initially by the designer and ultimately by the designer and regulator to develop the emerging design. As the design evolves the PRA will also be able to be developed to greater detail.

As the first box indicates, designers of a new plant are expected to arrive at an initial design which incorporates the protective strategies discussed above and earlier in this report. The objective of these strategies are restated here:

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

- The **Limit Initiating Event Frequency** 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 must be considered that can affect any source of radioactive material on-site in any chemical and physical form.

- The **Protective Systems** objective is to ensure that the systems that mitigate 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 **Accident Management** 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 can include emergency evacuation plans, drills, and training.

Incorporating these protective strategies implicitly incorporates a high-level structuralist defense-in-depth philosophy into the design process and into the future operation of the plant.

A risk assessment including estimated uncertainties is carried out as part of the design process as shown in Box 2.***

The third box in the figure depicts the start of the process of applying rationalist defense-in-depth elements within each of the protective strategies incorporated in the design. This is accomplished by examining the reliability, diversity, etc. of the systems, structures, components, procedures and other risk management activities that are used to accomplish the safety functions which determine the adequate performance of the protective strategy.

The first part of the examination is carried out by comparing against the risk assessment, as depicted in Box 4, and determining if the plant equipment and operator actions are reliable enough to achieve the safety function success probabilities needed to meet risk goals in terms of accident frequencies and consequences. The reliability assessment includes defenses against common cause failure mechanisms and human errors. This is the rationalist part of the application of defense-in-depth. A vital part of this step is inclusion of the uncertainties capable of being modeled in the risk assessment, and ensuring that the risk goals are still met with uncertainties included.

If the risk goals are not met then the process proceeds to Box 5, which calls for an addition to, or a revision of, the equipment and actions used to accomplish the safety functions that ensure adequate performance, thus adding to the defense-in-depth. Another rationalist assessment is then performed, with an appropriately revised risk assessment, as indicated in the figure.

When enough rationalist defense-in-depth to meet the risk goals, including uncertainty, has been demonstrated, the process proceeds to Box 6, which depicts the structuralist check on the elements of defense-in-depth implemented so far to ensure that the principles stated earlier are met. Here the equipment and actions are examined for aspects that are not directly related to quantitative reliability measures. For example the examination here ensures that the accomplishment of key safety functions is not dependent on a single element of design or operation, that there is a reasonable balance between preventive and mitigative strategies, that there is not an over-reliance on programmatic activities to compensate for weakness in design, etc. These considerations are applied both to the equipment and actions used in the risk analysis, as well as the analysis of design basis events. Ideally the principles should be met for each of the protective strategies individually, but exceptions may be permitted. However, all the principles have to be met in the aggregate for the protective strategies collectively.

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

When both Box 4 and Box 6 are satisfied the process proceeds to Box 7, where an overall examination of the protective strategy being examined is carried out to see if the identified uncertainties are adequately addressed, before proceeding to the examination of the next protective strategy, i.e., returning to Box 3.

*** (The degree to which physical protection will be quantitatively evaluated in the risk assessment is still under discussion in other programs. Future drafts of the Framework will address this aspect.)

When all protective strategies have been examined in this iterative manner, a final structuralist check is performed on the now revised design (Box 8) to ensure no degradation across the protective strategies can occur. Such a degradation may result from the use of common support systems, for example, to support mitigating systems as well as systems ensuring barrier integrity. When this check is satisfied, the design is finalized (Box 9), and provisions for performance monitoring and feedback, to be used during operation, are specified as part of the design finalization.

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

The process outlined in Figure 5-2 will be reflected in a series of requirements on what constitutes an acceptable application of defense-in-depth for new reactors. Applicants will be responsible for implementation of the process.

As indicated in the rationalist part of the defense-in-depth model depicted in Figure 5-1, the degree of reliability of the equipment and actions used to accomplish the safety functions that ensure the performance of the protective strategies depends on the the risk level specified in the acceptance criteria. This risk level, in turn, depends to some degree on the frequency of the initiating events.

The acceptance criteria, in terms of frequency-consequence limit curves advocated for future reactors, are presented in Chapter 4 of this report. Also in the Chapter 4 discussion initiating events were grouped by frequent, infrequent and rare, similar to the NEI approach [4].

For a well designed plant, the number and quality of defense-in-depth systems needed to achieve the desired limits on consequences will be highest for normal operations and frequent events, and decrease as the frequencies get smaller and consequences increase. This is consistent with other defense-in-depth approaches to issues in current reactors, such as the defense-in-depth matrix advocated by NEI [5] in the SSC categorization process of Option 2, and the EPRI Guideline for performing defense-in-depth for digital instrumentation and control upgrades [6].

5.5 How the Recommended Defense-in-depth Model Addresses Various Uncertainties

Completeness uncertainty is a key reason for maintaining a risk-informed approach that includes defense-in-depth as a key strategy, rather than a risk-based approach. The structuralist elements of the defense-in-depth model primarily address completeness uncertainties and the design needs to ensure that all the protective strategies previously identified in Chapter 2 and above have been adequately addressed by defense-in-depth measures. The implementation of the protective strategies, as indicated in Box 1 of Figure 5.2, and discussed throughout, i.e., providing physical protection, ensuring barrier integrity, limiting initiating events, ensuring reliability of mitigating systems, and availability of accident management are the fundamental means of addressing completeness uncertainty. Further measures are the qualitative defense-in-depth principles discussed in Section 5.3.1 and applied in Boxes 6 and 8 of Figure 5.2, and additional margins that can be added to the individuals strategy goals to set the total risk guidelines in Figure 5.1. Testing programs and careful tracking of operating experience can reduce completeness uncertainty.

