Attachment 1

FRAMEWORK FOR RISK-INFORMING THE TECHNICAL REQUIREMENTS OF 10 CFR 50

Draft, Revision 0

Prepared by
Office of Nuclear Regulatory Research
Division of Risk Analysis and Applications
Probabilistic Risk Analysis Branch

Mary Drouin
Alan Kuritzky

Sandia National Laboratories
Allen Camp
Jeff LaChance

ERI Consulting
Eric Haskin

Brookhaven National Laboratory
John Lehner
Vinod Mubayi
Chuen-Ching Lin
Trevor Pratt

April 2000

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

FRAMEWORK FOR RISK-INFORMING 10 CFR 50

1.0 INTRODUCTION

In any planned human endeavor it is essential to set forth goals and to develop and implement appropriate strategies and tactics. This suggests that the top-down hierarchy depicted in Figure 1-1 be used to develop a framework for risk-informing the regulations contained in Title 10 Parts 50 and 100 of the code of federal regulations (CFR). The depicted hierarchy is followed in this document. The framework that is developed herein will be used to guide the study proposed as Option 3 of SECY-98-300 (Ref. 1). The Option 3 study will review existing regulatory requirements, identify and prioritize candidates for risk-informed change, formulate and evaluate change options, and recommend specific changes. Guidance provided by the framework is expected to result in risk-informed regulatory requirements that support the objectives outlined in SECY-98-300, including the desire to reduce burden without compromising safety.

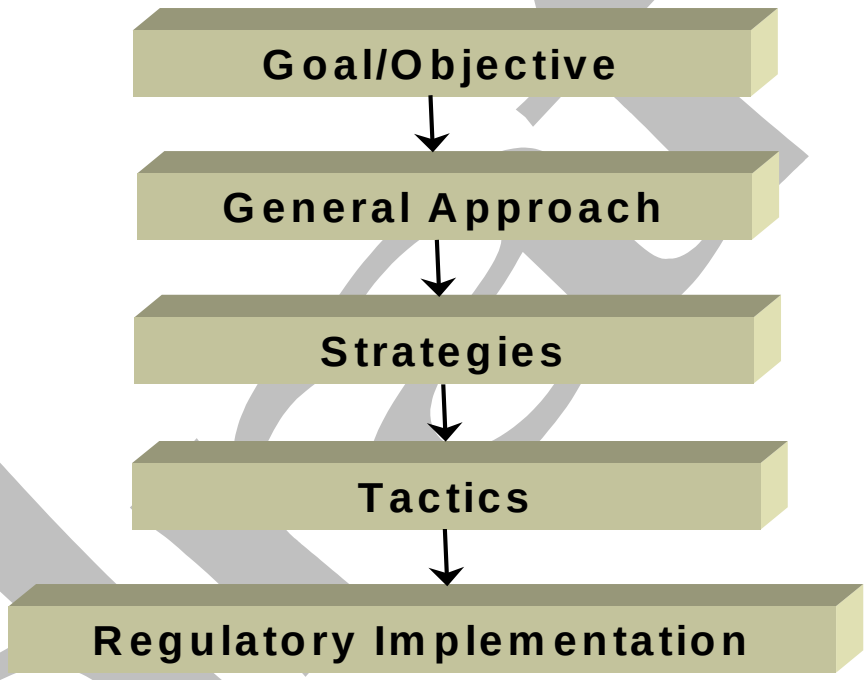


Figure 1-1. Framework Hierarchy.

An expanded representation of the framework is provided in Figure 1-2. The structure and elements are generally consistent with the regulatory philosophy that has evolved in the U.S. since the passage of the Atomic Energy Act. The goal is protection of the public health and safety. A balanced high-level defense-in-depth approach is proposed to achieve that goal. The approach is consistent with the cornerstones of safe nuclear power operation established during the development of risk-informed improvements to the Nuclear Regulatory Commission (NRC) Reactor Inspection and Oversight Program. The focus of the framework is on those cornerstones that defend against core damage accidents, because these accidents dominate public risk.

The term risk, as used herein, refers to risk as quantified in full-scope probabilistic risk assessments (PRAs). Full scope PRAs address

internal and external initiating events, as well as accidents initiated in any operating mode. Frequencies are, accordingly, stated per calender year rather than per year of reactor operation.

A top-down discussion of the framework depicted in Figure 1-2 is provided in the next section. The goal, approach, and strategies are developed, and examples of supporting tactics and regulatory documents are provided. The framework is then extended to include quantitative objectives and guidelines for risk informing existing technical requirements. Compatible criteria for identifying and prioritizing existing requirements that are candidates for change are discussed in Section 5.

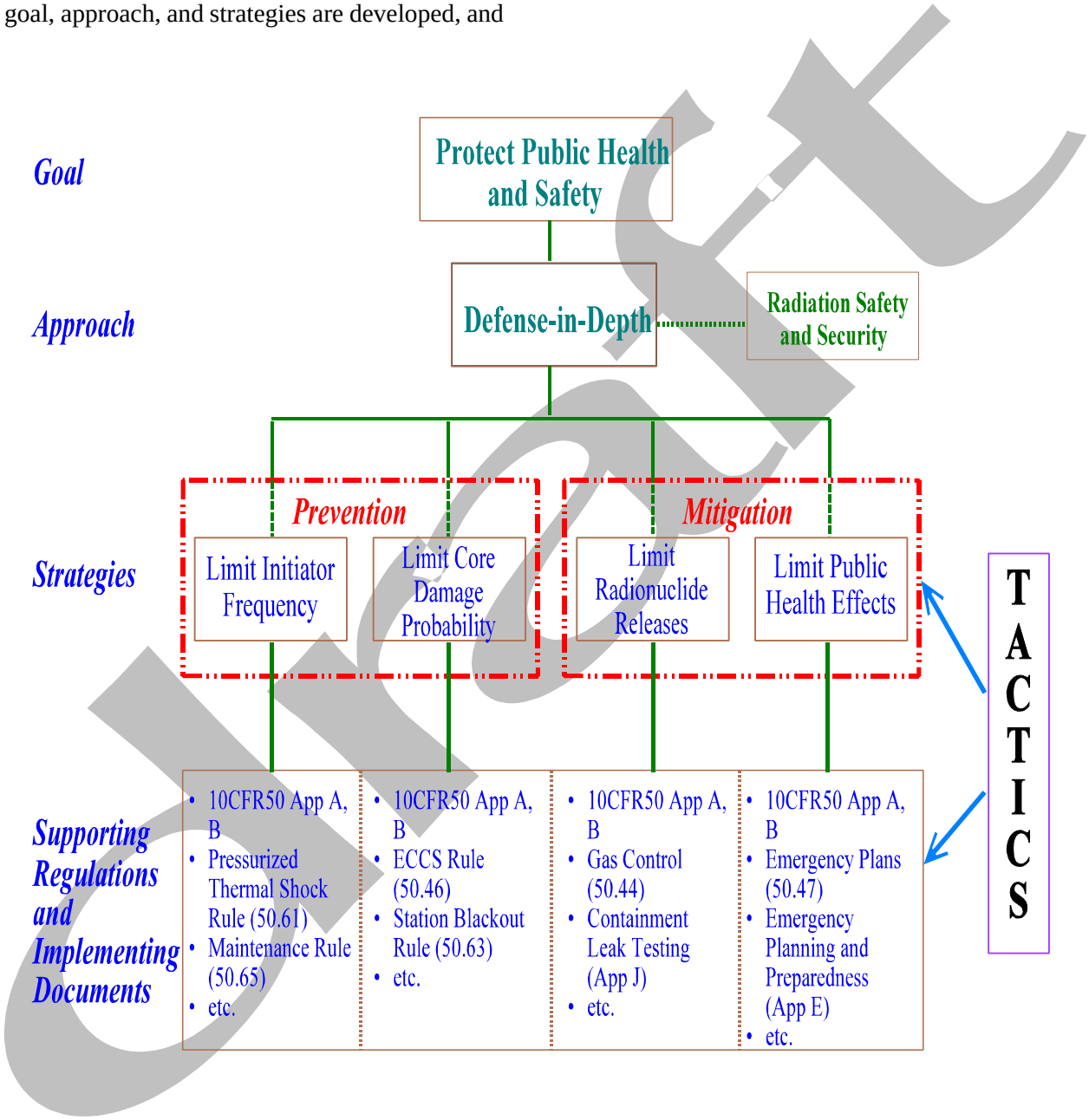


Figure 1-2. Top Down Development of the Framework

2.0TOP-DOWN DEVELOPMENT OF THE FRAMEWORK

2.1 Goal: Protect Public Health and Safety

Section 182(a) of the Atomic Energy Act requires the NRC to ensure that nuclear power plant operation provides adequate protection to the health and safety of the public. In its rules and decisions the Commission refers to this standard as either the "adequate protection" or the "no undue risk" standard. The interchangeable use of these two terms has been accepted in legal decisions. Whether risk-informed or not, the principal goal of nuclear power plant regulations is to protect the public health and safety.

The Commission has stated on many occasions that compliance with the NRC regulations "should provide a level of safety sufficient for adequate protection of the public health and safety and common defense and security under the Atomic Energy Act" (Ref. 2). However, adequate protection of the public health and safety is only presumptively assured by compliance with regulations and other license requirements. New information may reveal a significant unforeseen hazard, a substantially greater potential for a known hazard, or insufficient margins and backup capability. Continuous vigilance and engineering judgment must, therefore, be applied.

The possibility of developing a generally applicable definition of the level of protection required by the Atomic Energy Act has been discussed extensively (Ref. 1). It is correct to say that protection of the public health and safety does not require zero risk, that it does not permit undue risk, and that it involves both long-term and short-term considerations. These statements, however, do not eliminate the need for engineering judgement or provide a standard for its application in determining the required level of protection of public health and safety.

The NRC has established safety goals including quantitative health objectives that state the Commission's expectations with respect to how safe is safe enough. Although licensees are not required to demonstrate that they meet the quantitative goals, comparisons of PRA and Individual Plant Examination (IPE) results to the goals are common. Given the state of the art of quantitative risk assessment, however, it is not reasonable to expect that the NRC will make decisions based wholly on quantitative risk estimates. That would represent a risk-based rather than risk-informed approach.

It is proposed in this document that quantitative objectives be used to provide guidelines for risk-informing existing regulations. The intent is to develop risk-informed regulations, which retain deterministic characteristics, in such a way that compliance provides reasonable assurance that the public health and safety is protected. However, quantitative objectives would not generally appear in specific regulations.

