POLICY ISSUE
NOTATION VOTE

August 2, 2005 SECY-05-0138

FOR: The Commissioners

FROM: Luis A. Reyes
Executive Director for Operations

SUBJECT: RISK-INFORMED AND PERFORMANCE-BASED ALTERNATIVES TO THE SINGLE-FAILURE CRITERION

PURPOSE:

This paper has two purposes:

(1) Inform the Commission of the staff's findings regarding alternatives that represent a broader change to the single-failure criterion (SFC), as directed in the staff requirements memorandum (SRM) responding to SECY 02-0057, "Update to SECY-01-0133, 'Fourth Status Report on Study of Risk-Informed Changes to the Technical Requirements of 10 CFR Part 50 (Option 3) and Recommendations on Risk-Informed Changes to 10 CFR 50.46 (ECCS Acceptance Criteria)'," dated March 31, 2003.

(2) Request Commission approval to release to the public a draft report describing the potential alternatives, and continue this effort as part of the agency initiative to risk-inform Title 10, Part 50, of the *Code of Federal Regulations* (10 CFR Part 50).

SUMMARY:

In the SRM responding to SECY 02-0057, the Commission directed the staff to "pursue a broader change to the single failure criterion and inform the Commission of its findings." Toward that end, the staff has completed an initial evaluation of risk-informed alternatives to the SFC. This paper and its attachments present and discuss four alternatives.

CONTACTS: Hossein G. Hamzehee, RES/DRAA
301-415-6228

John C. Lane, RES/DRAA
301-415-6442

The staff believes that, while several alternatives have been evaluated, it would be premature to recommend any of these alternatives because implementation feasibility, resources, and costs have not been considered. For this reason, additional stakeholder involvement and further evaluation are recommended to assess the practicality of implementing any of these alternatives. In fact, stakeholder input may result in other viable alternatives meriting consideration. Therefore, the staff does not recommend one alternative over another at this time.

BACKGROUND:

In the early days of the nuclear power industry, the U.S. Nuclear Regulatory Commission (NRC) established the SFC as a comprehensive set of requirements, for which Appendix A to 10 CFR Part 50 defined "single-failure" as follows:

> "A single-failure means an occurrence which results in the loss of capability of a component to perform its intended safety functions. Multiple failures resulting from a single occurrence are considered to be a single-failure. Fluid and electric systems are considered to be designed against an assumed single-failure if neither (1) a single-failure of any active component (assuming passive components function properly) nor (2) a single-failure of a passive component (assuming active components function properly), results in a loss of the capability of the system to perform its safety functions."

Appendix A to 10 CFR Part 50 also included the following associated footnote:

> "Single failures of passive components in electric systems should be assumed in designing against a single failure. The conditions under which a single failure of a passive component in a fluid system should be considered in designing the system against a single failure are under development."

In June 1999, the Commission decided to implement risk-informed changes to the technical requirements of 10 CFR Part 50. The first of those risk-informed changes involved revising the combustible gas control requirements of 10 CFR 50.44. Another topic that the staff examined concerned the requirements for large-break loss-of-coolant accidents (LOCAs), for which the staff considered a number of possible changes. Specifically, the staff considered changes to General Design Criterion (GDC) 35, as well as changes to the acceptance criteria, evaluation models, and functional reliability requirements of 10 CFR 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light-Water Nuclear Power Reactors." In the SRM responding to SECY 02-0057, the Commission approved most of the staff recommendations regarding possible changes to LOCA requirements. The Commission also directed the staff to risk-inform the current requirements for consideration of a large-break loss-of-coolant accident (LBLOCA) coincident with a loss of offsite power (LOOP). In addition, the Commission directed the staff to "pursue a broader change to the single failure criterion [beyond what the staff is considering for the LOCA/LOOP exemption requested by the Boiling-Water Reactor Owners Group (BWROG)] and inform the Commission of its findings."

The objective of the evaluation discussed in this paper is to respond to the Commission's directive to "pursue a broader change to the single failure criterion." For this evaluation, the staff developed a process to identify risk-informed and performance-based alternatives to the SFC that will ensure continued plant safety. While the Commission's directive was primarily related to GDC 35 and the acceptance criteria for the emergency core cooling system (ECCS), the staff interpreted "broader change" to encompass alternatives to the SFC that could apply to all safety-related and non-safety-related plant functions and could lead to changes in

licensing, programmatic activities (such as testing and inspection), and plant performance monitoring.

DISCUSSION:

As one important element of the NRC's defense-in-depth safety philosophy, the SFC is a mechanism to promote reliability in the safety systems of the Nation's nuclear power plants. A number of regulations, guidelines, and programs (including quality assurance requirements, technical specifications, and requirements for testing, inspection, and maintenance) complement and act in concert with the SFC to promote high system reliability.

The SFC exists in two major contexts: (1) system design requirements, which are largely associated with the GDCs set forth in Appendix A to 10 CFR Part 50, and (2) guidance for use in analyzing design-basis accidents (DBAs), set forth in the NRC's Standard Review Plan (NUREG-0800) and Chapter 15 of Regulatory Guide 1.70, "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants." The first of these contexts requires that safety-related systems be designed to perform safety functions to mitigate design-basis initiating events, assuming a single failure. The second is directed toward demonstrating adequate design margins based upon defined acceptance criteria.

In pursuing a broader change to the SFC, the staff believes it is important to note that application of the SFC has sometimes led to redundant system components, which contribute to adequate and acceptable safety margins, but may have only minimal impact on risk, based on conventional risk assessment studies. The double-ended guillotine break LOCA in combination with a LOOP and diesel generator failure is often cited as an example because probabilistic risk assessments (PRAs) have shown that such a break is not risk-significant, but it contributes to the need for accumulators in pressurized-water reactors (PWRs) and limits their power operating level. While maintaining adequate safety margins is a major safety objective, the application of the worst single-failure assumption for all DBAs may, in some cases, result in unnecessary constraints on licensees.

The staff also notes that the current implementation of the SFC does not consider potentially risk-significant sequences involving multiple (rather than single) failures as part of the DBA analysis. Common-cause failures, support system failures, multiple independent failures, and multiple failures caused by spatial dependencies and multiple human errors, are phenomena that impact system reliability, which may not be mitigated by redundant system design alone. A risk-informed alternative might consider such failures in DBA analyses if they were more likely than postulated single-failure events. However, including multiple failures in DBA analyses would likely be more complicated and costly than addressing single failures as required today.

Another consideration is that the SFC has not always been uniformly applied to passive failures in fluid systems, and such passive failures should be considered in a risk-informed alternative to the existing SFC requirements. However, the NRC would need to resolve the question of which passive failures to include in such treatment. For example, the passive failure of a single check valve, pipe, or tank could have significant implications on the DBA analysis. Guidance for including passive failures in PRA models may be obtained from the "Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications" [which the American Society of Mechanical Engineers (ASME) promulgated as ASME RA-S-2002], as endorsed

in Regulatory Guide 1.200, “An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities,” dated February 2004.

In addition, application of the SFC has not always led to the design of safety systems that the NRC deemed to have adequate reliability commensurate with the frequency of important safety challenges. Generally, for more frequent challenges, higher system reliability is desirable to enable safety systems to respond in a manner that results in safe plant shutdown. On the basis of generic safety issue studies, rulemaking, and risk considerations, the NRC supplemented the SFC with additional regulations or licensing guidance applicable to selected safety systems. These led to plant modifications and licensee programs to either improve system reliability or demonstrate that the system design was otherwise adequate to cope with the postulated initiating events. Relevant examples include the station blackout rule, the anticipated transient without scram rule, and the post-Three Mile Island guidance to increase availability of PWR auxiliary feedwater systems.

Taken in concert with staff guidance, rulemaking, and programs, the current SFC requirement promoting redundant safety system design has contributed significantly toward maintaining an acceptable level of safety in the operation of U.S. nuclear power plants.

The Commission has established PRA and other regulatory policy guidance that applies to the implementation of any risk-informed and performance-based alternative to the SFC. Thus, a proposed alternative would need to demonstrate consistency with the following agency guidance and activities:

- Commission guidance on risk-informed and performance-based regulation, as set forth in the PRA Policy Statement and the Severe Accident Policy Statement regarding maintaining defense-in-depth, adequate safety margins, security constraint, and consideration of uncertainty. Risk-based approaches would not be consistent with the Commission policy
- Commission guidance on the phased approach to PRA quality, such that the necessary quality of licensee PRAs is ensured to support the particular alternative to the SFC
- Commission policy on backfit and regulatory analyses, including consideration of costs, benefits, and bundling of requirements
- Other ongoing risk-informed activities:
  - < rulemaking regarding LOCA redefinition (10 CFR 50.46)
  - < improvement of the technical specifications for nuclear power plant licensing
  - < activities associated with the Reactor Oversight Process
  - < consideration of the LOCA/LOOP exemption requested by BWROG
  - < development of a technology-neutral framework for advanced reactors
  - < consideration of the safety/security interface

In deriving alternatives to the SFC, the staff developed a process that highlighted necessary attributes for any risk-informed and performance-based alternative, which the staff derived from the NRC’s strategic goals and the Commission’s policy on risk-informed regulation. In particular, the necessary attributes include adherence to defense-in-depth concepts and acknowledgment that inherent uncertainties exist in risk estimates. From a larger number of alternatives, the staff then developed four that satisfy these attributes, as discussed in the remainder of this section. (Attachment 1 to this paper summarizes the four risk-informed

alternatives, while Attachment 2 provides more detailed descriptions.) Any risk-informed and performance-based changes to the current SFC are expected to be voluntary. As part of the followup activities, the staff will determine whether a backfit analysis will be necessary if any of these alternatives to the current SFC is implemented. These alternatives are not mutually exclusive, and it may be beneficial to consider combinations of approaches.

The baseline alternative is to maintain the current SFC, but continue to make risk-informed changes to associated regulatory requirements that involve specific activities or licensing issues. Under this alternative, the staff would consider changes to the SFC (or its scope of application) in the context of the particular activity or licensing issue. This alternative would encompass ongoing initiatives (previously discussed), such as the rulemaking regarding LOCA redefinition (10 CFR 50.46), consideration of the LOCA/LOOP exemption request, plant-specific risk-informed license amendments, risk-informed technical specification initiatives, and continued improvements to the reactor oversight process (ROP). In addition, this alternative would include updating the footnote to the single-failure definition in Appendix A to 10 CFR Part 50 (previously discussed), as it relates to passive failures.

Alternative 1 to the current SFC would risk-inform the DBA analysis. This alternative could eliminate sufficiently unlikely sequences and postulated single failures from DBA analysis. The proposed rulemaking regarding LOCA redefinition (10 CFR 50.46) could be considered a special case of Alternative 1, in which the SFC would not be applied for the double-ended pipe rupture, but would remain for LOCAs within the design basis. In addition to LOCAs, this alternative would consider the range of postulated challenges in a plant's accident and transient analysis. This alternative would also consider adding multiple-failure sequences to the design basis when the frequency of a series of failures in the sequence is sufficiently high; this may be a consideration for more frequent transients. To make these determinations, the staff would have to develop and apply screening criteria based on the Commission's risk-informed policy guidance. In addition, in applying this alternative, the staff would consider uncertainties in the frequency estimates, as well as the need to maintain defense-in-depth consistent with the Commission's guidance.

Alternative 2 would risk-inform the application of the SFC to safety systems based upon their safety significance. In so doing, the staff would define a risk-informed process to categorize the safety significance of all plant systems. Taking advantage of current categorization processes, this alternative would expand upon the approach set forth in 10 CFR 50.69, "Risk-Informed Categorization and Treatment of Structures, Systems, and Components for Nuclear Power Reactors." Similar to 10 CFR 50.69, the staff would consider requirements for safety-significant, non-safety-related systems.

Alternative 3 would develop and apply a blend of the following considerations:

- levels of redundancy and diversity for key safety functions
- quantitative targets for unreliability, applied at the following levels:
  - < core damage frequency (CDF) and large early release frequency (LERF)
  - < the safety function (such as reactor shutdown or post-trip decay heat removal) specified for categories of challenges (frequent initiators, infrequent initiators, and rare initiators), such that the unreliability targets for each function/initiator combination would be commensurate with the initiator frequency

This alternative would vary the redundancy requirement according to initiator frequency, and supplement it with diversity requirements. In so doing, this alternative would be roughly equivalent to the current SFC for some initiator/function combinations, while it might be more or less stringent than the SFC for others. Toward that end, the staff would provide guidance for the desired levels of redundancy and diversity for safety functions, and would apply compensatory treatment in plant responses to certain initiator categories in areas with less than the recommended redundancy or diversity. For example, for frequent initiators, low functional unreliability would be required, accommodation of multiple failures would be recommended, and acceptable defense (diversity) for common-cause failure (CCF) would be needed. The staff would also need to develop regulatory guidance for demonstration of the unreliability targets, and for establishing the requisite degree of failure tolerance and diversity.

RECOMMENDATION:

The staff believes that, while several alternatives have been evaluated, it would be premature to recommend any of these alternatives because implementation feasibility, resources, and costs have not been considered. For this reason, additional stakeholder involvement and further evaluation are recommended to assess the practicality of implementing any of these alternatives. In fact, stakeholder input may result in other viable alternatives meriting consideration. Therefore, the staff does not recommend one alternative over another at this time.

In addition, as directed in the SRM dated May 9, 2005, in response to a Commission briefing on programs administered by the Office of Nuclear Regulatory Research (RES), the RES staff is working with the Office of Nuclear Reactor Regulation (NRR) to develop a formal program plan to achieve a risk-informed, performance-based revision of 10 CFR Part 50. The staff believes that this formal program plan should include followup activities to risk-inform the SFC. This approach will ensure that the safety benefits of any potential changes to the current SFC are evaluated in the broader context of all potential changes to 10 CFR Part 50.

Therefore, the staff recommends that the Commission:

(1) Approve the issuance of the draft SFC technical report for public comment.

(2) Approve including any followup activities to risk-inform the SFC as part of the formal program plan to risk-inform 10 CFR Part 50.

RESOURCES:

The resources needed to engage stakeholders and obtain their feedback on the Draft Single-Failure Criterion Report (Attachment 2) are 0.2 full-time equivalent (FTE) and $50K, which are included in the RES budget for Fiscal Year 2006. Resources required to pursue any followup activities, beyond the near-term engagement of stakeholders, will be included in the formal program plan to risk-inform the requirements of 10 CFR Part 50.

COORDINATION:

The Office of the General Counsel has reviewed this paper and has no legal objections.

The Office of the Chief Financial Officer has reviewed this Commission paper for resource implications and has no objections.

The staff met with the Advisory Committee on Reactor Safeguards concerning this issue on June 1, 2005. In a letter dated June 10, 2005, the Committee supported the staff's positions that (1) it is premature to select any particular alternative at this time, (2) the NRC should seek additional input from stakeholders, and (3) any followup activities to risk-inform the SFC should be included and prioritized in the formal program plan to risk-inform the requirements of 10 CFR Part 50.

/RA by Martin J. Virgilio Acting For/

Luis A. Reyes
Executive Director
for Operations

Attachments: 1. Summary of Risk-Informed Alternatives
2. Draft Single-Failure Criterion Report

Attachment 1

Summary of Risk-Informed Alternatives

	BASELINE ALTERNATIVE (Current Approach): Retain Current SFC	ALTERNATIVE 1: Risk-Inform Application of SFC to DBA Analysis	ALTERNATIVE 2: Risk-Inform Application of SFC Based on Safety Significance	ALTERNATIVE 3: Replace SFC with Risk and Safety Function Reliability Guidelines
Rationale for the Alternative	The intent of the SFC, in part, is to promote high reliability of safety-related systems, and provide adequate safety margin in the event of a single failure of the safety system in response to a design-basis event. Specific licensing issues relating to the SFC arise periodically, providing the opportunity to reconsider application of the SFC from a risk-informed point of view.	Safety-insignificant single-failure event sequences are sometimes included in a plant's design basis, while some safety-significant multiple-failure sequences are not included. Alternative would risk-inform the selection of single-failure event sequences used in DBA analysis.	The intent of the SFC, in part, is to promote high safety-related system reliability. However, the SFC is sometimes not applied in a manner that is commensurate with the safety significance of the system. This alternative would risk-inform application of the SFC based on the safety significance of the system.	The intent of the SFC, in part, is to promote high safety-related system reliability. However, the SFC is sometimes not applied in a manner that is commensurate with the safety significance of the system. This alternative would replace the current SFC with functional reliability targets that relate to top-level risk targets.
Risk-Informed Approach	This alternative would risk-inform the regulatory framework by refining the scope of application of the SFC in selected areas. While the current regulatory structure for implementation of the SFC would not be altered, the staff will consider risk-informing the current SFC in the context of specific licensing issues as they arise (e.g., LBLOCA redefinition). The staff could also consider aspects of Alternatives 1–3 for application to a particular issue. The staff would also develop a position on single passive failures in fluid systems to replace the footnote that currently appears in the definitions in Appendix A to 10 CFR Part 50.	This alternative would risk-inform the event sequences postulated in DBA analysis: (1) Permit removal of sufficiently unlikely, non-risk-significant single-failure sequences from the design basis. (2) Require addition of multiple failure event sequences to the design basis when the frequency of multiple failure event sequences exceeds that of any single-failure sequence postulated for the same initiating event. The staff would also establish quantitative frequency criteria for addition and removal of event sequences to/from the design basis.	This alternative would risk-inform SFC application, such that system reliability would be commensurate with safety significance. System categorization would be consistent with 10 CFR 50.69. Approaches are identified for relaxing the level of defense-in-depth required for systems of low safety significance: (1) Alternative 2a proposes that redundant safety-related trains may be removed from service. The system would then comprise a single train. (2) Alternative 2b proposes that one train would remain safety-related, but the redundant trains could be reclassified as non-safety-related. (3) Alternative 2c proposes that all trains would remain safety-related, and the regulatory requirements for one would remain the same, but operational flexibility could be provided for redundant trains.	This alternative would replace the current SFC with a combination of quantitative targets and guidance: (1) top-level risk targets for CDF and LERF (2) lower-level functional reliability targets commensurate with challenge frequency (3) guidance for redundancy, diversity, and CCF Licensees would determine which plant features to credit to address the targets, and how much credit to take for those features.

	BASELINE ALTERNATIVE (Current Approach): Retain Current SFC	ALTERNATIVE 1: Risk-Inform Application of SFC to DBA Analysis	ALTERNATIVE 2: Risk-Inform Application of SFC Based on Safety Significance	ALTERNATIVE 3: Replace SFC with Risk and Safety Function Reliability Guidelines
Implementation Approach	Initial Licensing Changes: The staff would identify a regulatory issue that could involve some aspect of the SFC (e.g., system reliability or DBA analysis margins). Licensees would submit appropriate information in accordance with the revised requirements. The staff would develop a position on passive failures in fluid systems (considering industry standards), and work that position through the rulemaking process. Performance Monitoring: The staff would consider performance monitoring requirements, as appropriate, for changes in SFC requirements. These requirements could include approaches that are currently being used or developed in the ROP, or augmented approaches for the particular issue if new targets or goals are developed.	Initial Licensing Changes: The staff would issue new guidance for modifying the DBA analysis. Licensees would delineate all possible single- and multiple-event sequences and, on the basis of event sequence frequency, would propose which single-failure paths are to be removed and which multiple-failure paths are to be added to the current design basis. Plant changes proposed on the basis of Alternative 1, if any, would be reviewed based on the guidance in RG 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis." Performance Monitoring: This alternative would require monitoring of industry data related to the frequency of rare initiating events (such as large pipe breaks), as well as periodic revision of expert judgment regarding these frequencies. Plant-specific monitoring programs would be adapted as appropriate to verify PRA models and data used for DBA selection.	Initial Licensing Changes: The staff would develop a new regulation, which could take the form of an expanded version of 10 CFR 50.69 and would include an approach to risk-inform the SFC. The GDCs that relate to the SFC may also have to be modified. Licensees would use a high-quality PRA of their plants, and could make physical or operational changes to the plants' systems as long as the changes meet the guidelines specified in RG 1.174. Performance Monitoring: This alternative would require monitoring of system reliability for safety-significant systems (RISC-1 and RISC-2). Systems of low safety significance (RISC-3) would require monitoring, implemented appropriately for the three approaches for relaxing the level of defense-in-depth.	Initial Licensing Changes: The staff would replace or alter the current regulations., and define the top-level CDF and LERF measures. Licensees would develop functional unreliability targets to meet the top-level targets, and would establish train-level reliability targets. Licensees would also establish redundancy and diversity targets, along with heightened treatment for SSCs performing those functions without benefit of the target redundancy. Licensee changes proposed on the basis of Alternative 3 would be reviewed based on the guidance in RG 1.174. Performance Monitoring: Monitoring would confirm that assigned performance targets are actually met.

Technical Report

TECHNICAL WORK TO SUPPORT EVALUATION OF A BROADER CHANGE TO THE SINGLE-FAILURE CRITERION

Arthur Buslik, U.S. Nuclear Regulatory Commission
Ted Ginsberg, Brookhaven National Laboratory
Hossein Hamzehee, U.S. Nuclear Regulatory Commission
Eric Haskin, ERI Consulting
Jeffrey LaChance, Sandia National Laboratories
John Lane, U.S. Nuclear Regulatory Commission
John Lehner, Brookhaven National Laboratory
Gerardo Martinez-Guridi, Brookhaven National Laboratory
Scott Newberry, Information Systems Laboratories
Robert Youngblood, Information Systems Laboratories

July 2005

Prepared for

Division of Risk Analysis and Applications
Office of Nuclear Reactor Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Page left intentionally blank

TABLE OF CONTENTS

Page

TABLE OF CONTENTS
(continued)

Page

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

This report summarizes the work performed in response to the Commission's Staff Requirements Memorandum of March 31, 2003 that directs the NRC Office of Nuclear Regulatory Research (RES) staff to "pursue a broader change" to the single-failure criterion. The Commission directed that, "The staff should pursue a broader change to the single-failure criterion (SFC) and inform the Commission of its findings." To respond to this directive, a study was undertaken to develop risk-informed performance-based alternatives to the SFC. This report summarizes the background of the SFC, and describes the approach used in formulating the alternatives. Four alternatives, including the current SFC, are discussed. This work applies to the current generation of U.S. nuclear power plants.

The SFC was incorporated in the U.S. Code of Federal Regulations during the early days of the nuclear power industry. The SFC exists in two major contexts: (1) system design requirements, largely associated with the General Design Criteria (GDC) of 10 CFR Part 50 Appendix A, which require designing safety-related systems to perform safety functions to mitigate design-basis initiating events, assuming a single failure, and, (2) guidance on design-basis-accident analysis in Chapter 15 of Regulatory Guide 1.70 and of the Standard Review Plan, directed towards demonstrating adequate design margins based upon defined acceptance criteria. The SFC requirements, found in 10 CFR Part 50.55a(h), specify that plants must meet the requirements of the Institute of Electrical and Electronics Engineers (IEEE) 279 or IEEE 603, depending on the date of the construction permit (but after January 1, 1971). Both of these IEEE standards invoke the SFC. Other NRC regulatory guides and documents have additional guidance, as do other industry consensus standards **that the NRC uses, which are reviewed in this report.**

The intent of the SFC is to promote the high reliability of safety functions that are important to safety, and to help ensure that in the event of a single failure the intended safety function can still be performed. Several regulations, guidelines, and programs, including quality assurance requirements, technical specifications, testing-, inspection-, and maintenance-requirements, act in concert with the SFC to promote high system reliability. However, the SFC has not always led to the design of safety systems whose reliabilities were judged commensurate with the frequency of safety challenges to the plant. Consequently, the SFC was supplemented by other regulatory guidelines and regulations applicable to some safety systems. In turn, these measures led to plant modifications and licensee programs to either improve reliability or to demonstrate that the system's design was otherwise adequate to cope with postulated initiating events. Other actions by the NRC occasioned improvements to address phenomena, such as common cause failure whose impacts on plant safety are not mitigated by redundancy in the design of safety functions. Some additional measures were adopted to supplement the SFC, including the Reactor Oversight Process tracking of safety system availability. **In combination with such measures, regulations, guidelines, and programs, the SFC requirement for the redundant design of safety systems has contributed to maintaining an adequate level of safety of U.S. nuclear power plants.**

As demonstrated in this report, risk-assessment studies reveal that applying the SFC sometimes has led to redundant system elements which while providing an acceptable safety margin, have a minimal impact on risk. While maintaining adequate safety margins is a major safety objective, the benefits of assuming the worst single failure for all design-basis accidents may sometimes place unnecessary constraints on licensees.

Such risk insights suggest that alternatives to the SFC may be constructed that relate more directly to quantitative functional- or system-reliability than does the current SFC, while, at the same time, maintaining appropriate defense-in-depth and adequate safety margins. These alternatives would require the safety

systems to have a level of reliability commensurate with the frequency of challenges to them, and a design that addresses common cause failure, system dependencies, spatial dependencies, and multiple independent failures, that are not considered by the current SFC. In addition, alternatives may be considered which risk-inform the selection of accident sequences that are selected for design-basis analysis. This study explored potential risk-informed alternatives that would address these and other issues related to the SFC.

A process was devised to develop and evaluate potential risk-informed alternatives to the current SFC using a wide range of the NRC's PRA policy documents relating to risk-informing regulatory activities, together with other risk-informed perspectives; with them, a set of desired attributes for the SFC alternatives was developed. Ideally, these attributes should include the following features: (1) quantitatively address and relate safety function reliability to the frequency of challenges and to plant risk, taking uncertainties into consideration, (2) maintain defense-in-depth, (3) ensure risk-informed application of the worst single failure assumption in design-basis analysis, and (4) use performance-based regulatory approaches as much as possible. In addition, the alternatives should be amenable to effective implementation, coherent with other risk-informed regulatory initiatives and **consistent with the NRC's security requirements.**

The characteristics of the existing SFC were compared with these attributes, and its potential modifications were delineated. The potential modifications were then employed to develop risk-informed alternatives that address the GDC reliability context of the SFC, and the worst single failure DBA analysis context of the criterion.

A significant number of potential risk-informed alternatives were conceived that satisfied at least some of the attributes. When they were compared with each other, they demonstrated many similarities. The comparison allowed focusing and merging of the alternatives into four risk-informed alternatives that demonstrate the range of possible approaches to risk-informing the SFC. Table ES-1 summarizes the essential features of the alternatives. All alternatives use defense-in-depth concepts and acknowledge inherent uncertainties. Alternatives 1, 2, and 3 contain elements of performance-based concepts. The alternatives that were developed follow.

- The Baseline Alternative would continue to consider initiatives to change rules and guidance on single failure- and reliability-issues using risk-informed approaches. This approach would include rulemaking on 10 CFR 50.46, and focused improvements discussed in this report, such as updating requirements on passive failures of the components of fluid systems.

- Alternative 1 considers risk-informing the selection of single- and multiple-failure accident sequences for DBA analysis based upon their frequencies. This alternative could eliminate some single-failure accident sequences from the design basis, while it also could lead to the addition of some multiple-failure sequences. Alternative 1 would have a performance-based aspect: the reliability of certain components excluded from the DBA analysis would be monitored to assure their continued high reliability or integrity (e.g., reactor coolant pressure boundary). **This alternative does not consider the redundancy aspect of the SFC.**

- Alternative 2 considers risk-informing the application of the SFC to systems in a manner that is commensurate with their safety significance. This alternative draws upon, and extends, the Risk-Informed Safety Category approach of the special treatment effort in 10 CFR 50.69 as the framework of the safety-significance evaluation method. For non-safety significant safety-related

systems, the requirements of the current SFC would be relaxed. Performance monitoring of safety-significant systems would be required.

Table ES-1 Comparison of Risk-Informed Alternatives

	BASELINE ALTERNATIVE (CURRENT APPROACH) Retain Current SFC	ALTERNATIVE 1 Risk-Inform Application of SFC to DBA Analysis	ALTERNATIVE 2 Risk-Inform Application of SFC Based on Safety Significance	ALTERNATIVE 3 Generalize and Enhance the SFC
Risk-Informed Approach	The original motivation for the SFC was to promote high reliability of safety-related systems, and to provide an adequate safety margin in the event of a single failure in the safety system in response to a design-basis event. Specific licensing issues relating to the SFC arise periodically, providing the opportunity to reconsider application of the SFC from a risk-informed point of view. This alternative would risk-inform the regulatory framework by refining the scope of application of the SFC in selected areas, but would not change the current regulatory structure for implementing the SFC. Risk-informing the current SFC would be considered in the context of specific licensing issues as they arise (e.g., redefining LBLOCA). Aspects of Alternatives 1-3 could be considered for application to a particular issue. A position would be developed on single passive failures in fluid systems to replace the footnote now included in 10 CFR Part 50 Appendix A definitions.	Safety-insignificant single failure event sequences are sometimes included in the plant design basis, while some safety-significant multiple failure sequences are not. This alternative would risk-inform the selection of such sequences used in DBA thermal hydraulics analysis. Risk-inform event sequences postulated in DBA thermal-hydraulics analysis: (1) Permit the removal from the design basis of sufficiently unlikely single-failure sequences that are non-risk significant. (2) Require adding sequences of multiple failure events to the design basis when their frequency exceeds that of any single-failure sequence postulated for the same initiating event. Criteria for quantitative frequency would be established for removing and adding event sequences to the design basis.	The intent of the SFC, in part, is to promote high safety-related system reliability. However, sometimes the SFC is not applied in manner commensurate with the safety-significance of the safety system. Risk-inform application of the SFC such that a system's reliability is commensurate with its safety-significance. Categorizing the systems would be consistent with 10 CFR 50.69. Sub-alternatives are identified for the desired degree of relaxation of the level of defense-in-depth required for systems of low safety significance (RISC 3): (1) Alternative 2a proposes that redundant safety-related trains may be removed from service, leaving the system with a single train. (2) Alternative 2b proposes that one train would remain as safety-related, and reclassifying the redundant trains as non-safety-related. (3) Alternative 2c proposes that all trains would remain as safety-related. The regulatory requirements for one of them remain the same; the redundant trains can encompass operational flexibility.	Current practice, which applies the SFC to selected postulated events (and classifies the credited equipment accordingly), imposes burden that is incommensurate with SSC safety significance as analyzed in risk models. Alternative 3 generalizes the SFC and supplements it with reliability targets to better align safety resources to safety needs. Instead of requiring sufficient redundancy to withstand a single failure in plant's response to selected postulated events (current practice), Alternative 3 requires more redundancy and diversity in response to frequent events, and less for infrequent events. Where redundancy targets are not met, the alternative recommends enhancing the treatment of SSCs to compensate for the lower redundancy. Qualitative redundancy criteria are supplemented by quantitative targets on functional unreliability, and by integrated checks on CDF and LERF. Licensees determine which plant features to credit to address the targets, and how much credit they take for those features. Implementation (including monitoring) is informed by licensee choices.

Table ES-1 Comparison of Risk-Informed Alternatives (continued)

	BASELINE ALTERNATIVE (CURRENT APPROACH) Retain Current SFC	ALTERNATIVE 1 Risk-Inform Application of SFC to DBA Analysis	ALTERNATIVE 2 Risk-Inform Application of SFC Based on Safety Significance	ALTERNATIVE 3 Generalize and Enhance the SFC
Implementation Approach	Initial Licensing Changes: The NRC would identify a regulatory issue that could involve some aspect of the SFC, e.g., system reliability or DBA analysis margins. Licensees would submit appropriate information in accordance with the revised requirements. The position on passive failures in fluid systems would be developed considering industry standards, and worked through the rulemaking process.	Initial Licensing Changes: The NRC would issue new regulations or guidelines for modifying the DBA analysis. The licensee would delineate all possible single- and multiple-event sequences, and, on the basis of event sequence frequency, would propose which single-failure paths are to be removed and which multiple-failure paths are to be added. Any proposed changes to the plant based on Alternative 1 would be reviewed using RG 1.174 guidelines.	Initial Licensing Changes: The NRC would develop a new regulation, which could be an expanded version of 10 CFR 50.69, that would include the approach to risk-informing the SFC. The GDC that are related to the SFC also may have to be modified. The licensee would use the plant's PRA, and could make physical or operational changes to the plant's systems as long as the changes meet the guidelines in RG 1.174.	Initial Licensing Changes: The NRC would replace or change the current regulations. The Agency would define the targets for CDF and LERF, functional unreliability, and redundancy and diversity. The licensee would establish train-level reliability targets satisfying the above, and identify areas needing enhancement. These changes based on Alternative 3 would be reviewed using RG 1.174 guidelines.
	Programmatic Activities: Changes to current activities, such as the Maintenance Rule, ISI, IST, and QA,. would be considered for the particular activity and issue.	Programmatic Activities: No changes considered at this time.	Programmatic Activities: Each sub-alternative risk-informs these activities to some extent. For example, sub-alternative 2c allows operational flexibility, such as relaxation of AOTs, STIs, ISI and IST.	Programmatic Activities: Programmatic activities, such as IST, would be informed by the licensee's choices made to satisfy the targets (e.g., might need to be extended to some systems). A basis for the heightened SSC treatment for systems without target redundancy would need to be addressed.
	Performance Monitoring: Performance monitoring requirements would be considered as appropriate for changes in SFC requirements. They could include current approaches or those being developed in the ROP, or augmented for the particular issue if new targets or goals are developed.	Performance Monitoring: Monitoring would be required of industry data on the frequency of rare initiating events, such as large pipe breaks; also, periodic revision by experts would be needed. Plant-specific monitoring programs would be appropriately adapted to verify PRA models and the data used for DBA selection.	Performance Monitoring: Monitoring would be required of the reliability of safety-significant systems. Each sub-alternative proposes a different type of monitoring of safety-related non-safety-significant systems (see Section 4.4.2.2).	Performance Monitoring: Monitoring would confirm that assigned performance targets are met.