Research and testing programs can reduce parameter uncertainties and the application of safety margins can accommodate parameter uncertainties. Remaining parameter uncertainties can typically be characterized by establishing probability distributions on the parameter values and propagating them through the risk analysis. The rationalist elements of the defense-in-depth model applied in Box 4 of Figure 5.2 address parameter uncertainties. Prototype testing and performance monitoring and feedback are essential in determining, where possible, whether the values of the parameter uncertainties that were used in establishing the design are, in fact, reasonably accurate based on performance.

Model uncertainties are those associated with incomplete knowledge regarding how models used in traditional safety analyses and PRAs should be formulated. Both the structuralist and the rationalist elements of the defenses-in-depth model provide protection against state-of-knowledge uncertainties. A number of defense-in-depth elements are used depending on the nature and extent of the uncertainties. Sensitivity studies are an important tool for obtaining a qualitative and quantitative understanding of the uncertainties introduced by modeling assumptions, simplifications, and other limitations.

If uncertainty is driven by a lack of knowledge or understanding of the basic physical behavior or processes, or of the failure mechanisms, then it may be possible to reduce the uncertainty by additional research, which can be construed as part of a rationalist approach. It is expected that if a new future reactor is to operate in temperature and pressure regimes where experience is limited or use new or previously untested materials in these regimes that the design would be supported by an appropriate testing and analytical program. The question is how extensive does this program need to be. It was noted above that specific performance goals have been established in Chapter 4 against which designs can be compared. These rationalist goals can be used to help define the scope and data requirements of the research program needed to support acceptable uncertainty ranges.

Other rationalist elements such as the use of safety margins, level of confidence, and performance monitoring and feedback are used to ensure that the proposed future reactor design will meet the overall safety objectives. This is also done by comparing the results of the PRA to the goals. The exact combination of rationalist elements that will be used to demonstrate that the goals are met with the desired confidence levels is design specific. Monitoring and feedback also help in addressing model uncertainty with respect to such issues as human performance, common cause failures, and mechanistic failures of structures, systems, or components that were not adequately modeled in the PRA.

The work of PRA for future reactors will be to identify and evaluate initially unexpected scenarios.[****] 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, as discussed above. The whole range of uncertainties facing future reactor performance need to be considered. Figure 5-3 summarizes the activities that deal with the types of uncertainty discussed in detail in the previous sections.

All identified and quantified uncertainties (aleatory and epistemic) can be included in PRA that supports development of regulation (evaluation of design, construction and operation risks;

[****] Weick has pointed out that the real key to safe operations in any activity is a focus on managing the "unexpected." [ref] Note that searching for the unexpected is exactly what PRA originally did. With repeated application to current plants, the original creativity of PRA has given way to its routine application.

comparison with risk objectives; evaluation of the effectiveness of Protective Strategies). The PRA directly uses the results of parameter estimation in the data uncertainty distributions 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.