2.2 Defense-in-Depth Approach

The term defense-in-depth is used to describe applications of multiple measures to prevent or mitigate accidents. The measures applied can be embodied in structures, systems, and components (SSCs) or in procedures (including emergency plans). Defense-in-depth can be applied at various levels. Redundant or diverse means may be used to accomplish a function, the classic example being the use of multiple barriers (fuel, cladding, reactor coolant pressure boundary, spray or scrubbing systems, and containment) to limit the release of core radionuclides. Alternatively, as discussed in this section, redundant or diverse functions may be used to accomplish the higher goal of protecting the public from nuclear power plant accidents.

Defense-in-depth has evolved since the first research reactors were designed in the 1940s. In a recent letter to the NRC Chairman, the Advisory Committee on Reactor Safeguards (ACRS) discusses this evolution, identifies two schools of thought on the scope and nature of defense-in-depth, and recommends an approach for moving forward with risk-informed regulation (Ref. 3),(Ref. 4). The two schools of thought (models) of defense-in-depth are labeled "structuralist" and

"rationalist," but they could just as well be labeled "traditionalist" and "risk-based."

The structuralist or traditionalist model asserts that defense-in-depth is embodied in the structure of the regulations and in the design of the facilities built to comply with those regulations. The requirements for defense-in-depth are derived by repeated application of the question, "What if this barrier or safety feature fails?" The results of that process are documented in the regulations themselves, specifically in Title 10 of the Code of Federal Regulations.

It is also a characteristic of the structuralist model that balance must be preserved among the high-level lines of defense. Accidents resulting in the release of radionuclides from the reactor core are risk-dominant. The first line of defense is, therefore, to eliminate initiators that could conceivably lead to core damage. However, it is not possible to eliminate all initiators. The frequency of initiators, although significantly less than before the accident at Three Mile Island Unit 2 (TMI-2), is about 1 per plant year. As a second line of defense, systems such as the Emergency Core Cooling System (ECCS) are required to prevent core damage given postulated initiators. Although such systems are designed for a wide spectrum of initiators and compounding equipment failures, no prevention system is perfect. As a third line of defense, barriers including containment and associated heat and fission product removal systems are required. These barriers would be effective in preventing large radionuclide releases for many severe accidents, but scenarios exist in which containment would be breached or bypassed. A fourth line of defense, offsite emergency preparedness, is therefore required.

In contrast, the rationalist (or risk-based) model asserts that defense-in-depth is the aggregate of provisions made to compensate for uncertainty and incompleteness in our knowledge of accident initiation and progression. This is made practical by the ability to quantify risk and estimate uncertainty using PRA methods. The process envisioned by the rationalist is: (1) establish quantitative safety goals, such as the quantitative health objectives (QHOs), the core damage frequency (CDF) goal, and the large early release frequency (LERF) goal, (2) analyze the plant using PRA methods to establish that the safety goals are met, and (3) evaluate the uncertainties in the analysis, especially those due to model incompleteness, and determine what steps should be taken to compensate for the uncertainties.

What distinguishes the rationalist model from the structuralist model is the degree to which the rationalist model depends on establishing quantitative safety goals and carrying formal probabilistic analyses, including analyses of uncertainties, as far as the analytical methodology permits. The exercise of engineering judgement, to determine the kind and extent of defense in depth measures, occurs after the capabilities of the analyses have been exhausted.

The approach recommended by the ACRS and adopted herein is a structuralist high-level defense-in-depth approach which applies four strategies (functional lines of defense) to protect the public from core damage accidents. Emphasizing defense against core damage accidents is risk informed because public risk posed by core damage accidents far exceeds that posed by other accidents. As a working definition, for use in this study, *defense-in-depth is assessed by the application of the following strategies to protect the public:*

1. *limit the frequency of accident initiating events (initiators)*
2. *limit the probability of core damage given accident initiation*
3. *limit radionuclide releases during core damage accidents*
4. *limit public health effects due to core damage accidents*

In implementing the high-level defense-in-depth approach, both deterministic and probabilistic considerations are applied to preserve a reasonable balance between the four strategies and maintain the integrity of barriers. Probabilistic considerations and reasonable balance are discussed in Section 3. For risk significant accidents in which one or more of the high-level strategies are precluded (e.g., containment bypass accidents), the remaining

strategies may be more tightly regulated; that is, regulations should provide a very high confidence in the remaining strategies. Similarly, more stringent requirements may be imposed in the presence of large uncertainties regarding the effectiveness of one of the strategies. The treatment of uncertainties is discussed in Section 4.

In applying the strategies, good engineering practices will be maintained. The General Design Criteria (GDCs) provide many concise statements of good engineering practice. For example, negative prompt feedback, emergency AC power, residual heat removal, emergency core cooling, and containment are all called for in the GDCs and deemed essential to the defense-in-depth approach. Requirements that fuel design limits not be exceeded in anticipated operational occurrences and that the extent of fuel damage be limited in design basis accidents (DBAs) will be maintained. Although not a GDC, emergency planning will also be maintained to support the fourth strategy. Risk-informed changes to GDCs are not precluded. For example, it has been suggested that a number of regulatory requirements related to fuel design limits during normal operation could be eliminated because the intent of GDC-10 is being met for commercial reasons, and the requirements are not risk significant. Also, the risk significance of failure events delineated in the GDCs will be evaluated based on PRA results.

2.3 Strategies

In the process of developing risk-informed improvements to the NRC Reactor Inspection and Oversight Program (Ref. 5), general agreement was reached with the nuclear industry and the public regarding the following cornerstones of safe nuclear power plant operations:

Reactor Safety Cornerstones

1. Initiating Events — Minimizing events that could lead to an accident
2. Mitigation Systems — Assure the ability of safety systems to respond to and lessen the severity of an accident
3. Barrier Integrity — Maintain barriers to the release of radioactivity in an accident
4. Emergency Preparedness — Plans by the utility and governmental agencies to shelter or evacuate people in the community in the event of a severe accident

Radiation Safety Cornerstones

5. Plant Worker — Minimize exposure during routine operations
6. General Public — Provide adequate protection during routine operations

Security Cornerstone

7. Physical protection of plant and nuclear fuel

The four reactor safety cornerstones are directly addressed in PRAs and are, therefore, most relevant to the Option 3 study. As illustrated in Figure 2-1, the four reactor safety cornerstones are reflected in the framework by the four high-level defense-in-depth strategies. The strategies seek both to prevent core damage accidents and to mitigate the public impact should a core damage accident occur. The two preventive strategies are:

1. limit the frequency of accident initiating events (initiators), and
2. limit the probability of core damage given accident initiation.

The two mitigative strategies are:

3. limit radionuclide releases during core damage accidents, and
4. limit public health effects due to core damage accidents.

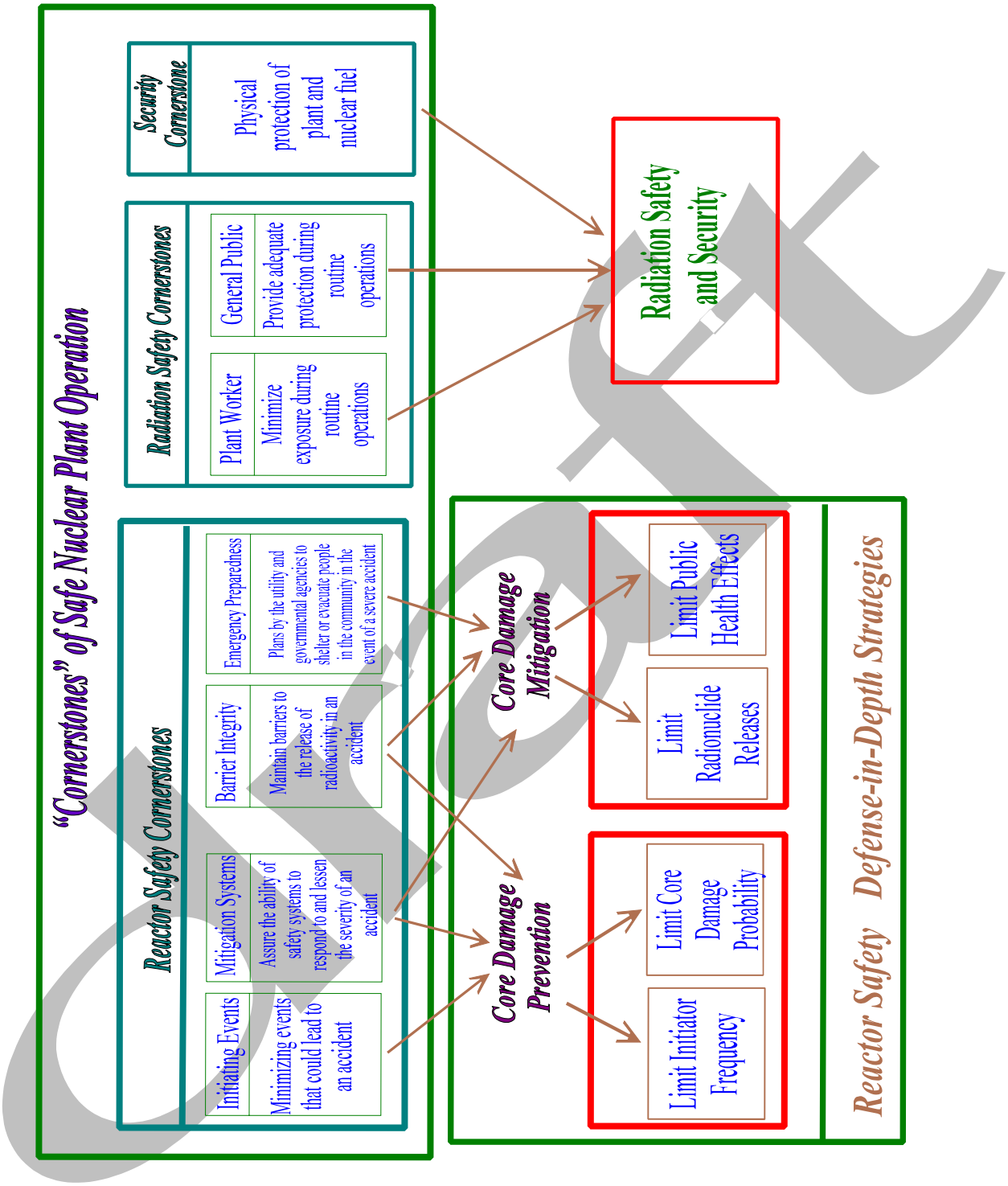


Figure 2-1. Translation from "Cornerstone" Language to "PRA/Risk-Informing" Language

Except for the implied emphasis on core damage accidents, Strategy 1 is identical to Reactor Safety Cornerstone 1. Similarly, for core damage accidents, Strategy 4 is equivalent to Reactor Safety Cornerstone 4, and Strategies 2 and 3 are functionally equivalent to Reactor Safety Cornerstones 2 and 3.