- Alternative 3 generalizes the SFC (varying the redundancy requirement according to the initiating event category, and providing guidance on diversity). It supplements the SFC with top-level risk guidelines and targets for safety-function reliability that also would be established corresponding to the frequency of challenges. The licensee would establish targets for lower-level (train-level) reliability satisfying the functional reliability targets upon which the SSC treatment, including performance monitoring, would be established.

In different ways, Alternatives 1, 2, and 3 each change the scope and range of application of the SFC in the regulatory process, and to various degrees, rely on risk perspectives to modify their implementation. Alternative 1 changes the need to consider the worst single active failure in accident analysis provided that the resulting event sequence has very low frequency. Alternative 2 applies the SFC and variations on the SFC according to the safety significance of systems. Alternative 3 applies the SFC and variations on the SFC to key safety functions, depending on the frequency at which those functions are challenged, and the consequences of their failures. All alternatives retain "structuralist" elements of defense-in-depth that are applied using risk-informed arguments, and all alternatives require some monitoring. **Furthermore, they all could include** developing a position on single passive failures in fluid systems to replace the footnote in the 10 CFR Part 50 Appendix A definitions. These alternatives demonstrate a range of concepts that might be used to pursue risk-informed and performance-based change to the SFC. Other alternatives could be constructed, involving different combinations of the basic concepts.

The report offers illustrative examples of how Alternatives 1, 2 and 3 could be applied in practice. Aspects of these examples demonstrate how a plant's risk models may be used to relax the requirements of the SFC, and thereby provide a licensee with increased operational- or performance-flexibility, while maintaining adequate plant safety. Other aspects demonstrate how the alternatives would enhance or maintain safety by requiring monitoring of non-safety-related, but risk-important safety systems. One example illustrates how the SFC can be generalized and supplemented with top-level risk guidelines and targets for safety-function reliability.

The major focus of this study was to identify potential alternative risk-informed approaches to the SFC. Additional examples or pilot activities would be necessary to better understand the potential usefulness of such alternatives, including approaches to implementation, and the resource implications for further development and implementation of the alternatives. The staff believes that, while a wide range of alternatives have been evaluated, additional stakeholder involvement and further evaluation will be necessary to assess the practicality of implementing any alternative. In fact, stakeholder input may result in other viable alternatives meriting consideration. Therefore, the staff does not recommend one alternative over another at this time. As directed in a staff requirements memorandum dated May 9, 2005, the Office of Nuclear Regulatory Research plans to work with the Office of Nuclear Reactor Regulation to develop a formal program plan to make a risk-informed, performance-based revision to 10 CFR Part 50. The staff could include any follow-up activities to risk-inform the SFC in this formal program plan.

ABBREVIATIONS AND ACRONYMS

AC	Alternating Current
ACRS	Advisory Committee on Reactor Safeguards
ACS	Accumulators
AEC	Atomic Energy Commission
AFW	Auxiliary Feedwater
AFWS	Auxiliary Feedwater System
ANSI	American National Standards Institute
AOT	Allowed Outage Time
ARI	Alternate Rod Injection
ARV	Atmospheric Relief Valve
ASME	American Society of Mechanical Engineers
ATWS	Anticipated Transient Without Scram
BWR	Boiling Water Reactor
CCF	Common Cause Failure
CCP	Centrifugal Charging Pump
CCW	Component Cooling Water
CD	Core Damage
CDF	Core Damage Frequency
CFR	Code of Federal Regulations
CLB	Current Licensing Basis
CRD	Control Rod Hydraulic System
CS	Core Spray
CV	Containment Venting
CVCS	Chemical and Volume Control System
DBA	Design-Basis Accident
DBE	Design-Basis Event
DC	Direct Current
DFC	Double Failure Criterion
DGA	Diesel Generator A
DHR	Decay Heat Removal
DiD (DID)	Defense-in-Depth
ECCS	Emergency Core Cooling System
ECW	Emergency Cooling Water
EDG	Emergency Diesel Generator
EFW	Emergency Feedwater
ESW	Emergency Service Water (BWR) or Essential Service Water System (PWR)
FAB	Feed And Bleed
FMEA	Failure Modes and Effects Analysis
FSAR	Final Safety Analysis Report
FTS	Fail To Start
FV	Fussell-Vesely
GDC	General Design Criterion
GSI	Generic Safety Issue
HFP	Hot Full Power
HPCI	High Pressure Coolant Injection

ABBREVIATIONS AND ACRONYMS
(continued)

HPI	High Pressure Injection
HPSW	High Pressure Service Water
HZP	Hot Zero Power
IEEE	Institute of Electrical and Electronics Engineers
IPE	Individual Plant Examination
IPEEE	Individual Plant Examination External Events
ISI	In-Service Inspection
IST	In-Service Testing
LB	Licensing Basis
LCO	Limiting Condition of Operation
LERF	Large Early Release Frequency
LOAC	Loss of all AC
LOCA	Loss of Coolant Accident
LOMF	Loss of Main Feedwater
LOOP	Loss of Offsite Power
LPCI	Low Pressure Coolant Injection
LPCS	Low Pressure Core Spray
MDP	Motor-Driven Pump
MSPI	Mitigating Systems Performance Index
MTC	Moderator Temperature Coefficient
NA	Not Applicable
NEI	Nuclear Energy Institute
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
NRR	Nuclear Regulatory Research (NRR)
PCT	Peak Cladding Temperature
PDP	Positive Displacement Pump
PIE	Postulated Initiating Event
PORV	Pilot-Operated Relief Valve
PRA	Probabilistic Risk Assessment
PWR	Pressurized Water Reactor
QA	Quality Assurance
QHO	Quantitative Health Objective
RAW	Risk Achievement Worth
RBCCW	Reactor Building Closed Cooling Water
RBPI	Risk-Based Performance Indicator
RCIC	Reactor Core Isolation Cooling
RCP	Reactor Coolant Pump
RCS	Reactor Coolant System
RES	Research (Office of)
RG	Regulatory Guide
RHR	Residual Heat Removal
RISC	Risk-Informed Safety Category

ROP	Reactor Oversight Process

ABBREVIATIONS AND ACRONYMS (continued)

RPS	Reactor Protection System
RSS	Reactor Safety Study
RTS	Reactor Trip System
SAR	Safety Analysis Report
SBO	Station Blackout
SDP	Significance Determination Process
SEP	Systematic Evaluation Program
SFC	Single-Failure Criterion
SG	Steam Generator
SGTR	Steam Generator Tube Rupture
SI	Safety Injection
SLC	Standby Liquid Control
SPAR	Standardized Plant Analysis Risk
SRM	Staff Requirements Memorandum
SRP	Standard Review Plan
SRVs/ADS	Safety Relief Valves/Automatic Depressurization System
SSC	Structure, System, and Component
STI	Surveillance Test Interval
SU	Startup
SUFP	Startup Feed Pump
TBCCW	Turbine Building Closed Cooling Water
TDP	Turbine-Driven Pump
T/H	Thermal Hydraulic
TMI	Three Mile Island
TS	Technical Specifications
US	United States
USI	Unresolved Safety Issue
USNRC	United States Nuclear Regulatory Commission
WSF	Worst Single Failure

1. INTRODUCTION

1.1 Commission Directive

In a Staff Requirements Memorandum (SRM) of March 31, 2003 [USNRC, 2003a] relating to risk-informing the technical requirements of 10 CFR 50.46, the Commission discusses the issue of risk-informing of the Emergency Core Cooling System's (ECCS's) functional reliability requirement of General Design Criterion (GDC) 35. The Commission also directs that "The staff should pursue a broader change to the single-failure criterion (SFC) and inform the Commission of its findings."

1.2 Objective

The objective of this technical report is to respond to the Commission directive to "...pursue a broader change" to the SFC. The NRC's RES staff developed a plan and process to identify risk-informed, performance-based alternatives to the SFC that will ensure safety efficiently and effectively. While the Commission's directive is associated with GDC 35 and the ECCS, the Staff's interpretation of "a broader change" is that alternatives to the SFC could apply to all plant safety (and non-safety) functions, and consequently, could lead to changes in licensing, programmatic activities (such as testing and inspection), and monitoring the plant's performance.

This study of SFC alternatives includes reviewing the background and applications of the SFC in the current regulatory process, developing a process to identify ways to use risk information and alternative implementation strategies in the regulatory process, and, finally, identifying and exploring alternatives to the SFC as requested by the Commission. Risk sensitivity calculations were undertaken to estimate the influence of redundancy on plant risk.

1.3 Organization of Report

Section 2 of this report reviews the background of the SFC requirements, guidance, and implementation. Section 3 describes the process established and used for developing alternatives to the SFC. These alternatives are discussed in Section 4. Section 5 summarizes the findings of this study.

2. BACKGROUND

The single-failure criterion (SFC) is a requirement that contributes to providing adequate levels of safety to the public from operating nuclear power plants. It ensures the high reliability of important safety functions through employing redundancy in design and operation. Plants are designed to cope with a set of safety challenges embodied in a set of design-basis initiating events. The SFC helps to assure that specific safety-related systems respond to the challenges with adequate reliability, and to establish safe end states with adequate safety margins. The criterion has been accepted as one element of the NRC's traditional defense-in-depth strategy of providing multiple means of satisfying important safety functions.

The SFC is found in NRC documents in two major contexts:

- Safety system design requirements, largely associated with the General Design Criteria of 10 CFR Part 50 Appendix A, expanded upon in Regulatory Guide 1.70 and the Standard Review Plan [USNRC, 1981a].

- Guidance on the design-basis-accident analysis of Chapter 15 of Regulatory Guide 1.70, of the Standard Review Plan, and of 10 CFR Part 50.46 and Appendix K, directed towards demonstrating adequate design margins based upon defined acceptance criteria.

Additional guidance pertaining to the SFC are found in industry consensus standards that are accepted for use by NRC. These NRC and standards documents are discussed below. It is important to emphasize that the SFC and its implementation are part of the larger set of requirements included in the NRC's regulatory process.

This section reviews the current implementation of the SFC with the objective of identifying issues that may be considered for developing risk-informed alternatives to it. Sections 2.1 and 2.2 review the SFC requirements in 10 CFR Part 50, and guidance contained in various regulatory and industry consensus documents. Additional background to the SFC is given in the remainder of this section, including a description of its current implementation in Section 2.3, defense-in-depth in Section 2.4, and various issues to take into account in developing alternatives in Section 2.5. Section 2.6 summarizes the results of sensitivity calculations that were performed to show the influence of redundancy on the core damage frequency of current light-water reactor NPPs in the United States. Section 2.7 discusses the SFC from a risk-informed perspective, and summarizes basic issues requiring attention in developing risk-informed alternatives to the SFC.

2.1 Single-Failure Criterion Requirements in 10 CFR Part 50

The single-failure requirement was established in the mid 1960s by the United States Atomic Energy Commission as a regulatory requirement for nuclear plants in the form of General Design Criteria (GDC), and was promulgated as a regulation in 1971. It was first applied to the plant protection system, and required that "A reliable protection system must be provided" [AEC, 1965], and then to the Emergency Core Cooling System (ECCS) [AEC, 1967]. The basic wording of the single failure requirement for the ECCS was retained over the years, and is found in the current GDC 35 [CFR, 2004]. This same wording also is used in applying the General Design Criteria to other safety systems.

The term "single failure" is defined in 10 CFR Part 50 Appendix A [CFR, 2004]:

"A single-failure means an occurrence which results in the loss of capability of a component to perform its intended safety functions. Multiple failures resulting from a single occurrence are considered to be a single-failure. Fluid and electric systems are considered to be designed against an assumed single-failure if neither (1) a single-failure of any active component (assuming passive components function properly) nor (2) a single-failure of a passive component (assuming active components function properly), results in a loss of the capability of the system to perform its safety functions."

[Associated footnote: "Single failures of passive components in electric systems should be assumed in designing against a single failure. The conditions under which a single failure of a passive component in a fluid system should be considered in designing the system against a single failure are under development."]

Table 2.1-1 lists the occurrences of "single failure" in 10 CFR Part 50. In addition to defining a single failure, the General Design Criteria (GDC) of Appendix A identifies safety functions and associated safety systems to which the single-failure requirement must be applied. Table 2.1-2 presents several redundancy requirements from 10 CFR Part 50 that do not use this single failure wording.

The GDC define functional requirements for each designated safety function, and a single-failure requirement is stated for each safety function. For example, Criterion 34 for the Residual Heat Removal safety function states [CFR, 2004]

"A system to remove residual heat shall be provided. The system safety function shall be to transfer fission product decay heat and other residual heat from the reactor core at a rate such that specified acceptable fuel design limits and the design conditions of the reactor coolant pressure boundary are not exceeded.

Suitable redundancy in components and features, and suitable interconnections, leak detection, and isolation capabilities shall be provided to assure that for onsite electric power system operation (assuming offsite power is not available) and for offsite electric power system operation (assuming onsite power is not available) the system safety function can be accomplished, assuming a single failure."

Table 2.1-1 Occurrences of "Single Failure" in 10 CFR Part 50

Location	Title of Part, Appendix, or GDC	Description of Use
50.2	Definitions	Contained in the definition of "station blackout"
50.34(f)(3)(vi)	Contents of applications; technical information (TMI requirements)	Provides for redundant dedicated containment-penetrations for connecting external hydrogen recombiners to the containment atmosphere
50.49(e)(3)	Environmental qualification of electric equipment important to safety for nuclear power plants	Used to establish the most severe chemical spray environment from the spray system, if the chemical spray composition can be affected by equipment malfunctions

Table 2.1-1 Occurrences of "Single Failure" in 10 CFR Part 50 (continued)

Location	Title of Part, Appendix, or GDC	Description of Use
50.55a(h)	Protection and Safety Systems	Requires using IEEE 279 and approves using IEEE Std. 603-1991, "Criteria for Safety Systems for Nuclear Power Generating Stations" for certain nuclear power plants. Standards define the "single-failure criterion", and contain the requirements for single-failure analysis of "safety systems".
Appendix A (Table of Contents)	General Design Criteria for Nuclear Power Plants	Included in Table of Contents, under "Definitions"
Appendix A (Introduction)	General Design Criteria for Nuclear Power Plants	Indicates that the conditions under which a single failure of a passive component in a fluid system should be considered are under development
Appendix A (Definitions and Explanations)	General Design Criteria for Nuclear Power Plants	Provides definition of "single failure" (Footnote [2] in definition also states that single failures of passive components in electrical systems should be assumed in designing against single failures, but that the conditions under which a single failure of a passive component in a fluid system should be considered are under development)
Appendix A, GDC 17	Electric power systems	Establishes the single failure requirement for onsite electric power supplies and distribution system
Appendix A, GDC 21	Protection system reliability and testability	Establishes the single failure requirement for the protection system.
Appendix A, GDC 34	Residual heat removal	Sets out the single failure requirement for the residual heat removal system
Appendix A, GDC 35	Emergency core cooling	States the single failure requirement for the emergency core cooling system
Appendix A, GDC 38	Containment heat removal	Establishes the single failure requirement for the containment heat removal system
Appendix A, GDC 41	Containment atmosphere cleanup	Establishes single failure requirement for containment atmosphere cleanup systems
Appendix A, GDC 44	Cooling water	Establishes the single failure requirement for cooling water systems used to transfer heat from systems important to safety to an ultimate heat sink
Appendix K(I)(A)	ECCS Evaluation Models	Establishes single failure requirement for determining the limiting power distribution assumed as part of the required and acceptable features of the evaluation model
Appendix K(I)(D)	ECCS Evaluation Models	Establishes the single failure requirement for evaluating post-blowdown heat removal by the ECCS

Table 2.1-1 Occurrences of "Single Failure" in 10 CFR Part 50 (continued)

Location	Title of Part, Appendix, or GDC	Description of Use
Appendix R(III)(L)(6)	Fire Protection Program for Nuclear Power Facilities Operating Prior to January 1, 1979	Establishes that single failure requirement does not apply to shutdown systems installed to ensure post-fire shutdown capability.

Table 2.1-2 Redundancy Requirements in 10 CFR Part 50

Location	Title of Part, Appendix, or GDC	Description of Use
50.62 (c)(2) 50.62 (c)(3)	Requirements for reduction of risk from ATWS	Each Combustion Engineering and Babcock and Wilcox plant must have a scram system that is diverse from the RTS. Each BWR must have an alternate rod injection (ARI) that is diverse from the RTS. Alternate rod injection system must have redundant scram air header exhaust valves.
50.63	Requirements for Loss of all alternating current power	Requirements for withstanding a station blackout include a consideration of onsite emergency ac power source redundancy
Appendix R III(A)	Fire Protection Program	Requires two separate water supplies to provide necessary water volume and pressure to the fire main loop...Two separate redundant suctions in one or more intake structures from a large body of water (river, lake, etc.) will satisfy the requirement for two separated water storage tanks.
Appendix A, Criterion 17	Offsite power system	Requires offsite source of electric power from the transmission network to the onsite electric distribution system consisting of two physically independent circuits designed and located to minimize the likelihood of their simultaneous failure under operating and postulated accident and environmental conditions.
Appendix A, Criterion 24	Separation of protection and control systems	Requires that redundancy, reliability and independence of protection system remain intact in event of failure of single control system or protection system component or channel[1] failure.
Appendix A, Criterion 26	Reactivity control system redundancy and capability	Two independent reactivity-control systems with different design principles are required.
Appendix A, Criterion 54	Piping systems penetrating containment	Piping systems penetrating primary reactor containment shall be provided with leak detection, isolation, and containment capabilities having redundancy, reliability, and performance capabilities which reflect the importance to safety of isolating these piping systems.

[1]A channel is a path through which a signal can flow.

The single-failure requirement of Criterion 34 is that redundancy shall be used to ensure the performance of the safety functions in the event of a single failure, given the additional assumptions about the availability of electric power identified in the second paragraph. This language is typical of the single failure requirements for the safety functions of GDC 34, 35, 38, 41, and 44 identified in Table 2.1-1.

In addition to the redundancy requirements associated with single failure language, Table 2.1-2 shows a number of redundancy requirements from 10 CFR Part 50 that do not use the single failure wording described above.

2.2 Guidance for Implementing the Single-Failure Criterion

The regulatory requirements of 10 CFR 50 for single failures cited in Section 2.1 are supplemented by several regulatory guides and industry consensus standards. The regulatory documents, guides, and standards are summarized in Table 2.2-1. 10 CFR 50.55a(h) contains the regulatory reference to industry consensus standards, which requires the plant's protection systems to satisfy either IEEE Std 279-1971 [IEEE, 1971] or IEEE Std 603-1991 [IEEE, 1991].

Table 2.2-1 Single -Failure Guidance Documents

Document	Content
"USNRC Standard Review Plan", NUREG-0800 - Safety Systems Design Criteria - Chapter 15 Accident Analysis	Chapters 4-10 present the review criteria for the SFC for a broad range of systems. Chapter 6 – Engineered Safety Features. Chapter 15- Accident Analysis describes the review criteria for analyzing transients and accidents, including the SFC.
Regulatory Guide 1.70 - Standard Format and Content of Safety Analysis Reports for NPPs - Safety Systems Design Criteria - Chapter 15 Accident Analysis	Chapters 6-10 delineate Engineered Safety Features and other systems, and specify the SFC's implementation. Chapter 6 – Engineered Safety Features. Chapter 15 describes DBAs with guidance on SFC assumptions.
"IEEE Criteria for Nuclear Power Plant Protection Systems", IEEE Std. 279-1971	Requires the plant's protection systems to satisfy single-failure criterion.
"IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," IEEE Std. 379-2000	This version broadens the application of the single-failure criterion from "protection systems" to "safety systems".
"IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," IEEE Std. 603-1991	The 603 standard defines the "single-failure criterion" and discusses its implementation for single-failure analysis of "safety systems". This standard refers to the 379 standard for details of implementing SFC. The NRC has not modified RG 1.153 to reflect the updated 603 standard.
"Regulatory Guide 1.153 – Criteria for Safety Systems"	Endorses IEEE Std 603-1991 as acceptable for the power-, control-, and instrumentation-portions of safety systems.
Regulatory Guide 1.53 - "Application of the Single-Failure Criterion to Safety Systems"	Endorses IEEE Std 379-2000 as an acceptable method for satisfying the single-failure criterion for "safety systems".
"Single-Failure Criteria for Light Water Reactor Safety-Related Fluid Systems", ANSI/ANS 58.9	The NRC has not endorsed the SFC for fluid systems. Not endorsed by NRC. May be in use from early licensing activities.

Since the regulations are rather general ones, including the GDC, the NRC's staff began in the early 1970s to issue review guidance for improving the quality and uniformity of its regulatory review. The two primary documents covering safety analysis and regulatory review are Regulatory Guide 1.70 [USNRC, 1978] and the Standard Review Plan. The former contains guidance on the format and content of safety analysis reports, and also on single-failure assumptions. Chapter 15 of both documents describe the scope of the accident analysis that should be given in the plant's safety-analysis reports the intent of which is to evaluate the safety of the plant in its response to postulated initiating events. SECY-77-439 [USNRC, 1977] and NUREG-1412 [USNRC, 1991] describe the evolution of this guidance.

Because of the intricacy of the many fluid and electrical systems, their interrelationships, and their supporting auxiliary systems, correspondingly, the guidance on the SFC, and its evolution, is complex. Staff documents indicate that its application is intended to be a systematic search for design weaknesses in certain prescribed safety missions. In some cases, increased redundancy compensates for the weaknesses. In others, using alternate systems, or the operator's action, is judged to be acceptable. Regulatory positions were developed for active and passive failures, and for operator errors, for a range of events and systems. They are embodied in the SRP and associated Regulatory Guides, and Branch Technical Positions. This study did not explore all of the particular SFC regulatory positions and guidance, but investigated many of them to better support consideration of potential alternatives. The following are some examples of the regulatory positions taken on the SFC in important reactor systems.

One of the more noteworthy ones is the Auxiliary Feedwater System. From lessons learned following the TMI accident, the requirements and guidance for AFW systems were enhanced beyond the SFC concept to ensure increased reliability and defense against common-mode failure. Section 10.4.9 of the SRP addresses these extensions. In addition to a system being able to perform its function assuming a single active failure, it must have diverse "motive power sources" and must undergo a reliability analysis in accordance with the criteria in NUREG-0737 [USNRC, 1980].

Risk assessments and operating experience related to offsite power systems and onsite emergency power sources indicated a need to increase plant capability. The NRC developed and issued 10 CFR 50.63, Loss of all AC Power that requires plants be able to withstand a station blackout for a specified duration, and recover from it. The duration is based on redundancy and reliability of onsite emergency power sources, the expected frequency of loss of offsite power, and the probable time needed to recover offsite power.

The NRC and industry explored the need to improve a plant's shutdown capability over many years to respond to frequent transients, such as turbine trips and loss of feedwater. After the failure of the trip breakers of the reactor protection system to function properly at the Salem plant due to a common-mode failure in 1983, the NRC developed and issued the Anticipated Transients Without Scram Rule, 10 CFR 50.62. This regulation requires plants to have diverse shutdown features to backup plant protection systems that are designed to strict regulatory requirements, including the SFC.

In addition to requiring a redundant, safety-grade system, Section 6.3 of the SRP discusses considering passive failures in the Emergency Core Cooling Systems during the recirculation cooling mode following emergency coolant injection; it does not define the specific failure. SECY-77-439, NUREG-0138 [USNRC, 1976a] and NUREG-0153 [USNRC, 1976b] describe the background and difficulty establishing a consensus on this issue. The NRC staff took the position in licensing reviews that applicants must consider the degradation of a pump or valve seal and the resulting leakages, in addition to the initiating failure (LOCA). Their rationale for applying this type of failure was the recognition of the relatively extended periods that

the systems must operate whilst in the recirculation mode. NUREG-0138 elaborated on the basis for excluding additional passive piping failures.

Section 5.4.7 of the SRP describes consideration of the SFC for the RHR system and the design of systems with redundant trains. The criterion is applied to the functioning of the decay heat removal system. Redundancy and diversity guidance is described for the isolation function between the high pressure reactor coolant system and the RHR system. A Branch Technical Position 5-1 is attached giving details for achieving cold shutdown using suitably redundant safety-grade systems.

The role of the operator also has been considered as a potential source of single failure, and judgements made in licensing reviews about the operator's "errors of omission" for essential actions. An example is Emergency Core Cooling System switch-over from injection to recirculation, which is done manually at older plants. Manual actions were judged to be acceptable for this switch-over, provided that there was sufficient time and information. New plants must have automatic means for this function.

Considerable regulatory guidance was developed, pertaining primarily to the reactor protection systems and engineered safety features, because of the need to have highly reliable instrumentation and control systems to monitor and control important plant systems. Regulatory Guide (RG) 1.53 [USNRC, 2003b] describes the application of the SFC to safety systems. Three related standards are discussed: IEEE Std 279-1971, IEEE Std 603-1991, and IEEE Std 379-2000. Standards 279 and 603 present minimum functional design standards for nuclear plant "protection" and "safety" systems, respectively. Both require that safety systems satisfy the SFC, and refer to Std 379 for guidance on applying the SFC. Std 603 includes protection systems within the general category of safety systems. RG 1.53 delineates those plants (by date of plant license) that must satisfy Std 603, and those that may continue to satisfy Std 279. It encourages the use of IEEE Std 603-1991 and IEEE Std 379-2000 in any future system-level modifications. While not endorsed by NRC, the ANSI/ANS Standard 58.9 provides single failure guidance for safety-related fluid systems. This standard, in part, recommends an approach for treatment of passive failures in these systems.

The IEEE standards provide guidance for systematically approaching the analysis of single failures to safety systems. They also offer guidance on selecting "credible" events and failures to include in these analyses. Both IEEE Std 603-1991 and IEEE Std 379-2000 state that the SFC is to be applied to "credible" events and failures, where probabilistic assessments may be used to assist in establishing credibility. IEEE Std 379-2000 states a position on excluding particular failures from single-failure analysis, as follows:

> "A probabilistic assessment shall not be used in lieu of the single failure analysis. However, reliability analysis, probability assessment, operating experience, engineering judgment, or a combination thereof, may be used to establish a basis for excluding a particular failure from the single failure analysis."[IEEE, 2000]

While this paragraph provides a position for excluding improbable failures from single failure analysis, as described earlier, exceptions have been granted for particular single failures consistent with this guidance. They include passive failures for accident initiators judged to have a very low frequency and the subsequent postulated piping failures (following a design-basis initiator), and for postulating active failures during equipment outages (technical specifications allowed outages)[2].

---

[2]The IAEA (whose guidelines the NRC does not use) also has similar guidance for selecting events and failures. In addition, the IAEA recognizes that system reliability should be related to initiating event frequency: "The reliability of the safety functions should be commensurate with the expected frequency of occurrence of PIEs

2.3 Implementation of the SFC in the Regulatory Process

The 10 CFR 50 requirements, along with the guidance by Regulatory Guide 1.70, the Standard Review Plan and applicable standards (discussed in Section 2.2), form the basis for implementing the SFC. As stated previously, this is a complex process. Studies of operating experience, the evolution of staff review guidance, the resolution of safety issues identified in the review process (related to the SFC), and the availability of risk-assessment information, have contributed to changes in NRC's requirements and oversight, plant design, operation, and maintenance. Implementation of the SFC is discussed in three categories: licensing activities, programmatic activities and performance monitoring.

Licensing Activities

The licensee proposes a plant design intended to provide safety functions and associated safety systems that meet the requirements in the GDCs of 10 CFR Part 50 Appendix A, subject to the guidance provided by RG 1.70, the Standard Review Plan, IEEE standards, and other standards. Some of these are discussed in Section 2.2. These GDCs specify that the single-failure criterion must be applied assuming that either onsite or offsite (not both) electric power is available[3]. Licensees apply the IEEE standards and other specific supporting staff guidance for each review area to their design. Many times failure modes and effects analyses, or other safety sequence logic studies, are performed as a basis to conclude that the single failure requirements are met. This work frequently is included in the FSAR.

A licensee performs safety analyses for a range of postulated transients and accidents to show that the consequences meet acceptable limits. As analysis and review guidance became better defined, the analyses undertaken were outlined in Chapters 15 of RG 1.70 and the Standard Review Plan. Consistent with the guidance described previously for each initiating event and for particular plant systems, the licensee defines those safety functions needed to maintain plant parameters within acceptable limits. For each required safety function for an event, the licensee identifies a safety system, or combination of them, that satisfy the essential safety function and the safety-protective actions.

NRC regulatory guidance specifies that the transients and accidents analyzed in the plant safety analysis report cover a sufficiently broad spectrum of events; to ensure that initiating events of certain types and expected frequencies of occurrence are analyzed; and to permit the consistent application of specific acceptance criteria for each postulated initiating event. In general, each initiating event is assigned to one of three frequency groups: incidents of moderate frequency, infrequent incidents, or limiting faults.

For an event of moderate frequency, the appropriate acceptance criteria for maintaining the reactor coolant pressure boundary and fuel integrity must be met. The most limiting plant systems single failure is to be identified and assumed in the analysis. Conservative input assumptions, such as the reactor's power level, the mitigating system's actuation set points, and the characteristics of the reactor scram are to be assumed.

(Postulated Initiating Events) whose effects they are called upon to prevent or mitigate." This stated view is similar to the NRC's Option 3 concept for the "Quantitative Guidelines for Risk-Informed Changes to Regulatory Requirements" [USNRC, 2000a]. It is also seen as one potential attribute of the proposed alternatives to the SFC.

[3]Additional specific assumptions about the loss of offsite power are given in Chapter 15 of the Standard Review Plan.

Guidance also is given for analyzing the lower probability limiting faults, such as large pipe ruptures. They are intended to be conservative and bounding, and should encompass the range of conservative inputs, the assumption of the worst-case single failure in the systems required to control the transient, and an assumed loss of offsite power. In some cases, the SRP guidance also discusses the need to study the timing of such failures and a review of how a specific system's single active failures could affect the course of the accident.

The NRC's staff reviews the licensee's safety analysis report. The single-failure criterion is applied in the context of the specific accident analyses and the particular systems analysis performed to meet the regulations. Before and after the license is issued, the NRC carries out an inspection and oversight process.

As the NRC's review of license applications and implementation of the regulations and guidance evolved over the years, they identified generic issues in the review process. Some of them pertained to the adequacy of the SFC in a certain context, or utilized redundancy, or the SFC, in the resolving the issue. These issues were pursued and addressed in the NRC generic safety issue (GSI) program. NUREG-0933, "A Prioritization of Generic Safety Issues" [USNRC, 1984], describes generic issues and their resolution. The issues were identified and resolved systematically, according to their safety significance. For example, a special group of 22 GSIs of special safety significance were judged to warrant high priority attention and were designated Unresolved Safety Issues (USIs). All USIs have been resolved. The following USIs, taken from NUREG-0933, illustrate how plant design issues have been resolved that relate to, or utilize the SFC:

> USI A9-Anticipated Transients Without Scram (ATWS). This issue involved a question as to whether Reactor Protection System design requirements, including the requirement for redundant shutdown systems, were sufficient for mitigating frequent transients. The resolution of this issue developed additional system requirements to prevent or mitigate an ATWS event.
>
> USI A-17-System Interactions. The primary issue addressed here was the sufficiency of independence of redundant trains–trains that were designed to meet the single-failure criterion. The complete resolution, described in NUREG-0933, included a generic communication and consideration of plant improvements to reduce the interdependencies.
>
> USI A-19-Digital Computer Protection Systems. Implementation of GDC 21 for digital systems was considered in this USI. Additional criteria for redundant software based systems were developed to ensure adequate reliability for these systems and were published in Regulatory Guide 1.152.
>
> USI A-26-Reactor Vessel Pressure Transient Protection. Early operating experience with pressurized water reactors indicated a need to add a reactor vessel over-pressure protection capability for low temperature operation. Resolution of this issue included a new requirement for a system that would prevent exceeding Appendix G limits of the reactor vessel, assuming a single failure. The regulatory position was published in RSB Branch Technical Position 5-2 associated with SRP section 5.2.2.
>
> USI A-31-RHR-Shutdown Requirements. SRP Section 5.4.7 was augmented to document the resolution of this issue. This SRP describes the regulatory position that light water reactors have the capability to proceed from hot shutdown to cold shutdown using safety grade systems that have suitable redundancy and can perform their functions assuming a single failure.
>
> USI-A-44-Station Blackout. A regulation was developed that required additional plant capability, beyond redundant systems, to respond to a loss of offsite power.

In 1977, the NRC initiated the Systematic Evaluation Program (SEP) to review the designs of 10 of the oldest operating nuclear power plants and thereby confirm and document their safety. Issues from this program also were factored into the regulatory process, including the GSI program. Their resolution encompassed numerous regulatory actions including reactor plant and system safety and reliability studies, new regulations such as the ATWS, Station Blackout, and Maintenance rules, generic letters and bulletins, and the Individual Plant Examinations for internal and external events (IPE and IPEEE). Improvements in design and enhancements in procedures were made in response to these NRC actions to put in place measures to counter vulnerabilities from common-mode failure, the potential for human error and for passive failures, and the functional reliability levels judged to be too low relative to their risk significance–all limitations of the SFC.