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

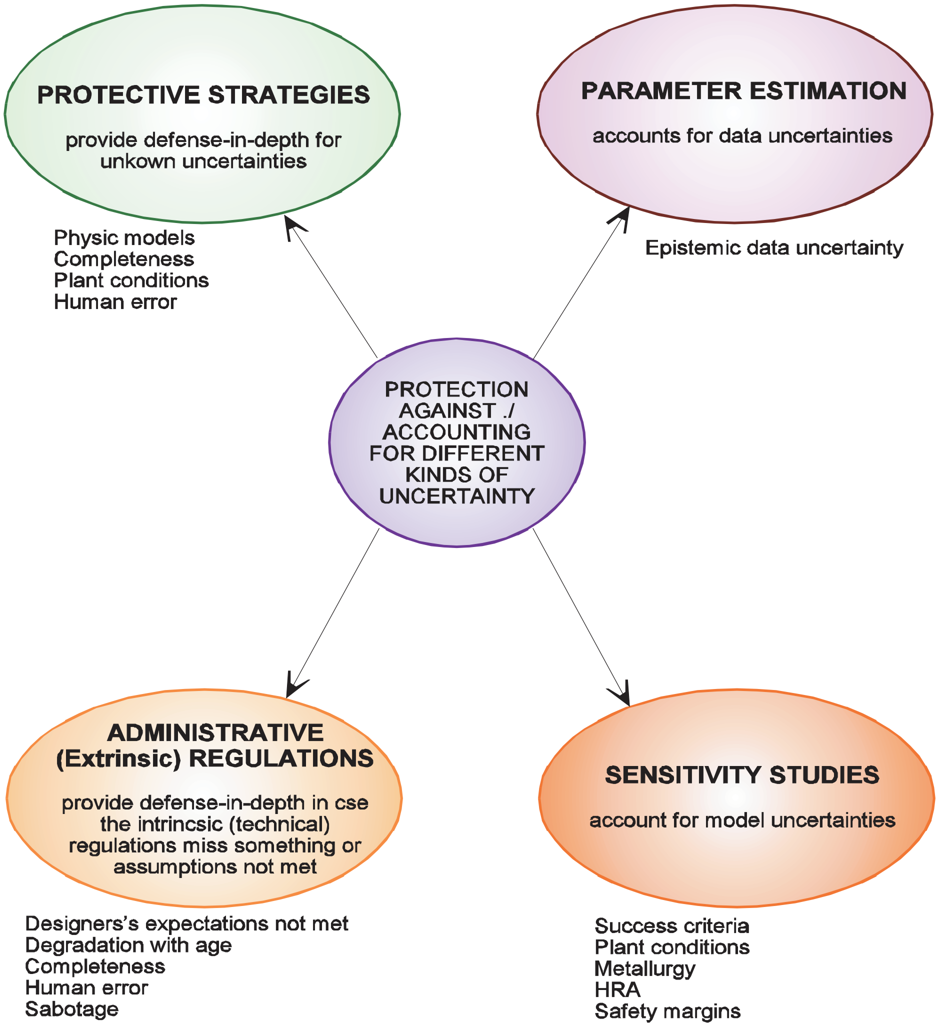

PROTECTIVE STRATEGIES
provide defense-in-depth for unkown uncertainties
Physic models
Completeness
Plant conditions
Human error
PARAMETER ESTIMATION
accounts for data uncertainties
Epistemic data uncertainty
PROTECTION AGAINST ./ ACCOUNTING FOR DIFFERENT KINDS OF UNCERTAINTY
ADMINISTRATIVE (Extrinsic) REGULATIONS
provide defense-in-depth in cse the intrincsic (technical) regulations miss something or assumptions not met
Designers's expectations not met
Degradation with age
Completeness
Human error
Sabotage
SENSITIVITY STUDIES
account for model uncertainties
Success criteria
Plant conditions
Metallurgy
HRA
Safety margins

Figure 5-3 Uncertainties Affecting Future Reactor Regulation and Means to Address Them

6. TECHNOLOGY-NEUTRAL REQUIREMENTS PROCESS DEVELOPMENT

The framework structure described in Chapters 2 through 5 define an overall set of safety objectives and criteria for a technology-neutral, risk-informed approach to new plant licensing. The next step is to identify and define the scope and content of detailed technical and administrative requirements that are necessary to ensure the safety objectives and criteria in Chapters 2 through 5 are met. After the scope and content of the technical and administrative requirements are identified, a check on their completeness also needs to be made. Discussed below are:

- identification of the scope and content of the detailed technical requirements necessary to ensure the overall safety objectives and criteria are met,

- identification of supporting administrative requirements, and

- verification of completeness.

6.1 Identification of the Scope and Content of Detailed Technical Requirements

Chapter 3 discussed a structure involving protective strategies whereby each protective strategy represents an important element of safety that, if accomplished, will ensure the design, construction and operation of the NPP results in achieving the overall safety objective. The protective strategies discussed in Chapter 3 are:

- physical protections,
- maintaining barrier integrity,
- limiting initiating events,
- protective system reliability, and
- accident management.

The process for identification of the scope and content of the detailed technical requirements was discussed in Chapter 3 and is shown in Figure 6-1.

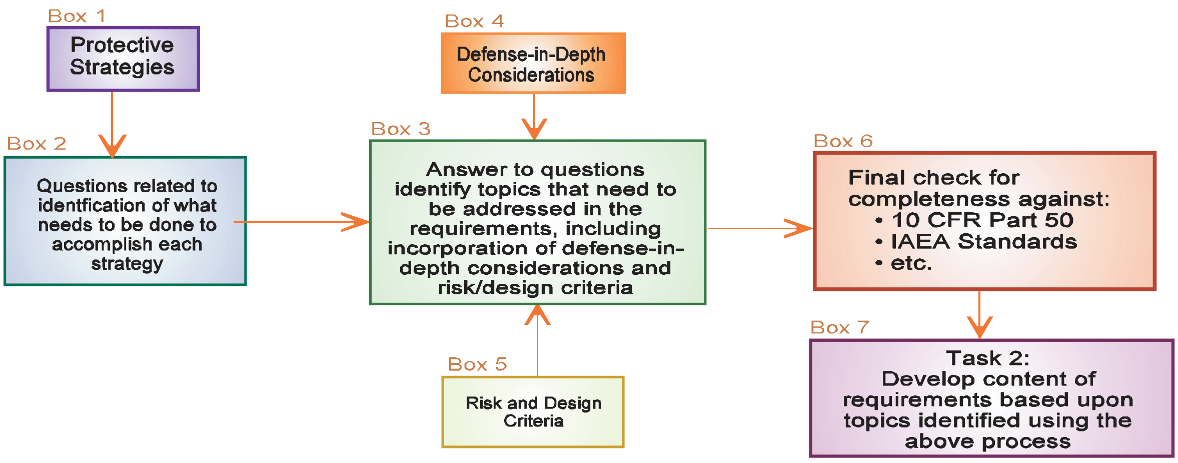

Box 1
Protective Strategies
Box 2
Questions related to identfication of what needs to be done to accomplish each strategy
Box 3
Answer to questions identify topics that need to be addressed in the requirements, including incorporation of defense-in-depth considerations and risk/design criteria
Box 4
Defense-in-Depth Considerations
Box 5
Risk and Design Criteria
Box 6
Final check for completeness against:
• 10 CFR Part 50
• IAEA Standards
• etc.
Box 7
Task 2:
Develop content of requirements based upon topics identified using the above process

Figure 6-1 Process for Identification of Topics to be Included in the Requirements

For each protective strategy (as illustrated by Box 1), a logic diagram is developed that identifies what would need to occur to threaten or challenge the Protective Strategy under construction. These logic diagrams 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. This process is then used to serve as a guide to identify what types of requirements need to be developed to guard against the root cause of failure, consistent with the overall safety philosophy and criteria discussed in Chapters 4 and 5.