The four high-level defense-in-depth strategies are intentionally more focused than the reactor safety cornerstones. The cornerstones also apply to accidents that can not lead to core damage (for example fuel-handling, fuel-storage, and radwaste storage tank rupture accidents). The strategy statements could easily be modified to match the reactor safety cornerstones; however, the emphasis on core damage accidents provides appropriate focus for the bulk of the effort to risk-inform existing regulatory requirements.

As indicated by the box on the right in the second row of Figure 1-2, items addressed in the cornerstones but not reflected in the high-level defense-in-depth strategies are not excluded from consideration in the framework. For example, the radiation safety and security cornerstones are part of the overall approach, but generally secondary considerations in risk-informing existing regulatory requirements. This is because they are not well-treated in probabilistic risk assessments.

In describing the cornerstones and strategies, the words "limit," "prevent," and "contain" are relative rather than absolute. Cutting a failure rate in half "prevents" half the failures that would otherwise occur in a given time period, and some fixes last for the life of a plant. However, it is not possible to prevent all accident initiators or to eliminate the possibility of core damage or containment failure for all conceivable accidents. The use of all four strategies constitutes a high-level, defense-in-depth approach, which compensates for the limitations of the individual strategies.

This document develops and advocates the use of an extended framework to guide the risk-informing process. The development of the extended framework begins with Section 3.

2.4 Tactics and Supporting Regulatory Requirements

Various tactics are applied to support the four high-level strategies, and existing regulatory requirements deal with the implementation of such tactics. Some requirements deal with specific strategies or accident types. Other regulations deal with broadly applicable tactics. For example, 10 CFR 50 Appendix B deals with Quality Assurance. Table 2-1 provides a partial list of tactics, divides the tactics into five broad categories, and cites examples of regulations and regulatory documents related to the listed tactics. Table 2-1 does not represent a complete list of tactics, and listing a tactic in Table 2-1 does not imply that it necessarily needs to be regulated. Assessing which, if any, tactics are required to support a given regulation is part of the Option 3 study. The primary responsibility for implementing tactics, whether required by regulations or not, resides with the licensee.

The defense-in-depth approach adopted herein uses <u>safety margin as a tactic</u> to account for uncertainties encountered in supporting the four high-level strategies. This is discussed in Section 4.

The single failure criterion is a tactic which the Nuclear Regulatory Commission has specifically asked the Option 3 study to address. Specifically, "the conditions under which a single failure of a passive component in a fluid system should be considered in designing the system" have yet to be developed (10 CFR 50 Appendix A). Insights from probabilistic risk assessments regarding the risk significance of passive single failures in fluid systems will be reviewed, and options for resolving this issue will be delineated consistent with the quantitative objectives developed in Section 3.

Table 2-1. Tactics and Examples of Related Regulatory Documents

Tactic	Examples of Related Regulatory Documents
DESIGN & ANALYSIS	
Design Basis Events	RG 1.70 & SRPs, Ch. 15
Acceptance Criteria and Safety Margin	SRP Acceptance Criteria
Design Criteria and Standards	Pt.50 App.A General Design Criteria (GDCs)
Single Failure Criteria	Pt.50 App A
Redundancy	GDCs 34, 35, 41, 44, 55
Diversity	GDCs 17, 55
Separation Criteria	GDC 24
Automation	GDC 20
Multiple Fission-Product Barriers	Pt.50 App.A Section II
Safety Analysis Reports	RG 1.70, SRPs
PRAs, IPEs	RG 1.174
Safety Goals	Safety Goal Policy Statement
Provide Emergency Response Facilities	50.47
PLANNING, PROCEDURES	
Operating Procedures	
Technical Specifications	50.36, RG 1.70 & SRP Ch.16
Severe Accident Guidelines	Generic Letter 88-20 Supplement 3
Maintenance Plans and Procedures	50.61
Inspection Plans and Procedures	NRC Inspection Manual
Testing Plans and Procedures	Appendix J
Emergency Plans	50.47
PERSONNEL TRAINING & TESTING	
Operator Training and Licensing	10 CFR Part 55
Fitness for Duty Program	10 CFR Part 26
Emergency Planning Drills	50.47
SPECIAL TREATMENT (Non-Scope)	
Design Considerations	50.55a, see DESIGN & ANALYSIS above
Qualification	50.49
Change Control	50.59
Documentation	50.34, 50.71
Reporting	50.71, 50.72, 50.73
Maintenance	50.65
Testing	GDCs 37, 40, 43, 46, Appendix J
Surveillance	50.61, GDCs 18, 32, 36, 39, 42, 45
Quality Assurance	GDC 1, Pt.50 App.B

3.0 QUANTITATIVE OBJECTIVES FOR THE FRAMEWORK

Established quantitative health objectives (QHOs) and related subsidiary quantitative objectives will be used to guide the development of risk-informed regulatory requirements. The intent is to develop requirements, which retain deterministic characteristics, in such a way that compliance will provide reasonable assurance of meeting the principal goal of protecting public health and safety. The quantitative objectives provide risk-informed guidance for the establishment of practical and enforceable regulatory requirements. They do not represent acceptance criteria and will not generally appear in risk-informed regulations.

To delineate quantitative objectives, the high-level strategies of the framework must be expressed using quantifiable measures of risk. One method of assessing the level of protection against accidents at a given nuclear power plant is to simply compare PRA results to the QHOs defined in the Safety Goal Policy Statement (Ref. 6):

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

These QHOs have been translated into two numerical objectives, as follows:

- The individual risk of a prompt fatality from all "other accidents to which members of the U.S. population are generally exposed," such as fatal automobile accident, etc., is about $5x10^{-4}$ per year. One-tenth of one percent of this figure implies that the individual risk of prompt fatality from a reactor accident should be less than $5x10^{-7}$ per reactor year (ry). The "vicinity" of a nuclear power plant is understood to be a distance extending to 1 mile from the reactor. The "average" individual risk is determined by dividing the number of prompt or early fatalities (societal risk) to 1 mile due to all accidents, weighted by the frequency of each accident, by the total population to 1 mile and summing over all accidents.

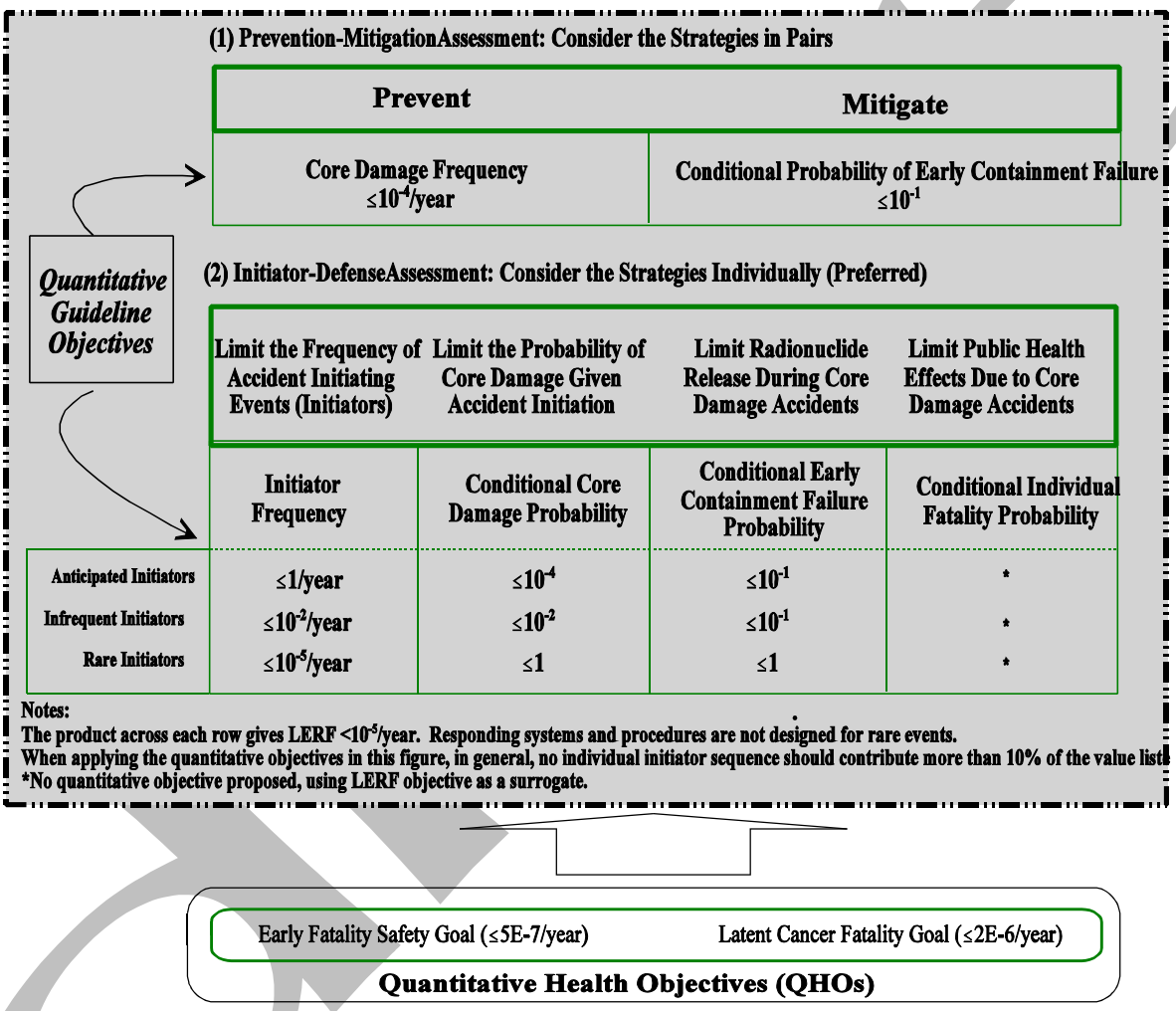
- "The sum of cancer fatality risks resulting from all other causes" is taken to be the cancer fatality rate in the U.S. which is about 1 in 500 or $2x10^{-3}$ per year. One-tenth of one percent of this implies that the risk of cancer to the population in the area near a nuclear power plant due to its operation should be limited to $2x10^{-6}$/ry. The "area" is understood to be an annulus of 10-mile radius centered on the plant. The cancer risk is also determined on the basis of an "average individual," i.e., by evaluating the number of latent cancers (societal risk) due to all accidents to a distance of 10 miles from the plant, weighted by the frequency of the accident, dividing the total population to 10 miles, and summing over all accidents.