NUREG-1412 [USNRC, 1991], "Foundation for the Adequacy of the Licensing Bases" describes these NRC programs. The NRC regulatory process, which assures that the plant-specific licensing bases contain reasonable assurance of safety, has provisions allowing this evolution of requirements, guidance, and licensing bases as lessons are learned and new information becomes available. The current licensing basis (CLB) is the set of NRC requirements applicable to a specific plant, and a licensee's written commitments for assuring compliance with, and operation within, applicable NRC requirements and the plant-specific **design basis** (including all modifications and additions to such commitments over the life of the license) that are docketed and in effect. Different plants have dissimilar CLBs, with diverse approaches to resolving issues, as described earlier. These distinctions arise because plants are licensed at different times, at different sites, with different designs and individual operating experience. The Commission determined that this regulatory process, including the plant-specific resolution of these issues, ensures an adequate level of safety.

After the issuance of the Commission's PRA policy statement in 1995, and direction from the Commission, the staff embarked on broadening uses of risk in the regulatory process. In SECY 98-300, options for proceeding with these programs were outlined and are now being implemented. Many options deal with the role of the SFC. For example, the staff is currently evaluating ways to redefine the design-basis LOCA regulations which are expected to include a different SFC approach for the spectrum of LOCAs. The activity described in this report is a step to consider additional alternatives to the current formulation and uses of the SFC in the regulatory process.

Continued Programmatic Activities to Assure Safety Margins and Promote Functional Reliability

As risk assessment tools improved, additional regulatory programs were begun to better focus on risk-important issues and manage the risk of plant operation–rather than relying solely on the deterministic aspects of the regulations, including the SFC. The South Texas plant received NRC's approval through the exemption process for implementing a graded approach to the treatment of plant systems, structures, and components. This risk-informed application was a proof-of-concept of the graded special-treatment approach to regulation. The experience set the stage for the current 10 CFR 50.69 rulemaking activity that would allow other plants to voluntarily pursue a similar approach. Work continues on improving the Technical Specifications by employing risk information to regulate a plant's operation. For example, In-Service Testing (IST) and In-Service Inspection (ISI) activities have been risk-informed. Allowed outage times, surveillance test intervals, and plant system and component maintenance configurations are being adjusted using risk information.

Monitoring Activities

The NRC programs that monitor the performance of the plant and its equipment also were modified to focus resources on safety issues, rather than using the requirement for redundancy as the programs' sole

objective. As part of continuing licensing and monitoring regulatory activities, the staff has recently approved a license amendment request to exclude a particular single failure from the design-basis of a certain Chapter 15 accident scenario provided that selected criteria are met [USNRC, 2004f]. Staff review and approval became necessary because the existing licensing basis was shown to not have considered the worst single failure scenario, although the risk implications were thought to be minimal. Hence, a more performance-based regulatory alternative to the current SFC has potential to improve the effectiveness and efficiency of licensee and NRC programs. A major step was taken by implementing the Maintenance Rule, 10 CFR 50.65, that focuses on reliability monitoring and managing risk while carrying out maintenance. The NRC's event reporting requirements were more closely aligned with the safety significance of the event or degraded equipment's condition. The Reactor Oversight Process (ROP) uses risk information to focus inspections, monitor a plant's safety performance, and to determine the significance of events and inspections findings. As experience is gained in this program, the performance indicators being used are being improved.

2.4 Defense-in-Depth and the Single-Failure Criterion

Defense-in-Depth Philosophy and RG 1.174

Defense-in-depth is a basic element of the NRC's safety philosophy, and the Commission stated that this concept always has been, and will continue to be a fundamental tenet of regulatory practice in the nuclear field. Defense-in-depth can be applied in various ways. 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 limit the release of radionuclides to the environment.

One of the principles of defense-in-depth is that accomplishing key safety functions should not depend upon a single element of design, construction, or operation. The SFC addresses this requirement by providing a measure of redundancy to fulfill key safety functions. Redundancy enhances the reliability of independent means; diversity protects against dependent (common-cause) failures of multiple means, and, therefore, protection against the uncertainty in the mechanism of dependent failures. The SFC ensures redundancy, but not necessarily diversity. For example, two similar trains of ECCS provide redundancy, while one motor-driven and one steam-driven source of injection offers redundancy and diversity; both satisfy the SFC. The SFC was supplemented to enhance levels of safety (e.g., by adding the requirements related to AFW, ATWS and SBO).

In 1995, the Commission issued the PRA policy statement directing that the use of PRA technology should be increased in all regulatory matters to the extent supported by the state-of-the-art in PRA methods and data, and in a manner that complements the NRC's deterministic approach and supports its traditional defense-in-depth philosophy. The role of defense-in-depth is also described further in staff guidance documents for using risk information to change a plant's current licensing basis. Regulatory Guide 1.174 and Chapter 19 of the SRP describe the principles of risk-informed regulation–one being defense-in-depth. This guidance is included here because it acknowledges the role of redundancy, and the viability of reconsidering it in a risk context. RG 1.174 states that

> "...the engineering evaluation should evaluate whether the impact of the proposed LB change (individually and cumulatively) is consistent with the defense-in-depth philosophy. In this regard, the intent of the principle is to ensure that the philosophy of defense-in-depth is maintained, not to prevent changes in the way defense-in-depth is achieved. The defense-in-depth philosophy has traditionally been applied in reactor design and operation to provide multiple means to accomplish

safety functions and prevent the release of radioactive material. It has been and continues to be an effective way to account for uncertainties in equipment and human performance. If a comprehensive risk analysis is done, it can be used to help determine the appropriate extent of defense-in-depth (e.g., balance among core damage prevention, containment failure, and consequence mitigation) to ensure protection of public health and safety. When a comprehensive risk analysis is not or cannot be done, traditional defense-in-depth considerations should be used or maintained to account for uncertainties. The evaluation should consider the intent of the general design criteria, national standards, and engineering principles such as the SFC. Further, the evaluation should consider the impact of the proposed LB change on barriers (both preventive and mitigative) to core damage, containment failure or bypass, and the balance among defense-in-depth attributes. As stated earlier, the licensee should select the engineering analysis techniques, whether quantitative or qualitative, traditional or probabilistic, appropriate to the proposed LB change.

The licensee should assess whether the proposed LB change meets the defense-in-depth principle. Defense-in-depth consists of a number of elements, as summarized below. These elements can be used as guidelines for making that assessment. Other equivalent acceptance guidelines may also be used.

Consistency with the defense-in-depth philosophy is maintained if:

- A reasonable balance is preserved among prevention of core damage, prevention of containment failure, and consequence mitigation.
- Over-reliance on programmatic activities to compensate for weaknesses in plant design is avoided.
- System redundancy, independence, and diversity are preserved commensurate with the expected frequency, consequences of challenges to the system, and uncertainties (e.g., no risk outliers).
- Defenses against potential common cause failures are preserved, and the potential for the introduction of new common cause failure mechanisms is assessed.
- Independence of barriers is not degraded.
- Defenses against human errors are preserved.
- The intent of the General Design Criteria in Appendix A to 10 CFR Part 50 is maintained."

This text from RG 1.174 recognizes that redundancy, the central feature of the SFC, is an important element of the defense-in-depth philosophy. However, the guide goes on to say that "...its use is to be preserved commensurate with the expected frequency, consequences of challenge to the system..." This wording reflects that RG 1.174 recognizes the usefulness of risk analysis in dealing with defense-in-depth considerations: "If a comprehensive risk analysis is done, it can be used to help determine the appropriate extent of defense-in-depth..." This statement is in keeping with more recent thinking on defense-in-depth wherein quantitative risk considerations are introduced. Risk insights can estimate the benefits of individual elements of defense-in-depth by quantifying their impact on risk, to the extent practicable. In this approach, the traditional defense-in-depth considerations are supplemented with quantitative criteria that assess the adequacy of such existing or proposed measures in terms of the expected frequency and consequences of challenges to the system, including the impact of uncertainties. Involving risk insights directly in deciding upon the adequacy of, or the need for, elements of defense-in-depth is made practical by the development of the ability to quantify risk and estimate uncertainty with PRA techniques.

Use of Risk Insights to Guide Defense-in-Depth Measures

The ACRS and others considered the use of quantitative risk assessments and risk insights to help determine the extent of defense-in-depth for a specific application [Sorenson, 1999]. The terms 'structuralist' and 'rationalist' are used to distinguish between the traditional approach to defense-in-depth and the risk-informed approach. These approaches are briefly summarized here because of their potential implications to developing alternatives to the SFC.

According to the structuralist model, defense-in-depth is embodied in the structure of the regulations and in the design of the facilities built following those regulations. The requirements for defense-in-depth result from repeatedly asking the question, "What if this barrier or safety feature fails?" This question does not encompass a quantitative estimate of the likelihood of such failure. Therefore, a characteristic of this approach to defense-in depth, used in the past, 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. The structuralist approach specifies qualitative requirements in the regulations to ensure that the accomplishment of key safety functions does not depend upon a single element of a plant's design or operation.

In the rationalist model, defense-in-depth is the aggregate of provisions made to compensate for the uncertainty of, and incompleteness in, knowledge of the initiation and progression of accidents. It seeks to evaluate the uncertainties in the analysis and to determine what steps should be taken to compensate for them. The probability of accidents is kept acceptably low by providing defense-in-depth measures in the plant's design, construction, and operation. The adequacy of these measures can be assessed in the rationalist approach via quantitative criteria that specify performance parameters, such as a large radionuclide-release goal, or an equipment reliability goal. In addition, the regulations include specific requirements on such issues as safety margins, levels of confidence, and monitoring and feedback, to ensure uncertainties are properly accounted for in meeting the goals.

One possible risk-informed approach is employing a defense-in-depth model that incorporates both the structuralist and rationalist approaches. At the high level of the cornerstones of the Reactor Oversight Program (initiating events, mitigative systems, barrier integrity, emergency preparedness) the structuralist model is used. By requiring that each cornerstone is met with a certain confidence, the structuralist aim is preserved of assuring several layers of defense, no matter how well any one layer may work. Within each cornerstone, a rationalist approach could determine how much defense-in-depth is needed to achieve the desired quantitative goals, for example, on the frequency of initiating events, or the reliability of mitigating systems, including uncertainty.

Risk-Informed Application of Defense-in-Depth to the Single-Failure Criterion

The SFC, established as an element of the traditional or structuralist, implementation of defense-in-depth, has proved very useful in assuring safety. However, in some cases, it needed to be supplemented to enhanced the levels of safety; in others, it was overly restrictive. Including rationalist, risk-informed considerations in formulating possible alternatives to the SFC in its present form can offer greater assurance that their implementation will be more commensurate with addressing the expected frequency and consequences of the challenges, including uncertainties. With such an approach, alternatives can be considered in which the extent of required structuralist elements (e.g., redundancy, diversity) for any specific safety system would be assessed on the basis of expected the frequency and consequences of challenges to the system, and uncertainties.

2.5 Issues to Consider in Developing the SFC Alternatives

2.5.1 Regulatory Policy Issues

In developing risk-informed alternatives to the SFC, the staff focused on alternative SFC concepts using risk-informed strategies. While implementation approaches were considered in this process, it is expected that there would be several associated technical and policy issues should any alternative be extended further into a proposed rule.

The Commission established both general and specific PRA regulatory policy that would apply to implementing any alternative to the SFC. Accordingly such alternatives would need to be

- Consistent with the Commission's guidance on risk-informed and performance-based regulations in the PRA policy statement and the severe accident policy statement on maintaining defense-in-depth, adequate safety margins, and considering uncertainty. Risk-based approaches would not be consistent with the Commission's policy.

  Consistent with the Commission's guidance on the "Phased approach to PRA quality", such that the necessary quality of the licensee's PRA will be defined to support the particular change in approach to the SFC.

- Consistent with Commission's Backfit and Regulatory Analysis policy, including consideration of costs, benefits, and bundling of requirements.

Some of these issues could parallel those previously identified in weighing risk-informed changes to 10 CFR 50.46, described in Attachment 3 to SECY-04-0037. All of the identified issues would have to be considered in finalizing and selecting a risk-informed alternative to the existing SFC, and in setting up acceptance criteria and regulatory guidance for establishing such an alternative. Similar to SECY-04-0037, but for the full range of postulated transients and accidents beyond LOCA, these issues would include mitigation capability beyond a new design basis accident, development of a new design-basis initiator from risk metrics, criteria for changing the plant and their reversibility, analytical methods and approaches, application of the defense-in-depth philosophy, and relationship to future plant activities. Because of the considerable range of regulations that include the SFC, the scope of pursuit of a broader change to the SFC would likely also be an issue.

Some particular issues associated with SFC alternatives are discussed below.

2.5.2 Relationship to Other Regulatory Requirements and Activities

The mandate for this study was explicitly stated to identify risk-informed alternatives to the single-failure criteria. As indicated in Table 2.1-2, there are regulatory redundancy requirements imposed on some systems and these requirements are independent of the SFC (e.g., the requirement for redundancy in reactivity control systems specified in GDC 26, and additional ATWS systems in 50.62). The issue here is whether, or how, an alternative to the SFC that allows changes to DBA analysis (Alternative 1) or to systems (Alternatives 2 and 3) also should be applied to systems with redundancy requirements that are not invoked by the single-failure criteria. For example, an alternative to including these redundancy requirements would be to identify explicit risk-informed alternatives for them (e.g., a risk-informed alternative to the ATWS rule).

The NRC staff is engaged in many risk-informed activities [USNRC, 2003d]. These include LOCA redefinition, technical specification improvement and ROP activities. For example, the NRC staff is now considering how a loss of offsite power (LOOP) will be considered when it is coincident with a LOCA because of their low frequency. From previous studies, the NRC's Office of Research recommended the

generic elimination of the ECCS's design requirement for considering an assumed LOOP coincident with large, and possibly medium, LOCAs [USNRC, 2002a]. The LOOP, along with the SFC, is part of other design-basis analyses, such that resolution of this issue would be important to each of the alternatives in this report. A coherent approach to these activities would be important.

2.5.3 Phenomena Not Addressed by the SFC

As a requirement to promote high safety-system reliability, the SFC very often results in the application of redundancy to help ensure that functionality is retained in the event of a single independent failure within a system. However, experience has shown that a system's functionality may be challenged by failure mechanisms other than a single independent failure. Phenomena such as common-cause failure, multiple independent failures, failures of support systems, multiple failures caused by spatial dependencies, and multiple human errors, impact system reliability but are not mitigated by redundant system design. A broader view of system reliability analysis is required to fully address these issues than is provided by single failure analysis. This was recognized in an earlier report to the Commission [USNRC 1977].

The ANSI/ANS single-failure criteria standard [ANSI/ANS 1981] for fluid systems contains guidance for treating their passive failures. In 1976, the Office of Standards Development reviewed an early version of this standard and found it contained several deficiencies, such as inconsistencies with existing regulatory practice [USNRC 1977]. The NRC did not approve the standard regulatory use, nor is it endorsed today.

Passive failures in fluid systems are generally excluded from single-failure assessments. In a risk-informed alternative to the existing SFC, not only active failures but also passive ones should be considered. The risk-informed alternatives to the SFC described in Section 4 potentially could be applied to formalize the treatment of passive failures of fluid systems. However, the question of which failures should be included must be addressed. For example, the failure of a single check valve, pipe, or tank could have significant implications on the DBA analysis. Further work covering demonstration analyses based on SPAR models or pilot-plant application might be required to identify whether any passive failures had to be addressed in the SFC alternative, and are sufficiently probable that they should be considered. The guidance for including passive failures in PRA models provided in the ASME PRA Standard potentially could be useful.

As discussed previously, the SFC excludes potentially risk-significant sequences involving multiple failures, as opposed to single ones, from inclusion in the design-basis analysis. Consequently, regulatory approaches to ATWS and SBO accidents took a considerable time to evolve. However, a risk-informed alternative would consider multiple failures in the DBA analysis if they were more likely than postulated single-failure events. Addressing multiple failures would be more complicated and costly than addressing just single failures.

2.5.4 PRA Issues

PRA issues related to risk-informed alternatives to the SFC are similar to those identified in conjunction with other risk-informed regulatory initiatives. They include issues related to the scope, quality, and adequacy of the PRA, treatment of uncertainties, and tracking of cumulative effects. The Commission recently approved a phased approach to achieving an appropriate quality for PRAs for NRC's risk-informed regulatory decision-making [USNRC, 2003c]. The proposed approach appears to be adaptable to the risk-informed alternatives to the SFC described in Chapter 4. Similar PRA requirements to those required for risk-informed alternatives to 50.46 and for 50.69 applications would likely be required for the alternatives identified in Chapter 4.

2.6 Demonstration of Influence of Redundancy on Core Damage Frequency for Selected Plants

The single-failure criterion requirements in the General Design Criteria of Appendix A to 10 CFR Part 50 and in the systems sections of the Standard Review Plan result in the redundant design of safety functions. These functions are implemented by safety systems; each safety system may have redundancy, or redundancy may be achieved by two or more single-train safety systems.

A system implementing redundancy (two or more trains) usually is more reliable than one with a single train. For this reason, the redundancy requirement of the SFC generally resulted in more reliable systems than single-train systems. In this way, the SFC contributed to more reliable systems, to an acceptable level of plant risk, and to the ability to test or maintain one train while retaining mitigation capability (without a single failure) for DBAs.

Since the SFC is a deterministic requirement applied to functions that mitigate DBAs, two questions arise about its effectiveness in promoting reliable systems and acceptable power plant risk: (1) Does a redundant safety system significantly lower risk compared to a single-train system, and, (2) is redundancy required for systems that do not contribute significantly to mitigating risk at a NPP.

To answer these questions quantitatively, several sensitivity calculations were conducted for one pressurized water reactor (PWR) plant and one boiling water reactor (BWR) plant. Here, the measure of risk is the core damage frequency (CDF) due to internal events during full-power operation. The evaluations were carried out for each plant by removing the redundancy of each safety-related system (one system at a time), and determining the increase in CDF compared with the base case. That is, a safety-related system having two or more trains was changed to a single-train system; the updated CDF then was obtained.

With regard to the first question, "Does a redundant safety system lead to lower risk at a NPP than a single-train system?," the evaluations show that for each type of plant, several systems cause a large increase in CDF when the redundancy of each system is removed. These results illustrate the extent to which the SFC (redundant design of safety-related systems) contributed to the low risk associated with operating NPPs. In discussing possible changes to the single-failure criterion, it is useful to understand the positive impact that redundant system design has had on risk.

In response to the second question, "Is redundancy required for systems that do not contribute significantly to reduce (or maintain) the risk at a NPP?," the evaluations show that for each type of plant, several systems cause a negligible increase in CDF when the redundancy of each system is removed. These results illustrate the extent to which the SFC (redundant design of safety-related systems) may be imposing unnecessary constraints on the licensees. If a safety-related system is not risk- (safety-) significant, then the requirements of the SFC, including redundant design, may be inappropriately heavy.

Appendix A details the approach used for the calculations, their results, and the insights obtained from them.

2.7 Risk-Informed Perspectives of the Single-Failure Criterion

The SFC appears as regulatory requirements and guidance in two contexts: As a safety function reliability-related redundancy requirement in the General Design Criteria, and as guidance for the "worst single failure" assumption in plant safety analysis, in RG 1.70 and Chapter 15 of the SRP. These are considered separately below.

2.7.1 SFC and Safety Function Reliability

The redundancy requirement of the SFC is, in part, a surrogate for a system-reliability requirement whose intent is to promote high reliability of safety functions that are judged important to reactor safety. Over the years since the introduction of the SFC as a regulatory requirement, it was recognized that the reliability performance of some safety systems, originally designed to meet the redundancy requirement of the SFC, should be improved to provide more reliable mitigation of specific events. The SFC was supplemented by regulatory guidelines applicable to some safety systems, examples of which are the Auxiliary Feedwater Systems (AFWS) that are needed to remove heat during various initiating events involving loss of main feedwater, and the emergency diesel generators (EDGs) that are required for loss of offsite power (LOOP) events. When the SFC was introduced as a regulatory requirement, risk and reliability methods were not yet applied to nuclear plant safety and regulation. The SFC, in combination with the requirements discussed above, quality assurance, maintenance and inspection programs, the Reactor Oversight Process tracking of safety system availability, and other elements of the regulatory framework, provided an adequate level of safety for U.S. nuclear power plants.

It is generally recognized that a system design that satisfies a redundancy requirement does not necessarily achieve an appropriate level of reliability. Moreover, the redundancy requirement of the SFC alone does not address the reliability issues related to multiple independent failures, common-cause failures, and support system and spatial dependencies, important issues that experience showed reduce the reliability of redundant systems. With state-of-the-art risk and reliability methods, alternative criteria can be considered that use quantitative estimates of functional or system reliability, and would, thereby, require explicit consideration of these reliability issues. Furthermore, risk insights gained since the introduction of the SFC suggest that alternatives to the criterion may be constructed that would require safety systems to have levels of system reliability commensurate with the frequency of challenge facing them. Alternatives that address these issues were sought in this study.

Implementing the redundancy requirement of the SFC in U.S. plants has led to safety function design that, in many instances, is characterized by two systems or trains that satisfy the requirement. Therefore, system- or train-outages for repair, test, maintenance, and inspection would leave one system or train temporarily in service. This limitation of the SFC is dealt with through risk management during these outages by technical specification requirements, and test, maintenance, and inspection programs. Alternative strategies would continue to consider risk importance of systems when undertaking tests, maintenance, and inspection.

2.7.2 "Worst Single Failure" Assumption in Plant Safety Analysis

A worst single-failure assumption is applied to deterministic analyses to assess the margins to predefined acceptance criteria of selected safety parameters to ensure the integrity of the fission-product barriers. For a given design-basis initiating event, a spectrum of single failures are postulated and corresponding safety analyses performed to identify the "worst" single failure. Experience with risk assessment methodology demonstrates that the combination of initiating event frequency and single failure probability sometimes

leads to design-basis accident sequences that assure acceptable margins, but are of very low frequency. An example that the NRC's staff are currently exploring is the analysis of double-ended guillotine LOCA related to risk-informing 10 CFR 50.46. The present approach to plant safety analysis, which compounds unlikely events with a low probability system failure, may be viewed as not being risk informed because it sometimes unrealistically focuses the calculations of design-basis margins on sequences that are not most frequent. By using risk assessment methodology, alternatives to the worst single-failure assumption might be considered that could focus the analysis on sequences that are risk-significant, while maintaining adequate safety margins.

The worst single-failure assumption does not require analyzing multiple independent failures, common-cause failures or dependent failures, in combination with design-basis events. PRAs treat these failure modes. Such multiple-failure sequences could engender complete safety-function failure, and have major impact on calculations of safety margins. If the frequency of such sequences is larger than other sequences included in the safety analysis, then it might be argued that the current approach is not as risk-informed **as it could be. PRA methodology can be employed to weigh alternatives to the existing worst single-failure assumption; this would guide the design-basis analyst to more realistically think about multiple independent failures, common-cause failures, or dependent failures in the safety analysis, if the accident sequence frequency is judged risk-significant.**

3. APPROACH TO DEVELOPMENT OF RISK-INFORMED ALTERNATIVES TO THE EXISTING SINGLE-FAILURE CRITERION

3.1 Scope

A study of risk-informed alternatives to the SFC was conducted after developing an understanding of the current implementation of the criterion (summarized in Section 2 of this report). The development of alternatives is based upon the risk perspectives discussed in Section 2.7. Alternatives were sought in the two regulatory contexts of the criterion that were identified in Section 2: (1) As a safety function reliability-related redundancy requirement in the General Design Criteria, and, (2) as guidance for the "worst single failure" assumption in plant safety analysis, in RG 1.70 and Chapter 15 of the SRP. The study of alternatives focused on the current generation of U.S. nuclear plants.

3.2 Process for Development of Risk-Informed Alternatives to the SFC

A process was established to formulate and evaluate potential alternatives to the SFC, along with a process flowchart to guide the implementation of the process. The flowchart is shown in Section 3.2.1, and elements of the process are detailed in Sections 3.2.1 through 3.2.6.

3.2.1 SFC Alternative Development Process

The process that was used to develop risk-informed alternatives to the SFC is depicted schematically in Figure 3.2-1. The evolution of SFC alternatives proceeded sequentially according to the order of the flowchart. After studying the background of the SFC (Element 1 of the flowchart) and gaining an understanding of its original intent (Element 2), the desired attributes of risk-informed alternatives were derived (Element 3). The characteristics of the existing SFC were compared with the attributes, and potential modifications to the SFC were listed (Element 5). These potential modifications were used to develop risk-informed alternatives to the SFC that applied to one or both of the contexts delineated in Section 2 (Element 6).

At the stage of Element 6, the alternatives were defined as a combination of qualitative- and quantitative-risk and/or reliability guidelines that define how aspects of the SFC would be risk-informed. After further development, several preliminary, complete, risk-informed alternatives to the SFC were defined, including the approach for implementing the alternative (Element 7).

The final risk-informed, performance-based alternatives were chosen (Element 9) after debating the application of identified constraints, and comparing the various preliminary alternatives and their common features. Some preliminary alternatives were combined because of their similarities. Section 4 discusses the resulting final set of alternatives. The specific steps of this process are described in more detail in the following sections.

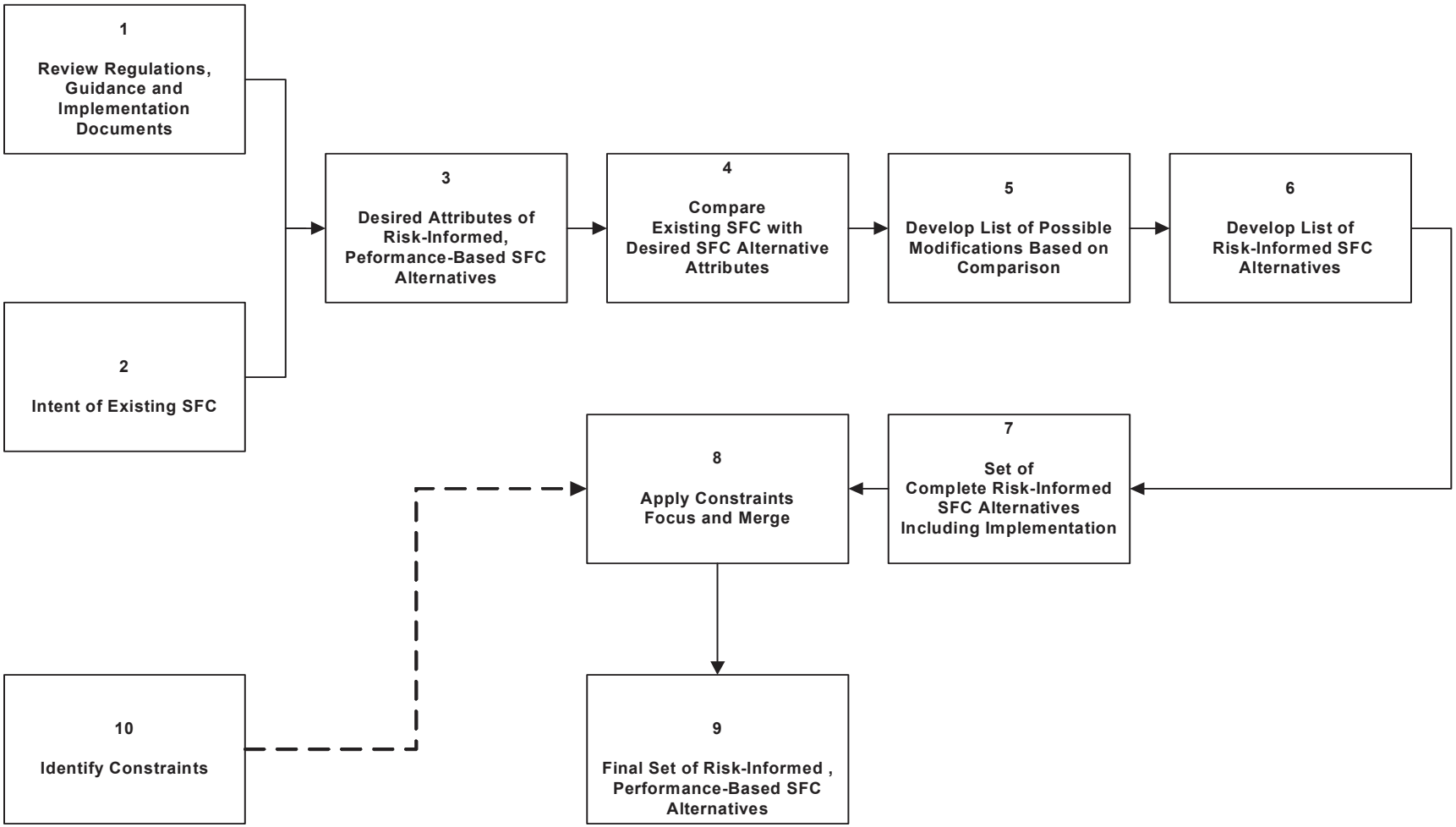


Figure 3.2-1 SFC Alternative Process Flowchart

3.2.2 SFC Background and Intent

The SFC alternative development process began with a review of regulations, guidance, and implementation documents relevant to aspects of the SFC (Element 1 of flowchart). This review is summarized in Section 2 of this report.

The review did not reveal a clear statement of the SFC's original intent. A generally accepted view (e.g., USNRC, 2002b) is that its intent is to promote high safety-system reliability. To proceed to develop concepts for risk-informing the SFC that would lead to concrete alternatives, a working understanding of the likely intent of the criterion was needed. After reviewing of the background of the SFC, a view of the criterion's original intent was developed (Element 2).

As discussed in Section 2, the SFC requirements and guidance in NRC documents occur in two major contexts:

- GDC Reliability: Safety system design requirements, largely associated with the General Design Criteria of 10 CFR 50 Part A, and expanded upon in Regulatory Guide 1.70 and the Standard Review Plan.

- DBA Analysis: Design-basis-accident analysis guidance of Chapter 15 of Regulatory Guide 1.70 and of the Standard Review Plan, directed towards demonstrating adequate design margins based upon defined acceptance criteria.

The criterion, furthermore, was accepted as one element of the traditional defense-in-depth strategy of providing multiple means of satisfying important safety functions. In this regard, it also has been used in regulatory positions taken on particular safety issues.

The following two-part intent of the SFC, which corresponds to these two contexts, was used in the process of elaborating alternatives:

- GDC Reliability: The intent of the SFC, in the context of the General Design Criteria, is to promote high reliability of safety functions that are judged to be significant to safety in order to reliably mitigate transients and accidents.

- DBA Analysis: The intent of the "worst single failure" assumption of the SFC, in the context of design-basis accident analysis, is to assure safety margins based upon deterministic transient and accident analysis, so that the actions required to mitigate the outcomes of initiating events are successfully provided by the safety systems essential to performing each required function.

3.2.3 Desired Attributes of Risk-Informed Alternatives

The next step in developing alternatives involved establishing the attributes of risk-informed performance-based alternatives to the SFC (Element 3). Building on the inherent risk-informed perspectives of the SFC (Section 2.5), the NRC Strategic Plan [USNRC, 2004a] and PRA policy documents were judged to be the appropriate guideposts to develop attributes that would assist in formulating, evaluating, revising, and implementing potential SFC alternatives. The Agency's strategic goals to ensure safety and security, and to ensure that Agency actions are effective, efficient, realistic, and timely, all rely on risk-informed outcomes, strategies, and means; these were helpful in deriving a set of attributes. Table 3.2-1 lists the attributes along with features describing their intent. The rationale for the attributes is discussed below.

Table 3.2-1 Attributes for Risk-Informed Alternatives

ATTRIBUTE NAME	ATTRIBUTE FEATURES
(1) Functional Reliability	Define risk-informed measures (e.g., CDF, function reliability) for alternatives that reflect important elements of system reliability, including common cause failure, human errors, spatial interactions, test- and maintenance-unavailability, and prevention of initiating events. Redundancy, independence, and diversity are commensurate with the frequency of challenges and their consequences, including uncertainty.
(2) Maintain Defense-in-Depth	Maintain defense-in-depth philosophy commensurate with safety significance and ensure consistency with RG 1.174 defense-in-depth elements.
(3) Ensure Risk-Informing Application of SFC in Design-Basis Safety Analysis	Risk-inform the application of the worst single-failure assumption in Chapter 15 design-basis accident analysis while maintaining an acceptable margin of safety.
(4) Use Performance-Based Regulatory Approach	Apply existing guidance using "Guidance for Performance-Based Regulation" [USNRC, 2002c] and other documents relating to a performance-based regulatory approach.
(5) Amenable to Effective Implementation	Amenable to licensing and regulatory oversight: Efficient use of NRC's and licensees' resources. Models used to evaluate risk impact should comply with PRA quality standards in existing regulatory and industry standards.
(6) Demonstrate Coherence	Alternatives should be consistent with other risk-informed regulatory initiatives and guidance (e.g., 10 CFR 50.69, 10 CFR 50.44, 10 CFR 50.46, Reactor Oversight Process, RG 1.174).
(7) Security	"...However, the scope of changes should be constrained in areas where engineering margins should be retained to satisfy the safety principles of RG 1.174 (e.g., containment design pressure, and severe accident mitigation capability). Finally, this scope should be constrained in areas where the current design requirements contribute significantly to the 'built-in capability' of the plant to resist security threats [USNRC, 2004e]."

The NRC Strategic Plan states that to ensure safety, it plans to "Develop and update risk-informed and performance-based standards, as appropriate, and Federal regulations to enable the safe use of radioactive materials, using the defense-in-depth principles and appropriately conservative and realistic practices that provide an acceptable margin of safety." A strategy to ensure that NRC's actions are effective, efficient, realistic, and timely is to "Use state-of-the art methods and risk insights to improve the effectiveness and realism of NRC actions." Adopting these strategies and the SFC perspectives discussed in Section 2.7, the first three attributes for an SFC alternative were identified, and are listed in Table 3.2-1.