Accordingly, the end point of each branch developed in the logic diagrams (i.e., “fault trees”) translates into a set of 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 is developed that form the basis for the requirements.

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

In developing the answers to each question, other issues will need to be considered (Boxes 4 and 5). The answers will need to be consistent with the defense-in-depth model (described in Chapter 5), the risk criteria (described in Chapter 4) and the design, construction and operation criteria, as applicable (described in Chapter 4).

Before finalizing the topics that need to be addressed by requirements, a final check for completeness will be made (Box 6). This check will be performed by comparing the developed list of topics against other references. One example is comparing against the requirements for advanced reactors developed by IAEA [ref.].

The last step of the process is the actual development of the technology-neutral requirements (Box 7). This step is performed under Part 2 of the regulatory structure.

6.1.1 Physical Protection

Physical protection is applied to all elements of plant design, including the other protective strategies, and involves both extrinsic protective measures ("guns, guard, and gates") to block access to attackers and intrinsic design features to minimize their possible success should they gain access.

LOGIC DIAGRAM AND TOPIC TABLE UNDER DEVELOPMENT

6.1.2 Barrier Integrity

Barrier integrity depends on design, construction and operation and, in some cases, on the success of protective systems. The logic diagram of Figure 6-x lays out the events that can lead to functional failure of the barriers. If at least one barrier remains, the public is protected and workers are given a measure of protection. Barrier integrity applies to those associated with the reactor as well as spent fuel storage. The order of analysis depends on the organizational scheme of the analyst, but, alternative approaches should yield the same results, i.e., the same cutsets (canonical sum of products in the language Boolean logic). The approach in Figure 6-x begins by partitioning the failure possibilities into three sets:

- Failure due to exceeding structural limits
- Bypass due to hardware or operational failure
- Breech due to an existing flaw

If any one of these occur, a barrier or the set of barriers will fail.

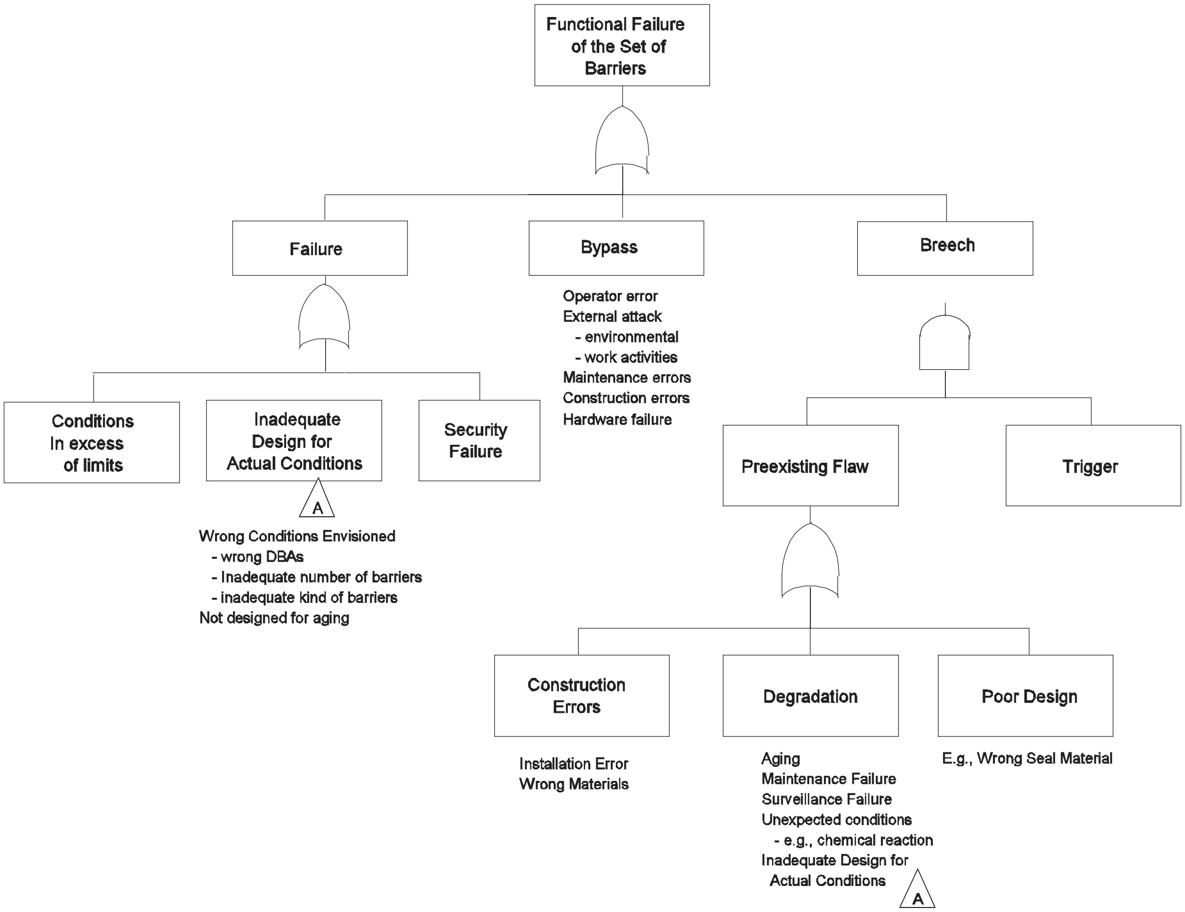


Figure 6-x Barrier Integrity Logic Diagram

Failure can occur because the design is inadequate for the actual conditions that occur. The lower level OR list is tagged by the letter "A" in the triangle. In other places in the logic of this or other trees, use of the triangle "transfer" gate with an "A" inside means that the same OR list applies. Failure can also occur by a failure of security, i.e., a loss of physical protection.