As discussed in Section 4, the QHOs and related subsidiary quantitative objectives set forth in this section apply to mean risk measures quantified in full scope PRAs. Unfortunately, the QHOs are difficult to apply in risk-informing existing regulations. Simply replacing existing regulations with the QHOs would be an entirely risk-based approach, which would not assure defense-in-depth against limitations and uncertainties inherent in PRA.

Public risks are dominated by accidents that involve core damage and containment failure. Accordingly, subsidiary quantitative objectives based on risk measures related to the four high-

level defense-in-depth strategies are developed in the following subsections. The subsidiary quantitative objectives are developed from the QHOs, and are generally consistent with subsidiary goals in current use (e.g., (Ref. 7)(Ref. 8)). A context for the development and a summary of the quantitative objectives is provided below and in Figure 3-1, which illustrates two methods of quantitatively assessing the level of protection against accidents at a given nuclear power plant.

Figure 3-1. Quantitative Objectives for Risk-Informing Regulatory Requirements



(1) The <u>prevention-mitigation method</u> assesses the impact of the two preventive strategies and that of the two mitigative strategies. The quantitative objectives are:

- the core damage frequency should be less than 10^{-4}/year, and
- the probability of early containment failure (breach or bypass) given a core damage accident should be less than 0.1.

If both of these goals are met, the large early release frequency (LERF) will be less than 10^{-5}/year.

(2) The <u>initiator-defense method</u> assesses the impact of each of the four strategies. In this

method, as discussed later, initiators are classified as anticipated, infrequent, or rare. The quantitative objectives for this method depend on the initiator type:

- The combined frequency of all anticipated initiators should be less than 1/year, the combined frequency of all infrequent initiators should be less than 10^{-2}/year, and the combined frequency of all rare initiators should be less than 10^{-5}/year.
- The probability of core damage should be less than 10^{-4} given an anticipated initiator, and less than 10^{-2} given an infrequent initiator.
- The probability of early containment failure or bypass in a core damage accident with an anticipated or infrequent initiator should be less than 0.1.
- No quantitative objective is proposed for conditional individual fatality probability because existing PRAs demonstrate that the QHOs can generally be met with the preceding three quantitative objectives. However, offsite protective actions are essential to protect the public.

While reading the discussions of the two methods in the following subsections, it is important to keep the following things in mind:

- The assessment methods are not mutually exclusive nor will they address all of the issues that will be encountered in risk-informing existing regulatory requirements.
- The quantification of risk measures to assess the effectiveness of high-level defense-in-depth strategies does not translate into regulatory requirements directly (i.e., it does not lead to a risk-based approach). Rather, the quantitative objectives in Figure 3-1 provide guidance to the developers of risk-informed regulations, helping to establish the intent of those regulations.
- The appropriate PRA results to compare to the quantitative objectives are mean values. The concept of mean values is discussed in Section 4, which deals with uncertainties.

3.1 Prevention-Mitigation Assessment, Consider the Four Strategies in Pairs

A prevention-mitigation assessment examines the effectiveness of the two preventive strategies and that of the two mitigative strategies. A plant's estimated (mean) core damage frequency (CDF) is compared to the quantitative objective of 10^{-4}/year, and the conditional probability of early containment failure given a core damage accident is compared to the quantitative objective of 10^{-1}. Based on existing PRAs the proposed quantitative objectives provide a reasonable balance between the preventive and mitigative strategies. It would not be prudent to simply replace existing regulations with the quantitative objectives. However, compliance with risk-informed regulations should provide reasonable assurance that the proposed quantitative objectives are met.

The early fatality safety goal is generally more limiting than the latent cancer safety goal. In fact, if the core damage frequency objective of 10^{-4} per year is met, the latent cancer safety goal is usually met. The early fatality safety goal has, therefore, been chosen as the basis for the subsidiary quantitative objectives in Figure 3-1. This does not imply that latent-cancer or environmental-contamination risks associated with late containment failure can or will be ignored, but, in the process of risk-informing current regulations, attention will first be given to preventing early releases. Potential causes of late containment failure and associated mechanisms for radionuclide removal prior to containment failure will then be considered.

3.2 Initiator-Defense Assessment, Consider the Four Strategies Individually

An initiator-defense assessment divides accident initiators into three categories and establishes quantitative objectives for each category and each of the four defense-in-depth strategies. The paragraphs that follow present the initiator categories and quantitative objectives for this type

of assessment and discuss the potential utility of the proposed quantitative objectives for risk-informing existing regulations.

Events that could conceivably initiate a core damage accident are divided into three categories: anticipated, infrequent, and rare. For each initiator category a quantitative objective is established for each of the four defense-in-depth strategies. Accident sequences postulated during low power should be weighted according to the anticipated duration of the fuel cycle. For example, an accident that can only happen during one week every two years but which has an occurrence probability of 10^{-4} during that week has a frequency of (10^{-4}/week)*(1 week/2 years) = $5x10^{-5}$/year.

In probabilistic risk assessments, accidents are binned (grouped) by their initiators. Accidents that cause similar behavior and require functionally identical responses to avoid core damage or containment failure are binned together. For example, loss-of-coolant accidents (LOCAs) are often classified as small, intermediate, or large depending on the systems required to respond. Some accidents types (e.g., anticipated transients without scram [ATWS] and station blackout [SBO]) reflect functionally similar sequences of events. The anticipated, infrequent, and rare initiator categories are too coarse to be useful in risk-informing regulatory requirements pertaining to particular accident bins. Consideration is, therefore, given to the application of more restrictive quantitative objectives to accident bins within the three initiator categories.

Anticipated initiators are either expected to occur or may well occur during the plant life. Examples include inadvertent opening of a steam generator relief or safety valve, steam pressure regulator malfunction, reactor coolant pump trip, and loss of offsite power. The term anticipated operational occurrence (AOO), as used in safety analysis reports, describes a sequence of events started by an anticipated initiator and compounded by one or more single active failures. Plants are generally designed to withstand anticipated operational occurrences with no fuel damage.

The frequency of a significant group (bin) of anticipated initiators is typically greater than 10^{-2} per year. Anticipated initiators could be risk-significant if multiple failures of responding systems and components lead to core damage. Since the 1979 accident at TMI-2, industry efforts to reduce the frequency of anticipated initiators have been quite successful. The quantitative objective of less than 1 anticipated initiator per year, which is indicated in Figure 3-1, is both achievable and monitorable.

The quantitative objective proposed for the probability of core damage conditional on the occurrence of an anticipated initiator is 10^{-4}. This is reasonable because core damage as a result of an anticipated initiator generally requires the failure of two or more responding systems, and the failure probability of each system is typically less than 10^{-2}. For example, typical PWR high-pressure injection and auxiliary feedwater systems have redundant AC-powered trains, substantial margin over the required flow, capability to withstand any single active failure, and automatic actuation so that early operator action is not required. Even when common-cause failures and human errors are accounted for, most plants can meet the proposed quantitative objective.

In contrast, the quantitative objective listed in Figure 3-1 for the conditional probability of early containment failure (breach or bypass), given an anticipated initiator that leads to core damage, is 0.1. The dominant early containment loads imposed during postulated severe accidents generally accompany reactor vessel bottom head failure. In some accidents, core degradation is arrested in-vessel, and bottom head failure is prevented. Containment failure is less likely for degraded-core accidents, but it is the average containment failure probability for all core damage accidents with anticipated initiators that is compared to the quantitative objective of 0.1.

A quantitative objective has not been set for the fourth line of defense, that is, for the probability of early fatality given a core damage accident and early containment failure. This risk measure has

not been explicitly considered in past studies, but NUREG-1150 and other Level 3 risk assessments demonstrate that the QHOs are generally met if the subsidiary objectives for the first three strategies are met. In part, this is because wind and rain patterns generally assist in limiting the fraction of the population exposed to offsite radionuclide releases. Offsite protective actions are, nevertheless, essential for protecting people that would otherwise be exposed.

Infrequent initiators are not expected to occur over the life of the plant but are, nevertheless, risk significant. The frequency of a significant group (bin) of infrequent initiators is typically less than 10^{-3}/year. Existing plants were designed to withstand many infrequent initiators including pipe breaks in nuclear steam supply systems (NSSSs) and safe-shutdown earthquakes.

The quantitative objective for the frequency of all initiators in the infrequent category is 10^{-2}. On an industry-wide basis it is possible to monitor performance against this quantitative objective. The quantitative objective for the conditional probability of core damage given an infrequent initiator is 10^{-2}. Based on existing PRAs the proposed quantitative objectives provide a reasonable balance between initiator prevention and core damage prevention. The objectives for the two mitigative strategies are the same as those for anticipated initiators because the need for containment and offsite emergency response depends on the occurrence of a meltdown, rather than the initiator leading to the meltdown.

For accidents in which one or more of the four high-level defense-in-depth strategies is precluded, the individual strategy quantitative objectives may be less important than their products; that is, more emphasis needs to be placed on the strategies that remain. For example, consider a PWR interfacing-system loss-of-coolant accident (ISLOCA) in which containment is bypassed. The early containment failure probability is 1.0, therefore the quantitative objective of 0.1 cannot be achieved. Since no special ECCS is provided for ISLOCAs, there is a need to limit the relative frequency of such LOCAs and consider them in emergency planning. On a related matter, some argue that ECCS systems should not have to cope with "very large" reactor coolant system pipe breaks. This argument becomes much more difficult to defend if "very large" includes interfacing system breaks.

Rare initiators are those excluded from the anticipated and infrequent categories because they are extremely unlikely. Examples of rare initiators include aircraft impact, meteor strikes, and very large earthquakes. As a quantitative objective, the total frequency of all rare initiators should be less than 10^{-5}/year. Although some rare initiators could fail containment or preclude emergency response, this is not true for all rare initiators, and existing Level 3 PRAs indicate the rare initiator frequency goal of 10^{-5}/yr should not cause the QHOs to be exceeded. Given the fact that the collection of rare events is not completely known and that the uncertainties are large, initiators of a specific type (bin) should be classified as infrequent unless their frequency is demonstrably less than about 10^{-6} per year. This is consistent, for example, with current regulatory guidance regarding aircraft crashes.

The defense-in-depth approach does not ignore rare events. Tactics such as research, inspection, testing, and monitoring are applied to validate the low frequencies of rare initiators. Generally, however, a risk-informed regulation will not require plant structures, systems, and components be specifically designed to cope with rare initiators. Existing plant features provide some degree of protection against core damage and radionuclide releases for many rare initiators, and risks posed by rare initiators should certainly be addressed in PRAs. However, to focus on reducing risks associated with rare initiators would draw attention away from, and potentially increase risks associated with, more likely initiators.