The NRC's policy supports the use of performance-based regulation to minimize unnecessarily prescriptive requirements as a strategy to not only to ensure regulatory effectiveness, but where appropriate, as a strategy to ensure safety. "Guidance for Performance-Based Regulation" (NUREG/BR-0303) gives guidance on a

process for developing performance-based alternatives for consideration, along with other more prescriptive alternatives, in regulatory decision-making. The NRC Management Directive 6.3, "Rulemaking," **[USNRC, 2001]** calls for the consideration of a performance-based alternative. It is included as the fourth attribute for an SFC alternative in Table 3.2-1.

Attribute 5 was added to explicitly identify support to the NRC's strategic goal of Effectiveness, identified in the NRC Strategic Plan. An SFC alternative would need to contribute to a "stable, reliable, and responsive regulatory environment," as discussed in the Strategic Plan.

In 2003, the NRC noted in its Risk Informed Regulation Implementation Plan that, "...although a great deal of progress has been made toward risk-informing regulatory activities, the staff believed that some existing reactor arena activities (regulations, staff programs and processes) may be inconsistent (or incoherent) with risk-informed practices." The staff believed that the program would offer an approach in which the reactor regulations, staff programs, and processes are built on a unified safety concept and are properly integrated to complement each another. Attribute 6 for coherence was included because of the importance of consistency between a potential SFC alternative and other risk-informed programs at the NRC.

The PRA policy statement, Risk Informed Regulation Implementation Plan **[USNRC, 2003d]** and Commission guidance on recent initiatives were reviewed. Information from them was encompassed in formulating the attributes, and the risk-informed principles of RG 1.174 were used to more fully develop several of the specific attributes.

A strategic goal of the NRC is ensuring the secure use and management of radioactive materials. The Commission's direction on assuring security in activities involving LOCA redefinition was issued in a recent direction to the staff.. Accordingly, Attribute 7 was added, consistent with this specific guidance.

3.2.4 Potential Directions for Risk-Informed Modifications

The current regulatory implementation of the SFC in both the GDC and DBA contexts defined above was evaluated against the desired attributes of risk-informed alternatives of Table 3.2-1 (Element 4 of the process flowchart).

The evaluation (Element 4 of the flowchart) of the current implementation of the SFC with the attributes presented in Section 3.2.3 led to considering several potential modifications to the current SFC to develop risk-informed alternatives (Element 5). **The potential technical modifications are derived primarily from Attributes 1, 2, 3, and 4. However, any modifications discussed here must also be consistent with Attributes 5-7.** Table 3.2-2 summarizes these potential modifications; they are discussed below.

The risk-informed perspectives discussed in Section 2.5.1 suggest that while the SFC has played a role in achieving high system reliability in U.S. plants, the criterion does not address system reliability directly and quantitatively, and does not require applying the criterion in a manner commensurate with initiating-event frequency. Table 3.2-2 identifies potential modifications that would risk-inform the SFC based upon risk and reliability considerations derived from Attribute 1. A risk-informed alternative to the current GDC might employ system- or functional-reliability as a quantitative alternative to the SFC. A higher-level risk measure, such as CDF or LERF, could be used in the context of a PRA as a measure to anchor specification of the system or functional reliabilities. The PRA can also be used in this context to guide specification of system reliabilities that are commensurate with the challenge frequency. These alternatives would address elements of reliability (e.g., common-cause failure) that are not directly addressed by the current SFC.

Table 3.2-2 - Potential Modifications of SFC

	POTENTIAL SFC MODIFICATIONS BY ATTRIBUTE
GDC Reliability Context	Attribute 1: • **use quantitative criterion for function reliability** • **use overall plant risk measure to anchor quantitative reliability criterion** • address significant elements of reliability not currently addressed by SFC: CCF, human error, passive failure (fluid systems) and multiple independent failures. • ensure reliability is commensurate with challenge frequency Attribute 2: • apply defense-in-depth commensurate with safety significance •Attribute 4: • use performance-based guidance for developing implementation strategy
DBA Safety Analysis Context	Attribute 2: • apply defense-in-depth commensurate with safety significance Attribute 3: • **risk-inform selection of sequences for worst single failure assumption** • **risk-inform selection of initiating events for inclusion in design basis** • **use a more realistic approach to DBA analysis**

Table 3.2-2 identifies modification of the application of defense-in-depth, derived from Attribute 2, as potentially applied in both the GDC Reliability and DBA Analysis contexts. As discussed in Section 2.3.3, the system redundancy feature of the SFC has been thought of as an element of the traditional, or structuralist, implementation of defense-in-depth. While this approach was useful in promoting reliable system design, in some cases supplemental guidance was required to achieve enhanced levels of safety, while, in other cases, the redundancy requirement was overly restrictive (see Section 2.3.1). Hence, the redundancy element of defense-in-depth might be modified, with the objective of providing sufficient flexibility so that its application is related more closely with the expected frequency and consequences of the challenges than is embodied in current practice. The required minimum level of redundancy for any **specific safety system would be evaluated on the basis of its safety significance.**

Table 3.2-2 suggests potential modifications to the worst SFC, based upon Attribute 3. The selection of the set of specific initiating events for the design-basis-accident safety analysis partly rests on the expected frequency of their occurrence [USNRC, 1978]. Pressure vessel failure, for example, is considered to have too low a frequency event for inclusion in the design basis. The proposed LOCA redefinition **[USNRC, 2004b] is based** upon the concept that the frequency of ruptures of primary pipe above some specified diameter is sufficiently low that breaks of larger diameter pipes should be considered as beyond the design basis. Similarly, the worst single-failure principle is applied to design-basis analysis, using arguments based upon risk, so that, some single failures do not always have to be considered. For example, failures of passive components in fluid systems and common-cause failures do not have to be included as single failures in DBA analyses. The modifications identified in Table 3.2-2 could risk-inform the selection of initiating events for inclusion in the design basis. They could also risk-inform accident sequences (combinations of

initiating events and safety-system failures) chosen for application of the worst single-failure assumption. Such modifications would be consistent with both the Commission's policy [USNRC, 1995] requiring the continued support of the NRC's traditional defense-in-depth philosophy, and with RG 1.174 which supports "...system redundancy, independence, and diversity are preserved commensurate with the expected frequency, consequences of challenges to the system, and uncertainties..." These approaches would also introduce more realism into the safety analysis framework in keeping with the goal of the NRC's Strategic Plan to ensure effective regulation by using realistically conservative, safety-focused programs to resolve safety-related issues.

Table 3.2-2 suggests that potential modifications of the SFC might be directed towards developing a more performance-based set of requirements. The current implementation of the SFC was assessed from the perspective of Attribute 4, the extent that the requirements are "performance-based" as opposed to "prescriptive". In its white paper on risk-informed and performance-based regulation [USNRC, 1999a], the Commission endorsed the continued evolution of performance-based regulations, and defined such a regulation as one that "...relies upon measurable (or calculable) outcomes (i.e., performance results) to be met, but provides more flexibility to the licensee as to the means of meeting those outcomes. A performance-based regulatory approach is one that establishes performance and results as the primary basis for regulatory decision-making...." A prescriptive approach, on the other hand, gives the licensee detailed instructions on how to reach specific results. Subsequent NRC reports [USNRC, 2000b; USNRC, 2002c] offered further guidance. The current SFC was evaluated from the perspective of the degree to which it has performance-based characteristics as opposed to prescriptive ones. The redundancy requirement of the SFC specifies how the intent of "high reliability" is to be achieved. The intent of "adequate margins" is to be achieved, in part, by using the worst single-failure criterion. From this point of view, the existing SFC is judged to be largely prescriptive. Potential modifications would be directed towards establishing an alternative that is more performance-based.

3.2.5 Development of Risk-Informed Performance-Based Alternatives

The potential directions for modifying the SFC (Section 3.2.4) were chosen as the starting point for developing specific alternatives to the SFC.

Each alternative formulated had two components:

- Risk-Informed Approach:

  A combination of qualitative- and quantitative-deterministic, and risk and/or reliability, guidelines establishing the levels of performance that the regulator expects the function or system to achieve to satisfy regulatory objectives.

  This approach would combine structuralist and rationalist views. For example, it might contain quantitative goals for system or functional reliability that could replace or supplement the redundancy requirement of the SFC, or could propose using event-sequence frequency criteria as a basis for excluding specific events in the licensing basis.

- Implementation Guidelines:

  Implementation guidelines describe the regulatory processes and requirements that assure the achievement of the risk-informing guidelines.

These guidelines would describe the changes in the licensing basis that would be needed to implement the risk-informing guidelines. They also would denote the performance measures that must be implemented to monitor achievement of the performance goals proposed as part of the risk-informing guidelines. Section 3.2.6 discusses the elements of implementation.

A range of possible alternatives were developed and discussed (Element 6 of flowchart). Some were very similar in one or both of the two components defined above. As the risk-informed approaches became better defined, the means of putting them into effect was discussed. The result was a set of SFC alternatives consisting of both Risk-Informed Approach and Implementation Guidelines (Element 7).

An important part of identifying alternatives to the SFC is to highlight those regulatory constraints that could impact their viability or implementation. Such constraints were considered in the development of the proposed rulemaking to risk-inform the large break LOCA requirements. Past regulatory experience and recent Commission directives were reviewed to identify such constraints (Element 10 of flowchart). One of them derives from the Commission's PRA policy statement, and specifies that changes to the regulations should not implement risk-based decision-making [USNRC, 1995]. Alternatives that did not adequately regard risk-informed principles were either modified or eliminated. No other constraints were identified. Important limitations (e.g., resistance to security threats) were included in the attributes used for the SFC alternatives.

The attributes developed for identifying SFC alternatives were guided by the Commission's risk-informed regulatory policy and the NRC's Strategic Plan. Reviewing of the alternatives using this guidance focused and merged their features into a small set of final alternatives (Element 9); they are presented in Section 4.

3.2.6 Implementing the SFC Alternatives in the Regulatory Process

The SFC alternatives considered represent different risk-informed approaches that modify the use of the SFC in the regulatory process. Each alternative has a strategy for achieving the safety objectives of high system reliability and adequate safety margins. They employ a combination performance requirements, involving risk requirements, system- or function-reliability requirements, structural elements such as redundancy, and a requirement to maintain safety margins.

Each alternative requires an elaboration of the means by which its approach would be put into practice. Implementation should address the attributes discussed earlier in this report: performance-based approaches should be used where appropriate, and the implementation should be efficient and effective and improve coherence with other risk-informed regulatory initiatives and guidance. The systems' performance would be measured against these qualitative and quantitative requirements of the risk-informed approach. This conceptual structure is discussed in [NRC, 2003].

The alternatives proposed in the present study focused primarily on the specification of the risk-informed approach, with consideration of some elements of implementation. Basic implementation concepts that might be discussed for the alternatives are described in a preliminary way.

At present, it is useful to distinguish three aspects of implementation:

- Initial Licensing Activities
- Continuing Programmatic Activities to Assure Safety Margins and Promote Functional Reliability
- Monitoring Activities

Licensing Activities

The SFC alternatives identified change certain details about the way in which safety is achieved. The NRC would likely need to promulgate new regulations and guidance to licensees who, in turn, would be presented with new requirements associated with using the alternatives. Licensing activities would be carried out by NRC and by the licensees as required by any of the alternatives discussed here.

From a safety point of view, the licensing process necessitates demonstrating the adequacy of the plant's ability to respond to particular safety challenges, defined by a set of initiating events. The NRC would specify the set of safety challenges (which may or may not differ from the existing set of initiating events), and would define licensee and NRC measures that would be required to show compliance with the new requirements.

The new regulations and guidance would need to address the following:

- Specification of the challenges (initiating events, design-basis accidents, …) to be addressed. This might be explicit, as at present, or process-based, as in a requirement to conduct comprehensive hazard identification as part of a PRA.

- Requirements on the demonstration of the plant's system or functional capability: Safety criteria, performance criteria, reliability targets (if applicable), basis for addressing such targets, and redundancy requirements (if applicable).

- Thermal-hydraulic evaluation guidance (such as found in Appendix K), including performance criteria, such as fuel cladding temperature, required assumptions (e.g., decay heat, system characteristic inputs), numerical methods, and models (e.g., heat transfer correlation).

Continuing Programmatic Activities to Assure Safety Margins and Promote Functional Reliability

Programmatic activities are mandated by regulation and by guidance to provide reasonable assurance that performance will be maintained. For the present alternatives, these may include

- Technical Specifications to address LCOs aimed at system operability
- Availability and performance targets (Technical Specifications originally focused on assuring the SFC is met)
- Capability requirements (flow, actuation time) aimed at safety-analysis assumptions
- Surveillance Requirements
- Appendix B QA in procurement, installation, and operation
- Seismic qualification
- Environmental qualification
- Inservice Testing (IST) and Inservice Inspection (ISI) to help satisfy the reliability targets considered in formulating the SFC alternative

Alternatives to the SFC could include new technical specifications. Other programmatic activities might be included for graded treatment commensurate with the systems' or components' role.

Monitoring Activities

Monitoring activities trigger corrective action whenever SSC performance declines below a specified level. These levels are determined during the licensing process, and might be tied to the plant's risk assessment or safety goal. Monitoring activities may include the following:

- Plant data to support ROP-type performance indicators
- Maintenance Rule programs
- Licensee monitoring program commitments: FSAR program descriptions and responses to NRC's generic communications involving licensee monitoring programs
- Appendix B Corrective Action programs
- 50.59 change in design or procedures
- Reports to the NRC.

4. RISK-INFORMED PERFORMANCE-BASED ALTERNATIVES TO THE SINGLE-FAILURE CRITERION

4.1 Overview

The review of the background and the NRC's implementation of the SFC discussed in Section 2 demonstrates that the SFC is applied in two regulatory contexts: (1) Design-basis accident analyses following Chapter 15 of RG 1.70 and the Standard Review Plan, and, (2) safety-system design as specified within the General Design Criteria. The SFC was examined from a risk-informed perspective, and the process described in Section 3 of this report was applied to developing risk-informed performance-based alternatives to the existing SFC in both of its regulatory contexts. The resulting alternatives are identified in Table 4.1-1, and are further discussed in later sections. The current SFC approach, identified as the Baseline Approach in Table 4.1-1, is one possible alternative for continued implementation

Table 4.1-1 Risk-Informed Performance-Based SFC Alternatives

ALTERNATIVE	TITLE
Baseline (Current) Approach	Retain the Current Approach - Risk-Inform the SFC for Particular Issues (Section 4.2)
Alternative 1	Risk-Inform Application of SFC for DBA Analysis (Section 4.3)
Alternative 2	Risk-Inform the SFC According to the Safety Significance of Systems (Section 4.4)
Alternative 3	Generalize and Enhance the SFC (Section 4.5)

The Baseline Alternative would continue to consider initiatives, as needed, to change the rules and guidance on single failure and reliability issues using risk-informed approaches. This would include rulemaking on 10 CFR 50.46, and the focused improvements discussed in this report, such as updating requirements on passive failures of components of fluid systems. The Baseline Alternative also would encompass decisions to retain current regulations and not pursue modification to the SFC or its scope of application.

Alternative 1 would modify the design-basis accident analysis of Chapter 15 of Regulatory Guide 1.70 and of the Standard Review Plan. It would risk-inform the application of the worst single-failure assumption of the SFC. Design-basis sequences of events that do not significantly contribute to risk could be excluded from DBA analysis. For low-frequency initiating events, single failures of sufficiently low probability would not have to be considered in DBA analysis. On the other hand, multiple-failure events that involve sequences

whose frequencies are safety significant could become part of the design basis, thereby requiring DBA analysis. The plant's PRA would be used to demonstrate that any plant changes entail an acceptably small change in CDF and LERF, using RG 1.174 as a guide.

Alternative 2 would modify the SFC by risk-informing application of it based upon the safety significance of the specific system. From the plant's PRA, the safety systems would be categorized according to their safety significance, similar to the proposed "special treatment" categorization scheme. The SFC would be applied to those with high risk significance, while the SFC requirements for systems of low safety significance would be eliminated or relaxed. The plant's PRA would be used to demonstrate that any plant changes lead to an acceptably small change in CDF and LERF, using RG 1.174 as a guide. Performance monitoring parameters would be defined requiring the licensee to monitor the reliability of safety-significant systems[4].

Alternative 3 would replace the SFC with functional reliability targets anchored to plant-level risk measures, such as CDF and LERF. Qualitative targets on redundancy and diversity would be required of systems depending on their importance to safety. Reliability targets for each function-initiator combination would be commensurate with initiator frequency. The licensee would use such targets to establish lower level system- or train-level reliability targets, for which programs for measuring performance would be devised. Performance measures would be established to monitor compliance with the lower level targets.

4.2 Baseline (Current) Alternative - Risk-Inform the SFC for Particular Licensing Issues

4.2.1 Background

The NRC staff continues their initiatives to risk-inform the regulatory requirements, including some that deal with the SFC. The SFC has a long history in the regulations, in the existing body of the NRC and industry standards to define the application of the principle, and also in the many modifications to regulatory requirements, processes, and plant systems that involve the SFC. Section 2 of this report reviewed the background of the current single-failure criterion's requirements, its implementation, and changes made over the years.

4.2.2 Discussion

This alternative would be to continue to make risk-informed changes to regulatory requirements that involve particular issues. It would not embody a broad change to the current licensing requirements or processes to risk-inform the SFC, as envisioned by the other alternatives. Changes to the SFC would be deliberated within the context of the particular activity or licensing issue. This would include initiatives underway on particular issues, such as the 10 CFR 50.46 rulemaking, generic activities on LOOP/LOCA requirements, plant-specific risk-informed license amendments, risk-informed technical specification initiatives, and continued improvements to the ROP. This would also include continued development of standards related to PRA quality, and the use of PRA in particular programs consistent with the Commission's guidance on the phased approach to PRA quality.

[4]A safety-significant system is one whose loss or degradation could significantly degrade safety.

This approach would include applying possible selected elements of the broader alternatives discussed in later sections of this report, perhaps as follow-ons to the current initiatives for particular regulations or licensing issues.

Regulatory Position on Single Passive Failures in Fluid Systems

One particular issue identified in this project is the continued existence of the footnote to the definition of single failure in 10 CFR 50 Appendix A stating that the regulatory position on considering passive failures in fluid systems is under development. Tools and experience now exist to replace or remove this footnote. Development of such a rule change and regulatory guidance are included here as part of the current process rather than a distinctly different alternative.

4.2.2.1 Risk-Informed Approach

The Commission and staff have established PRA policies, risk-informed licensing guidance, and currently have undertaken significant risk-informed initiatives. Risk-informed alternatives to the SFC, whether as an alternative DBA approach or as a consideration of a particular system's reliability approach or concern, would be applied within the context of a particular licensing issue, rather than taking a broad-based approach. This essentially is now being done through the 10 CFR 50.46 and 10 CFR 50.69 rulemakings, use of RG1.174 to amend plant licenses, and the technical specification improvement program. Other instances of using risk-informed approaches in the context of specific licensing issues have involved auxiliary feedwater, reactor protection, and on-site emergency electric power systems. In addition, the NRC completed new AFW reliability guidance, the ATWS and SBO regulations, and 10 CFR 50.59 and 10 CFR 50.65 rulemakings in response to particular issues.

While addressing particular issues that may arise, consideration could be given to limiting the application of the SFC to those plant challenges whose likelihood warrants that level of mitigation, thereby producing a better match between the burden implied by the SFC and the resulting level of safety. However, rather than undertake a sweeping review of all initiating events and related regulations and guidance, this alternative would proceed one licensing issue (e.g. initiating event, mitigation capability) or one regulation at a time, in the hope that measurable progress could be realized sooner.

After implementing this alternative, changes could be made to the set of challenges that require single-failure-proof mitigation; the needed implementation measures would be set for systems and components to fulfill safety requirements. After redefining the design basis for a large break LOCA, other initiators might be explored, such as large secondary pipe breaks or reactivity addition events.

This alternative also would include replacing the current footnote in 10 CFR 50 on passive failures for fluid systems with a definition based on current practice as modified by risk considerations and/or endorsement, with any necessary limitations, of industry consensus standards, such as ANSI/ANS 58.9.

4.2.2.2 Implementation Approach

The NRC would conduct appropriate rulemaking and revision of guidance for the regulation or licensing issue being considered, probably preceded by a pilot program.

Initial Licensing Activities

The regulatory implementation related to any new DBA, associated analysis, or revised mitigation strategy would be modified for the particular licensing issue to which aspects of the alternatives that were discussed could be applied. Licensees would propose new analyses or changes consistent with the new requirements. Unless the regulatory requirement is specifically altered, safety systems would continue to perform their safety functions after demonstrating adequate safety margins in the plant's licensing basis in the event of the worst single failure, following the guidance in RG 1.70 and the Standard Review Plan. The practice of using conservative licensing judgements for these requirements would go on for all unchanged requirements. All other aspects of the licensing basis would not change, including those where risk information and studies were used as a basis for developing the requirement. The priorities for changing the licensing basis would consider stakeholder input and be managed with existing processes. Current regulatory implementation strategies would be employed unless modified in the rulemaking process. The back-fit and forward-fit provisions of a new regulatory position on passive failures in fluid systems in 10 CFR Part50 would need to be determined during the rulemaking process.

Continuing Programmatic Activities

Current programmatic work, discussed in Section 3.2.6, cover such activities as Technical Specification requirements for operability and surveillance, quality assurance, and other qualification requirements. Changes in these would be considered along with the particular alternatives to the SFC being considered for the particular issue.

Monitoring Activities

The ROP would continue in the same way, relying upon risk information to determine the significance of a non-compliance and to focus the NRC's inspection resources. Additional monitoring could be necessary, depending on the SFC alternative being proposed for the particular issue. These alternatives are discussed further in ths following section.

4.2.3 Evaluation

Previous sections of the report point out the limitations of the SFC from a risk perspective. Basically, it does not always ensure that the system design requirements are keyed to the frequency and consequence of all initiators. The major benefit of this alternative is to make progress, one licensing issue at a time. Risk-informed changes to the SFC would consider the input from stakeholders, evaluation by the NRC's staff, and the Commission's direction. Licensees would gain flexibility in mitigating certain rare events, or possibly, they would be made to invoke more mitigation (if an event not currently under the SFC was shown to need more than it gets).

Because requirements are so interrelated, they may turn out to be locked in by the multiplicity of scenarios, so that eliminating one scenario may have little impact. Furthermore, individual changes to the SFC's scope also may have little real impact on the requirements.

Without a broader approach, this alternative would probably not convey coherence across systems and safety analyses. It would leave for later resolution issues of incoherence between unchanged regulatory requirements and the ROP. Table 4.2-1 briefly discusses this approach relative to each of the developed attributes for risk-informing the SFC.

4.2.4 Summary

Table 4.2-2 summarizes the essential features of the current approach to risk-informing aspects of the single-failure criterion.

Table 4.2-1 Baseline Alternative Attributes

BASELINE (CURRENT) ALTERNATIVE Risk Inform the SFC for Particular Licensing Issues	
Risk-Informing Approach	This alternative seeks to risk-inform the regulatory framework by refining the scope of application of the SFC in particular areas for particular licensing issues.
Implementation	A particular regulation or set of regulations/licensing requirements would be revised through rulemaking for a particular issue.
	The implementation approaches are revised accordingly to include re-analysis or approaches that provide more flexible regulatory approaches, perhaps performance monitoring, commensurate with the risk associated with the particular issue, but assuring adequate system reliability, safety margin, and defense-in-depth.
Attribute 1: **Functional Reliability**	Focused improvements would be made for a particular mitigating system. Other system requirements would continue to utilize the current SFC.
Attribute 2: **Defense-in-Depth**	Defense-in -depth would be maintained per RG 1.174 guidelines. Appropriate existing safety margins would be maintained. Analyses would validate the margin for any new DBA required for the particular sequences. Analysis and success criteria would need to be determined.
Attribute 3: **Risk Inform Consideration of SFC in Safety Analysis**	Some new DBAs could result from this alternative, or some current ones could be eliminated. For sequences determined to be "beyond a DBA", resources would no longer be devoted to analyzing sufficiently unlikely event sequences. Other DBAs would not be affected and would retain their current methodology.
Attribute 4: **Performance-Based Regulatory Approach**	The validity of frequency data and PRA models used would be monitored much as today. Performance-based approaches would focus on the particular issue.
Attribute 5: **Amenable to Efficient Implementation**	This approach could be implemented using existing processes. Further effort, probably a pilot plant-application, would likely be needed to develop regulatory guidance and acceptance criteria for identifying and analyzing a new multiple failure DBA or an approach to regulating functional reliability. By addressing one particular regulation or issue, progress might be made efficiently.
Attribute 6: **Coherence**	This approach would improve coherence in a limited way.
Attribute 7: **Security**	As for other alternatives, plant-specific changes would not be permitted to adversely impact security.

Table 4.2-2 Baseline Alternative Summary Description

BASELINE (CURRENT) ALTERNATIVE Risk Inform the SFC for Particular Licensing Issues	
Basic Motivating Factors for Alternative	This alternative is motivated primarily by the possibility that measurably more progress can be made by considering individual issues, rather than by addressing many issues simultaneously. While the SFC's regulatory requirements are clearly stated and relatively straightforward to implement, they do not, by themselves, necessarily achieve high system reliability, that is closely linked with the frequency of challenges to the system.
Risk-Informed Approach	This alternative seeks to risk-inform the regulatory framework by refining the scope of application of the SFC in particular areas. The SFC requirements will be applied to challenges whose likelihood warrants that level of mitigation, thereby better matching the burden implied by the SFC and the resulting level of safety. However, rather than undertake a sweeping review of all initiating events, this alternative would proceed one licensing issue at a time. A position on single passive failures in fluid systems would replace the footnote now defined in 10 CFR Part 50 Appendix A.
Implementation Approach	Initial Licensing: A particular regulation or set of regulations/licensing requirements would be revised through rulemaking for a particular issue/system reliability or DBA approach. Licensees would submit information in accordance with these revisions. The position on passive failures in fluid systems would be developed considering industry standards and worked through the rulemaking process.
	Programmatic Activities: Credit for, or changes, to current activities such as the Maintenance Rule, ISI, ISI, or QA would be considered for the particular issue. Changes could be made comparable with the risk associated with the particular issue.
	Monitoring Activities: These activities could include approaches currently used or being developed in the ROP, or augmented for the particular issue if new targets or goals are developed. A performance-monitoring approach based on one of the alternatives in this study could be used that is linked with the risk associated with the issue.
Potential Major Achievement	The major benefit of this alternative is to make progress one issue at a time.
Pros and Cons	Risk-informed changes to the SFC would consider the input from stakeholders, evaluation by the NRC staff, and the Commission's directions. Licensees would gain flexibility in mitigating rare events, or possibly, they would have to invoke more mitigation (if an event not under the SFC needs more mitigation than it presently gets). Because requirements are so interrelated, the SFC may turn out to be locked in by a multiplicity of scenarios, so that eliminating one scenario may have little impact. Further, individual changes to the scope of the SFC may have little effects on the requirements. Any improvement in the coherence between programs would be limited.

4.3 Alternative 1 - Risk Informed Application of SFC for DBA Analyses

4.3.1 Background

The term, design-basis sequence, is used in this report to denote a sequence of postulated failure and success events for which regulatory acceptance criteria must be met. A design-basis sequence always includes a design-basis initiating event (DBE) and a single failure event. For the safety functions delineated in GDCs 34, 35, 38, 41, and 44, a loss of electric power event and an additional single failure event must be postulated. Otherwise, loss of electric power events are included in the set of potential single-failure events. Only safety-related SSCs are credited in DBA analyses; consequently, success events in design-basis sequences are successes of safety-related SSCs.

DBA analyses demonstrate that regulatory acceptance criteria are met for design-basis sequences. The criteria are selected to assure adequate safety margin in the plant's response. Design-basis analyses of postulated pipe breaks inside the containment are used to develop the containment's design parameters (pressure and temperature) and the qualification envelope for components inside containment, and to demonstrate that the design limits are not exceeded during postulated design-basis accidents. Design-basis LOCA analyses demonstrate that the calculated ECCS performance meets the ECCS acceptance criteria in 10 CFR 50.46. When changes are proposed to plant structures, systems, and components (including changes in fuel design), DBAs that could potentially be impacted are re-analyzed to assure that acceptance criteria are still met.

DBA analyses are not carried out to establish PRA success criteria or identify PRA success paths. Nevertheless, the results of DBA analyses often form the basis for some PRA success criteria, and design-basis sequences generally constitute a subset of the success paths modeled in PRA event trees.

DBA analyses are not performed for every design-basis sequence. Instead, for each design-basis initiating event, the spectrum of postulated single failure events is inspected to identify the worst single-failure event (i.e., the one that results in the least predicted margin) with respect to the stipulated regulatory acceptance criteria for the analysis. The fact that the worst failure may result in a very unlikely sequence of events is not considered. The worst event may be one that results in failure of a redundant train of one or more safety systems. For example, the peak containment pressure is often computed when loss-of-offsite power (LOOP) and failure of one train of emergency electric power are postulated because this scenario disables one of the containment spray trains and one of the containment fan coolers. On the other hand, the possibility must be considered that no single failure may engender the worst predicted outcome. For example, the worst failure in design-basis analyses of ECCS performance is sometimes "no failure"; that is, the peak cladding temperature may be predicted when all trains of the ECCS function.

Under current practice, as described in regulatory guides and industry standards, some events do not have to be postulated as single failures in system design or DBA analyses. Specifically, failures of passive components in fluid systems, check-valve failures, and many common-cause failures do not have to be postulated. No quantitative criteria were applied to justify the exclusion of such failures from the design basis. Heuristically, however, they are excluded because their probabilities are perceived to be sufficiently low relative to those of single failures that are not excluded from the design basis. This does not mean that such excluded events do not merit regulatory attention. Design, fabrication, maintenance, inspection, testing, and performance monitoring all assure that their contributions to risk remains small, that is, that they do not become significant contributors to CDF or LERF.

Except for design-basis sequences in which both a loss of electric power event and an additional single failure must be postulated (see GDCs 34, 35, 38, 41, and 44), multiple failure events are not postulated in DBA analyses. However, a proposed revision to the Standard Review Plan implies new applications should postulate loss of offsite power plus an additional single failure for all design-basis initiators: "The impact of various single failures on the course of anticipated operational occurrences and postulated accidents is considered. For new applications, loss of offsite power should not be considered as a single failure event, rather, it should be assumed in the analysis of each event without changing the event category" [USNRC, 1996].

In the past, licensing issues pertaining to accident sequences involving multiple versus single failures were resolved on a case-by-case basis without modifying the single-failure criterion. For example, the ATWS issue was ultimately resolved by prescriptive, vendor-specific changes after nearly two decades of studies. The issue of station blackout was resolved by requiring licensees to perform plant-specific analyses to demonstrate the ability to withstand a station blackout for a plant-specific time [Haskin et al., 2002].

4.3.2 Alternative Discussion

4.3.2.1 Risk-Informed Approach

Alternative 1 considers risk-informing the sequences of events postulated in DBA analyses based, in part, on the frequencies of the sequences. Both removals and additions to the current set of design-basis sequences would be allowable. Failures resulting in sequences with sufficiently low frequency would no longer have to be postulated. Those eliminated could include both initiating events (DBEs) and single-failure events currently postulated in DBA analyses. Licensees could benefit from this approach if the event with the least predicted margin to a regulatory acceptance criterion could be eliminated from a DBA analysis. From a practical standpoint, failure events that could potentially be eliminated appear in design-basis sequences with small initiating-event frequencies, such as large LOCAs, main-steam-line breaks, and main-feedwater-line breaks. On the other hand, under Alternative 1, sufficiently high-frequency sequences involving multiple failure events would have to be considered as potential additional design-basis sequences. Any such added sequences would probably involve high-frequency DBEs, such as transients. Quantitative frequency criteria would be established for removals from, and additions to, the current design basis. Such criteria would have to be consistent with those applied in risk-informing other regulations.

Alternative 1 would offer a consistent basis for including or excluding events as single failures in design-basis sequences. Failures of either specific components, or of entire trains of redundant systems could potentially be eliminated as postulated single failures in DBA analyses for low frequency DBEs. The licensee would be required to demonstrate that the collective frequency of sequences proposed for elimination from the design basis is small. DBA analyses would no longer have to cover sequences eliminated from the design basis. As a result, plant changes could conceivably be proposed, based on Alternative 1. These might include, for example, changes to core-peaking factors, equipment -qualification requirements, allowed outage times, test requirements, and possible power upgrades. Any plant changes proposed based on Alternative 1 would have to be consistent with RG 1.174 guidelines regarding preservation of safety margin and defense-in-depth. Any associated increase in CDF and LERF would have to be shown to be very small.

While allowing sufficiently unlikely design-basis sequences involving single-failure events to be eliminated, Alternative 1 would require sufficiently likely sequences involving multiple-failure events to be viewed as candidates for addition to the design basis. DBA analyses would have to demonstrate compliance with suitable regulatory acceptance criteria, which would have to be delineated for new design-basis sequences.

As a whole, Alternative 1 would focus DBA analysis on demonstrating that functional requirements would be met for design-basis sequences with risk-significant frequencies.