A bypass of the barrier can occur by operator error (e.g., leaving a purge valve open), external attack by environmental forces (e.g., earthquake, corrosion) or by work activities (say a crane failure), maintenance error or construction error. All these are shown as an OR list.

Breech due to an existing flaw requires both a preexisting flaw AND some "trigger" event that provides sufficient additional forces to breech the flaw (perhaps thermal or physical stress). The preexisting flaw may occur as a result of construction errors, degradation, or bad design. Example causes for each of these are provided in the given OR lists. Note that the trigger event must be considered conditionally on the extent of the preexisting flaw. Combinations of the bottom level events form the cutsets of the tree and in this simple logic it is easy to describe them: any one of the OR list events from the left half of the tree (failure or bypass) or any of the OR list events for preexisting flaws combined with suitable trigger events. These simple one and two element cutsets define the issues to be addressed by questions, the answers to which will identify the topics to be addressed in the technology-neutral requirements.

Table 6-x shows examples of a set of questions and answers associated with the Barrier Integrity protective strategy. The questions are organized by the top level branches of the logic diagram (i.e., failure, bypass, breech) and the answers (i.e., the topics which must be covered by the requirements) are arranged by whether they apply to design, construction or operation. Summarized below are the key considerations that went into developing the questions and their answers.

Table 6-x Barrier Integrity

Protective Strategy Questions	**Topics to be Addressed in the Requirements**		
	Design	**Construction**	**Operation**
Failure Prevention			
What barriers should be included in the design?	• fission product retention (in the fuel) • coolant retention (in the reactor and spent fuel cooling system) • Defense-in-depth independent capability		
To what conditions should the barriers be designed?	• Chapter 4 event selection criteria • Chapter 4 acceptance criteria (probabilistic and deterministic)		
How should barrier integrity and reliability be assured?	• quality assurance and control • materials qualification • use of accepted design codes	• quality assurance and control • testing • inspection • use of qualified construction methods	• maintenance • inspections • testing • inservice inspection • safety classification • technical specifications
How should barrier performance be confirmed?	• research and development • code validation	• testing	• testing
What security related measures should be provided?			

Table 6-x Barrier Integrity

Protective Strategy Questions	Topics to be Addressed in the Requirements		
	Design	Construction	Operation
Bypass Prevention			
How can barrier bypass be prevented?	• consider corrosion, erosion, aging in design	• quality assurance and control to ensure quality construction (e.g., use of correct materials)	• procedures • training • inservice inspection • testing • work control • maintenance
Flaw Prevention			
How can pre-existing flaws be prevented?	• design with qualified materials • consider corrosion, erosion, aging in design	• quality assurance and control • testing • inspection	• inspection • testing • inservice inspection • maintenance • corrective action

The questions range from what barriers need to be in the design to how should they be designed and similarly for construction and operation. Reliability, performance and risk are the key considerations for design. For normal operation, reliable barriers to retain the fission products in the reactor and reactor coolant in the coolant system are necessary to meet the low level s of radioactive material release specified for normal operation. To ensure reliable barriers, the barriers should be designed and built to accepted design codes using materials qualified for the intended service and accepted quality assurance measures.

For off-normal conditions, the event selection criteria discussed in Chapter 4 can be used to define the event scenarios which must be considered in designing the barriers. These criteria categorize event scenarios in to those that are expected to occur one or more times during the life of the plant (anticipated operational occurrences - AOOs), those that need to be considered for siting purposes (design basis accidents - DBAs) and those considered in assessing overall plant risk and emergency preparedness (beyond design basis accidents - BDBAs).

Deterministic acceptance criteria for AOOs and DBAs have been developed in Chapter 4. A criterion on overall plant risk (large release frequency) has also been developed in Chapter 4. To ensure the barriers perform as intended, they need to be qualified for the service conditions expected. This may involve research and development to verify fuel performance and equipment qualification (EQ) to verify the performance of mechanical items. Also, the analysis of barrier performance under normal and off-normal conditions will require safety analysis tools that also need to be validated against experimental data.

Depending upon the importance of the barriers to meeting the acceptance criteria, they may be assigned a safety classification (as described in Chapter 4) that will ensure their pedigree is maintained over the life of the plant.

Finally, as described in Chapter 4, the deterministic acceptance criteria for AOOs and DBAs ensure the barriers are designed such that two barriers to the release of radioactive material are always maintained for normal operation and AOOs, and that for DBAs, at least one barrier remains intact. As a final defense-in-depth provision, Chapter 5 discusses providing the capability to establish a controlled leakage barrier independent of the first two barriers in the event the first two barriers fail. This capability should be able to be established rapidly for designs where accident scenarios can progress rapidly. For designs with long accident scenario response time, this capability need not be established rapidly. The degree of controlled leakage will be technology and design dependent.

Potential failures related to construction are addressed by including topics such as quality assurance and quality control to ensure quality construction.