3.3 Additional Thoughts on Quantitative Objectives

As stated earlier, the quantitative objectives presented in Figure 3-1 will, in most cases, not

appear in risk-informed regulatory requirements; however, in developing such requirements, it is important to have quantitative objectives in mind. Compliance with risk-informed regulations should provide a reasonable expectation that the quantitative objectives in Figure 3-1 will be met. Additional thoughts related to these quantitative objectives are presented below.

The quantitative health objectives are the highest-level quantitative goals. The QHOs were originally set as a measure of "safe enough." Given this position of the Commission, there are no risk arguments for setting subsidiary quantitative objectives more stringent than the QHOs.

While there is no basis for being more stringent than the QHOs, both defense-in-depth and uncertainties, which tend to grow as postulated accidents proceed in time, influence the quantitative allocation among the four defense-in-depth strategies (or pairs of strategies). The simplest approach would be to allocate the risk equally among the four strategies (~.027 for each strategy). Realistically, however, existing U.S. plants allocate more to prevention than to containment and emergency planning. The quantitative objectives in Figure 3-1 represent a more reasonable risk allocation.

When the first two strategies, prevent initiators and prevent core damage, are considered as a pair, the relevant quantitative objective is a CDF less than 10^{-4}/year. When these strategies are considered individually, the products of the quantitative objectives for the two strategies is the 10^{-4}/year CDF quantitative objective. That is, meeting the risk-informed regulations should be consistent with achieving a CDF less than 10^{-4}/year. The regulations should assure a higher response reliability (perhaps more redundancy and diversity) for more frequent initiators.

A different approach has been taken for rare events. Some of these events, should they occur, have the potential to progress directly to offsite releases of radionuclides. Because the core damage prevention and containment strategies may be unavailable for rare initiators, the frequency quantitative objective for rare initiators is set more stringently than 10^{-4}/year. Specifically, the quantitative objective is less than 10^{-5} rare initiators per year. The subsidiary quantitative objective of 10^{-6}/year for any single type of rare initiator is also applied.

Figure 3-1 identifies a containment performance quantitative objective of 0.1 for anticipated and infrequent initiators. That is, the conditional probability of failure or bypass that could lead to significant early releases (i.e., small leaks are not included) should be less than 0.1 for such initiators. It is recognized that this quantitative objective can not be met for all such initiators, but it should be met on average. Restricting the target to early containment failures does not assure compliance with the latent cancer safety goal, although, as stated earlier, the early fatality goal is generally more limiting. <u>To specifically deal with latent-cancers, a quantitative objective of ≤0.1 is proposed for the probability of a late large release in a core damage accident.</u>

The fourth high-level defense-in-depth strategy involves emergency planning and response, which are essential for protecting the public health and safety. Although a quantitative objective has not been set for this strategy, credit has been taken for its effectiveness in establishing subsidiary quantitative objectives compatible with the QHOs for the first three strategies. As noted earlier, pre-planned protective actions may be particularly important for accident scenarios in which one or more of the first three strategies are compromised. For example, for an ISLOCA, which bypasses containment, an early containment failure objective cannot be used; therefore, the fourth strategy becomes necessary.

The product of the quantitative objectives for the two strategies in method (1) and the three strategies for each of the three initiator types in method (2) is a LERF of $<10^{-5}$/year. As stated earlier, this generally assures that the early fatality QHO of $\leq 5\times10^{-7}$/year will be met. Setting the individual strategy quantitative objectives to yield a lower aggregate value would be unnecessarily conservative.

Table 3-1 provides a list of guidelines for risk-informing regulations. Each of the listed guidelines is derived from and consistent with the framework as discussed in the preceding paragraphs. It is anticipated that additional guidelines may be developed as work progresses.

Table 3-1 Guidelines for Each Strategy

Strategy 1 - limit the frequency of accident initiating events

- Provide assurance that the combined frequency of all anticipated initiators that could lead to core damage is less than 1/year per plant.
- Provide assurance that the combined frequency of all infrequent initiators is less than 10^{-2}/year per plant.
- Provide assurance that reasons used to classify initiators as rare remain valid, that the combined frequency of all rare initiators is less than 10^{-5}/year per plant, and that the frequency of specific initiator types (bins) is less than 10^{-6}/year per plant.

Strategy 2 - limit the probability of core damage given accident initiation

- Provide assurance that the probability of core damage given any anticipated initiator is less than 10^{-4}.
- Provide assurance that the probability of core damage given any infrequent initiator is less than 10^{-2}.

Strategy 3 - limit radionuclide releases during core damage accidents

- Provide assurance that the probability of early containment failure is less than 10^{-1} given a core damage accident with an anticipated or infrequent initiator.
- Provide assurance that the probability of a large late release is less than 10^{-1} given a core damage accident with an anticipated or infrequent initiator.

Strategy 4 - limit public health effects due to core damage accidents

- Pre-planned offsite protective actions are essential to protect the public health and safety. Although a quantitative objective has not been set for this strategy, its impact has been considered in developing the preceding guidelines. In addition, for example, for an ISLOCA, which bypasses containment, an early containment failure objective cannot be used; therefore, this strategy becomes necessary

3.4 Core Damage and Containment Failure

When quantitative objectives are set for frequencies and conditional probabilities of core damage and containment failure, it is important to provide a risk-informed interpretation of these terms, in effect, to describe the applicable failure

criteria. To be risk significant, core damage must involve a significant release of fission products from the UO_2 fuel. A typical PRA criteria for core damage requires the water level to be below a certain level with no imminent restoration of coolant to the core region so a melt release of fission products from the fuel is assured. This corresponds roughly to the point where computer analyses become complicated by geometry changes associated with melting and relocation of core materials.

A risk-significant level of core damage far exceeds that specified in the ECCS acceptance criteria of 10 CFR 50.46. The ECCS acceptance criteria permit only one percent of the cladding to be oxidized. The purpose of the ECCS acceptance criteria is, however, not to establish a risk-significant level of core damage but to set a level of core damage appropriate for a design basis accident. It is not reasonable to assert that a plant is designed to withstand an accident if that accident would lead to extensive cladding oxidation or relocation of fuel assembly or control assembly materials due to melting. Nevertheless, 10 CFR 50.46 is an appropriate candidate for the Option 3 study, and existing ECCS acceptance criteria will be evaluated.

To be risk-significant containment leakage must significantly exceed the design basis containment leak rate. Integrated containment leak rate requirements associated with Appendix J of 10 CFR 50 have been revised to change the required frequency of such tests. However, further risk informing Appendix J may be considered as part of the Option 3 study.

The terms core damage and containment failure, as well other acceptance and failure criteria, will be examined as part of the Option 3 study.

4.0 TREATMENT OF UNCERTAINTIES

In risk-informing existing regulatory requirements it is important to consider the treatment of uncertainties from two perspectives: (1) the risk assessment perspective, and (2) the design basis perspective. Both perspectives are discussed below. A discussion of the linkage between the two perspectives follows. NUREG-1489 provides a more tutorial discussion of terms and methods employed in uncertainty analyses (Ref. 9).

4.1 Risk Assessment Perspective

The risk assessment perspective applies to the quantitative objectives presented in Figure 3-1. These subsidiary quantitative objectives are based on the QHOs, which reflect the Commission's view of how safe is safe enough. The appropriate numerical measures to use in comparing PRA results to the quantitative objectives in Figure 3-1 are mean values. The mean values referred to are those that result from the propagation of distributions assigned to uncertain input parameters (and occasionally to alternative models). Methods for propagating input parameter distributions have been developed and, except for dispersion and health effects models, were applied in the NUREG-1150 risk assessments. The resulting uncertainties are large, exceeding two orders of magnitude from the 5-th to 95-th percentile on core damage frequency. The spread in CDF results from the IPEs is generally consistent with the NUREG-1150 uncertainty estimates. As previously mentioned, uncertainties pertaining to phenomenological models tend to increase as accident scenarios progress. In many cases, this leads to significant uncertainties in containment failure probabilities. As part of the NUREG-1150 effort, formal expert elicitation methods were used to quantify key phenomenological uncertainties. Except where significant subsequent research has been conducted, the NUREG-1150 results generally provide the best available quantifications of such uncertainties.

4.2 Design-Basis Perspective (Safety Margin)

The treatment of uncertainty from the design basis perspective involves the notion of safety margin. Colloquially, terms like safety margin and safety factor imply a measure of the conservatism employed in a design or process to assure a high degree of confidence that it will work to perform a needed function. If no uncertainties existed, there would be no need for safety margin. The greater the uncertainty the greater the need for compensating safety margin.

There are, in the literature, many different definitions of safety margin. Some are probabilistic. Others are deterministic. For example, safety margin is sometimes defined as the ratio of the ultimate failure stress to the design stress. The following probabilistic definition is broadly applicable: *safety margin is the probability (or level of confidence) that a design or process will perform an intended function.*

To illustrate the significance of a probabilistic definition, 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 stress and no uncertainty in the capacity of the SSC, there is no uncertainty in the answer. Assume a known stress is only slightly less than a known capacity. Replacing the SSC with one that is twice as strong would be useless because the failure probability would still be zero.

Generally, of course, there is uncertainty in the imposed stress, the capacity, or both. Safety margin may indicate the probability that an uncertain stress exceeds a known capacity or the probability that a known stress exceeds an uncertain capacity. Often there is uncertainty in both the stress imposed and the capacity. In some of these cases, the overlap of the stress and performance distributions can be quantified. More frequently, in formulating regulatory requirements, *acceptance criteria* or *failure criteria* are delineated to, in effect, fix the capacity so that safety margin can be stated as the probability of exceeding the acceptance criteria. For example, compliance with the ECCS

acceptance criteria of 10 CFR 50.46 can be demonstrated using best-estimate codes provided that "*uncertainty is accounted for, so that, when the calculated ECCS cooling performance is compared to the criteria, there is a high level of probability that the criteria would not be exceeded*."

The working definition of safety margin does not preclude the use of conservative or bounding calculations to demonstrate acceptable safety margin. For example, ECCS calculations based on 10 CFR 50 Appendix K, provide a conservative alternative to best-estimate calculations with uncertainty propagation.

4.3 Linking the Perspectives

Guidance regarding the treatment of uncertainties will evolve as the Option 3 study progresses; current perspective is provided below by considering three questions.

(1) How will risk insights be utilized in delineating or evaluating acceptance criteria?