Eliminating Sufficiently Unlikely Sequences from the Design Basis

Alternative 1 would enable the licensee to identify unlikely design-basis sequences as candidates for elimination. This might require the licensee to demonstrate that the collective frequency of these sequences is less than a predefined screening criterion. For example, the licensee might be asked to demonstrate that

$$\sum_{i=1}^{N} F(S_i) < 10^{-5} \text{ per year}$$

Here $F(S_i)$ denotes the frequency of design-basis sequence, S_i, and the sum is taken over all of the sequences to be excluded from DBA analyses. The frequency of 10^{-5} per reactor year represents a surrogate screening criterion. A final screening criterion would be selected while developing regulatory guidance. Using such a criterion essentially limits the design-basis sequences that can be eliminated to those with low frequency initiating events, such as LOCAs, main-steam-line breaks, and main-feedwater-line breaks. Design-basis sequences with higher frequency initiating events, such as transients, generally would not meet the surrogate screening criterion. Such a criterion would restrict the number of sequences that could be removed from the design basis even if each individual sequence had a very low frequency (e.g., fewer than ten sequences, each having a frequency of 10^{-6} per year, could be eliminated based on the surrogate screening criterion).

In lieu of a numerical screening criterion, the elimination part of Alternative 1 could be based on the fact that only those design-basis sequences with low frequency initiating events would be reasonable candidates for elimination. In particular, sequences initiated by large pipe breaks (e.g., double-ended main-steam and feedwater breaks) would be primary elimination candidates. In place of a screening criterion like the surrogate presented above, Alternative 1 could build on the effort to risk-inform 10 CFR 50.46 by risk-informing low frequency design-basis initiating events, starting with main steam- and feedwater-line breaks. The proposed rule-making for risk-informing 50.46 specifies that the transition break **size is to be determined by considering the mean of the break sizes from an expert elicitation process, with adjustments for uncertainties, and then adjustment to the largest attached piping**. Breaks larger than the transition break size can be removed from the design-basis event category. Traditional methods and assumptions for ECCS evaluation must be used for breaks up to the transition size. Although breaks larger than the transition size do not require DBA analyses, the ability to mitigate them still must be demonstrated; but different acceptance criteria and more realistic boundary conditions and analysis methods can be used. Specifically, the assumption of LOOP and an additional single failure would not be required. To initiate the elimination part of Alternative 1, similar efforts could be undertaken to define transition break sizes and to risk-inform design-basis sequences for main steam- and feedwater-line breaks.

Any plant changes proposed based on Alternative 1 would have to be consistent with RG 1.174 guidelines regarding the preservation of defense-in-depth and safety margin. The licensee would be required to demonstrate that changes in CDF and LERF under Alternative 1 would be very small. For example, the licensee might be asked to show that

$$\Delta CDF < 10^{-6} \text{ per year}$$

and

$$\Delta LERF < 10^{-7} \text{ per year}$$

In RG 1.174 terminology, these surrogate criteria would assure "very small" changes in CDF and LERF. Final quantitative criteria and regulatory guidelines for Alternative 1 would be developed during the rulemaking process.

Adherence to the acceptance criteria for ΔCDF and ΔLERF could be demonstrated either by performing a bounding assessment or by utilizing the plant's PRA to get a more realistic estimate. For example, in the absence of changes to the plant, the increase in CDF could be bounded by arbitrarily assigning a core-damage or a large-early-release outcome to the eliminated sequences. In reality, no increase in CDF or LERF would occur without plant changes. If plant changes were proposed based on Alternative 1, a more realistic evaluation of the impact on CDF and LERF could be obtained from PRA models. In this case, best-estimate thermal-hydraulic evaluations could be required to assess the impact of the proposed changes on PRA success criteria or success paths. DBA analyses still would be required for design-basis sequences retained or added under Alternative 1.

Alternative 1 may not interest licensees unless sequences involving postulated failures of redundant trains can be eliminated; this is because the limiting failure postulated for DBA analyses often is that of one train of a redundant system. Section 4.3.5 illustrates such an application of Alternative 1.

Adding Sufficiently Likely Sequences to the Design Basis

Alternative 1 would use frequencies to identify candidate sequences for additions to the design basis. Candidates would be selected from safety-related PRA success paths currently excluded as design-basis sequences because they involve either multiple events or excluded single-failure events. Only safety-related PRA success paths (i.e., ones involving successes of only safety-related SSCs) would be considered because DBA analyses do not credit non-safety-related SSCs. Any sequence meeting this description would become a candidate for addition provided that its frequency exceeded some criterion, for example, that of any current design-basis sequence that is not an elimination candidate.

For low frequency DBEs, such as large primary- or secondary-pipe breaks, new design-basis sequences are unlikely to be identified because the frequency of any potential candidate would likely fall below any reasonable quantitative selection criterion. However, the inclusion of new design-basis sequences would have to be deliberated for higher frequency DBEs, such as transients.

Multiple failures that might qualify include the combination of LOOP and an additional single failure that is currently postulated in design-basis sequences related to GDCs 34, 35, 38, 41 and 44. Section 4.3.2.2 delineates methods that could potentially be used to identify additional design-basis sequences involving multiple failures.

Non-frequency considerations, such as the following, would also be applied in determining whether to add a particular candidate sequence to the design basis:

> Design Margin: Would the addition of a particular sequence to the design basis effectively assure the maintenance of an adequate margin ? For example, there is little uncertainty that one out of four Low Pressure Coolant Injection (LPCI) pumps, or one out of four Low Pressure Core Spray (LPCS) pumps is sufficient to prevent core damage given rapid depressurization following a transient or small LOCA initiator. On the other hand, for

transients initiators without depressurization, injection capacity may be sensitive to valve configurations and flow resistances; accordingly, it may be effective to augment the design basis to assure that adequate margin is maintained.

Type of Margin to be Maintained: The type of margin to be maintained may be mechanical, electrical, or structural. DBAs used to assure adequate margins of mechanical systems based on thermal hydraulic analyses are the focus of Chapter 15 of the Standard Format and Content Guide for SARs. In contrast, some PRA success paths rely on margins inherent in structures or electrical systems. For example, analyses performed to resolve the station blackout issue assure there is sufficient DC power to cope with blackouts for a plant-specific time.

Acceptance criteria for any new design-basis sequence should be set to maintain acceptable margins, not to arbitrarily impose new margins, which probably would not be cost-beneficial. NRC-specified acceptance criteria or NRC guidelines that would permit licensees to set plant-specific acceptance criteria would have to be developed when implementing the addition part of Alternative 1. Systematically implementing this part will require extra work with the risk model, and closer than usual coordination between the T/H model and the risk model.

4.3.2.2 Implementation Approach

Implementation strategy is a key part of any risk-informed alternative to a regulation. Section 3.2.6 of this report identifies three activities:

- Initial Licensing Activities
- Continuing Programmatic Activities to Assure Safety Margins and Promote Functional Reliability
- Monitoring Activities

For Alternative 1, the implementation strategy is primarily related to the initial licensing activities involving the performance of DBA analyses. However, there is also a monitoring activity related to tracking the probability of component failures that are eliminated as single failures.

Initial Licensing Activities

Under Alternative 1, the licensee would be responsible for proposing the sequences to be eliminated from, and added to, the current design basis. Any of several methods could potentially be used to identify candidate sequences These include current methods such as Failure Modes and Effects Analysis (FMEA) and the use of PRA models and data (e.g., analyze event-tree success sequences, construct a special fault tree to identify the candidates, or examine the success paths constructed by complementing minimal cut sets). Following the guideline for performance-based licensing to avoid employing prescriptive methods, the licensees would be free to propose methods that the NRC would have to approve. Proposed methods, or applications thereof, could differ from or require extensions of existing PRA methods or applications. For example, the event trees applied in the example given in Section 4.3.5 differ from, but are based upon, PRA event trees.

As noted earlier, sequences proposed as candidates for elimination from the current design basis would likely have low frequency initiators, such as large breaks in the reactor coolant or secondary pressure boundary. It would be important to properly characterize their frequencies to properly encompass the scope of initiators that the DBE represents. For example, DBA analyses of large break LOCAs can cover pipe breaks initiated

randomly or during earthquakes as severe as the safe-shutdown earthquake, pressurizer failure, valve-bonnet failures, or pump ruptures. In evaluating the frequencies of DBEs for Alternative 1, all relevant failure modes and locations would have to be considered. Because of the large uncertainties associated with estimating the frequencies of such initiating events, periodically updated expert elicitation could be required, incorporating any pertinent data. Such a process was started for breaks in the reactor coolant system pipe in the LOCA redefinition initiative. To support Alternative 1, a similar process could be undertaken for secondary breaks.

Additional effort by the NRC would be required to select an effective approach for implementing Alternative 1, and to assess the impact on existing regulations, regulatory processes, regulatory guidance, and the licensees. As noted earlier, any plant changes proposed based on Alternative 1 would have to be consistent with RG 1.174 guidelines regarding preservation of defense-in-depth and safety margin, and any associated change in baseline CDF or LERF would have to be demonstrated to be very small. Pending the development of specific regulatory guidance for Alternative 1, licensees could propose under RG 1.174 the types of changes envisioned under this alternative.

Uncertainties would have to be addressed in implementing any SFC alternative. Specifically for Alternative 1, uncertainties associated with the frequencies and probabilities used to justify eliminating or adding sequences to the design basis would have to be considered in making comparisons to any quantitative criteria. This report is not the forum for setting out detailed guidelines on when and how to address such uncertainties. RG 1.174 has some guidance, but guidance specific to Alternative 1 would have to be developed during rulemaking.

The frequency of any sequence that could be a candidate for addition to the current design basis would have to be comparable to that of current design-basis sequences. In analyses of many DBAs, the limiting single failure is that of one of two redundant safety-related trains. The corresponding sequence involving failure of both trains typically would be far less likely. In addition, it would be an unacceptable addition to the design basis because, without credit for non-safety related SSCs or major plant modifications, failure of both trains would defeat the intended safety function. These observations indicate that the set of sequences added to the design basis under Alternative 1 could be sparse. Therefore, until there is clear interest in Alternative 1, it seems premature to initiate detailed studies to identify plant-specific candidates for elimination from or addition to the current design basis. If Alternative 1 is pursued, pilot plant studies probably would be appropriate (see Table 4.3-1).

Monitoring Activities

Alternative 1 would require monitoring data relevant to the frequency of rare initiating events, such as large pipe breaks, and periodically revising expert-judgement regarding these frequencies. In addition, any operational events related to sequences removed from the design basis would need to be monitored to maintain the justification for removal. Otherwise, Alternative 1 would not significantly change current monitoring practices. Plant-specific monitoring programs would be adapted to verify the models and data used in the selection of design-basis sequences.

4.3.2.3 Additional Considerations

Under Alternative 1, PRA sequences involving successes of non-safety-related SSCs are still excluded from the design basis, and no attempt is made to risk-inform the choice of design-basis initiating events. These topics exceed the scope of an alternative to the single-failure criterion; however, serious consideration of

Alternative 1 should probably address whether it should be expanded to address these topics. In this case, the following additional considerations would apply.

> Crediting Non-Safety-Related SSCs in DBA Analyses: Some PRA success paths with frequencies that would otherwise meet Alternative 1 criteria for inclusion as design-basis sequences involve successes of non-safety-grade equipment. In the terminology of 10 CFR 50.69, this equipment most likely would be classified as non-safety-related but safety-significant or Risk-Informed Safety Category 2 (RISC-2). Historically, design-basis analyses have not credited successes of RISC-2 SSCs; that is, the success events in design-basis sequences are those of safety-related SSCs. Changing this practice was not considered in formulating Alternative 1 because it would go beyond risk-informing the single-failure criterion. However, the level of scrutiny afforded to deterministic analyses of PRA success paths that credit non-safety related SSCs and have risk-significant frequencies could warrant further debate.
>
> DBA Initiator Selection: Current design-basis initiating events are delineated in the Standard Format and Content Guide for Safety Analysis Reports [USNRC, 1978]; they have not changed significantly based on PRA insights. For example, station blackouts are dominant contributors in PRAs but are excluded as DBAs. The frequency-based rationale for Alternative 1 could logically be expanded to consider a broader set of potential design-basis initiating events, including those at low power and shutdown. The scope of such an expansion could be quite broad, requiring extensive credit for non-safety-grade SSCs in analyses of new DBAs. This would go beyond risk-informing the SFC, and was, therefore, excluded in formulating Alternative 1. Nevertheless, a risk-informed approach for selecting design-basis initiating events, or guidelines for deterministic analysis of sequences with non-design-basis initiating events but risk-significant frequencies, could deserve more detailed examination.

4.3.3 Evaluation

Table 4.3-1 summarizes the key attributes of Alternative 1 in a format that facilitates comparisons with other alternatives. It summarizes the risk-informing approach, the implementation, and the relevance of Alternative 1 to the seven desirable attributes of SFC alternatives.

Alternative 1 would risk-inform the SFC as it impacts failure events postulated in DBA analyses, by focusing such analyses on demonstrating that functional requirements would be met for design-basis sequences with risk-significant frequencies. Single failures that entail lower frequencies would not have to be postulated. On the other hand, multiple failures that generate risk-significant frequencies would be postulated. The analysis of each DBA would still seek to identify the worst failure or combination of failures from the set of postulated single- or multiple-failures.

By eliminating sequences with low frequencies and very small risk implications from DBA analyses, the requirements for design-basis analyses could potentially be reduced and operating margins increased. Plant changes proposed based on Alternative 1 would be permitted only if they involved reductions, or very small increases, in CDF and LERF and maintained defense-in-depth and safety margin per RG 1.174 guidelines.

Any plant changes proposed based on Alternative 1 would have to be consistent with RG 1.174 guidelines. The key elements of defense-in-depth delineated in that document would be maintained. Safety margins would be maintained for all design-basis sequences that are not excluded based on small frequency and very

small CDF and LERF implications. Quantifying the change in CDF and LERF would require either bounding assessments, or the use of PRA models. Issues related to PRA scope and quality would need to be defined. The NRC's policy of a phased approach to PRA quality would be followed.

Appropriate NRC guidance would be needed to implement Alternative 1; specifically, guidance would have to be developed on selecting candidate sequences for elimination from or addition to the design basis. Additional effort, perhaps involving BWR and PWR pilot plants, would be required to accomplish this task.

Table 4.3-1 Alternative 1 Attributes

ALTERNATIVE 1 **Risk Inform Application of SFC for DBA Analyses**	
Attribute 1: **Functional Reliability**	Improvement, if any, to functional reliability would indirectly result from additional focus on multiple-failure success paths.
Attribute 2: **Defense-in -Depth**	Defense -in-depth would be maintained per RG 1.174 guidelines. Appropriate safety margin as evaluated in the DBA analysis would be maintained. The margin for any important safety-related, multiple-failure success paths would be demonstrated by analyses of new DBAs. The ability to mitigate excluded DBEs would be maintained, in line with the requirement in the proposed 10 CFR 50.46 rule to demonstrate the ability to mitigate beyond transition breaks.
Attribute 3: **Risk-informed Consideration of SFC in Safety Analysis**	Resources would no longer be devoted to analyzing very unlikely design-basis sequences. The current set of design-basis initiating events would not change (although transition break sizes could be used to remove some primary and secondary breaks from the design basis),but DBA analyses for these initiators would be augmented to address sufficiently likely safety-related multiple-failure success paths.
Attribute 4: **Performance-based Regulatory Approach**	The validity of frequency data and models used for Alternative 1 would be monitored much as it is today. Monitoring would not have to support a reliability-achievement program.
Attribute 5: **Amenable to Efficient Implementation**	Alternative 1 could be implemented relatively efficiently. A pilot plant application would probably be needed to develop appropriate regulatory guidance and acceptance criteria for identifying and analyzing new multiple-failure DBAs.
Attribute 6: **Coherence**	Alternative 1 appears consistent with ongoing efforts, including LOCA redefinition, risk-informing design-basis LOCA-LOOP assumptions, and developing a framework for advanced reactor licensing.
Attribute 7: **Security**	As for other alternatives, plant-specific changes would not be permitted to degrade security.

Practical applications of Alternative 1 for potentially eliminating single failures currently postulated in DBA analyses would be limited to DBAs with small initiating event frequencies, such as large LOCAs, and breaks in main steam- and main feedwater-lines. Work is well underway to redefine the large-break LOCA by risk-informing 10 CFR 50.46 and related GDCs. Transition break sizes have been identified for BWRs and PWRs. The draft rule language for 50.46 ECCS LOCA redefinition stipulates that, for LOCAs involving

breaks larger than the transition break size, neither loss of offsite power nor a single failure would have to be postulated. In addition, the BWR owner's group has separately proposed criteria for excluding LOOP as a design-basis assumption for sufficiently large LOCAs. Completion of these ongoing efforts to risk-inform the large-break LOCA and the associated LOOP assumption could reduce the potential impact of Alternative 1. However, similar efforts to define transition sizes for steam line- and feedwater line-breaks and to provide similar DBA treatment as is proposed for LOCAs. In addition, proposed changes could be plant-specific rather than generic. At least in principle, changes consistent with Alternative 1 could already be proposed by licensees based on Regulatory Guide 1.174.

Alternative 1 suggests a method for addressing passive failures in fluid systems. The frequency arguments used provide a consistent basis for excluding or including such low probability failures in design-basis sequences. However, it should be recognized that some passive failure sequences might meet the frequency screening criteria, but constitute failure paths and, therefore, would be unsuitable as design-basis sequences.

Finally, Alternative 1 would not risk-inform the choice of design-basis initiating events or consider success paths that credit non-safety-related SSCs as potential DBAs.

4.3.4 Summary

Table 4.3-2 summarizes Alternative 1 in a format that facilitates comparisons with other alternatives. It covers the motivating factors for the alternative, the risk-informed approach, the implementation approach, the potential achievements or positive aspects of the alternative, and its negative features.

4.3.5 Alternative 1 Example

Description

The purpose of Alternative 1 is to risk-inform the failure assumptions in a DBA analysis, using sequence frequencies to determine the failure events to be postulated in the DBA analyses. Sequences could be removed or added. This example is intended to illustrate the potential removal of low-frequency sequences from a DBA analysis that is part of the design basis for a PWR containment. A double-ended guillotine break (DEGB) of a main steam line(MSL) is the limiting DBA; it results in peak pressure and/or temperature in the containment of some PWRs because any break in the MSL dumps the maximum amount of mass and energy into the containment. Such breaks occurring at 102% hot full power (HFP) conditions as well as hot zero power (HZP) conditions typically are considered in the FSARs of these PWRs. Impacts on the reactor core also are analyzed, but this example focuses on the containment.

The following assumptions are made in a typical MSLB analysis:

6. The shutdown margin is the minimum allowed by the plant's technical specifications (TS).
7. The most reactive single control rod does not insert on reactor scram.
8. Only steam is allowed to flow out of the break.
9. The moderator temperature coefficient (MTC) is at its minimum allowed TS value.
10. The boron concentration in the SI flow is at the minimum value allowed by the plant's TS.

The licensee undertakes thermal hydraulic analyses of design-basis sequences, each with different postulated single failures, to establish the limiting MSLB sequence for pressure loading on the containment. The single failures can include

1. Failure of a main steam line check valve (results in blowdown from more than one steam generator until the MSIVs close).
2. Failure of the feedwater regulator valve.
3. Failure of a run-out limiter on the steam driven auxiliary feedwater system.
4. Electrical bus failure, resulting in the loss of one containment spray pump and two containment cooler fans.

Table 4.3-2 Alternative 1 Summary Description

ALTERNATIVE 1 Risk Inform Application of SFC for DBA Analyses	
Basic Motivating Factors for Alternative	Alternative 1 is motivated by the desire to risk-inform the failure events postulated in DBA analyses, and to ameliorate the SFC's inherent limitations with respect to multiple failures.
Risk-Informing Approach	For current design-basis initiating events: (1) Remove sufficiently unlikely, non-risk-significant single-failure sequences from the design basis. This also eliminates unlikely initiating events from the DBE category. (2) Add safety-related success paths involving multiple-failure events to the design basis when the frequency of a multiple failure success path exceeds a criterion, such as the frequency of any single-failure sequence postulated for the same initiating event.
Implementation Approach	Licensing At the licensing stage, the licensee delineates the proposed safety-related success paths for design-basis initiating events, which single-failure paths are to be eliminated, and which multiple-failure paths are to be added to the current design basis. Any plant changes proposed based on Alternative 1 would have to be consistent with RG 1.174 guidelines.
	Operations Monitoring At the operational stage, Alternative 1 would require monitoring data relevant to the frequency of rare initiating events, such as large pipe breaks, and periodic revision of expert-judgement regarding these frequencies. Plant-specific monitoring programs would be adapted to verify models and data used for selecting sequences for the design basis.
Potential Major Achievements	Alternative 1 would concentrate analyses of current design-basis initiating events on risk-significant safety-related success paths. It would explicitly address the SFC exclusion of multiple failure success paths from the current design basis.
Pros and Cons	Alternative 1 could give an additional predicted margin that could be used to justify plant changes consistent with RG 1.174 guidelines. Alternative 1 does not attempt to directly impact safety-function reliability. It appears to be consistent with ongoing efforts, including LOCA redefinition, risk-informing design-basis LOCA-LOOP assumptions, and developing a framework for advanced reactor licensing. Within this document, the scope of Alternative 1 has been limited; however, the frequency-based logic of Alternative 1 could be applied to more generally risk-inform DBA selection, including LOCA-LOOP assumptions, the choice of design-basis initiators, and, potentially, the inclusion of safety-significant, non-safety systems (RISC-2) in the DBA evaluation.

For one PWR studied for this example, the limiting MSLB scenario for the containment pressurization is the HZP case with the failure of the main steam check valve. Here, steam from more than one steam generator is dumped out of the break until the isolation valves shut (at 12 seconds). The calculated peak pressure is 41.85 psig. The containment's design pressure is 42.0 psig. For another PWR wherein electrical dependencies affect both feedwater isolation and containment cooling, the electrical-bus-failure sequence represents the limiting case. The licensee runs thermal hydraulic calculations for the different cases to show that the resulting peak pressure is below the containment's design pressure.

Key Features and Application

To illustrate Alternative 1, the frequencies of the MSLB design-basis sequences are identified. This highlights unlikely sequences that might be removed from the design basis. A probabilistic risk assessment, including the appropriate event tree, fault tree models, and failure probabilities, is developed for the particular plant to evaluate the postulated initiator of the MSLB, the plant and sequence thermal hydraulic conditions and assumptions (e.g., break flow rates), and subsequent postulated single failures. In an actual analysis, an acceptable basis would need to be established for the probabilistic data and the models used. It is expected that regulatory guidance would be established to define an acceptable approach.

Figure 4.3-1 is a simplified event tree for the containment loading MSLB DBA. It was specifically constructed for this example and not taken from a PRA. It represents a PWR for which the loss of electrical bus failure is the limiting sequence in its FSAR DBA analyses. The event tree's top event and end state definitions are shown in Table 4.3-3. Event probabilities that are meant to be reasonably representative are based on a limited review of several plant IPEs. Some assumptions in the analysis (like those listed above) were not quantified. For this PWR, the limiting FSAR design-basis sequence is sequence 7 on the event tree.

It includes the MSLB at low power and the loss of one DC bus that leads directly to the failure of the MFW to isolate and the loss of one train of both containment spray and fan coolers. Sequences 24-45 deal with sequences at higher power levels that tend to be limiting for containment temperature; they are not applicable for this example. Sequences 2-23 are associated with the low power cases and subsequent postulated failures that could over-pressurize the containment.

The top events on the event tree account for only those judged to be significant from the standpoint of the containment's pressurization. Other events could be shown, and some more likely failures postulated. Although not analyzed in detail for this example, it is expected that these events and the more likely sequences would not threaten the containment.

On the other hand, the event tree contains sequences (13-23) involving multiple failures that would not be bounded by the current DBA in that they would add more mass to the containment and further degrade containment cooling. They all are very low frequency sequences, and currently are judged to be of acceptably low risk. (For this example, they all include the failure of main steam isolation valves to close).

Assuming an initiating event frequency of 5E-4 /yr for the MSLB, a low probability of being at low reactor power (5.5E-3 /yr), and a failure probability for the loss of a DC bus of 2E-4/yr, the frequency estimate for the current limiting DBA (sequence 7) is very low (about 5E-10/yr). Because of the low frequency of the initiating event, the probability of the plant's condition, and the demand-failure probability for different failures that would maximize the event's severity, the DBA and other possible sequences involving these single failures all would be very low. Current FSARs show that the current design-basis sequences "bound" these other lower frequency sequences that could challenge the containment. They all involve postulated single failures.

The licensee would evaluate the design-basis sequences in detail, assess which ones can be considered for removal from the DBA, and demonstrate that their collective frequency is acceptably small. In addition to sequence 7, the event tree illustrates sequences that could be proposed to no longer be in the DBA (8 through 12) because of their very low frequency. These quantified estimates are not included here because they are all in the same range as sequence 7, or even lower.

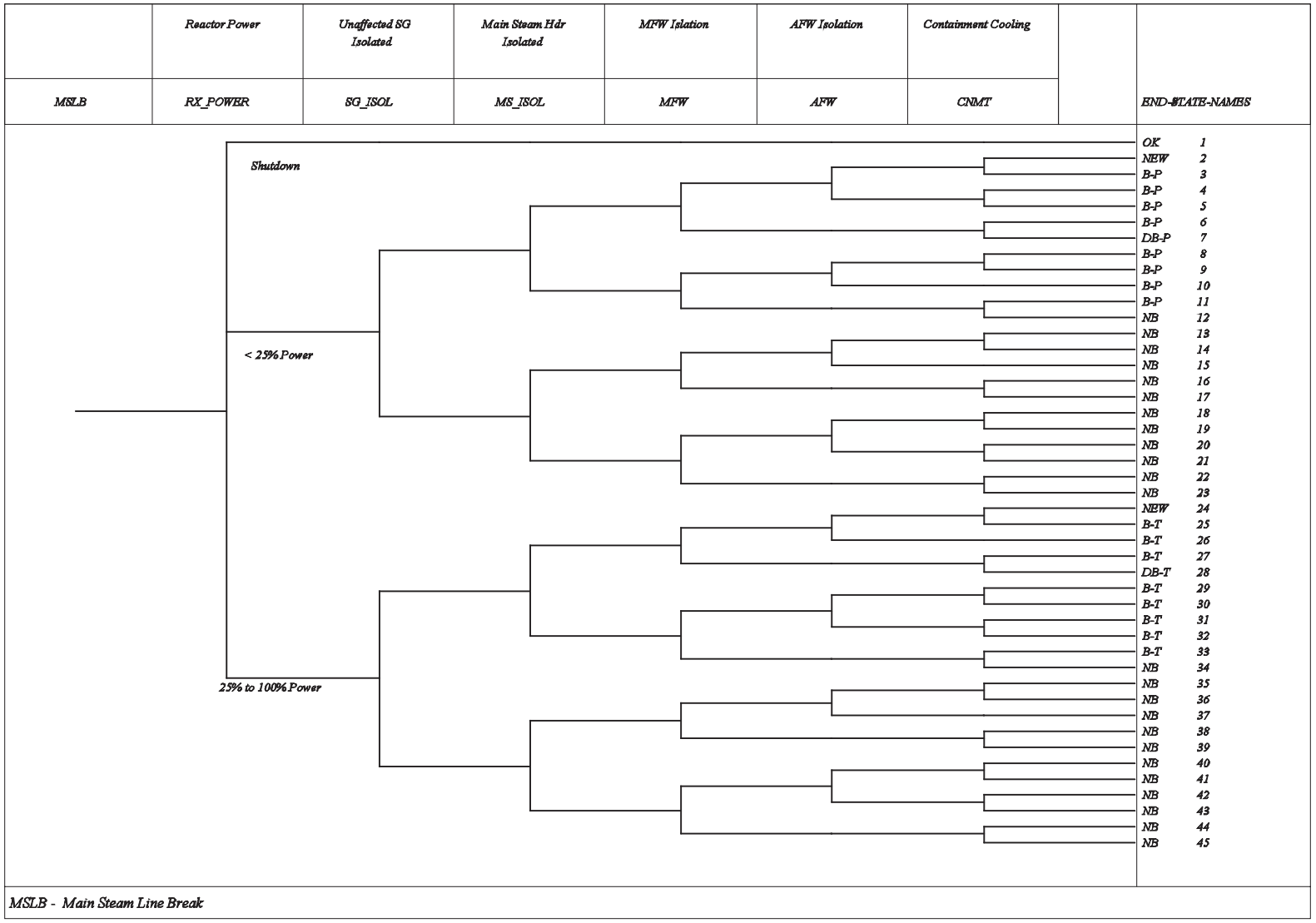


Figure 4.3-1 MSLB DBA Containment Event Tree

-52-

Table 4.3-3 MSLB DBA Containment Event Tree -Definitions

Initiating Event:	
MSLB	Large Main Steam Line Break within Containment (5E-4/yr frequency)
Top Events	
RX_POWER	Top event that represents the probability of the plant being at different power levels. In this example, it is assumed that the plant is at less than 25% power for 2 days per year. (5.5E-3)
SG_ISOL	Top event estimates the likelihood of the both MSIVs failing to close on demand. (1E-4)
MS-ISOL	Top event estimates the likelihood of the failure of the Main Steam non-return check valves to close on demand. (1E-3)
MFW	Top event estimates the likelihood that either the Main Feedwater Discharge valves or the Main Feedwater isolation valves fail to close on demand. (2E-3)*
AFW	Top event estimates the likelihood that AFW feed to the affected SG fails to isolate on demand. (1E-3)
CNMT	Top event estimates the likelihood that a single train of cooling (containment spray and containment fan coolers) fails. (2E-4)*
*Note: The model includes a single DC dependency on MFW and CNMT to represent the design bases limiting failure. The loss of one DC bus fails the feedwater control and one train of both the containment spray and containment cooling systems (2E-4). Such estimates are plant specific and will vary.	
End States	
NEW	Sequences not subject to single failure
B-P	Sequences estimated to be bounded by the design-basis containment pressure accident
B-T	Sequences estimated to be bounded by the design-basis containment temperature accident
DB-P	Sequence representing the design-basis containment pressure accident
DB-T	Sequence representing the design-basis containment temperature accident
NB	Sequences unlikely to be bounded by the design-basis event

The licensee would need to complete a process to assess how the DBAs should be modified. The risk analysis helps to develop a rationale for what sequences could be considered for the modified DBA from a MSLB perspective. Reviewing the MSLB event in the example event tree indicates that a new DBA might include the low-probability pipe break initiator, but no additional failures and/or different considerations of the reactor's power level and the steam generator's conditions-all of which are very important in estimating

the sequence frequencies. Such a sequence is sequence 2 in Figure 4.3-1. It represents only the initiator, and, for this example, the time at low power, which maximizes the steam generator mass. Its frequency would be about 3E-6/yr, which does not factor in the probabilities of other assumptions in the analysis, such as the stuck rod, or break flow.

Eliminating single failures from the design-basis analysis would engender a considerable lowering of the calculated peak containment pressure because a) the energy release to the containment would be reduced, and, b) the containment's pressure suppression system would be fully available. For example, from results given in the H. B. Robinson FSAR, the elimination of all single failures from the MSLB containment-pressure calculations would lower the peak pressure from 41.85 psig to 32 – 36 psi for the very low frequency DEGB.

As mentioned in the description of this alternative, changing the design-basis main steam line break size would have a major impact on the analysis of containment pressurization. Although this is not shown on the example event tree, a smaller break would dramatically reduce the release of mass and energy to containment. A similar analysis could be performed as another possible application for this alternative. Similar to the NRC's current work on 10 CFR 50.46, this approach could retain the single failure for the new DBA initiator. This would appear to have the benefit of providing stronger defense-in-depth, and could be a policy issue (as outlined in Section 2.5.6). That is, for the more likely smaller design-basis pipe break, mitigation still would be provided, assuming a single failure. A challenge with this approach is establishing, in the licensing basis, the new design-basis main steam line pipe break and its frequency.

Revising the DBA potentially would offer licensees additional operating margin, allowing them to consider plant changes, which would need to conform to the guidelines in RG 1.174. The change in risk resulting from a change would need to be small and the defense-in-depth provided by the containment would need to be confirmed. For example, it is expected that challenges to the containment for events removed from the DBA would need to be considered, including options to consider the margin to failure for unlikely events. Uncertainties also would have to be included. Thus, removing single failures from the DBA would need to be assessed carefully. As stated above, an approach that establishes a DBA that retains the SFC for smaller pipe breaks, would appear to have advantages. This would depend on many factors, including potential plant changes that are considered. Consistent with the Commission's guidance used to develop these alternatives, it is expected that a significant reduction in the containment's pressure retention capability would not be allowed.

A review of PWR FSARs offers other insights into postulated failures and conservatively established plant conditions for MSLB analysis. Some are discussed below. They can affect the analysis of the reactor core, as well as the containment.

Eliminating the single failure (loss of an HHSI pump) would not greatly affect calculations of the MSLB core response. This is because, even if Safety Injection (SI) began at the earliest possible time, under the present analyses' assumptions borated SI flow would not reach the core until about 200 seconds, at which time the core has already reached its maximum power level.

If the MSLB analysis' assumption of a stuck rod, which really is a component failure of a safety system, were eliminated for the DEGB MSLB, then the calculated behavior of the core would change dramatically. Without the stuck rod, the core very likely would not return to power. Even if it were calculated to do so, local peaking factors would be so low in the absence of a stuck rod that it is unlikely that there would be any fuel damage. The frequency of the occurrence of a stuck rod during reactor scram can be estimated from historical data.