Potential failures related to operation are also addressed with topics such as human reliability, condition monitoring and monitoring and control of plant aging. The items shown in the table are standard practices for ensuring reliable operation and control of the plant condition.

6.1.3 Limit Frequency of Initiating Events

Initiating events occur when the operating design is not robust for the actual conditions that can occur or if the plant fails to continue steady-state operations as illustrated in Figure 6-x. The design may not be robust if it is inadequate for the actual conditions seen by the plant or if there is a failure of security.

LOGIC DIAGRAM AND TOPIC TABLE UNDER DEVELOPMENT

6.1.4 Protective Systems

The functional failure of a set of protective systems is investigated in the logic of Figure 6-x. In this logic diagram, the possible failures are partitioned into system failures and support failure. Support systems are those systems that provide needed services to the actual protective systems (e.g., I&C, electric power, and cooling). Note that the actual definition of protective system sets that must fail to lead to actual loss of protective function will depend on the details of final system design. For one system, actual system failure is further partitioned into fail-to-start and fail-to-run for equipment that is in standby or already operating respectively. Under either case there can be sudden failure or failure when degraded conditions are combined with a sufficient trigger (challenging condition).

LOGIC DIAGRAM AND TOPIC TABLE UNDER DEVELOPMENT

6.1.5 Accident Management

Accident management can fail due to either on-site or off-site failures as shown in Figure 6-x. On-site failures are associated with procedures, new hardware and software, training or design are sufficient to interfere with the planned control of operations. Off-site failures can be in areas monitored by NRC or those controlled by other agencies. For example, NRC is responsible for setting the EPZ and ensuring the licensee has plans for working with local emergency preparedness organizations and first responders.

LOGIC DIAGRAM AND TOPIC TABLE UNDER DEVELOPMENT

6.1.6 Summary

As can been seen in examining Tables 6-x thru 6-xx, many topics are included on more than one table. This duplication is because they have general applicability in many areas (e.g., QA) and, accordingly, are candidates to be written in general terms applicable across all the protective strategies. Accordingly, as a final step, the technical topics listed in Tables 6-x thru 6-xx have been consolidated (to eliminate duplication), arranged according to design, construction and operation and organized by key plant features and safety functions. The results are shown in Table 6-z.

TABLE Z UNDER DEVELOPMENT

6.2 Administrative Requirements

As discussed earlier in this document, the framework is to define the scope and content, and provide the overall technical basis for a new part to 10 CFR containing technology- neutral, risk-informed and performance-based requirements for new plant licensing which can serve as an alternative to 10 CFR 50. Accordingly, as an alternative to 10 CFR 50, the new part should address the administrative aspects of licensing using the new process, similar to the administrative aspects of 10 CFR 50, where possible, existing administrative requirements will be used. However, the administrative aspects of this new part will have some differences from those in 10 CFR 50 because of the technology-neutral, risk-informed and performance-based nature of the new part.

6.2.1 Technology-Neutral, Risk-Informed and Performance-Based Administrative Considerations

The administrative requirements associated with the technology-neutral, risk-informed and performance-based aspects of the new part must address the:

- analysis methods and qualification of those methods
- monitoring and feedback necessary to confirm key aspects of plant performance consistent with the safety analysis and compliance with performance-based requirements
- PRA scope and quality
- format and content of applications
- change control methods, including a requirement to maintain a living PRA and reflect updated PRA insights into the plant licensing basis
- reporting and record keeping

Each of these areas is discussed briefly below.

6.2.1.1 Analysis Methods and Qualification

To help ensure consistency in application of the technical requirements, a uniform approach for analysis is envisioned. Accordingly, in the development of administrative requirements associated with analysis methods, an approach that utilizes best estimate analysis methods with quantified uncertainties shall be used, as described below.

In the past, confidence in the analysis and safety margins was achieved by requiring conservative calculations to model plant performance during normal operation, as well as during postulated design basis accidents and other off-normal conditions, and by defining the acceptance criteria these calculations have to meet in a conservative manner. While this approach of conservative calculations and conservative acceptance criteria assures some confidence and margins in capability, it has drawbacks. From this way of proceeding it is not always clear what level of confidence or how large the resulting margins actually are. Also, the margins achieved in this manner can sometimes be larger than needed, thus imposing unnecessary burden on designers, operators, licensees, etc.

It is desirable to allocate the margins implemented in some reasonable fashion so that they are in proportion to the uncertainties being addressed. Therefore, establishing an estimate of the uncertainties is essential to determining the level of confidence and margins. A necessary first step in trying to estimate uncertainties is to have a baseline[*****] that represents the best estimate of the values of the important parameters of interest, and to investigate the impact of the distributions of these important parameters. Such a baseline is also valuable because it is an attempt to obtain a realistic estimate of the physical conditions and processes that one is designing for.

Some guidance on best-estimate calculations can be found in Regulatory Guide 1.157, entitled “Best-Estimate Calculations of Emergency Core Cooling Calculations.” As the title indicates, the main focus of this Reg Guide is on the features of acceptable thermal hydraulic best-estimate codes that can be used to calculate ECCS performance in accordance with paragraph 50.46(a)(i) of Title 10 of the Code of Federal Regulations. However, the Reg Guide also has some useful discussion on the regulatory position regarding best-estimate calculations in general.