Regulatory requirements impacting the design of existing plants were, for the most part, promulgated before PRA was broadly applied. Yet, it is fair to say that a driving intent of existing regulations is to define the design envelope of plants such that events within the design envelope are not significant contributors to risk. PRAs and IPEs tend to confirm that this intent has been realized; that is, risk-dominant accident scenarios are generally those involving initiators or multiple failures not postulated in the design of existing plants.

Risk-informed regulation will continue to assure that events within the design envelope are not significant contributors to risk. For example, cladding failures will still be precluded for anticipated operational occurrences, and risk significant levels of core damage will not be accepted for design basis accidents.

To the extent possible, revised or new deterministic requirements will be based on probabilistic considerations. For example, the structural capacity of a component might be set to assure a structural failure probability that is comparable to the probabilities of other failure modes. There is little to be gained by requiring more capacity as long as the structural failure cannot cause other failure events. Relevant probabilistic considerations will include:

- quantitative objectives for each defense-in-depth layer
- probabilities of other failure modes, and
- significance of SSCs in an overall system context

The last item above is intended to prevent the imposition of excess conservatism. For example, given independent SSCs to perform a given function, less safety margin is needed for each SSC than if only one SSC is present.

(2) How risk-significant will the changes be?

The quantitative objectives in Figure 3-1 and Table 3-1 are consistent with the safety goals, which are, in turn, statements of the Commission's position on how safe is safe enough. Changes to existing regulatory requirements should not, therefore, lead to changes in risk measures that go beyond the level of safety implied by the quantitative objectives.

In considering a change to an existing regulatory requirement it is important to estimate the overall impact on risk measures of the actual plant changes (to SSCs, inspections, testing, operating procedures, training, emergency plans, etc.) that would ensue. An overall assessment is required to preclude unintended repercussions. For example, if it were demonstrated that very large pipe breaks could be excluded from consideration under the ECCS acceptance criteria of 10 CFR 50.46 based on CDF, such breaks might still represent reasonable design-basis events for containment to account for uncertainties.

(3) How will uncertainties be accounted for in risk-informing existing regulatory

requirements?

In addition to parameter and model uncertainties, completeness uncertainty must be considered in the Option 3 study. Completeness uncertainty includes that associated with processes, events, and modes of operation that are not well-modeled in existing risk assessments. Examples include aging, human errors of commission, and, for the near term, accidents at low power and shutdown. Although the quality and coverage of risk assessments continues to evolve, completion uncertainty can never fully be eliminated. This is a principal reason for adopting the high-level defense-in-depth approach and strategies described in Sections 2.2 and 2.3. Similarly, at the tactical level of the framework hierarchy, when risk insights regarding specific threats are limited it will be necessary to maintain appropriate levels of diversity, redundancy, and safety margin.

In evaluating risk-informed alternatives to existing regulatory requirements, the impacts of associated plant changes on risk measures will be estimated and compared to the quantitative objectives in Figure 3-1 and Table 3-1. In some cases, it will be straightforward to characterize the risk impact of a potential regulatory change using available PRA and IPE results. For example, decisions regarding lower-level defense-in-depth in the form of redundancy or diversity are generally well-suited to this type of analysis. In other cases, formal analyses of changes to risk measures may be required. In all cases, the values compared will be estimated means of risk measures, with due consideration of uncertainty.

Safety margin is generally imposed to account for uncertainties in data and models used to demonstrate compliance with acceptance criteria. The approach taken in evaluating changes that impact safety margins will be the same as the approach taken in evaluating other changes. Specifically, the impacts of the changes on risk measures will be estimated and compared with the quantitative objectives. However, because safety margin is imposed to account for uncertainties, its treatment deserves special consideration.

Excessive safety margins benefit neither the NRC nor the nuclear industry. Excessively conservative requirements can, in fact, lead to incorrect safety conclusions and regulatory decisions, that may actually reduce plant safety by masking issues of higher safety significance. Mandated excessive conservatism can also produce artificial regulatory concerns.

What constitutes adequate margin and what constitutes excess margin? Answers to these questions, like the question of what constitutes protection of the public health and safety, will always involve engineering judgement. Preliminary guidance for the Option 3 study is offered below, but it is anticipated that guidance regarding safety margin will evolve as the study progresses.

Safety margin exists due to conservatisms placed in acceptance criteria and methods for demonstrating compliance with acceptance criteria. The approach preferred for the Option 3 study is (1) to specify reasonable safety margin in acceptance criteria based on probabilistic considerations and risk insights, and (2) to use best-estimate code calculations with uncertainty propagation to demonstrate compliance based on a computed 95th percentile. When this approach is precluded, an attempt will be made to achieve and equivalent level of safety margin in order to avoid excessive conservatism.

5.0 IMPLEMENTATION OF FRAMEWORK

As stated in the introduction the framework will be used to guide the Option 3 efforts to risk inform the 10 CFR 50. This includes identifying regulations and DBAs that are candidates for risk-informed change, prioritizing the candidates, analyzing high-priority candidates and, where warranted, formulating change options, evaluating these options, and making recommendations to the Nuclear Regulatory Commission.

This section outlines general steps that will be followed in implementing the framework and provides examples to illustrate approaches that seem appropriate based on foresight and experience gained to date (i.e., in risk-informing 10 CFR 50.44). The process of developing implementation guidelines will be iterative. Guidelines will evolve as experience is gained in risk-informing existing regulatory requirements. Considering the wide variety of existing regulatory requirements, implementation guidelines may remain rather general.

Simply replacing existing regulatory requirements with quantitative health objectives, or subsidiary quantitative objectives such as those presented in Figure 3-1 would be a risk-based not a risk-informed approach. Such an approach would ignore limitations associated with the existing PRA data base, and the need for high-level defense-in-depth to compensate for uncertainties, in particular, for the completeness uncertainty. Since licensees will have the option of choosing between existing regulations and their risk-informed counterpart, there is little purpose in promulgating risk-informed regulations that no licensee would choose.

Replacing existing regulations with high-level functional goals may be appropriate in some situations, but, without additional regulatory guidance, licensees might not be able to judge whether to adopt such requirements or not. For example, it has been proposed that 10 CFR 50.44 requirements for hydrogen control systems in Mark III and ice-condenser containments be risk-informed as follows (Ref. 10):

> "Each licensee with a boiling light-water nuclear power reactor with a Mark III type of containment and each licensee with an ice condenser type of containment shall provide its nuclear power reactor containment with a hydrogen control system. The hydrogen control system must be capable of handling (based on realistic calculations) the hydrogen equivalent to that generated from a metal-water reaction involving 75% of the fuel cladding surrounding the active fuel region (excluding the cladding surrounding the plenum volume)."

Accepting this proposal, for the sake of argument, the key to its adoption by licensees would be understanding what constitutes an acceptable spectrum of accidents to be analyzed and what constitutes acceptable "realistic" calculations. Analysis methods regarding hydrogen generation, hydrogen discharge rates to containment, random ignition, and phenomena occurring at vessel breach would need to be understood.

Phase 1 of the Option 3 study will rely for the most part on the existing PRA and IPE database. Although the IPEs applied a wide variety of assumptions and methodologies and did not treat external events or accidents at low power and shutdown, this database is adequate for Phase 1, which will, for the most part, analyze existing regulations by NSSS and containment type. It is anticipated that Phase 1 will identify:

- existing requirements that will not be changed
- existing requirements that can be replaced by a risk-informed alternative
- existing requirements that can be eliminated
- existing requirements that require further evaluation to determine whether or not they can be eliminated or replaced by a risk-informed alternative
- new regulatory requirements

Some plant-specific analyses based on example plants may be initiated during Phase 1; however, most such studies would deal with existing requirements that fall in category 4 above.

Figure 5-1 indicates the general steps taken in risk-informing a specific regulation. These steps will now be discussed.

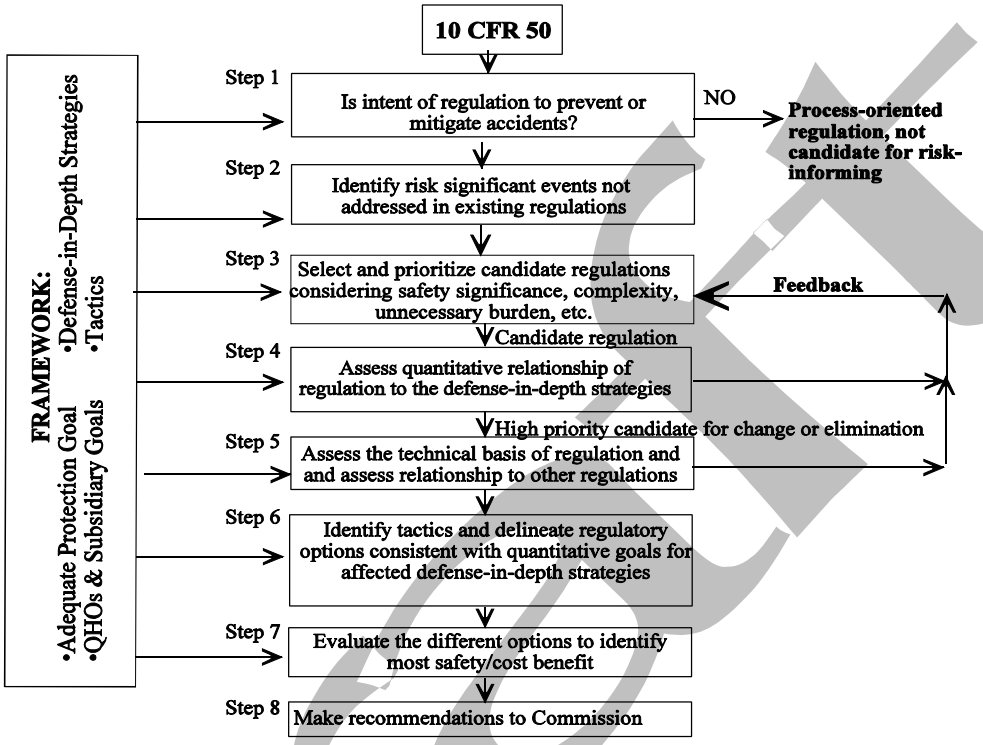


Figure 5-1. Framework Implementation Flow-chart

5.1 Step 1 - Identify existing regulatory requirements tied to accident prevention or mitigation

To be a candidate for risk-informed change an existing regulation must address accident prevention or mitigation; that is, it must have some tie or relevance to the safe design, operation, and maintenance of the plant. In contrast, regulations that are process-oriented are not candidates. For example, Parts 50.20 through 50.23 discuss the required licenses for a nuclear facility and do not directly affect accident prevention or mitigation. A coarse screening has been conducted to place each regulation of Parts 50 and 100 in one of two bins:

1. Regulations that do not have a direct link to safe plant design, operation, or maintenance. These consist of sections that are:
   - purely procedural or provide legal or technical definitions,
   - refer to enforcement provisions and/or penalties for misconduct,
   - concern financial and insurance requirements,
   - specify routine exposure limits from plant operation, or
   - pertain to decommissioning.
2. Regulations that have a potential relevance to safe plant design, operation, or maintenance.