The probability is small of the reactor having only the TS-allowed minimum shutdown margin available (assumption 1, above). Likewise, the probability also is small of the reactor having a MTC value near the TS minimum l. The MTC is considerably greater than the TS minimum value throughout most of a fuel cycle, approaching to within 10 – 20% of the minimum TS value only at the end-of-cycle.

Realistic estimates of water entrainment out of the break during a DEGB MSLB, rather than assuming a steam-only break flow, could entail as much as a 40EF additional margin in the containment's peak temperature ("Development of an Entrainment Model for the Steam Line Break Mass and Energy Release Analysis", J.Y. Lee, et. al., paper presented at ICAPP, May 2003). This is a significant factor in qualification analyses for equipment.

Results

This example illustrates how the revision of a current DBA analysis, including SFC assumptions that provide a basis for determining limiting plant conditions at some PWRs, could be considered. Applying Alternative 1 to the MSLB DBA analysis for a PWR could potentially remove some MLSB sequences, thereby affording the licensee opportunities for plant changes and operational flexibility. The MSLB DBA would need to be modified. In addition to the advantages of possible plant changes, including up-rating power, there is a possible reduction in surveillance and testing of some systems. A risk-informed DBA would be more closely aligned with other risk-informed NRC processes, such as the reactor oversight process (ROP). The major disadvantage is the complexity of the analysis and defining a new DBA to satisfy the principles of RG 1.174; this might include defining a suitable alternate methodology for defining a new size for DBA breaks, and maintaining defense-in-depth and safety margins for the DEGB MSLBs.

4.4 Alternative 2 - Risk-Inform the SFC According to the Safety Significance of Systems

4.4.1 Background

The current implementation of the single-failure criterion (SFC) requires redundancy as a tactic to promote high reliability of those safety systems required to respond to design-basis events. It also requires redundant system design as a surrogate for system reliability, along with the application of the redundancy design principle to most safety systems[5], regardless of their safety significance. A risk-informed change to the SFC would establish that a system's reliability is commensurate with its safety significance.

Alternative 2 proposes to classify a plant's systems according to their safety significance. Thereafter, safety-related systems that are safety significant would still have to meet the SFC's current requirements. On the other hand, since this classification relates the reliability of a system with its safety significance, these requirements can be relaxed to some extent for safety-related systems that have low-safety significance.

4.4.2 Alternative Discussion

4.4.2.1 Risk-Informed Approach

The SFC, as implemented in the General Design Criteria of Appendix A to 10 CFR Part 50, requires systems be designed to accomplish their safety functions to mitigate design-basis accidents, assuming a single failure. Such systems are deterministically classified as safety-related, and, in many cases, incorporate redundant design allowing them to fulfill safety functions assuming a single failure.

Alternative 2 proposes to risk-inform the application of the SFC according to the safety significance of safety-related systems. Those contributing to maintaining the current level of a plant's safety are considered safety significant, and the SFC is maintained for them. On the other hand, the safety-related systems that do not significantly contribute to maintaining the current level of safety are considered low-safety-significant. Alternative 2 proposes to relax the requirements of the SFC for the latter.

Nuclear power plants also have many other non-safety-related systems. Typically, licensees credit some of them in strategies for mitigating challenges to the plant that are not initiated by a design-basis event. In attempting to realistically evaluate the risk of a plant, probabilistic risk assessments (PRAs) assessed the impact of non-safety-related systems in mitigating accidents, and have shown that some non-safety-related systems can significantly lower the risk of a plant. Since this risk is related to the safety of a plant, these systems can significantly affect the safety of a plant.

The objective of the SFC is to promote high reliability of the plant's systems; hence, Alternative 2 also proposes maintaining the system reliability of non-safety-related systems that are safety-significant.

Two characteristics of Alternative 2 are that

- It explicitly relates the SFC to the safety (risk) of the plant. As mentioned in Section 3.2.2, the intent

[5]The SFC is applied to safety functions. A minimum of two safety groups (trains or systems) are required to satisfy the SFC for a given safety function. In practice, safety systems have redundant design, except for a few.

of the SFC, in the context of the General Design Criteria, is to promote high reliability of safety functions that are judged to be significant to safety, thereby reliably mitigating accidents. In this intent, there is an implicit relationship between the SFC, the reliability of safety systems (functions), and the plant's safety (risk). Alternative 2 explicitly and quantitatively relates the plant's safety to the reliability of safety-related and non-safety-related systems.

- Its scope extends beyond risk-informing the current SFC, applied to safety-related systems, to include the non-safety-related systems. Alternative 2 risk-informs the former by relaxing the level of regulatory requirements for systems of low-safety-significance, and the latter by increasing the level of regulatory requirements for safety-significant systems.

The safety significance of systems is determined by an integrated decision-making process that incorporates both risk and traditional deterministic insights. In other words, Alternative 2 defines "safety-significant system" as one whose loss or degradation could have a significant adverse effect on safety. The focus is on "safety-significant" instead of "risk-significant" because the Alternative 2's proposed categorization process considers probabilistic and deterministic information.

The probabilistic (risk) information used in the decision process comes from evaluating a **PRA whose quality is consistent with this application, and with the NRC's policy of a phased approach to PRA quality. Through using** PRA methods of systems analysis, elements of system reliability, such as common cause failures, human errors, passive failures, and multiple independent failures, which are not addressed by the SFC's redundancy requirements, will be accounted for.

The deterministic information used in the decision process consists of deterministic evaluations and the views of a panel of plant-knowledgeable members whose expertise includes PRA, safety analysis, plant operation, design engineering, and system engineering. The evaluations cover the relevance of a system in maintaining important aspects of safety, such as defense-in-depth and safety margins. This panel also will integrate the insights from probabilistic and deterministic information into their decision-making process on the safety significance of systems.

Ideally, a full-scope **PRA** is used to obtain the risk information that includes (1) internal and external events, (2) levels 1 (CDF) and 2 (LERF) of PRA[6], and, (3) all the risk-significant modes of operation, including full power and shutdown operation. Should a **full-scope PRA** not be available, concerns about the scope of the PRA could be handled in a way similar to that employed by10 CFR 50.69. In particular, the panel could contribute to address them.

From the probabilistic (risk) point of view, one possibility is to classify the systems in a similar way to the categorization proposed in 10 CFR 50.69, "Risk-informed Categorization and Treatment of Structures, Systems and Components for Nuclear Power Reactors." This categorization has advantages in that (1) the work to risk-inform the SFC using Alternative 2 can build upon the foundation and framework developed in 10 CFR 50.69, and, (2) the approach of Alternative 2 to risk-informing the SFC would be consistent and coherent with the NRC's current approaches to risk-inform the regulations.

Table 4.4-1 conceptually represents the proposed scheme for risk-informed system categorization that is consistent with 10 CFR 50.69. It overlays the current safety-related versus non-safety-related system

[6]Ideally, an evaluation of level 3 of PRA would be included. However, the NRC's current policy is to use CDF and LERF as surrogates.

categorization scheme with the proposed safety-significant categorization. In the traditional deterministic approach, systems generally were categorized as either "safety-related" (as defined in 10 CFR 50.2) or non-safety-related, as shown by the vertical line. Probabilistic and deterministic information can identify systems as being either safety significant or low safety-significant (shown by the horizontal line). Accordingly, the systems are grouped into one of four risk-informed safety classification (RISC) categories, represented by the four boxes. It is envisioned that some safety-related systems would be safety significant, but others would have low safety significance. Thus, the safety-related systems would be classified into "boxes" 1 and 3 of Table 4.4-1, according to their safety significance. Similarly, non-safety-related systems, classified according to their safety significance, would be allocated to boxes 2 and 4.

Table 4.4-1 Alternative 2 Categories
(bold indicates the type of applicable regulatory treatment)

[1] Risk-informed [,]	[1] Deterministic [,]	
	1 RISC-1 Systems Safety-related Safety Significant **Current requirements, plus performance monitoring of system reliability.**	2 RISC-2 Systems Non-safety-related Safety Significant **Current requirements, plus performance monitoring of system reliability.**
	3 RISC-3 Systems Safety-related Low Safety Significant **Alternative 2a: SFC (redundancy) may be removed. Current requirements for the remaining train.** **Alternative 2b: Current requirements for one safety-related train, and requirements that are consistent with non-safety-related equipment would be assigned to the redundant trains that are re-classified as non-safety-related.** **Alternative 2c: Current requirements for one safety-related train; operational requirements of redundant safety-related trains may be relaxed.**	4 RISC-4 Systems Non-safety-related Low Safety Significant **Current requirements.**

Using the framework of 10 CFR 50.69, licensees would use a risk-informed process for categorizing structures, systems, and components (SSCs). It appears that, in practice, licensees following 10 CFR 50.69 would be categorizing components. Hence, an important difference between the approach of Alternative 2 and 10 CFR 50.69 is that the former is applied at the system level, while the latter mainly is applied at the component level. This difference also can be interpreted as an advantage of Alternative 2 because appropriate requirements can be applied at the system level, instead of at the component level. Accordingly, the discussion of the RISC categories of Table 4.4-1 is at the system level.

Individual trains of a system are not always identical and each may have a different safety significance. Accordingly, another possibility would be to classify trains as being safety significant or not, instead of classifying the entire system. This approach has several attractive features: 1) an entire system might not meet the criteria to be of low safety significance but a single train could, 2) classifying individual trains would identify those that are low safety significant, and hence, they would become candidates for relief on

regulatory requirements, and, 3) the safety significance of systems comprised of a single train could be compared to the significance of other system's trains. For brevity, the discussion of Alternative 2 is mainly presented in terms of entire systems.

A system that is safety significant is expected to receive more stringent regulatory requirements than one that is low-safety significant. In other words, the regulatory requirements of a system (safety-related or non-safety-related) should be commensurate with its safety significance. Thus, the requirements of safety-related systems that have low safety significance can be relaxed to some extent, while the requirements of non-safety-related systems that are safety significant may be increased.

Three variations, a, b, and c of Alternative 2 are considered. The difference between them is the way in which each allows some relaxation of the SFC requirements for RISC-3 systems. In summary, for a RISC-3 safety-related system having redundant trains,

- Alternative 2a proposes that the redundant safety-related trains can be removed from service. The system then would have a single train.

- Alternative 2b proposes that one train would remain as safety-related, while re-classifying the redundant trains as non-safety-related.

- Alternative 2c proposes that all trains would remain as safety-related. The regulatory requirements for one of them would remain the same, while providing operational flexibility for the redundant trains.

The requirements applicable to each RISC are as follows. RISC-1 systems are safety-related and are safety significant. Since these systems are safety significant, it is proposed that performance monitoring of system reliability be required, in addition to the current regulatory requirements, such as the maintenance rule.

RISC-2 systems are non-safety-related ones that are safety significant. Since they are safety significant, it is proposed that a greater level of regulatory requirements than the current ones is applied to them. Specifically, since non-safety-related systems are not now required to satisfy the SFC, in addition to imposing the current requirements, the level of regulatory requirement would be increased by performance monitoring of system reliability to maintain their current reliability.

RISC-3 systems are safety-related ones that have low safety significance. Since they are safety-related, the requirements of the SFC are applicable. However, due to their low safety significance, this alternative proposes that the requirements of the SFC can be relaxed to some extent. The difference between sub-alternatives 2a, 2b, and 2c is the way in which each allows some relaxation of the SFC requirements for RISC-3 systems. These differences are described in the paragraphs above; they reflect the degree to which defense-in-depth (DID), expressed by redundancy, is risk-informed. Figure 4.4-1 compares this degree with the current SFC which is based on a structural interpretation of DID. Alternative 2c incorporates some rationalist considerations in the SFC by allowing operational flexibility. Alternative 2b also does so by allowing redundant trains to be re-classified as non-safety-related. Alternative 2a is based on a rationalist interpretation of DID; thus, this sub-alternative permits redundancy to be removed.

The three sub-alternatives propose keeping one train as safety related, so that all the requirements associated with this train would remain unchanged. Therefore, the functionality of this train would remain unaffected. For all or some RISC-3 systems to obtain a relaxation of regulatory requirements, the guidelines specified in Regulatory Guide (RG) 1.174, in particular the following ones, would have to be satisfied:

- The cumulative postulated changes would have to meet the guidelines for CDF and LERF specified in RG 1.174. An approach to evaluating the cumulative impact on risk of a proposed change is to remove redundancy in the PRA model for all (or selected) RISC-3 systems and obtain the updated risk measure, such as the CDF. If relaxation of regulations is initially proposed for all RISC-3 systems, the cumulative impact may exceed the guidelines for CDF and LERF, in which case, a subset of the RISC-3 systems may be selected that satisfies these guidelines.

- The proposed changes should be consistent with the defense-in-depth principle, i.e., for acceptability, it is necessary to confirm that this principle is preserved. Confirmation would consist of evaluating the remaining level of defense-in-depth after the proposed changes would be implemented. One possibility is to use the evaluation of defense-in-depth presented in NEI 00-04 (Nuclear Energy Institute, 2004). For example, for preventing core damage, NEI 00-04 describes a "defense-in-depth matrix" that can be used to confirm the low safety significance of a system. RG 1.174 sets out the elements of defense-in-depth that also can be used as guidelines for confirming that the principle is preserved.

For RISC-3 systems, the redundant train(s) that is a candidate for relaxation serves the structuralist intent and allows mitigation of DBAs during the unavailability of the other safety-related train. Sub-alternative 2a allows redundancy to be removed, so this redundant train(s) could be taken out of service. Sub-alternative 2a illustrates a higher degree of risk-informing defense-in-depth than do the sub-alternatives 2b and 2c, and, in this way, helps to provide a context for the sub-alternatives 2b and 2c. However, since sub-alternative 2a does not serve the structuralist intent, it is unlikely that it would be considered a feasible replacement of the SFC.

RISC-4 systems are non-safety-related ones that have low safety significance. It is expected that any current regulatory requirements would be maintained for them.

As discussed above, Alternative 2 applies to the system level. Accordingly, once the plant's systems are classified into the four RISC categories, the regulatory requirements can be relaxed for those components of the systems categorized as low-safety significant. In particular, to be consistent with 10 CFR 50.69, "special treatment" is one regulatory requirement that could be relaxed under Alternative 2.

From the point of view of the risk significance of a system, one possibility for categorizing systems as "safety significant" or "low safety significant" is to use the risk-importance measures known as "Risk Achievement

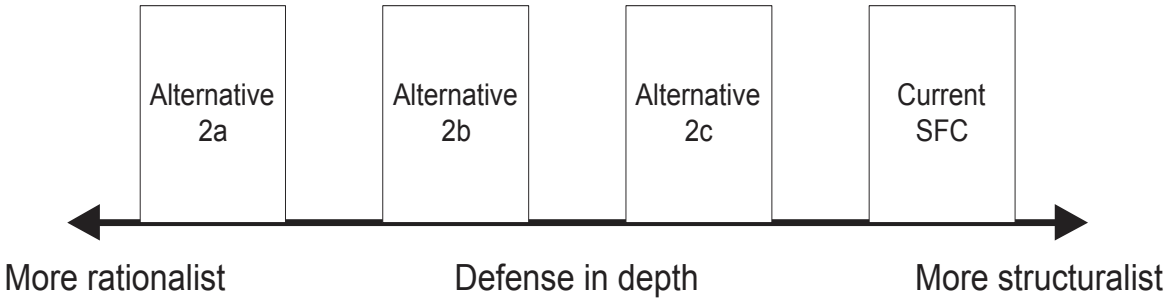


Figure 4.4-1 Illustration of Defense-in-Depth Aspect of Alternative 2

Worth" (RAW) and Fussell-Vesely (FV) at the system level; this categorization would be consistent with 10 CFR 50.69. Accordingly, a system would be safety significant if its RAW or FV measure of risk importance exceeded certain thresholds. These thresholds might be set using the following scheme put forward in 10 CFR 50.69: each system with a RAW greater than 2 or a FV greater than 0.005 is considered "safety significant"; all others are "low safety significant."

The RAW and FV measures of risk importance would have to be calculated at the levels of core damage frequency (CDF), and of large early release frequency (LERF). If a system's RAW or FV at the CDF level, or its RAW or FV at the LERF level, is greater than the CDF-or the LERF-threshold, the system is considered "safety significant"; otherwise, it is "low safety significant."

Should the RAW or FV identify a system as safety significant, it would be assigned to RISC box 1 or 2 in Table 4.4-1, depending on the system's deterministic characterization (safety-related or non-safety-related). Those systems not determined to be safety-significant are considered to be low safety-significant, and, therefore, would be classified in RISC box 3 or 4 (depending on whether the system is safety-related or not).

RISC-3 systems are safety-related ones that have low safety significance; hence, relaxation of their regulatory requirements would be proposed for them. Only the systems classified as RISC-3 are candidates to obtain this relaxation because they were not identified as important to safety by the probabilistic importance measures RAW or FV, nor by deterministic considerations.

As mentioned earlier, one choice is to classify individual trains of systems as being safety significant or not, instead of classifying an entire system. In this case, each train's RAW and FV would be calculated.

4.4.2.2 Implementation Approach

The NRC and a licensee would implement Alternative 2 according to the following major steps:

- The NRC would issue a new regulation as an alternative to the SFC; it could be an expanded version of 10 CFR 50.69 that would include the approach to risk-informing proposed by Alternative 2. The GDC that are related to the SFC also may have to be modified to be consistent with the proposed changes.

- Typically, the licensee would classify the plant's systems into the four RISC categories using its PRA. **The quality of this PRA must be consistent with this application.**

- The licensee could change the plant's systems as described in this Alternative, as long as the cumulative postulated changes meet the guidelines for CDF and LERF specified in RG 1.174. In particular, relaxed regulatory requirements could be applied to "low-safety-significant" (RISC-3) systems, and enhanced ones to "safety-significant" (RISC-1 and RISC-2) systems.

- The licensee would monitor the performance of system reliability for safety-significant systems, i.e., RISC-1 and RISC-2 systems. Monitoring activities for RISC-3 systems may be relaxed to some extent, as described later in this subsection.

The last three steps would be carried out by the licensee with NRC's oversight.

RISC-4 systems are non-safety-related ones of low safety significance. It is expected that the current regulatory requirements would be maintained for them.

Section 3.2.6 presents three aspects of the basic concepts of implementing an SFC alternative in the regulatory process:

- Initial Licensing changes
- Continuing Programmatic Activities
- Monitoring Activities

Each aspect of implementation is discussed next for each sub-alternative of Alternative 2.

Initial Licensing Changes

Each sub-alternative of alternative 2 affects the redundancy requirements for RISC-3 systems differently. Table 4.4-2 discusses the potential impact of each sub-alternative on these requirements.

Table 4.4-2 Potential Impact of Alternative 2 on Redundancy Requirements for RISC-3 Systems

For a RISC-3 safety-related system having redundant trains...	Trains credited in DBA analysis	Initial licensing change regarding DBA analysis
Alternative 2a proposes removing the redundant safety-related trains from service. The system then would consist of a single safety-related train.	A single safety-related train.	The DBA analyses that rely on this system for mitigating accidents would have to be re-evaluated to demonstrate that the safety-margin requirements are satisfied with the new configuration; this would include all the RISC-3 systems that were changed to one safety-related remaining train. The worst single failure (WSF) in DBA analyses would have to be waived because a single safety-related train cannot meet it.
Alternative 2b proposes that one train would remain as safety-related, and the redundant ones re-classified as non-safety-related.	The non-safety-related train(s) are not credited to satisfy requirements of the safety margin. Only the safety-related train is credited in DBA analysis.	
Alternative 2c proposes that all trains would remain as safety-related.	All current safety-related trains remain in service	No change needed in DBA analysis.

For a RISC-3 safety-related system having redundant trains, Alternative 2a proposes leaving one train as safety-related, while taking the redundant trains out of service. To allow this change, the licensing basis would have to be modified.

For a RISC-3 safety-related system with redundant trains, Alternative 2b proposes that one train would remain as safety-related, while re-classifying the redundant ones as non-safety-related. Accordingly, the licensing basis would have to be modified to allow these redundant trains to be re-classified from safety-related to non-safety-related. This modification would have to meet RG 1.174 guidelines, including those

on defense-in-depth and safety margins. Satisfying them may entail maintaining selected deterministic design criteria (e.g., separation criteria for power and control circuits).

Finally, for a RISC-3 safety-related system having redundant trains, Alternative 2c proposes that all trains would remain as safety-related. The regulatory requirements for one of them remain the same; operational flexibility can be provided for redundant ones. **Examples of operational flexibility are less stringent requirements on the systems' components, extensions of the requirements of Technical Specifications such as Allowed Outage Times (AOTs) and Surveillance Test Intervals (STIs), and risk-informed In-Service Inspection (ISI) and In-Service Testing (IST).** Accordingly, implementing Alternative 2c would allow revising those aspects of the licensing basis associated with a RISC-3 system's operational requirements.

Alternative 2 also proposes monitoring the performance of systems' reliability for systems that are safety significant, i.e., those in categories RISC-1 and RISC-2. This monitoring would be added to the current regulatory requirements applicable to these systems. Monitoring is considered to be particularly relevant for non-safety-related systems that are safety significant because the current regulatory requirements may not offer an acceptable degree of confidence that their reliability conforms with their importance to safety.

The reliability of a system is the probability that the system, on demand, will successfully carry out its function during its mission time. Performance monitoring of a system's reliability can be established by tracking a calculated system-level indicator built up from component-level contributions in two major steps, as follows:

- Developing the approach to performance monitoring of system reliability requires specifying a certain numerical "target" of reliability for each safety-significant system. A starting point for an acceptable "reliability target" is the current reliability of each system; the so-called "baseline reliability." Alternatively, a certain numerical "target" can be specified for each system.

- The operational events of a system, such as the number of failures in a certain period and the length of time that the system or some of its components are unavailable, can be gathered and used to update the probabilistic parameters for the system's components, such as failure rates. These updated parameters can then be input to the PRA to render an updated assessment of the system's reliability. In this way, the licensee and the NRC can quantify and monitor the actual reliability of a system The updated value can be compared with the baseline figure to assess whether the system's reliability is deteriorating, and, if so, take timely corrective actions.

The "baseline reliability" (step 1) is established during the initial licensing changes. Step 2 is conducted during the monitoring activities (further discussed under Monitoring Activities, below). The same PRA that is used to classify the systems can be used to establish the "baseline reliability," and also for subsequent evaluations supporting the performance monitoring of system reliability.

Continuing Programmatic Activities

Table 4.4-3 discusses the continuing programmatic activities for Alternative 2.

Monitoring Activities

Monitoring activities depend on each class of system; RISC-1 systems are safety-related ones that are safety significant. Since these systems are safety significant, performance monitoring of system reliability is proposed, in addition to current regulatory requirements, such as the maintenance rule.

RISC-2 systems are non-safety-related ones that are safety significant; therefore, the application of a greater level of regulatory requirements than the current ones is proposed for them. Since non-safety-related systems are not now required to satisfy the SFC, Alternative 2 proposes that on top of the current requirements, the level of regulatory requirements is increased for RISC-2 systems by requiring performance monitoring of system reliability to maintain their current reliability.

The activities for the performance monitoring of a system's reliability require two major steps:

- gathering operational events of a system, such as the number of failures in a certain period, and the length of time that the system or some of its components are unavailable.

- using the data gathered in the first step to update the probabilistic parameters for the system's components, such as failure rates. These revised values can be used as input to the PRA to obtain an updated system reliability. In this way, the licensee and the NRC can quantify and monitor the actual reliability of a system, and compare it with the baseline reliability to assess whether there is any deterioration, and if so, take timely corrective actions.

Table 4.4-3 Continuing Programmatic Activities for Alternative 2

For a RISC-3 safety-related system having redundant trains...	Programmatic Activities
Alternative 2a proposes removing the redundant safety-related trains from service. The system then would consist of a single safety-related train.	The current programmatic activities for the remaining safety-related train are not changed. Since the redundant safety-related trains are taken out of service, their current programmatic activities are eliminated.
Alternative 2b proposes that one train would remain as safety-related, and the redundant ones re-classified as non-safety-related.	The current programmatic activities for the remaining safety-related train are not changed. Programmatic activities that are consistent with non-safety-related equipment would be assigned to the re-classified redundant trains.
Alternative 2c proposes that all trains would remain as safety-related.	The regulatory requirements for one of the trains remain the same. Since operational flexibility can be provided for redundant trains, some of the current Programmatic Activities, such as **Technical Specifications (AOTs and STIs**) and ISI and IST can be relaxed.

Performance monitoring of a system's reliability should be conducted such that any decline in this reliability can be identified before the plant's safety becomes unacceptable, without incorrectly identifying normal variations as degradations. The NRC already has worked in similar areas, such as developing the Risk-Based Performance Indicators (RBPIs) (for example, NRC, 2000c) and the Mitigating Systems Performance Indices (MSPIs) upon which the performance monitoring of system reliability proposed by Alternative 2 can consistently build.

RISC-3 systems are safety-related ones with low safety significance; Table 4.4-4 describes monitoring activities for them.

Table 4.4-4 Alternative 2 Monitoring Activities for RISC-3 Systems

For a RISC-3 safety-related system having redundant trains...	Monitoring Activities for RISC-3 systems
Alternative 2a proposes taking out of service the redundant safety-related trains. The system would then be comprised of a single safety-related train.	The current monitoring activities for the remaining safety-related train are unchanged. Since the redundant safety-related trains are removed, their current monitoring activities are eliminated.
Alternative 2b proposes that one train would remain as safety-related, and the redundant trains can be re-classified as non-safety-related.	Current monitoring activities for the remaining safety-related train are not changed. Monitoring activities that are consistent with non-safety-related equipment would be assigned to the redundant trains re-classified as non-safety-related.
Alternative 2c proposes that all trains would remain as safety-related.	The current monitoring activities for all trains of the system are not changed.

RISC-4 systems are non-safety-related ones having low safety significance. Their current regulatory requirements are expected to be maintained.

4.4.3 Evaluation

Pros and Cons

Alternative 2 offers a framework (for both the NRC and licensee) indicating the importance of systems to safety. In general, classifying systems defines a set of relationships for assigning regulatory requirements to systems according to their safety significance. In this way, Alternative 2 relates the requirements of the SFC to the safety significance of a system. The safety significance of a system in turn, is related to the plant's safety.

Alternative 2 risk-informs the deterministic requirement of the SFC for safety-related systems that are not safety significant, but raises the level of regulatory requirements for non-safety-related systems that are safety significant. Thus, this alternative supports the NRC's goals of ensuring plant safety and efficiency of regulatory oversight, as follows:

- Ensuring Plant Safety - Using a framework for classifying the plant's systems, Alternative 2 identifies those non-safety systems that are significant to safety (RISC-2 systems), and proposes performance monitoring of system reliability for them. Alternative 2 thereby encompasses non-safety systems that the SFC does not address. The safety of a plant is expected to be ensured, or at least maintained, by implementing performance monitoring of the reliability for non-safety systems that are significant to safety.

- Efficiency of Regulatory Oversight - Alternative 2 allows some reduction of regulatory burden. Specifically, it lowers the regulatory requirements for RISC-3 systems, i.e., systems that are safety-related but of low safety significance, so resulting in efficient regulatory activity. In other words, this relaxation would effectively use the resources of the NRC and of the licensees.

Alternative 2 is consistent with, and extends the scope of, 10 CFR 50.69 to risk-inform the SFC.

In addition to the above benefits, Alternative 2 addresses the seven attributes of risk-informed alternatives to the SFC, so it fulfills the requirements for a risk-informed alternative to the SFC. Table 4.4-5 shows the main characteristics of Alternative 2, including the way it addresses these seven attributes.

Two relatively minor cons were identified. Alternative 2 requires PRA models of adequate quality. In addition, the alternative requires effort on the part of both NRC and industry to develop regulatory guidance and possible rulemaking.

Table 4.4-5 Alternative 2 Attributes

ALTERNATIVE 2 Risk-Inform Application of SFC According to the Safety Significance of Systems	
Attribute 1: **Functional Reliability**	Alternative 2 addresses functional reliability because 1) it relates the safety significance of a system to a plant's overall risk measures; 2) it uses a quantitative criterion to classify a system according to its safety significance; 3) since it uses a PRA, it addresses significant elements of reliability such as CCF, human error, passive failure, and multiple independent failures; and, 4) a system's reliability would be commensurate with the frequency of challenges. Thus, those systems classified as safety significant would be required to maintain the current reliability. By contrast, systems classified as low safety significant could have "low" reliability.
Attribute 2: **Defense-in-Depth**	Sub-alternatives 2a, 2b, and 2c implement different degrees of risk-informing DiD, the objective of which is to tie DiD to the safety significance of systems.
Attribute 3: **Risk Inform Consideration of SFC in Safety Analysis**	Sub-alternatives 2a and 2b propose that a safety-related system with redundant trains would have only one remaining safety-related train. The WSF in DBA analyses would have to be waived because it cannot be met by a single safety-related train. In this sense, 2a and 2b risk-inform the consideration of SFC in safety analysis. Sub-alternative 2c does not do this.
Attribute 4: **Performance-based Regulatory Approach**	Sub-alternatives 2a and 2b propose changing the licensing basis of a plant by allowing a single safety-related train instead of a safety-related system with redundant trains. Accordingly, performance monitoring would be required to meet the guidelines of RG 1.174. In addition, all three, 2a, 2b, and 2c, require performance monitoring of the reliability of safety-significant systems (RISC-1 and RISC-2).
Attribute 5: **Efficient Implementation**	Alternative 2 is considered amenable to efficient implementation because it uses concepts that are used by other risk-informed initiatives by the NRC.
Attribute 6: **Coherence**	Alternative 2 satisfies this attribute because the concepts it uses are similar to those in 10 CFR 50.69 in that it categorizes the elements of interest by their safety significance.
Attribute 7: **Security**	Alternative 2 satisfies this attribute because plant-specific changes would not be permitted to adversely impact the "built-in capability" of the plant to resist security threats.

Relationship of Alternative 2 to Current NRC's Activities

Alternative 2 is related to 10 CFR 50.69, "Risk-informed Categorization and Treatment of Structures, Systems and Components for Nuclear Power Reactors," in that it categorizes the elements of interest by their safety significance.

Alternative 2 is related to the NRC's programs developing and establishing performance indicators, such as the Risk-Based Performance Indicators (RBPIs) and the Mitigating Systems Performance Indices (MSPIs). These indicators reveal changes in unreliability and unavailability. Evaluating these changes is similar to

the objective of performance monitoring of system reliability for safety-significant systems, i.e., identifying and correcting any drop-off in a system's reliability before the plant's safety deteriorates unacceptably.

Impact of Alternative 2 on NRC and industry

Alternative 2 has the following main impacts on NRC and industry:

- Reducing the regulatory requirements for RISC-3 systems, i.e., systems that are safety-related but that are of low safety significance. This change would result in efficient regulatory activity, i.e., relaxation would lead to an efficient use of the resources of the NRC and the licensee. Specifically, for a RISC-3 safety-related system having redundant trains

  Alternative 2a proposes that one train would remain as safety-related, while removing the redundant trains from service.

  Alternative 2b proposes that one train would remain as safety-related, while re-classifying the redundant trains as non-safety-related.

  Alternative 2c proposes that all trains would remain as safety-related. The regulatory requirements for one of them remain the same; operational flexibility can be provided for redundant trains.

- Requiring performance monitoring of system reliability for safety-significant systems (RISC-1 and RISC-2). This change is expected to maintain the reliability of this type of system, thereby maintaining the plant's safety.

4.4.4 Summary

Table 4.4-6 summarizes the main characteristics of Alternative 2.

Table 4.4-6 Alternative 2 Summary Description

ALTERNATIVE 2 Risk-Inform Application of SFC According to the Safety Significance of Systems	
Basic Motivating Factors for Alternative 2	Alternative 2 recognizes that the SFC's current implementation requires redundancy as a tactic to maintain plant safety by promoting high reliability of safety systems that must respond to design-basis events. This implementation necessitates functional redundancy as a surrogate for functional reliability, and requires applying redundancy to most safety systems, regardless of their safety significance. Alternative 2 proposes risk-informing the SFC, such that a system's reliability is commensurate with its safety significance.
Risk-informing Approach	The safety significance of systems is determined by an integrated decision-making process that incorporates risk and traditional deterministic insights. From the point of view of the risk significance of a system, one possibility to categorize systems as "safety significant" or "low safety significant" is to use the RAW and FV at the system level, a categorization that would be consistent with 10 CFR 50.69. Accordingly, for each system, if either its RAW (FV) at the CDF level, or its RAW (FV) at the LERF level, is greater than 2 (0.005), the system is considered "safety significant"; otherwise, it is "low safety significant."