A best-estimate calculation uses modeling that attempts to realistically describe the physical processes that can occur. A best-estimate model should provide a realistic calculation of the important parameters associated with a particular phenomenon to the degree practical with the currently available data and knowledge of the phenomenon. A key part of a best-estimate calculation is the quantification of the uncertainty associated with the calculation. The effects of all important variables should be considered. The model should be compared with applicable experimental data. It should strive to predict the mean of the data, rather than a bound or some other conservative estimate of the data.

Included in the uncertainties that need to be considered are both the stochastic, or aleatory, uncertainty as well as the so called state-of-knowledge, or epistemic, uncertainties. The stochastic uncertainty results from the inherent variability in measurable quantities of physical processes. The state-of-knowledge uncertainty includes parameter uncertainty, resulting from imperfect knowledge as to the correct inputs to the models used, model uncertainty, since perfect models cannot be created in practice, and completeness uncertainty, which involves uncertainty as to whether all important phenomena and relationships have been identified. This latter uncertainty is obviously most difficult to include in the overall uncertainty estimate. While reasonably sound technical estimates can often be made of the stochastic, parameter and model uncertainty, based on analysis and data from experience and tests, the completeness uncertainty usually cannot be quantified. One way the completeness uncertainty can be indirectly addressed is by additional conservatism in setting margins. Fifty years of experience with the current generation of light water reactors provides some assurance that by now completeness uncertainty should not be a large component of the overall uncertainty involved in calculations for current reactors. The same cannot

[*****] This baseline represents a most likely state of the system. Risk will also come from other states, although with less likely values of the parameters.

be said for the future reactors which involve designs for which little or no experience exists.

In carrying out the best-estimate calculations, it must also be demonstrated that the model used is applicable to the facility being modeled over the possible range of the parameters being calculated including accounting for plant lifetime. When comparing the model used in the best-estimate calculation to data, it should be ascertained what the applicability of the data is to the actual situation in the reactor being modeled. Correlations should not be extrapolated beyond the range over which they were developed or assessed. If a model has to be extrapolated beyond the conditions for which valid data comparisons exist, judgements should be made as to the effect of this extrapolation and the effect should be included in the uncertainty calculation. The uncertainty that results from extrapolation should be estimated using sensitivity calculations, as well as the fundamental laws of physics and any applicable well established data bases.

The above discussion applies to all safety analysis, whether done for the PRA or for analysis of anticipated operational occurrences and design basis accidents. In addition, the use of scenario specific source terms for siting determinations has been approved by the Commission for non-LWRs. As discussed in Section 4.3.1.4, these source terms should be based upon best estimate analysis (based upon experimental data) of the accident scenario and fission product/radioactive material release, with an uncertainty estimate. The results shall then be compared to the acceptance criteria for DBAs as described in Chapter 4.

6.2.1.2 Monitoring and Feedback

A program of monitoring and feedback should be required that will support the concept of a living PRA (discussed in Chapter 4 and Section 6.3.1.5) and will ensure performance-based requirements are properly implemented. The monitoring and feedback should be applied to key parameters and assumptions used in the safety analysis (including those related to defense-in-depth as well as all performance-based requirements, and address issues such as:

- how often to monitor
- documentation and reporting of the results
- corrective actions

6.2.1.3 PRA Scope and Quality

All applicants are responsible to meet the reporting, record keeping, and administrative controls requirements. Administrative controls are the provisions relating to organization and management, procedures, record keeping, review and audit, and reporting as necessary to assure operation of the facility in a safe manner. As an alternative to 10 CFR Part 50, the new part should address the administrative aspects of licensing using the new process similar to the record keeping of 10 CFR Part 50, where possible, existing requirements will be used. However, administrative part will be different from those in 10 CFR Part 50 because, the new part will be based on technology-neutral and risk-informed.

6.2.1.4 Format and Content of Applications

The requirements will need to specify what information should be supplied by an applicant. Issues that need to be addressed include:

- Will the entire PRA need to be submitted? If not, what information from the PRA should be part of the application?

- What level of design, construction and operational detail needs to be submitted?

- What supporting research and development information needs to be submitted?

6.2.1.5 Change Control

The requirements will need to address criteria for when licenses can make changes to the plant configuration or operation without NRC approval (e.g., 50.59 type process) and when NRC approval is required. Also, requirements for when changes in equipment performance and reliability need to be fed back into the PRA (i.e., living PRA) and when changes in PRA results require a change in the safety analysis, and possibly safety classification, plant configuration or operation, need to be developed. These need to be developed in consideration of 10 CFR Part 52 which certifies design via rulemaking and requires changes to the design to be made through rulemaking.

6.2.1.6 Reporting and Record Keeping

UNDER DEVELOPMENT

6.2.2 Research and Development

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

- fuel performance testing
- passive decay heat removal system testing
- reactor shutdown system testing

New plants may propose the use of a license-by-test approach, in lieu of conducting extensive research and development. The use of a license by test approach results primarily from the new technologies and reactor designs that could be proposed in the future (e.g., HTGRs, modular reactor designs), whereby one module could be built and used to demonstrate the safety of the design in lieu of a series of separate research and development efforts. If a licence-by-test approach is to be accepted requirements need to be developed that address:

- What would be the objective of the test program:
  - Which aspects of plant safety can be addressed by demonstration plant testing?
  - which types of analytical tools could be validated?
  - what phenomena could be addressed?