The results of the screening are presented in Appendix A. Bin 2 includes all of the possible candidates for risk informing identified in a recent Nuclear Energy Institute (NEI) letter. The prime candidates identified by NEI for risk-informed

assessment and change are (Ref. 11):

- LOCA, ECCS analyses, 10 CFR 50.46 and Appendix K to Part 50
- Codes and Standards, 10 CFR 50.55a
- GDC 4, Appendix A to Part 50 and associated regulatory guidance documents that are linked to pipe-whip and dynamic effects
- Environmental qualification of electric equipment important to safety for nuclear power plants, 10 CFR 50.49
- Standards for combustible gas control system in light-water-cooled power reactors, 10 CFR 50.44
- GDC 19, Appendix A to Part 50 and associated regulatory guidance documents linked to control room ventilation
- GDC 17, Appendix A to Part 50 and associated guidance documents related to electrical power systems

All of the potential candidates in bin (2) are prioritized in Step 3. High priority candidates identified are evaluated in detail in subsequent steps. Those that do not significantly impact the quantitative framework objectives depicted in Figure 3-1 become elimination candidates. The rest become change candidates. Option 3 efforts have already been initiated on 10 CFR 50.44 and 10 CFR 50.46.

While the regulations falling into bin (1) are not themselves candidates for risk-informing, it is conceivable that some of them may have to be changed for the sake of consistency due to risk-informed changes made to regulations in bin (2).

5.2 Step 2 - Identify risk-significant events not addressed in existing regulations

In the process of risk-informing existing regulations, it is also important to identify risk-significant events not explicitly addressed in current regulations. An initial attempt has been made to find "holes" in the current Part 50 regulations on issues that are important to accident risks. Table 5-1 shows a mapping of accident types that are important to CDF or LERF to Part 50 regulations. One feature that is immediately obvious from the table is the fact that many of the risk-significant accident types are only covered by 50.34 (f) (..), the "TMI-related regulations." This set of regulations applies only to plants whose license applications were pending as of February 1982. (The paragraph under 50.34 (f) identifies a specific set of plants to which these rules were applicable; none of these plants have been constructed.) By inference, these regulations do not apply to the current set of operating plants, so there is, in principle, a rather large "hole" that needs to be assessed in the risk-informed process.

Table 5-1. Regulatory Coverage of Some Accidents Important to Risk (Preliminary)

Accident Types Important to CDF/LERF	Regulations in Part 50
SBO	50.63, 50.34 (f) (ix)
ATWS	50.62
LOCAs	50.34 (f) (iv) - Small Break LOCA, 50.46 - ECCS Acceptance Criteria, App. K, App. J
Transients with DHR Loss	50.34 (f) (i) - DHR Reliability

Table 5-1. Regulatory Coverage of Some Accidents Important to Risk (Preliminary)

Accident Types Important to CDF/LERF	Regulations in Part 50
Transients with Injection Loss	50.34 (f) (v), 50.34 (f) (vii), 50.34 (f) (viii), 50.34 (f) (x), 50.34 (f) (xi)
Early Containment Failure	50.34 (f) (xii), 50.44 - H2 control, App. A
Containment Bypass- ISLOCA/SGTR	App. A (very indirectly)
Loss of Containment Isolation	App. A
Internal Fire	App. R
Internal Flood	
External Events	(Part 100 for siting), App. S
Events at Low Power and Shutdown	

Some risk-significant accident types and related events do not find any mention in the current regulations. Examples include seal LOCAs, which are important contributors to PWR core damage frequencies, and liner melt-through, which can be a significant contributor to LERF for BWRs with Mark I containments. Except for hydrogen, threats posed by severe accidents are not specifically mentioned in existing regulations. Often, one has to "stretch" the rather general language contained in the regulation to infer its applicability to a particular accident class. An example would be interpreting the contents of Appendix A to cover the containment bypass accident category.

Where the risk-informed process identifies candidate new requirements, the role of the backfit rule needs to be considered. In general, if the new requirement would pass the backfit rule, it would be a candidate for mandatory application to all applicable plants.

5.3 Step 3 - Prioritize and select candidate regulations for detailed analysis

The coarse screening performed in Step 1 results in the identification of regulations that, at least by intent, address accident prevention or mitigation. Further analysis is required to prioritize these regulations (and their associated implementing documents) for evaluation under Option 3. In particular, Step 3 identifies high-priority candidates for risk informing and selects the highest priority candidates for detailed evaluation in subsequent steps. The factors considered in Step 3 include unnecessary burden imposed by the regulation (to both the NRC and the licensees), as well as the risk (safety) significance of the regulation. These factors are also relevant to the prioritization and selection of DBAs for detailed evaluation.

It is generally straightforward to determine which, if any, of the four high-level defense-in-depth strategies an existing regulatory requirement impacts. The magnitude of the impact can, in some cases, be characterized qualitatively. In other cases simple quantitative analyses may be required as discussed under Step 4.

A regulation or DBA may become a **potential elimination candidate** if it has an insignificant or negative impact on safety, or if it is redundant or contradictory to other regulatory requirements. A regulation or DBA potentially warrants elimination from a safety perspective if it does not

impact any of the four defense-in-depth strategies depicted in Figure 1-2, or it has an insignificant impact on the quantitative objectives delineated in Figure 3-1. For example, a regulation that deals solely with an initiating event whose frequency is demonstrably less than 1E-6/yr or a regulation that deals solely with accidents that contribute less than 1E-7/yr to core damage frequency may be a candidate for elimination. Exceptions would include regulatory requirements designed to assure suitably low frequencies of rare initiating events (Strategy 1). A guiding principle is that **adequate justification must be provided for regulations beyond those necessary to achieve the quantitative objectives and maintain the four defense-in-depth strategies**.

Regulatory requirements that pass the coarse screening (Step 1) and are not potential elimination candidates are **potential change candidates**. Change may be appropriate if more effective means are available to support the high-level defense-in-depth strategies. An alternative may be more effective because it is more consistent with the high-level safety strategies and quantitative objectives, because it eliminates unnecessary burden, or both. Unnecessary burden may include that imposed by methods, assumptions, or acceptance criteria that require safety margin, redundancy, or diversity above that necessary to account for uncertainty.

The word potential is used in the preceding paragraphs to emphasize the point that an existing regulatory requirement does not become a current candidate for elimination or change until a decision is made to devote the resources required for its detailed evaluation in Steps 4 through 8. In order to improve safety decisions and reduce unnecessary burden as rapidly as possible, it is necessary to prioritize the order in which the potential candidates become current candidates in the risk-informing process. The factors used to prioritize the potential candidates include:

- the potential for improving safety,
- the complexity of the regulation,
- the resources required for risk-informing the regulation (both short and long term), and
- the potential for reducing both licensee and NRC unnecessary burden.

A proposed decision tree for prioritizing regulations is shown in Figure 5-2. The decision tree combines the four factors identified above to determine which regulations should be given the highest priority. Guidelines for assigning a "HIGH" or "LOW" rating for each of these factors will be developed. It is anticipated that forced rankings based on qualitative assessments of each factor will suffice in most cases; however, it may be necessary to develop more detailed information as described under Steps 4 and 5 in some cases. A "HIGH/LOW" in Figure 5-2 indicates that the final ranking will depend on detailed assessment of the indicated factors.

High priority will be given to regulations that have the most potential for improving safety. Both the impact of a regulation on the quantitative objectives in Figure 3-1 and the number of plants affected by the regulation will be considered. Regulations that do not have a relationship with other regulations (determined in Step 5) can be addressed unilaterally in the risk-informed process and will, generally, be assigned a high priority in the complexity column of Figure 5-2. Similarly, regulations that require relatively small levels of effort to identify and implement risk-informed options will be given higher priority than those that require more resources. Estimates of the short- and long-term costs of risk-informing some regulations may be required to fully utilize this factor in the prioritization effort. Finally, regulations that impose unnecessary burden on the NRC or licensees will be given higher priority over those regulations that do not impose unnecessary burden. Input for this determination will be obtained from the stakeholders.

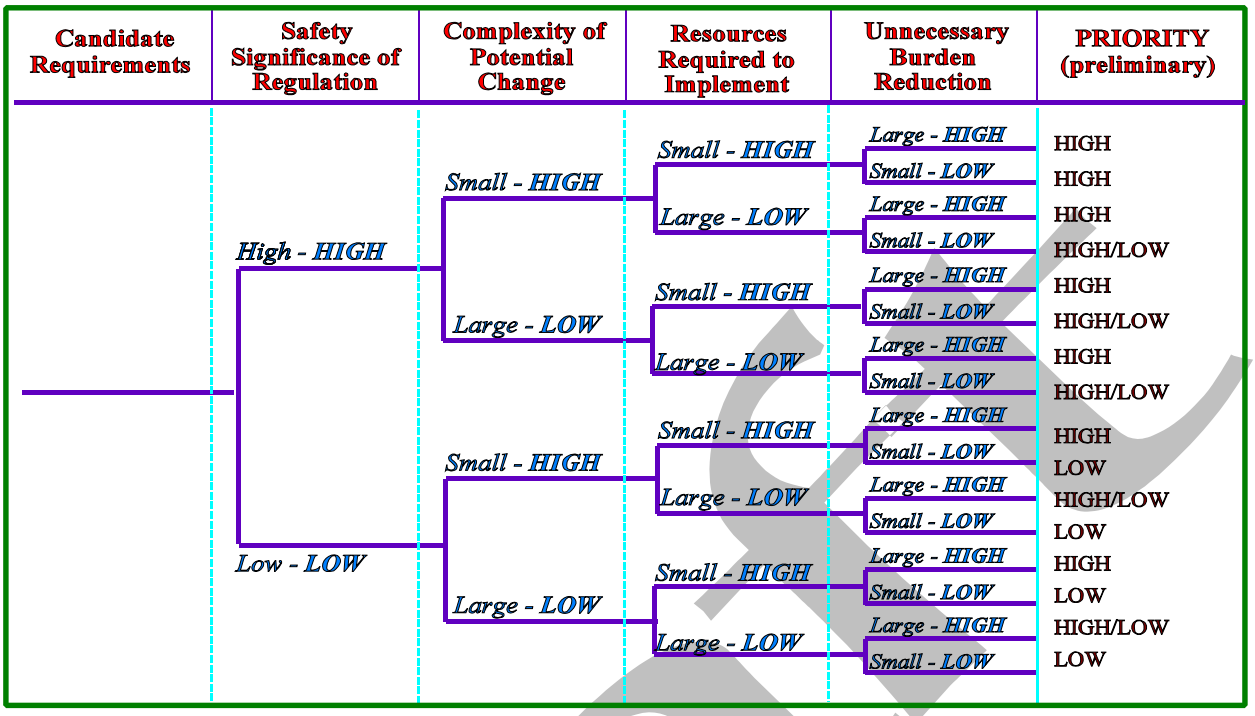


Figure 5-2. Example Prioritization Decision Tree

5.4 Step 4 - Assess relationship of regulation to the defense-in-depth strategies

When changes to current risk-significant regulations (regulations that clearly impact the targets in Figure 3-1) are contemplated, rational as to why the changes would not negatively impact the quantitative objectives will be established. When adequate for the task, existing PRA information will be used to assess the risk-significance of existing regulations relative to elimination or contemplated options by assessing the impact the changes would have on relevant quantitative objectives in Figure 3-1.