Table 4.4-6 Alternative 2 Summary Description (continued)

ALTERNATIVE 2 Risk-Inform Application of SFC According to the Safety Significance of Systems	
Implementation Approach	Initial Licensing Changes: Sub-alternatives 2a and 2b propose that a safety-related system with redundant trains would have only one safety-related remaining train. The DBA analyses that rely on this system for mitigating accidents would have to be re-evaluated to demonstrate that the new configuration satisfies safety margins; this configuration would include all RISC-3 systems that were changed to one safety-related remaining train. Sub-alternative 2c does not change the DBA analysis. The 3 sub-alternatives require performance monitoring for reliability of safety-significant systems (RISC-1 and RISC-2). The "targets" for system reliability could be established during the initial licensing changes.
	Continuing Programmatic Activities: Alternative 2a: The current activities for the remaining safety-related train are not changed. Since the redundant safety-related trains are removed from service, the current activities for them are eliminated. Alternative 2b: The current activities for the remaining safety-related train are not changed. Activities that are consistent with non-safety-related equipment would be assigned to the redundant trains that are re-classified as non-safety-related. Alternative 2c: The regulatory requirements for one of the trains remain the same. Since operational flexibility can be provided for redundant trains, some current activities, such as **Technical Specifications (AOTs and STIs**) and ISI and IST can be relaxed. Monitoring Activities: Performance monitoring of reliability for systems that are safety significant, i.e., those in categories RISC-1 and RISC-2. Alternative 2a: For RISC-3 systems, the current monitoring activities for the remaining safety-related train are not changed. Since the redundant safety-related trains are taken out of service, their current monitoring activities are eliminated. Alternative 2b: For RISC-3 systems, the current monitoring activities for the remaining safety-related train are not changed. Monitoring activities that are consistent with non-safety-related equipment would be assigned to the redundant trains that are re-classified as non-safety-related. Alternative 2c: The current monitoring activities for all trains of the system are not changed for RISC-3 systems. The current regulatory requirements would be maintained for RISC-4 systems.
Potential Major Achievements	Alternative 2 would risk-inform the simple deterministic requirement of the SFC for safety-related systems that are not safety significant, and increase the level of regulatory requirements for non-safety-related systems that are safety significant. Hence, this alternative supports the NRC's goals of ensuring plant safety and efficiency of regulatory oversight.

Table 4.4-6 Alternative 2 Summary Description (continued)

ALTERNATIVE 2 Risk-Inform Application of SFC According to the Safety Significance of Systems	
Pros and Cons	The following are Alternative 2's advantages: 1) it provides a framework (for both NRC and licensee) demonstrating the importance of systems for safety. In general, classifying systems provides a basis for assigning regulatory requirements to systems according to their safety significance. In this way, Alternative 2 relates the requirements of the SFC to the safety significance of a system that, in turn, is related to the plant's safety. 2) using a framework for classifying the plant's systems, Alternative 2 identifies those non-safety systems that are significant to safety (RISC-2 systems), and proposes performance monitoring of their reliability. In this way, Alternative 2 encompasses non-safety systems which the SFC does not address. 3) it extends the scope of 10 CFR 50.69 to risk-inform the SFC. 4) it addresses all seven desired attributes for replacing the current SFC. Two relatively minor cons were identified: Alternative 2 requires PRA models of adequate quality. In addition, the alternative requires effort on the part of both NRC and industry to develop regulatory guidance and possible rulemaking.

4.4.5 Alternative 2 Example

Description

This example places the systems in a NPP into one of four risk-informed safety classification (RISC) categories, depending on its deterministic class, and safety significance. Then, the regulatory requirements, especially those related to the SFC, can be relaxed for those identified as safety related and "low safety significant." For example, applying sub-alternative 2b to each of these systems, one train would remain as safety-related, and the redundant trains would be re-classified as non-safety-related.

The NPP selected for this example of Alternative 2 is a BWR/4 with a Mark I containment. These are the most common type of BWR in the United States. Most have Mark I containments.

Key Features

The main features of Alternative 2 are the following:

(a) The systems in a nuclear power plant have different safety significance, and regulatory requirements can be applied in a way that is commensurate with this significance. Stricter requirements can hold for systems classified as "safety significant" than for systems classified as "low safety significant."

(b) The systems in a NPP currently are classified in a deterministic way as "safety related" or "non-safety related." Accordingly, a system can be placed into one of four RISC categories, depending on its deterministic class, and its safety significance.

(c) Systems that are classified as "safety significant" keep the current regulatory requirements, plus performance monitoring of their reliability. This is particularly relevant for safety-significant but non-

safety-related systems whose current requirements do not include the SFC, and so may not be commensurate with their safety significance.

(d) The single-failure criterion (SFC) applies to systems currently classified as safety related. Alternative 2 proposes that regulatory requirements, especially those involving the SFC, can be relaxed for safety-related systems designated as "low safety significant." The three sub-alternatives, 2a, 2b, and 2c, propose different levels of relaxation of regulatory requirements for such "low safety significant" systems, depending upon what is considered an adequate degree of risk-informing defense-in-depth.

Concepts (a) through (c) are illustrated by classifying each system in a selected NPP into one of the four RISC categories. Concept (d) is demonstrated by relaxing the SFC for safety-related low-safety-significant systems according to the options offered by 2a, 2b, and 2c.

Application

The "mechanics" of using Alternative 2 involve the following main steps:

- Select a plant.

  The NPP selected is a BWR/4 with a Mark I containment. These plants are the commonest type of BWR in the United States. Most have Mark I containments.

- Obtain RAWs (and FVs) of systems at the CDF level.

  Some current PRA computer codes may not be able to automatically calculate the probabilistic importance of a system, such as the system's "Risk Achievement Worth" (RAW). In this case, the system's probabilistic importance can be calculated manually by making the appropriate changes to the PRA model and then running the model. This is the approach used in these evaluations.

  The risk-importance of each system (safety-related and non-safety-related) is assessed individually by making the system unavailable in the Standardized Plant Analysis Risk (SPAR) model[7], and then re-quantifying the model to obtain an updated CDF. This new value then can be used to obtain a RAW of the system, and all systems then ranked according to their RAW (risk importance). Thus, this ranking will classify the plant's systems in terms of their risk significance. Deterministic considerations were not included in this classification. Accordingly, in this example, the safety significance of the systems is considered to be equal to their risk significance.

  The scheme using RAW proposed as part of 10 CFR 50.69 categorizes systems as "safety significant" or "low safety significant." Following this guideline, each system with a RAW greater than 2 is considered "safety significant"; all others are "low safety significant." In this example, the FV importance measure was not used to characterize safety significance, only the RAW.

  Table 4.4-7 presents the results of these evaluations. Starting from the left side, the first column is the system evaluated, except for the bottom row that is the plant's base case. The second column is the deterministic classification of the system, i.e., safety-related or not. The third column is the resulting point-estimate CDF per year after making each system unavailable. Finally, the fourth column is the

[7]The SPAR model is used for these evaluations because it is the PRA model that is currently available.

system's RAW, i.e., the point-estimate ratio of the sensitivity-case CDF to the base-case CDF for each system. The systems are sorted by descending RAW.

The "low-safety-significant" systems, i.e., those with a RAW less than 2, are shown between heavy lines in Table 4.4-7. They are the ECW, SLC, CS, and RBCCW.

The evaluations of CDF only include the mitigating contribution of the unavailability of a system. Accordingly, for a system whose loss causes an initiating event, only the mitigating contribution of this loss is included in the resulting CDF, and not that due to the initiating event. The loss of the Reactor Building Closed Cooling Water (RBCCW) is modeled as an initiating event by the SPAR model of the BWR plant. Therefore, the safety significance of the RBCCW may be higher than that shown in the table. Since the objective of the evaluations was to illustrate the concepts of Alternative 2, investigation of the RBCCW's safety significance was not pursued further.

- Obtain RAWs (and FVs) of systems at the LERF level.

  Since the purpose of this example is to illustrate the concepts and use of Alternative 2, the RAWs of systems at the LERF level were not obtained for this example at this time. As mentioned above, the FV importance measure is not used in this example.

- Classify the systems in RISC categories using RAWs at both levels.

  Since the RAWs of systems were calculated only at the CDF level, the systems are classified according to them in this example. Following the categorization of systems proposed by Alternative 2, discussed above, and the results in Table 4.4-7, the systems can be designated as in Table 4.4-8.

- Identify systems in category RISC-3 as candidates for relaxing the regulatory requirements.

  The RISC-3 systems, ECW, SLC, CS, and RBCCW, are the candidates for relaxing regulatory requirements.

- For each system in category RISC-3, and for the purpose of the calculations, eliminate the redundancy, and make a single-train system.

  This step is carried out by modifying the SPAR model (or the available PRA model) of the BWR plant. The ECW has one pump that supplies cooling water to the diesels and room coolers in the event of loss of ESW. It was made unavailable. The SLC has two pumps; one was made unavailable. The CS has two loops, each with two pumps. One loop was considered unavailable. The RBCCW has two pumps and two heat exchangers; one of each was considered unavailable.

- Evaluate the model containing the single-train RISC-3 systems to obtain the cumulative CDF and LERF. Obtain the cumulative CDF and LERF.

  Cumulative CDF and LERF means that they include the effect of the changes in all RISC-3 systems. Carrying out the evaluations after removing the redundancy for the RISC-3 systems yields somewhat conservative results for sub-alternatives 2b and 2c. As a first screening to identify candidates for relaxing the regulatory requirements, this evaluation is adequate. If it indicates that relaxation cannot be obtained by sub-alternatives 2b or 2c, more detailed evaluations can be undertaken.

Table 4.4-7 RAW Evaluations for Alternative 2 for a BWR Plant

System	Safety-related?	Pt. Est. CDF /yr	RAW
DC Power	Yes	2.1e+00	178260.87
AC Power	Yes	7.8e-01	68086.96
Control Rod Drive Hydraulic System (CRD)	Yes	5.3e-01	45691.49
Residual Heat Removal (RHR)	Yes	7.8e-03	680.78
High Pressure Service Water (HPSW)	Yes	5.6e-03	488.70
Safety Relief Valves/Automatic Depressurization System (SRVs/ADS)	Yes	5.2e-03	454.78
Emergency Diesel Generators (EDGs) (see note 1)	Yes	3.0e-03	263.48
Power Conversion System (feedwater cycle)	No	2.1e-03	184.42
Emergency Service Water (ESW)	Yes	4.1e-04	35.48
Containment Venting (CV)	Yes	9.3e-05	8.09
Reactor Core Isolation Cooling (RCIC)	Yes	4.0e-05	3.43
High Pressure Coolant Injection (HPCI)	Yes	3.7e-05	3.23
Turbine Building Closed Cooling Water (TBCCW)	No	2.7e-05	2.33
Emergency Cooling Water (ECW)	Yes	2.3e-05	1.96
Standby Liquid Control (SLC)	Yes	1.5e-05	1.33
Core Spray (CS)	Yes	1.2e-05	1.03
Reactor Building Closed Cooling Water (RBCCW)	Yes	1.2e-05	1.00
Base case	Not applicable	1.2e-05	1.00

1. When making the Emergency Diesel Generators (EDGs) unavailable, it was noted that the SPAR model of the BWR plant includes the recovery of AC power after a station blackout as the combination of two events: recovery of offsite power, and the operator setting up an additional offsite electrical power source. These two recovery actions are treated by the SPAR model as independent events, and the resulting probability of failing to recover AC power appears to be lower than the corresponding generic values. For example, the SPAR model's probabilities of failure to recover offsite power in 2 hours and failure to set up an additional offsite electrical power source in 2 hours are 6.4E-02 and 1.0e-01, respectively. Using these values, the SPAR model obtains a probability of failure to recover offsite power in 2 hours equal to 6.4e-03. To obtain a probability of failure to recover AC power considered more consistent with the generic values, no credit was given to setting up the offsite power source. Without it, the total probability of failure to recover offsite power in 2 hours is equal to 6.4e-02. By making this change in the SPAR model, the safety significance of the EDGs is more realistic. This change in the SPAR model was only applied in calculating the CDF when the EDGs are unavailable; all other evaluations used the base-case SPAR model with respect to the model of recovery of AC power. Using this base-case SPAR model is not expected to change the insights obtained from the evaluations.

Table 4.4-8 Classification of the BWR Plant's Systems

¹ Risk-informed ¸	¹ Deterministic ¸	
	1 RISC-1 Systems (Safety-related and Safety Significant): DC Power, AC Power, CRD, RHR, HPSW, SRVs/ADS, EDGs, ESW, RCIC, CV, HPCI	2 RISC-2 Systems (Non-safety-related and Safety Significant): Power Conversion System, TBCCW
	3 RISC-3 Systems (Safety-related and Low Safety Significant): ECW, SLC, CS, RBCCW	4 RISC-4 Systems (Non-safety-related and Low Safety Significant): None identified.

This plant's baseline CDF is 1.2E-5/yr. The cumulative CDF is 2.3E-5/yr, given that the redundancy was eliminated for each system in category RISC-3, and corresponds to a CDF of 1.2E-5/yr. This baseline CDF and CDF are in the border between Regions II and III in the acceptance guidelines for CDF of RG 1.174. Region II allows small changes to the plant, so the relaxation of regulatory requirements for RISC-3 systems appears permissible, as proposed by sub-alternatives 2a, 2b, and 2c.

The contribution to the cumulative CDF for all RISC-3 systems is dominated by the change in the ECW system. If the CDF for all RISC-3 systems is not considered acceptable, then a change for the remaining RISC-3 systems could be considered. When a "single-train" system is modeled for SLC, CS, and RBCCW, the resulting cumulative CDF is 1.2E-5/yr, corresponding to a CDF of 4.1E-7/yr. This increase in CDF is negligible so the relaxation of regulatory requirements for these RISC-3 systems seems allowable, as proposed by sub-alternatives 2a, 2b, and 2c. The licensee's relief would come from this relaxation.

Since the purpose of this example is to illustrate the concepts and use of Alternative 2, the cumulative LERF and the LERF were not obtained for this example.

- The licensee would carry out performance monitoring of system reliability for the systems identified in categories RISC-1 and RISC-2 because they are safety significant.

Table 4.4-8 lists the RISC-1 and RISC-2 systems. The licensee would carry out performance monitoring of their reliability. Monitoring can build upon, and be consistent with, current indicators such as the MSPIs. This activity is not illustrated by this example.

Results

Potential for Reduction in Unnecessary Requirements or Improvements to Safety

According to the results presented in the previous subsection, "Application," Alternative 2 offers both potential benefits, i.e., improvement to safety, and reduction in unnecessary requirements. The former consists of classifying the Power Conversion System and the TBCCW as RISC-2 systems because the reliability of these non-safety-related but safety significant systems should be monitored and maintained. Assuming that the CDF of 4.1E-7/yr (for SLC, CS, and RBCCW) is acceptable, each sub-alternative offers a different reduction in unnecessary requirements. Alternative 2a proposes removing from service one pump train of SLC, two pump trains of CS, and one pump train and one heat exchanger of RBCCW. Alternative

2b proposes reclassifying them all as non-safety-related. Alternative 2c proposes that all trains would remain operational and classified as safety-related. The regulatory requirements for one of them remain the same; operational flexibility can be provided for one pump train of SLC, two pump trains of CS, and one pump train and one heat exchanger of RBCCW. The potential negative impact on safety of the changes proposed by each sub-alternative is considered negligible because the CDF of 4.1E-7/yr is negligible.

Major Pros and Cons

(a) Alternative 2 provides a framework for the NRC and licensee indicating the importance of systems to safety. In general, classifying systems helps assigning them regulatory requirements according to their safety significance. In this way, Alternative 2 relates the reliability of a system with its safety significance that, in turn, is related to the plant's safety. This example illustrates this benefit by classifying each system in the selected NPP into one of four RISC categories.

(b) Ensuring Plant Safety - The way in which the example illustrates this benefit is discussed above under "Potential for Reduction in Unnecessary Requirements or Improvements to Safety." A potential option for the regulatory treatment of RISC-2 systems, not included in the current version of this alternative, is including other requirements that are applied to safety systems.

©) Efficiency of Regulatory Oversight - Alternative 2 allows some reduction of regulatory burden. Specifically, it lowers the regulatory requirements for RISC-3 systems, i.e., systems that are safety-related but that are of low safety significance, a change that would result in efficient regulatory activity. How the example illustrates this benefit is discussed above under "Potential for Reduction in Unnecessary Requirements or Improvements to Safety."

In addition, Alternative 2 addresses all seven desired attributes for replacing the current SFC, so it fulfills the requirements for a risk-informed alternative. Attribute 1 - Provides Functional Reliability: This advantage is illustrated by classifying each system in a selected NPP into one of four RISC categories because this classification includes the reliability of each system. Attribute 2 - Defense in Depth: Risk-informing the DiD is illustrated by Figure 4.4-1, "Illustration of Defense in Depth Aspect of Alternative 2." Attribute 3 - Risk Inform Consideration of SFC in Safety Analysis: Due to the limited scope of the example, this advantage was not illustrated. Attribute 4 - Performance-Based Regulatory Approach: This benefit is highlighted by requiring performance monitoring of system reliability for the systems that are safety significant (RISC-1 and RISC-2) at the selected NPP. Attribute 5 - Amenable to Efficient Implementation: Alternative 2 is considered amenable to efficient implementation because it employs concepts used in other risk-informed initiatives by the NRC. Attribute 6 - Coherence: This advantage is attained by classifying each system in the selected NPP into one of four RISC categories because this classification is consistent with that of 10 CFR 50.69. Attribute 7 - Security: The proposed changes in the selected plant must be reviewed to afford an acceptable degree of confidence that the "built-in capability" of the plant to resist security threats is not degraded. This review is outside the scope of this example.

Insights from Applying the Example

The BWR plant selected for this example illustrates the concepts and benefits of Alternative 2. While this plant is representative of many BWRs in the country, it was selected randomly. The benefits of Alternative 2 are expected to be applicable to any NPP.

4.5 Alternative 3 - Generalize and Enhance the SFC

4.5.1 Background

As discussed earlier, the SFC is a surrogate for a high-level objective relating to safety, and has been used in this way for decades. Surrogates are employed when it is impractical to directly model performance measures that accurately reflect the degree of attainment of the particular objective. In recent decades, improvements were made in the ability to model the risk posed to the public by commercial plants, and it is now possible to improve on the **SFC**. However, risk models are not perfect, and so it is appropriate to consider an alternative that continues to supplement risk models with the kind of structuralist guidance that the SFC exemplifies. See, for example, discussions of "risk-informed" in RG 1.174 [USNRC, 2002d]. (For a discussion of "structuralist" and "rationalist," see [Powers, 1999].)

After WASH-1400 [USNRC, 1975], it was realized that the relative dominance of transients and small breaks in PWR CDF was due, in part, to the circumstance that the functional unreliability of plant's response to those challenges was not commensurable with their frequency. After TMI [USNRC, 1979], the unreliability of AFWS systems was examined at a high level, and the results were presented in NUREG-0611 [USNRC, 1980a] (for Westinghouse plants) and NUREG – 0635 [USNRC, 1980b] (for Combustion Engineering plants). Those NUREGs did not systematically develop fault trees for each plant, but some attempt was made to relate the essential features of a system to a quantitative functional-unreliability metric. Based on the resulting insights, a requirement was promulgated [USNRC, 1981b] for plants to submit studies establishing that AFWS unreliability was "in the range of 10^{-4} to 10^{-5} per demand," using methods and data from these NUREGs that supplied numbers for demand-failure probabilities and maintenance unavailabilities. For this requirement, it also was possible to credit "...other reliable methods of cooling the reactor core during abnormal conditions."

NUREG-0611 and NUREG-0635, considered three challenges to AFWS: loss of main feedwater (LMFW), loss of offsite power (LOOP), and loss of all AC (LOAC, now called station blackout, or "SBO"). It showed that a plant with two AFW trains generally would estimate a functional unreliability around 10^{-4} per demand, conditional on LOOP. In practice, staff reviewers used the estimate conditional on LOOP for comparison with the target range. Therefore, two-train plants needed more redundancy to satisfy the requirement's intent. Accordingly, some plants arranged to supply emergency AC power to startup pumps, effectively making their AFWSs three-train systems conditional on LOOP. Others went back to the "other reliable methods" language, and invoked credit for bleed and feed.

Observations

- The requirement was described as an AFWS requirement, but implemented to include primary bleed and feed. Thus, it addressed the safety function (post-trip removal of decay heat from a PWR RCS) rather than the specific system. Since failure of this front-line safety function goes to core damage, this form of the requirement links a functional unreliability directly to a conditional core-damage requirement. This functional level of specificity worked well; specifying a system-level allocation instead would have created problems for two-train plants that were able to satisfy the target, but not with AFWS alone.

- This requirement did not supplant any prescriptive requirements, either in the design or in implementation; it overlaid the existing ones. Its purpose was to bring functional unreliability in line

with challenge frequency for an important safety function, a job that the SFC had not done completely. Any possible shortcomings in implementation were correspondingly less serious than they would be if existing requirements had been *replaced by* this unreliability requirement.

- The AFW unreliability requirement did not address common-cause failure (apparently, nor did the NUREGs cited above). Thus, this evaluation did not penalize AFWS systems comprising only pumps of a single type. Single phenomena (e.g., "steam binding") were not analyzed.

- Support systems were not analyzed in much detail. The evaluations reflected the dependence of motor-driven pumps on emergency AC, but auxiliary cooling systems, DC, and so on were not thoroughly analyzed.

- No particular requirements were placed on T/H analysis to support credit taken for any alternative method of core cooling. Some plants required flow to two SGs, some only one. Bleed and feed calculations typically were not submitted. The need for, or credit for, steam generator depressurization to help bleed and feed were not considered in these submittals.

- The notion of "success" was not always made clear. For example, some defined AFWS success in terms of preventing core damage; on the other hand, a delay in the AFWS response to the point where a PORV opened (and perhaps stayed open) might not qualify as AFWS "success" in the sense of the requirement's intent. To see why this might be considered an issue, note that both the TMI-2 event of 1979 [USNRC, 1979Y] and the Davis-Besse event of 1985 [USNRC, 1985Y] represent AFWS "success," in that both TMI's EFW and Davis-Besse's AFWS actuated in time to prevent core damage. TMI-2's core damage was not due to AFW failure (EFW, in their case).

- This requirement was explicitly implemented only as a licensing evaluation of design capability. At that time, there was no monitoring to see that the numbers used in the analysis were satisfied. It is impractical to verify, by counting complete functional failures, that functional unreliability is currently in the range of 10^{-4} to 10^{-5}, but train-level monitoring could have been carried out (as it is now under the ROP). This requirement, implemented at the licensing evaluation stage, caused many licensees to upgrade the capability of their startup pumps, or contemplate more seriously the prospect of going to bleed and feed.

- Since the numbers used in the evaluation were based, to some extent, on operating experience acquired under the prescriptive requirements of the time, ongoing satisfaction of them afforded some evidence that the desired low level of functional unreliability was being approached. In other words, if the previous conditions continued to hold (compliance with tech specs, IST, QA, and so on), there would be grounds for believing that AFWS unreliability would remain low. Hence, the already existing prescriptive requirements (proactive measures such as IST) ensure the establishment of proactive measures, while the existing oversight process, eventually supplemented by the maintenance rule, carried out the monitoring portions of the implementation.

The purpose of Alternative 3 is not to propose new requirements overlaying the existing SFC, in the same sense that the AFW requirement overlaid previously existing ones. Rather, the point is to *replace* old requirements with new ones, or alter existing requirements so that they achieve the objectives more effectively and efficiently. The above observations suggest the following.

- Since the intent is to replace existing requirements, rather than supplement them, the new requirements must be complete so that no gaps are created by eliminating the old ones.

- The decision in the TMI action plan to go beyond the SFC for certain initiating events illustrates the desirability of tailoring the mitigating capability to the challenge frequency. Such an approach might lead to a balanced risk profile: that is, no single family of accident sequences dominates risk. This point is discussed in the Framework document [King *et al.*, 2000].

- It should be possible to determine, through combining inspections, performance monitoring, and analysis, what level of safety is being accomplished in practice.

- Meaning must be given to the concept of "noncompliance" with requirements that set unreliability targets. This is a generic difficulty for performance-based requirements. Some concept should be formulated of the licensees' and NRC staff's response to such "noncompliance." Alternatively, some paradigm other than "compliance" could be articulated, along with whatever form the response of the licensee and the NRC staff to performance issues might take.

4.5.2 Alternative Discussion

4.5.2.1 Risk-Informed Approach

This alternative proposes to develop and apply a blend of

1. preferred levels of redundancy and diversity for key safety functions,

and,

2. quantitative targets on unreliability, applied at two levels:

    (a) the level of CDF, LERF, and

    (b) the level of specified safety functions (such as reactor shutdown, post-trip DHR), specified for categories of challenges (frequent, infrequent, and rare initiators), such that the unreliability targets for each combination of function/initiator are commensurate with initiator frequency.

This alternative approach generalizes the SFC by considering different levels of redundancy, and blends it with a generalization of the post-TMI action plan on AFWS unreliability. This alternative proposes to address more functions; the redundancy requirement is varied according to the initiating-event frequency, and the redundancy requirement is supplemented with diversity requirements. For some initiator/function combinations, this development would be roughly equivalent to the current SFC; but, for others, it would be less stringent than the SFC, and for still others, would be more stringent than the SFC.

Within this approach, the functional targets must also be addressed, and, in some cases, the functionality credited to make the case must incorporate functionally diverse means, as well as redundancy. In these respects, this approach addresses some aspects of defense-in-depth: high-level targets are supplemented with function-level targets, and redundancy and diversity are applied in a graded fashion.

Table 4.5-1 summarizes and compares Alternative 3 at a high level to current practice. As shown in the earlier discussion, the SFC does not act by itself: there is significantly more to regulation than simply requiring single-failure-proof redundancy, and Alternative 3 seeks also to address some of these other elements. Table 4.5-1 lists some of them, and their analogs in Alternative 3. To be coherent, Alternative 3 conceptually includes and applies these other elements, together with redundancy targets, in a graded fashion to initiators according to their frequency.

Table 4.5-1 High-Level Comparison of Current Practice to Alternative 3

Area	Current Practice	Alternative 3
Top-level Objectives	Health & Safety of the Public, Environmental Protection (presumptively assured by complying with prescriptive requirements)	Top-level Risk Metrics: CDF, LERF
Subsidiary Objectives	AFWS Unreliability target. Implicit objectives to address SBO, ATWS	Functional Unreliability Targets for Key Safety Functions, graded to challenge frequency
Scope of Challenges to Mitigating Systems	SAR Initiating Events together with postulated concurrent failures (such as LOOP), and using nonmechanistic challenges as surrogates for real challenges (e.g., to containment function)	PRA initiating events and functional challenges
Demonstration of Ability of Mitigating Systems to Meet Challenges with Margin	Accident analysis, conservative assumptions, functional performance criteria, all resulting in significant margins for those success paths addressed in accident analysis	Show some margin for PRA success paths: Licensing quality analysis of credited success paths, no grossly non-mechanistic assumptions, margins adequate to support PRA credit for success paths. Variations of this alternative consider modifying DBA analysis.
Demonstration of Low Unreliability of Mitigating Systems	Credited complement of SSCs must tolerate single failure and still mitigate successfully (N+1). AFWS Unreliability Studies. Other requirements (ATWS rule, ...).	Graded redundancy requirements. Key safety functions should meet unreliability targets. Explicit redundancy and diversity requirements, graded to frequency of challenge and consequences of failure
Uncertainty/Defense-in-Depth	"N+1" redundancy; Margin; Challenges specified for certain functions (such as containment) to assure balance between prevention and mitigation	DID addressed through explicit redundancy and diversity requirements at the functional level to preclude excessive reliance on particular elements of licensing basis (CCF to be addressed in demonstration of low unreliability).
Character of Licensing Finding	Adequate protection follows from high level of system capability established in accident analysis; DID principles are satisfied for SAR events	Top-level metrics are addressed with high assurance, because lower-level metrics are satisfied, no single family of sequences is dominant, DID principles are satisfied from a PRA point of view

Area	Current Practice	Alternative 3
Implementation	SSCs credited receive special treatment, and QA, IST, ISI, tech specs requirements	{"Current"} plus {implementation measures needed to show allocated targets are satisfied} less {implementation measures NOT needed to show targets are satisfied}

The details of Alternative 3 would need to be developed for key safety functions for different plant types. The AFWS requirement was promulgated generically for PWRs; this suggests that high-level broadly applicable functional targets could be developed. However, even when developing guidance for PWRs, it would be desirable to consider differences between vendors. Table 4.5-2 illustrates the nature and scope of this development, which, for a single safety function, summarizes key elements of a possible evolution based on initiating event categories used in King *et al.*[2000]. Numerous variations on this basic idea are possible: the unreliability numbers could be varied, as could the list of functions, and the redundancy and diversity requirements.

Table 4.5-2 Example of Functional Unreliability and Redundancy Requirements

Example of Functional Unreliability and Redundancy Requirements[1]			
Post-Trip Decay Heat Removal (For PWRs: Secondary Side Cooling + Bleed and Feed)			
	Frequent Initiators	**Infrequent Initiators**	**Rare Initiators**
Functional Unreliability Criteria	1E-4[2]	1E-2[2]	5E-2[2]
Level of Redundancy	Withstand two failures[3]	Withstand a single failure[3]	Redundancy is not required
Diversity Required	Yes[4]	Yes[4]	No

Notes:
1. This table is only an example.
2. Implementing guidance would need to be developed, establishing the evaluation basis for demonstrating satisfaction of the targets.
3. As an alternative to incorporating full redundancy in the licensing basis, it would be acceptable to identify bottlenecks (areas having less redundancy than desired) and enhancing their treatment to assure exceptional levels of prevention of functional failure.
4. Regulatory guidance would need to be developed to specify the meaning of "diversity" before implementing this requirement.

The phrase "functional unreliability" is being used to mean "the probability that a safety function will fail when demanded," with due consideration of such factors as

- train unavailability due to test or maintenance,
- human error pre- or post-challenge,
- common-cause failure,
- margins,

- physical phenomena that defeat the function even when all hardware is nominally "good" and no operational human errors occur, including things like steam binding and sump blockage.

The formulation of Table 4.5-2 in terms of three categories of initiating events (as opposed to two or four categories) is offered as an illustration (based, in part, on the Framework document). The SFC currently is applied to events in all three categories, but, over time, was supplemented with guidance on specific functions responding to specific more-frequent initiating events. The recommendation to withstand two failures for frequent challenges (instead of only one) is derived from the same considerations that drove the formulation of the TMI action plan in regards to AFWS: reviewing certain functions against the SFC alone does not drive risk low enough. Forgoing redundancy requirements entirely in favor of pure unreliability requirements is very difficult to implement. Some difficulties are illustrated in the example in Section 4.5.5.

Given a complete development along the lines of Table 4.5-2, a licensee establishing this alternative would proceed analogously to implementing the AFWS requirement, with certain modifications. Each function would need to be analyzed using the PRA model to show that the function-level unreliability target is met. But, instead of assuming the component unreliability numbers from NUREG-0611 or NUREG-0635, licensees would choose target values at lower levels (typically at the train level), and demonstrate that they satisfy both the functional and the top-level objectives.[8] Thus, licensees would need to address the functional targets, but would have flexibility in doing so. Regulatory guidance on this demonstration would need to set up acceptable ways to address common-cause failure. In addition, the licensee must respond to the redundancy and diversity targets, either by showing that they are satisfied, or by identifying where they are not, and proposing enhanced treatment for preventing failures where redundancy and diversity fall short of their targets.

The scope of regulatory interest would be defined by the success paths[9] invoked by the licensee to satisfy the above targets. The treatment of SSCs in these success paths would be determined by the stringency of the performance targets that the licensees assign to them; the assignment process would be carried out in light of this consideration. Regulatory oversight would also be informed by the assignment of these performance targets.

4.5.2.2 Implementation Approach

Alternative 3 proposes the development of target levels of performance. To complete the specification of the alternative, it is necessary to address implementation, or decide how to make those targets "come true" in practice. NUREG/BR-0303 [USNRC, 2002c] has substantial guidance in this area.

For essentially any regulatory alternative, after completing the initial licensing changes, a body of conditions (design features and various proactive measures, such as process requirements, license conditions, technical

[8]Selection of train-level targets, and showing that these combine to satisfy higher-level objectives, is not simple. Guidance will be needed to achieve the right balance between simplicity and precision.

[9]A "success path," is a complement of SSCs whose operation successfully mitigates a given initiating event. For a fluid system, for example, a success path typically includes a suction source, components in the flow paths, one or more pumps, support systems, instrumentation, and so on. In the context of a PRA, "success path" refers to a conjunction of basic events whose occurrence (in success space) accomplishes the applicable mission's success criterion.

specifications) has to be identified for which failure to satisfy can lead to actions up to, and including, plant shutdown.

What form can these conditions take in practice, if the requirements were functional unreliability specifications? Recall that the TMI action plan discussed above (allocating 10^{-4} to 10^{-5} per demand) was applied, in effect, only in evaluating the design, and was based on *given* unreliability data; thereafter, licensees simply complied with already existing prescriptive programmatic requirements. One practical advantage of the latter is that noncompliance with them is readily determined. It is much more difficult to assess "noncompliance" with functional unreliability targets. To make functional unreliability a practical part of oversight, a mapping between functional unreliability and lower level observables must be established, such as train-level unreliability, the physical state of a system, and performance trends.

Within this alternative, the licensee would need to do the following:

1. Beginning with the safety-function targets on functional unreliability, redundancy, and diversity, assign performance targets at a level at which achievement could meaningfully be assessed (e.g., the train level). First, choose SSCs to credit in satisfying the functional redundancy and diversity requirements. Then, assign unreliability and unavailability targets to this complement of SSCs, such that the top-level objectives (CDF, LERF) and functional reliability objectives are satisfied. Provide special discussions of unreliability targets assigned to areas where redundancy and diversity targets are not met (e.g., very high reliability of major suction sources).

2. Show, by analyses submitted to the NRC's staff, that nominal satisfaction of these targets meets the top-level objectives. The following elements are to be considered:

    - PRA quality issues consistent with the NRC's phased approach
    - Regulatory guidance limiting credit for non-diverse systems, human actions
    - Process requirements on assessing CCF, the potential for single phenomena compromising system function, and the like.