- What would be the scope of the test program:
  - How would the test program be selected?
  - Would it be conducted during initial startup only?
  - How will plant aging, irradiation, burnup effects be tested?
  - Will tests cover the full range of the accidents or only partial ranges, with the remainder

done by analysis?
- What instrumentation will be required?

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

- How would equipment reliability assumptions be verified?

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

- Would there be any limitations on future design changes?

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

Also, documentation that would be necessary to apply for a license-by-test and the documentation for the test program results needs to be specified.

6.2.3 Other Areas

Other administrative areas that need to be addressed, not related to a specific technology or a risk-informed approach, will be similar to those in 10 CFR 50 and include:

- document control
- exemptions
- license amendments
- environmental conditions
- backfitting
- enforcement

Table 6-zz provides examples of topics that should be addressed by the administrative requirements.

Table 6-zz Administrative Topics

- Format and Content of Applications
  - Design information
  - Risk information
- PRA Scope and Quality
  - Standards
  - Living PRA
- Analysis Methods/Criteria
  - Best estimate/realistic
  - Use of mean values
  - Level of confidence
  - Source term
  - Acceptance criteria
- Change Control
  - How often risk info should be updated
  - What to do with updated information
  - What changes need NRC approval
  - Relation of changes to design certification
- Monitoring and Feedback
- Reporting and Record Keeping
- Research and Development
  - Design confirmation
  - License-by-test
- License Amendments
- Exemptions
- Environmental Monitoring
- Backfitting
- Enforcement

6.3 Framework Verification and Completeness

Although the framework was developed in a top down, systematic fashion a check was made to see if the desired characteristics listed in Section 1.4 were achieved and if the document is complete and practical.

6.3.1 Desired Characteristics

The characteristics desired of the framework are:

- ***Reproducible, traceable, and understandable***. The technical bases for the criteria and guidance developed as part of this approach are clearly articulated, and therefore, each step of the process is identified and clearly described.

- ***Defensible***. The technical bases developed are derived from known technology where the assumptions and approximations and their impacts are known and understood. In particular, the technical bases are consistent with the Commission's Safety Goal Policy.

- ***Flexible***. The guidance and criteria will be technology-neutral such that they allow, in an efficient and effective manner, for changes and modifications to occur that are based on new information, knowledge, etc., and can be adapted to any technology-specific reactor design.

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

- ***Completeness.*** The guidance and criteria will produce the topics for which a set of safety requirements are needed to meet the mission of protecting the public health and safety, and that will cover design, construction and operation and that address the public, worker and environment.

- ***Uncertainty***. The guidance and criteria have to address the uncertainties.

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

- ***Consistency.*** The guidance and criteria need to address and implement the policy issues approved by the Commission in its June 26, 2003 SRM. In addition, the guidance and criteria need to be compatible with other applicable parts of 10 CFR (e.g., Part 100, Part 20, etc.).

6.3.2 Verification of Completeness

A systematic approach was applied to identify the subject matter that the technical requirements would need to address to assure the overall safety objective is met. To check the completeness of the output of the systematic approach, several checks against other documents were made.

As a check on the completeness of the framework, the list of topics identified in Section 6.1 and 6.2 are to be compared to the following documents:

- 10 CFR Part 50 and its Standard Review Plan
- IAEA Safety Standard Series NS-R-1 “Safety of Nuclear Power Plants: Design”
- INSAG-12

This comparison will identify what items in the above documents are included in the framework, which ones are not (and why) and where the framework included potential requirements not in any of the above documents (and why).

The results of the comparison of the framework against the requirements in these documents is discussed in Appendix F.

6.3.3 Practicality

Application of the framework to an actual future reactor design will be tested to see if the criteria proposed can be practically applied and if they are reasonable with respect to the safety attributes of the future designs. The reactor design to be used in this test is the Very High Temperature Reactor (VHTR) being developed by the Department of Energy at the Idaho National Engineering and Environmental Laboratory.

The VHTR comparison will be conducted jointly with DOE (and its contractor INEEL).

As a final test of practicality, a comparison against existing LWR designs will be conducted. This comparison will have two purposes. The first will be to see how well existing LWRs meet the proposed criteria. The second will be to see how well the framework addresses and prevents previously identified LWR issues such as:

- MK-I containment melt thru
- containment strength

- direct containment heating

REFERENCES

4-1 NCRP 64: Influence of Dose and Its Distribution in Time on Dose-Response Relationships for Low-LET Radiations (1980)

4-2 ICRP 41: Non-stochastic effects of ionizing radiation, 1984

4-3 UNSCEAR 1988: Early effects in man of high doses of radiation, United nations Scientific Committee on the Effects of Atomic Radiation, Annex G, 1988

4-4 US NRC, NUREG/CR-4214, Health Effects Models for Nuclear Power Plant Consequence Analysis: Low LET Radiation, 1989

4-5 NUREG/CR-6613, Code manual for MACCS2, 1998

1-1. Commission's Policy Statement on the Regulation of Advanced Nuclear Power Plants, 59 FR 35461, July 12, 1994

1-2.

1-3. Commission's Policy Statement on the Regulation of Advanced Nuclear Power Plants, 59 FR 35461, July 12, 1994

1-4.need John/Vinode old three-region footnote [11]

1-5. ”NRC Reactor Oversight Process,” NUREG-1649, Rev. 3, U.S. Nuclear Regulatory Commission, July 2000.

1-6. NCRP 64: Influence of Dose and Its Distribution in Time on Dose-Response Relationships for Low-LET Radiations (1980)