The risk-significance of a regulatory requirement will be determined based on the risk from accident scenarios that are impacted by the requirement; that is, the effect of the requirement on accident initiators, core damage accidents, and containment failure modes will be estimated. The relationship of the regulations to the quantitative objectives of Figure 3-1 may require information identified during the review of the technical basis of the regulation/DBA (Step 5). Quantitative assessments of impact will be based on industry risk values and will consider the range in the risk parameters and relevant uncertainties. For requirements specific to a particular plant or containment type, risk values for the affected plants will be used (e.g, for a requirement pertaining to steam generators, only the risk values from PWRs will be used).

One source of risk information that will be used in this effort is the results of the IPEs. The IPEs represent the broadest base of risk estimates during full power operation that is available. However, it is recognized that there are substantial variations in the risk parameters calculated in the IPEs, some of which can be attributed to modeling assumptions rather than actual plant differences. The effect of the

assumptions on the IPE results was addressed in NUREG-1560 and will be considered when using this information in the risk-informed process. In addition to the IPEs, other PRA information such as the results of the NUREG-1150 and other NRC and industry studies will be used in this effort.

Ideally, risk parameters used in this process would be estimated for all modes of operation and include the risk from external events. However, risk profiles for low power and shutdown and for external events are less developed, and the process of estimating the effect of an existing regulatory requirement on such risks will have to rely more on the judgement of qualified risk analysts. In some cases, this may preclude risk-informing specific existing requirements until relevant risk information is developed.

5.5 Step 5 - Assess technical basis of regulation and relationship to other regulations

In order to identify potential risk-informed options (including elimination), it is necessary that the technical bases for current regulations and their related material (e.g., the Standard Review Plan, and regulatory guides) be understood. A review of the technical bases will help identify how the regulations and the technical requirements imposed by them relate to the defense-in-depth strategies for providing protection of the public health and safety. The review will also identify interrelationships and linkages among the requirements.

For the candidate requirements, a review of the current technical basis will involve identifying:

- the safety function intended to be addressed by the requirement;
- the analysis methods, assumptions and acceptance criteria used; and
- the extent to which defense-in-depth and safety margin are addressed.

In addition to examining individual requirements, how defense-in-depth and safety margins are applied across requirements will be considered looking at factors such as the balance between accident prevention and mitigation.

A related task involves the determination of the bases for the existing DBAs. The challenges to safe operation (i.e., design basis accidents), traditionally considered as part of the plant's design basis, contained in Chapter 15 of Regulatory Guide 1.70 (Format and Content of SAR), Chapter 15 of the Standard Review Plan (NUREG-0800) plus any other specific accidents identified in the regulations (e.g., SBO and ATWS) will be reviewed. The review will focus on the bases for selection of the DBAs and the associated requirements that they impose on plant design and operation. The assessment of each accident will involve identifying:

- the definition of the accident
- the actual requirement(s) for mitigating the accident
  - deterministic values of critical parameters such as temperatures, pressures, flow rates, extent of fuel damage, etc., used as success criteria for recovery from the various design basis accident initiating events
  - the SSCs required to be functional for the accident
- the technical bases for each requirement
  - the analysis methods and assumptions
  - the extent to which plant instrumentation, controls, and reactor protection systems are assumed to function
  - the credit taken for success of operator actions in recovery
  - the extent to which plant malfunctions (single active failures of systems and components), such as stuck control rods or stuck-open valves, and system dependencies, e.g., between safety systems and support systems, are accounted for in the course of the transient

The risk contribution and safety margins of such scenarios will be compared to Figure 3-1 and the safety margins definition, and changes will be proposed where necessary to bring the DBAs in

line with the risk-informed framework.

5.6 Step 6 - Identify relevant tactics and delineate regulatory options consistent with quantitative objectives for affected defense-in-depth strategies

This is a key step in the implementation process. The general guidelines presented below will evolve as experience is gained in risk informing specific regulations.

When it is determined, based on the preceding steps, that a risk-informed alternative (other than elimination) to an existing regulatory requirement may be appropriate, reasonable options will be delineated. As mentioned in step 1, a simple statement of the functional goal of a regulation will generally not be sufficient for licensees to decide on adopting a risk informed option. Sufficient detailed guidance will have to developed regarding each option to permit relative risks and burdens (for both licensees and NRC) to be estimated. In an ideal world both the safety impact and the cost burden of each option would be precisely quantified. However, some options may be eliminated based on the quantitative objectives of Figure 3-1. Relative measures of risk and burden may, in some cases, suffice for comparing feasible options.

Each feasible option should be consistent with the quantitative objectives set for the defense-in-depth strategies impacted by the existing regulation. In cases where the options involve decisions regarding plant structures, systems, and components, quantitative comparisons to the impacted quantitative objective will be made, if possible, for affected plant types. For example, risk measures could be quantified to permit comparison of a diversity requirement to a redundancy requirement. Quantification would also apply to options involving different levels of operator action. Uncertainties in failure rates should generally be considered in making such comparisons because the quantitative objectives are for means.

In some cases it will also be possible to quantitatively compare the safety margins associated with risk-informed options; however, relative measures of safety margin may also suffice provided the safety margin associated with each option is deemed reasonable.

When direct risk comparisons between options cannot be made, qualitative comparisons will be used. For example, this might be true when considering special treatment options, optional computational methods for demonstrating compliance, or options for performance monitoring. Generally, in such cases, burden measures will dominate the decision process.

Information regarding the relative burden imposed by the delineated options will also be developed. Licensee and NRC burdens must be considered both for implementing and applying each option. Factors impacting implementation burden may include:

- level of completeness and confidence required in licensee PRAs
- existence of acceptable computational methods for demonstrating compliance
- level of regulatory guidance required
- whether a new rulemaking is required

- impact on training, procedures, hardware, performance requirements
- whether a demonstration plant application is required
- overall time required for implementation

Factors impacting application burden may include:

- impact on maintenance, testing, inspection,

and performance monitoring

- impact on documentation and reporting requirements, including PRA and Final Safety Analysis Report (FSAR) updates
- improvements in efficient use of personnel
- special treatment requirements

The list of relevant burden factors will vary depending on the regulatory requirement being risk informed.

For high-priority potential elimination candidates, consideration needs to be given to whether or not the existing requirement has a significant impact on any of the following:

- radiation safety cornerstones
- security cornerstone
- environmental considerations
- other regulations

If the potential elimination candidate has no significant impact on any of the above areas, then its elimination may be justified.

5.7 Step 7 - Evaluate the different options to identify the most safety/cost benefit

The risk and burden information developed in Step 6 will be used to identify the preferred option. For cases in which two or more options have comparable risk implications, the option imposing the least burden is preferable. In situations in which the risk implications differ, the option offering the most safety benefit per unit cost is preferable. Where quantitative comparisons are not possible or inconclusive, qualitative evaluations of relevant factors may be applied. Stakeholder feedback may be particularly relevant in such cases.

5.8 Step 8 - Make recommendations

Based on the comparisons made in Step 7, the preferable risk-informed option to an existing regulatory requirement will be recommended.

6.0SUMMARY

This document presents a framework and guidelines to be used in risk-informing existing regulatory requirements. The approach maintains four high-level defense-in-depth functions, which support the protection of the public health and safety goal and are consistent with the reactor safety cornerstones developed for regulatory oversight. Risk information is used to evaluate the effectiveness of the defense-in-depth approach. Although regulations will be revised or originated based on risk information, they will retain deterministic characteristics. The development of risk-informed regulatory requirements will be guided by quantitative safety objectives, insights derived from PRAs and IPEs, and the need to account for uncertainty, particularly in cases where one or more of the high-level defense-in-depth functions is precluded.

7.0 REFERENCES

1. USNRC, SECY-98-300, "Options for Risk-informed Revision to 10 CFR Part 50 - ‘Domestic Licensing of Production and Utilization Facilities,’" December 23, 1998.

2. FR Doc. 88-12624, Statement of Considerations, Revisions to Backfit Rule, 10 CFR 50.109, July 6, 1988.

3. Letter from D. A. Powers, Chairman, Advisory Committee on Reactor Safeguards, to The Honorable Shirley Ann Jackson, Chairman, U. S. Nuclear Regulatory Commission, "The Role of Defense in Depth in a Risk-Informed Regulatory System," May 19, 1999.

4. J. N. Sorensen, G. E. Apostolakis, T. S. Kress, D. A. Powers, "On the Role of Defense in Depth in Risk-Informed Regulation," Presented at PSA '99, Washington, D.C., August 22-25, 1999.

5. USNRC, "New NRC Reactor Inspection and Oversight Program," NUREG-1649, Rev. 1, May 1999.

6. USNRC, "Safety Goals for the Operation of Nuclear Power Plants; Policy Statement," *Federal Register*, Vol. 51, p. 30028, August 21, 1986.

7. USNRC, SECY-99-007, "Recommendations for Reactor Oversight Process Improvements," January 8, 1999.

8. USNRC, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis," Regulatory Guide 1.174, July 1998.

9. USNRC, "A Review of NRC Staff Uses of Probabilistic Risk Assessment," NUREG-1489, March 1994.

10. Letter from Bob Christi, Performance Technology, to U.S. Nuclear Regulatory Commissioners, October 7, 1999.

11. Letter from Joe F. Colvin, President, Nuclear Energy Institute, to Richard A. Meserve, Chairman, U.S. Nuclear Regulatory Commission, January 19, 2000.