For the AFWS requirement, this was done by a simple, limited-scope system fault tree analysis, using numbers provided in NUREG documents. Here, a much more comprehensive evaluation is contemplated. Another key difference is that the unreliability numbers that the licensees choose to demonstrate performance are ultimately codified as performance targets. The analysis discussed here is one of performance targets, not of the supposed current state of the plant. Target unreliability values should be greater than (i.e., worse than) "best estimate" performance, or else the licensee is set up for failure during a later phase. There is an argument for requiring specification of an uncertainty distribution (or perhaps a "variability" distribution), against some upper percentile of which performance would be measured and trended. This level of detail is beyond the scope of the present document.

The PRA demonstration contemplated in this alternative entails licensing-quality validation of the success paths credited in the PRA, a departure from current practice. The intent is to assure that PRA success paths have sufficient margin to justify the customary neglect of functional failure induced by T/H variability. Improved guidance is needed on an evaluation methodology for T/H analysis of these success paths.

3. Commit to a body of proactive measures that can be inspected (e.g., IST) whose implementation would tend to drive performance to the levels needed.

4. Commit to data reporting to support both the licensee's and the NRC staff's monitoring of functional unreliability performance.

5. Commit to corrective action measures, such as the maintenance rule, thereby providing a first line of defense against downward-trending performance.

This blend of proactive inspections, programmatic provisions, and objective performance indicators needs to be formulated so as to assure good performance and clearly indicate when regulatory intervention is warranted. Within current licensing practice, declining reliability performance does not violate regulatory requirements, but under the Reactor Oversight Process, it increases regulatory attention. This alternative's use of unreliability targets goes beyond the TMI action plan, in that the latter was applied only as a design-review tool, while the present intention is to also confirm satisfactory performance during operations. Correspondingly, a graded regulatory response to indications of declining reliability must be formulated as part of this alternative, starting with the Reactor Oversight Process.

Specifics of Initial Licensing Changes

Alternative 3 has some elements in common with the AFWS unreliability requirement: it is formulated at the functional level and articulates an unreliability target that would drive a class of accident sequences to a low frequency commensurate with QHOs. However, there are key differences. One relates to so-called "PRA quality." The demonstrations contemplated here have much higher needs for "PRA quality" than those of the AFWS study, especially if they are to address CCF and "phenomena" such as steam binding and sump blockage. This follows because the AFWS evaluation was an *overlay* onto existing requirements, whereas the present requirements would *replace* some existing ones. Phenomena of this kind are not well addressed in classic PRA; therefore, there is an argument for imposing additional process requirements[10] that would mandate the licensee's attention to things like phenomenon -related failure mechanisms, perhaps including CCF mechanisms. Alternatively, the NRC's staff could develop prescriptive guidance on these evaluations.

However, Alternative 3 does not consider using the PRA as a licensing document. Rather, the licensing basis would incorporate elements of the PRA as a technical basis, and elements of the PRA would be incorporated, but the PRA as an integrated document would not be part of the licensing basis. Consistent with the NRC's existing and emergent guidance, PRA quality under Alternative 3 would be driven by the nature of the findings based on the PRA. Quality for this alternative would need to be defined consistent with the staff's guidance presently under development as part of the Commission's Phased Approach to PRA Quality.

Under Alternative 3, the following would be developed based on the PRA. The licensing basis would identify a "prevention set" of SSCs, and make certain representations about the level of safety accomplished by satisfactory performance of the elements of that set. The "prevention set" is a complement of SSCs chosen to satisfy the alternative's targets on CDF, LERF, functional unreliability, redundancy, and diversity. In today's licensing basis, the prevention set is the complement of SSCs that are classified as safety-class, plus

[10] Process requirements differ from prescriptive requirements (which tell licensees exactly what to do) and performance-based requirements (which tell them what outcome to try to achieve). A process-based requirement tells the licensees to set up a process for analyzing or monitoring some issue. The maintenance rule is a process requirement; it does not tell the licensees what unreliability to achieve, nor how to achieve low unreliability, but rather tells them to impose upon themselves a performance-based process. NRC inspectors judge a licensee's process by its own qualities, not by its success. The ROP, to some extent, implicitly judges a licensee's implementation of the maintenance rule by its success.

certain other SSCs needed to meet special regulatory requirements (the ATWS rule, for example). Under today's regulatory approach, if it is found after licensing that the licensing-basis prevention set is not single-failure-proof for a design-basis event because of an error or a change in the plant, the regulatory responses are known. Analogously, under Alternative 3, a claim would be made for ensuring the prevention set satisfies Alternative 3's targets, and the regulatory response to a failure to meet these claims would be similarly predefined. The role of the PRA model is to affirm that the complement of success paths comprised in the prevention set actually satisfies the targets, based on the licensee's allocation of performance over elements of this set.

Therefore, the main "PRA quality" needs are that the logic model is complete, that dependencies are reflected faithfully, that initiating events are identified and binned appropriately, and so on. As in today's licensing basis, minor numerical errors would not undermine these claims, but instances of compromised redundancy would do so, while loss of margin for credited success paths might do so.

Design-Basis Analysis in Alternative 3

A spectrum of possible approaches to design-basis analysis can be envisioned for Alternative 3. An essential requirement here is to show that all credited success paths have margin; the question is whether additional engineering analysis is necessary or desirable.

At one end of the spectrum, DBA analysis might be eliminated entirely, and instead, current "PRA quality" guidance accepted for analyzing the mission success criteria of PRA success paths. However, the current PRA quality guidance is arguably not sufficient to justify relying on it for licensing decisions, without the underpinning of today's DBA analysis. Eliminating current DBA analysis in favor of current PRA analysis of success criteria would relinquish margin in an uncontrolled way.

At the other end of the spectrum, the DBA analysis could be left unchanged, and applied in conjunction with the requirements of Alternative 3 as a separate analysis. However, application of the SFC in DBA analysis would contradict Alternative 3's possible relaxation of the required single-failure assumption in analysis of mitigation of large LOCA, and possibly other severe initiating events.

One compromise would be to continue to require today's T/H evaluation methodology for the single success path required by Alternative 3 for sufficiently rare initiating events, but without the requirement to postulate an additional single failure. This would leave one success path having the same margin as before, instead of redundant success paths having that margin. Alternative 3's requirements on PRA success paths would assure margin for them as well, based on something like a best-estimate but licensing-quality T/H evaluation methodology.

Another approach would subsume all of today's DBA guidance into demonstrating an adequate margin in all credited success paths, as is intended in Alternative 3. Alternative 3's aim is to go beyond current PRA quality guidance on T/H: To require that credited success paths are shown to have sufficient margin so that the probability of functional failure due to its lack, conditional on hardware success (formerly called "T/H uncertainty"), is completely dominated by the probability of functional failure due to non-functioning hardware. This could be augmented by adding guidance to demonstrate functional performance for other postulated severe challenges, analogous to existing guidance in analyzing the containment's performance conditional on a hypothetical set of loads and in-containment source terms.

Depending on the provisions for the T/H analysis of credited success paths, some of these options could essentially be equivalent. Several explicitly address margin: they may enhance it for frequent initiators, while maintaining it for rare ones.

Continuing Programmatic Activities

A fundamental question in regulatory practice is the effect of certain engineering practices on performance (e.g., functional unreliability). Although there is broad consensus that some existing proactive measures promote reliability, it is difficult to say by how much. Judgment will be required to justify selecting certain proactive measures. A fundamental challenge of the Reactor Oversight Process's Significance Determination Process (PDP), for example, is to try to map perceived programmatic shortcomings into changes in risk. No generally accepted analysis explicitly demonstrates what numerical value of unreliability obtains under a given treatment regime of QA, maintenance, testing, environmental qualification, and so on. However, it is widely presumed that real correlations exist, and various data bases recommend imposing scale factors on nominal failure probabilities to get situation-specific failure probabilities.

Elements of today's proactive measures could continue to be applied. The benefits of doing so must be justified in terms of their real effect in achieving the allocated performance target. It would be desirable to be able to apply more (or less) stringent proactive measures to more (or less) ambitious unreliability goals in the spirit of existing work on "special treatment."

Monitoring Program

Alternative 3 establishes explicit targets for functional unreliability that can directly drive the formulation of the monitoring program. In many areas, performance will have substantial margin (in unreliability space) to these targets. The program can be formulated to gather and apply information to test *whether* the targets are being met, a much simpler task than explicitly re-quantifying current functional unreliability.

4.5.3 Evaluation

Pros and Cons

This alternative uses the strengths of both the structuralist and rationalist approaches to safety, while avoiding some of the weaknesses associated with relying entirely on one or the other. It would tend to drive the plant's risk profile towards desirable characteristics:

- the overall level of risk would be commensurable with the QHOs,
- the risk profile would be balanced in the sense that no single family of sequences would be dominant,
- vulnerabilities would be addressed, and,
- these outcomes would not be completely dependent upon traditional PRA "quality" issues.

The licensee's performance targets would directly inform the implementation measures, including regulatory oversight, and residual uncertainties would be partly addressed through the supplementary requirements on redundancy and diversity.

The main drawback to this alternative is that it would require a substantial rethinking and modification of the regulatory framework and the plant licensing basis on the part of both NRC and the licensee. However, much of the significant effort demanded could be harnessed to address many other regulatory issues

simultaneously and coherently. The drawback is not that the rewards would not justify the expenditure, but rather, that the undertaking would be a major one.

Table 4.5-3 summarizes the chief characteristics of this alternative.

Relationship to Other Activities

This alternative would go a long way towards bettering coherence. Numerous improvements in the regulatory process are underway, but their stepwise character creates issues of consistency and coordination. Reformulating the plant licensing basis would create an opportunity to address these other improvements in a unified fashion.

This alternative also is arguably a good way to go about licensing advanced plants, some aspects of which were not anticipated by current Part 50 requirements.

It would be reasonable to combine a version of this alternative with Alternative 1 (Section 4.3) because the present alternative changes the approach to DBA analysis by calling for more realistic T/H validation of a broader set of success paths.

Table 4.5-3 Alternative 3 Attributes

ALTERNATIVE 3 Generalize and Enhance the SFC	
Attribute 1: **Functional Reliability**	This alternative grades functional unreliability requirements according to the frequency of the initiator category, and additionally, applies redundancy and diversity criteria to provide added assurance of the actual realization of ambitious unreliability targets.
Attribute 2: **Defense-in-Depth**	Defense-in-depth is addressed in the following ways. • Criteria are applied at multiple levels, at the CDF/LERF level, and at the functional level. • The functional requirements are tailored so that no single category of sequences is risk-dominant. • Quantitative unreliability requirements are supplemented by redundancy and diversity requirements.
Attribute 3: **Risk-Inform Consideration of SFC in Safety Analysis**	All event tree paths credited as "success" in the licensing basis would be shown to succeed by licensing quality, but best-estimate, T/H analysis. This alternative would combine naturally with Alternative 1, described in 4.3.1. Variations of this alternative can be formulated: DBA analysis could be retained as is, supplanted by enhanced PRA success path analysis, or the DBA analysis requirements could be reformulated, based on reconsidered challenges to the plant's safety functions.
Attribute 4: **Performance Based Regulatory Approach**	Implementation would follow guidance in NUREG/BR-0303, and would be performance-based as appropriate.
Attribute 5: **Amenable to Efficient Implementation**	The licensing stage of this alternative would entail significant effort, culminating in a coherent licensing basis. Thereafter, this alternative would be amenable to efficient implementation.
Attribute 6: **Coherence**	This alternative would provide a basis for reconciling regulatory activities in different areas, and thereby promote coherence in regulating a given plant.
Attribute 7: **Security**	Like other alternatives proposed, this alternative satisfies this attribute because plant-specific changes would not be permitted to adversely impact security.

Impact on NRC and Industry

Potential Benefits to the Licensee:

Requirements on infrequently challenged functions could be reduced under this alternative. Substantial flexibility also is available to licensees in responding to the functional requirements contemplated in this alternative: licensees can choose what to credit, and, in areas where redundancy is sufficient, compensatory measures might be applied. This flexibility partially offsets the potential increases in requirements in some areas.

Where a substantial reliability margin exists and is credited, a basis is created for easier monitoring of targets and more flexibility in configuration-specific completion times for on-line maintenance. (This is clarified in the example treated in the next subsection.)

Potential Benefits to the NRC:

This approach has the potential to unify the NRC's treatment of functional requirements in diverse areas, including rationalizing flexible completion times for on-line maintenance, and allows for more fine-tuning to achieve a balanced risk profile in the operating fleet.

Effort Required:

As noted previously, this alternative would initially require significant effort from both the NRC and industry.

The NRC would be required to think through a spectrum of unreliability and redundancy requirements, and develop regulatory guidance spelling out the evaluation basis for licensees to follow, showing how the requirements are addressed. The licensees would need to pro-actively develop performance targets for SSCs credited in their licensing bases. Both would need to agree on a set of implementation measures to ensure that the targets are "coming true."

The benefits of the undertaking would extend beyond improving plant risk profiles and licensee flexibility: coherence could result from implementing this alternative. Much of this work could beneficially subsume certain other ongoing regulatory activities.

For example, the ROP might change. Presently, it uses as a baseline the current "point estimate" of CDF, and measures the significance of performance issues by estimating a change in CDF from that baseline. Instead, the ROP might judge performance issues by the plant's standing with respect to its own targets.

4.5.4 Summary

The SFC currently is applied to a very broad range of initiating events. In most areas, it is not supplemented by requirements on functional unreliability, though related characteristics are trended as part of the ROP and maintenance-rule-related activities. The present alternative proposes to replace the current implementation of the SFC with a blend of

- functional redundancy and diversity requirements,
- functional unreliability requirements,
- high-level quantitative requirements on CDF, LERF.

Areas where redundancy and diversity targets are not nominally fulfilled would be targets for enhanced attention by the licensee with the concomitant regulatory oversight.

Some precedent for an approach like this exists, and was discussed above.

As proposed, this alternative would use the plant PRAs in a slightly different way from most current risk-informed activities. Licensees would use them first to choose SSCs to be credited, assign a set of unreliability targets at the train level to form the basis for implementation, and then use the PRA again to show that these train-level unreliability targets satisfy the high-level requirements.

Both licensees and the NRC's staff would undertake a great deal of work in carrying out this alternative. However, it would generate a coherent regulatory framework, including a coherent approach to regulatory oversight.

Table 4.5-4, below, summarizes these characteristics.

Table 4.5-4 Alternative 3 Summary Description

ALTERNATIVE 3 **Alternative 3 Summary Description and Attribute Comparison** **Generalize and Enhance the SFC**	
Basic Motivating Factors for Alternative	Among other things, the SFC is a surrogate for functional reliability. In some areas, it does too much, and in other areas, too little. It might be improved by grading the application of unreliability requirements as follows: More stringent unreliability requirements for more frequent functional challenges; consider not only redundancy but also quantitative measures of unreliability, including CCF potential, and defense-in-depth (diversity). The process of allocating performance for determining SSC treatment can be carried out in light of the costs of implementing licensing-basis credit for features that are not presently safety-class.
Risk-Informing Approach	Establish the following: (1) requirements on functional redundancy and diversity, (2) top-level CDF and LERF targets, (3) lower-level functional unreliability targets pegged to the frequency of challenges (initiating events). The tests include guidance on redundancy, diversity, and CCF. Licensees determine which plant features to credit to address the targets, and how much credit they take for those features.
Implementation Approach	Initial Licensing Changes: This would confirm the feasibility of the proposed licensing basis: The success paths will succeed with margin, and that the assignment of performance credit to SSCs, operator actions, and maintenance actions is credible and implementable; and, it addresses the functional unreliability targets. The required treatment of SSCs is determined through identifying all elements of all credited success paths, and establishing that the proposed treatment conforms with the assigned unreliability performance. Where redundancy targets are not met, heightened treatment is assigned to elements performing those functions without benefit of the target redundancy.
	Continuing Programmatic Activities: Depending on the actual performance allocation, programmatic activities such as IST might need to be extended to systems newly credited in PRA success paths. A basis for such heightened treatment also would need to be addressed.
	Operations Monitoring: Monitoring would confirm that assigned performance targets are met.

Table 4.5-4 Alternative 3 Summary Description
(continued)

ALTERNATIVE 3 Alternative 3 Summary Description and Attribute Comparison Generalize and Enhance the SFC	
Potential Major Achievements	This would improve on the one-size-fits-all approach of the SFC, reducing requirements on infrequently challenged functions and increasing requirements on more frequently challenged ones. It would rationalize regulatory involvement in the plants' satisfaction of performance targets, and promote regulatory emphasis on areas of plant-specific relative weakness. This would engender a very substantial coherence of regulatory oversight of a given plant, and increased flexibility for the licensee in some areas.
Pros and Cons	The above benefits would require significant effort in reformulation of the plant's licensing basis and the regulatory oversight process.

4.5.5 Alternative 3 Example

Description

The present example illustrates the effects of establishing Alternative 3, mainly with reference to the safety function "short-term removal of decay heat given a loss of offsite power during full-power operation" in a PWR. This example is closely based on current regulatory practice, because, as discussed earlier and mentioned above, the TMI action plan for auxiliary feedwater systems already contains major portions of Alternative 3.

In general, the effect of Alternative 3 on burden is mixed: in some areas, it increases, while in others, it could potentially decrease. The present example illustrates the thought process on a function where it was found to be appropriate to go beyond the SFC. To see a case in which burden would largely decrease, the process should be applied to an infrequently challenged function for which burden now is significant. Moreover, the overall implications of the alternative can only be assessed realistically through a complete example, examining all safety functions.

Before the TMI action plan was imposed, the auxiliary feedwater system had to be single-failure-proof. Currently, there is no explicit requirement for added redundancy; practically, however, the TMI's reliability target effectively drove the plant's configuration either to three or more trains of secondary heat removal, or to supplementing single-failure-proof secondary heat removal with primary feed and bleed, thereby forcing functional unreliability to the "range of" 1E-4 to 1E-5 conditional on loss of offsite power (LOOP), based on the evaluation methodology applied in NUREG-0611 and NUREG-0635. Alternative 3 is a generalization of this approach, in that it

- integrates consideration of redundancy and functional reliability,
- considers more safety functions,
- includes more categories of challenges,
- covers more support systems, and

- considers prevention of a broader range of failure modes.

This alternative involves several major steps. The present example focuses on the steps that the licensee would take. The NRC's initial steps would include the following:

- Specifying targets on high-level metrics (CDF, LERF)
- Specifying safety functions to be addressed
- Specifying categories of initiating event frequencies for which safety functions must be addressed
- Specifying target levels of functional unreliability for the safety functions identified, for specific initiating event categories, including guidance on defining functional success
- Specifying target levels of redundancy and diversity
- Developing guidance on compensatory measures to be taken when target redundancy or diversity is not reached
- Formally declaring regulatory guidance on the evaluation bases recommended for licensee use, and promulgating standard review guidance for the staff to apply, addressing such matters as credit taken for compensatory measures applied in areas where redundancy is less than desired.

The above remain to be developed, except that parts are in place in the TMI action plan for AFWS reliability. The example presented below presumes that the steps identified above have been accomplished. The licensee is assumed to be addressing the following targets:

- Initiating Event Frequency Category: "Frequent" [> 1E-2 /yr (The example is done for LOOP, having a frequency of 0.03 /yr)]
- Redundancy: Withstand two failures; enhanced prevention of basic events in areas having less redundancy
- Functional Unreliability Target (Probability of failure of post-trip decay heat removal): < 1E-4
- Overall CDF Target: < 1E-4 /yr

Key Features

The mechanics of this alternative could be discussed at the design stage, when the plant's configuration is being decided. Instead, it will be illustrated assuming an existing plant. The decision being made is what capability the plant must invoke to satisfy the intent of the alternative, and how best for licensees and regulators to go about assuring that the implied levels of SSC and operator performance "come true." The question is not "what capability does the plant 'really' have?" but rather "what capability does the regulator need to be assured of?" The alternative intends that licensees propose a choice that satisfies the regulatory intent and is operationally and economically optimal.

The safety function treated in this illustration is post-trip removal of decay heat at a PWR for frequent initiating events.

- First, a high-level description will be provided of systems in a particular PWR that might provide the desired functional capability. The plant model used offers a representative range of possibilities.

- Next, options for satisfying the redundancy requirements for the sample plant will be considered. It is natural to do this before looking at the probabilities because this portion of the alternative resembles traditional licensing practice, except that the DFC ("Double Failure Criterion", i.e., withstand 2 failures)

replaces the SFC for frequent initiators, and systematic logic model analyses replace failure modes and effects analysis (FMEA). In reviewing redundancy from a risk-informed perspective, it can be seen how common-cause- and passive-failures can be addressed properly in a logic-model-based evaluation of effective redundancy. It can also be seen how options for satisfying one function for one initiating event category involve some of the same hardware satisfying another function in another initiating event category; thus, an integrated view of the whole problem (all functions, all challenges) is supported by systematically applying a comprehensive risk model, even before probabilities are considered explicitly.

- Once the set of candidate options has been culled by considering redundancy and diversity, the surviving ones are compared from the point of view of functional unreliability and top-level CDF targets.

- At this point, more than one way remains to satisfy the guidelines. The implications of performance of these options now are compared: what sort of performance commitments need the licensees make, and what are the implications for monitoring and inspection?

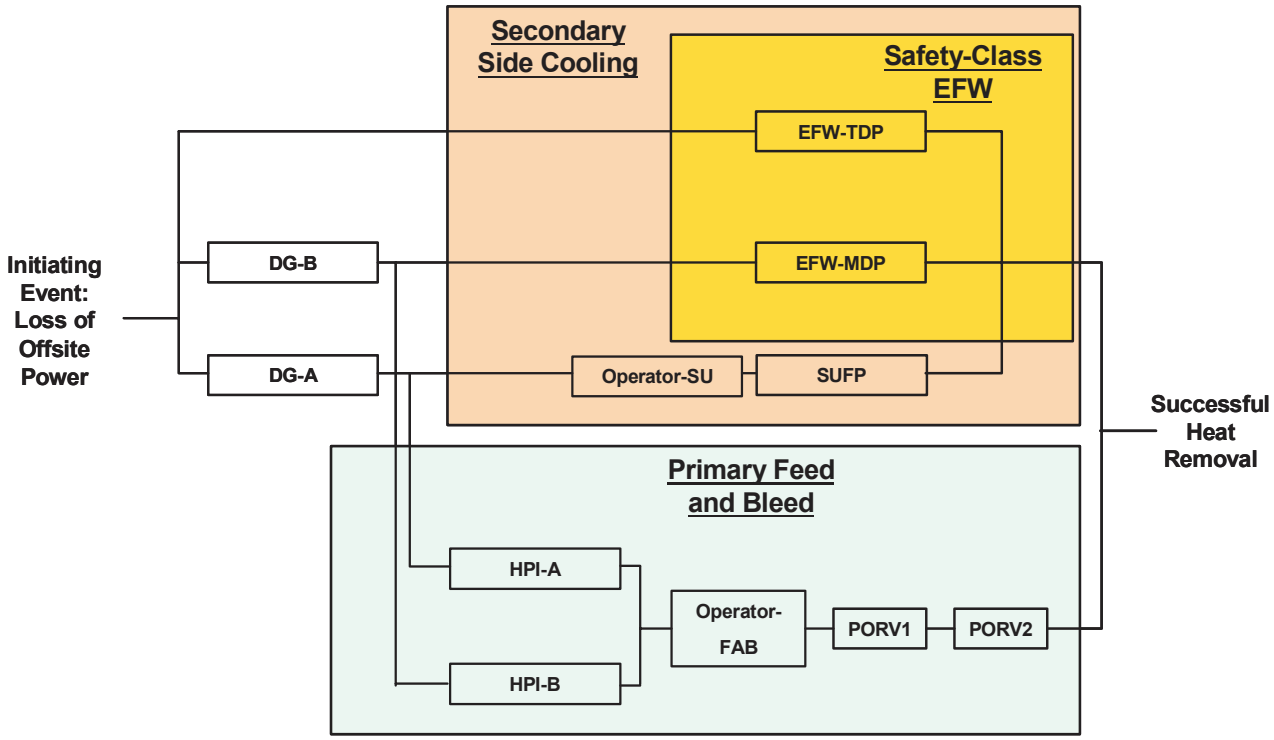
Application

At the example plant, the subject function (post-trip removal of decay heat) can be accomplished either by secondary heat removal using one train of emergency feedwater (EFW) or the startup feedwater pump (SUFP), or through primary feed and bleed (FAB) using at least one high-pressure injection (HPI) pump for "feed" and two pilot-operated relief valves (PORVs) for "bleed." During a loss of offsite power (the event

analyzed here), the SUFP requires an operator to align it to a bus receiving emergency power. FAB also must be initiated by an operator.

Figure 4.5-1 shows this capability conceptually. This figure is a highly simplified reliability block diagram, reflecting not the physical configuration but rather, the logical relationships between selected major components. Starting on the left, at the initiating event, any path across the diagram to the right ("Successful Heat Removal") corresponds to a way of achieving functional success. For example, after a loss of offsite power, success can be attained, for instance, with the turbine-driven pump (TDP); with diesel generator (DG) B and the motor-driven EFW pump (EFW-MDP); or with DGA, HPI-A, Operator initiation of Feed and Bleed, and success of both PORVs. This diagram illustrates certain points about redundancy and

Figure 4.5-1 Potential Redundancy and Diversity in Post-Trip Decay Heat Removal Resources: Example



Note: Many support systems not shown (DC, Service Water, Component Cooling Water, Room Cooling, ...)

diversity.

Given that only one of these pumps needs to succeed, it may at first appear that many combinations could satisfy the DFC. However, for many reasons, the practical possibilities are much more limited than that. Consider the following:

- Given a loss of offsite power, failure of two DGs leaves only the TDP. Therefore, because of station blackout (SBO), all solutions to "DFC given LOOP" must contain the TDP and both DGs.

- The need for both PORVs means that the effective redundancy of FAB by itself is 1-fold, not 2-fold. Therefore, even with credit for FAB, at least two of the secondary heat removal trains are needed, and to address a SBO, one of those two must be the TDP. One might resort to the "enhanced prevention" clause to argue that the effective redundancy of FAB is really twofold, since two pumps are available. But this would require invoking exceptional failure prevention both for the operator and for the PORVs (and, at some plants, for certain support systems). This possibility arguably strains credulity, and it is not considered further here.

At this stage, the reasonable minimal options satisfying the DFC are the following:

- All three trains of secondary cooling; OR
- The TDP AND one of the motor-driven trains of secondary cooling (either EFW-MDP or SUFP), AND FAB using at least the HPI pump on the AC division opposite the selected secondary feed pump (otherwise there would be a two-element cut set consisting of TDP and one DG, violating the DFC).

At plants unable to invoke a second MDP or a SUFP, this latter option is the only way to satisfy the DFC. Some existing ones fall into this category.

In addition, for the plant illustrated, there is a non-minimal option:

- All three trains of secondary cooling, and FAB using at least one HPI pump.

Finally, for comparison, the bare-EFW configuration is be discussed. There, credit is taken for the two-train EFW, but not for the SUFP and not for FAB. This two-train option satisfies the SFC, but not the DFC.

All of the options discussed in this particular example have some functional diversity, in the sense that both steam-driven and electric-motor-driven capabilities are invoked for this function. In the context of a different example (three TDPs, or a three-DG plant with three MDPs), a diversity goal would be seen to penalize a non-diverse AFW system, arguing for including FAB in the licensing basis. (Such an approach still would be vulnerable to SBO.) For purposes of this alternative, guidance on diversity remains to be developed.

For counting redundancy, the operator's actions needed to actuate SUFP and FAB are essentially equated to active failures. To evaluate functional unreliability and top-level metrics, the failure probability of these actions must be quantified, recognizing that the actions would be carried out in scenarios involving multiple failures. Failure of these actions can dominate the probabilities of SUFP failure and FAB failure. Taking credit for these actions will cause them to be addressed in the implementation phase, including reducing the potential for coupling between failures of these actions.

Many plants have more trains of secondary cooling and/or more trains of high-pressure injection able to play a role in FAB. Thus, while aspects of this configuration can be found in the operating fleet, no plant may have all of these characteristics. This example was been tailored to illustrate, in a simple way, the process of developing and comparing options for addressing the requirements developed in this alternative.

Bare EFW (No SUFP, no FAB)

Prevention of Low-Order Cut Sets

There are single-element cut sets corresponding to events such as common-cause failures of SG inlet check valves or CCF of all pumps. Such cut sets require clarification of what kind of event counts as a "failure"

in evaluating satisfaction of the DFC (or the SFC). In traditional licensing practice, such events do not count as single failures. Within the present alternative, they are identified through logic modeling and then assigned very low probability, based either on their inherent characteristics, the commitment to highly efficacious prevention, or some combination. The task in implementation is to assure that low probabilities are realized. For example, to address pump CCF, it may be argued that the pumps are essentially dissimilar. On the other hand, steam binding might cause all three to fail. In principle, largely successful prevention of CCF of these pumps appears to be achievable through the kinds of engineering practices already in place.

This illustrates a general property of failure-counting approaches: it is easy to postulate "events" that transcend redundancy, and that must be prevented to satisfy redundancy and defense-in-depth targets. Many such events will have very low probabilities for reasons that require no particular allocation of the licensee's resources (meteor strikes, extreme seismic events). Some events (CCF of similar check valves, failure of all suction sources, steam binding of all pumps) do require the licensee's attention in principle, but, in most cases, the activities in place (including treatment, testing, inspection, and response to initiating events) collectively provide the needed assurance and checks on performance. To keep such events from dominating functional unreliability, they need to be prevented at the E-5 level or better, and the programmatic activities intended to prevent them should be formulated with such an explicit goal.

In the bare-EFW option, failure of the two EFW pump trains fails the function. Therefore, the intent of the DFC cannot be satisfied with credit for EFW alone. For the sake of argument, applying the "enhanced prevention" argument to the active components could be proposed, but as will be seen later, this is troublesome.

Credit All Three Trains of Secondary Cooling (EFW + SUFP)

Prevention of Low-Order Cut Sets

The same comments apply here as for the bare-EFW option. The comments on CCF need to be extended to include the SUFP.

Prevention of Cut Sets of Order 3 or higher

All events in all cut sets of order 3 must be prevented to satisfy the DFC. For example, because the SUFP requires operator action given LOOP, this action counts as part of the prevention set, and its failure must be prevented at a probability level commensurate with active failure probabilities in general. A decision not to address any element of such a cut set would imply enhanced prevention of the other elements.

Prevention of Higher Order Cut Sets

Depending on a plant's configuration, higher order cut sets might arise from the EFW flow paths (which are highly redundant at many plants) or {combinations of flow paths and support trains}, {combinations of flow paths and pump trains} and the like. Looking only at transient events, it might be concluded that the DFC on heat removal could be satisfied with only one or two SGs. However, considering a broader class of initiating events (SGTR in any SG, feedwater line breaks at any SG, stuck-open SG relief valves,) would lead to requirements on SSCs associated with all four, even allowing that the redundancy requirement would be reduced from 3 to comport with the lower frequencies of such events.

TDP, One MD Train of Secondary Cooling, and FAB Powered by the DG Opposite the DG Powering the EFW MDP

For reasons given below, this option is taken to be "EFW + FAB but not SUFP."

Prevention of Low-order Cut Sets

Again, there are cut sets of order less than 3 associated with common-cause failures, and suction sources. However, to defeat this configuration, a CCF must cut across systems, and so it is relatively easy to credit their enhanced prevention. Enhanced prevention of the failure of suction sources is desirable.

Prevention of Cut Sets of Order 3 or Higher

Two formal possibilities exist, even within this alternative: In addition to the TDP and one HPI, either the EFW-MDP could be chosen, or, for the sake of argument, the SUFP. Obviously, designers intended the EFW-MDP to be the basis for the EFW safety case, and many reasons favor this choice. Since this plant is licensed and operating, appropriate treatment is already present for the EFW-MDP, but not necessarily for the SUFP. Moreover, the SUFP requires (more) operator action. Formally, one can cite an advantage for selecting the SUFP: depending on the configuration the flow paths to the SGs, the SUFP might offer some diversity in principle relative to the EFW-MDP. But this does not offset the advantages associated with the designer's intention.

Prevention of Higher Order Cut Sets

The same formal considerations apply to this case as to the **EFW+SUFP** case discussed above. In addition, apart from the cut sets associated with SBO, the higher-order cut sets must contain elements from both EFW and HPI, whose diverse character makes their joint prevention easier to argue (they are more clearly independent).

All Three Trains of Secondary Cooling, and FAB Using At Least One HPI Pump

Prevention of Low-order Cut Sets

The low-order cut sets for this option correspond again to CCFs or other highly improbable events, and comments made above continue to apply.

Prevention of Cut Sets of Order 3

Although this option comprises five pumps, the SBO still contributes at the level of 3 because the diesels are shared across front-line systems.

There also could be coupling between the two operator's actions shown on the figure (Operator-SU [Startup] and Operator-FAB). If so, then failure of EFW is triggered by two active failures, and failure of SUFP and FAB is accomplished by a failure somehow coupled to the two depicted operator actions. Satisfying the DFC for this option means that this coupled failure needs to be made highly unlikely: either the coupling must be prevented somehow, or the two operator-action failures must be made so unlikely individually that they do not contribute much to functional unreliability even if they are coupled.

Prevention of Higher Order Cut Sets

Cut sets of order N+3 or higher are, by themselves, preventable in many ways. One such cut set is "failure of all pumps shown." Since there are five pumps, and three must be addressed, there are many ways to do this. However, one of them must be the TDP, and the other two need to be on opposite diesels.

Addressing CDF and Functional Reliability Targets

Table 4.5-5 shows functional unreliability (failure probability of post-trip DHR, conditional on LOOP) and CDF for each of the options described above.

Computational Notes

These calculations were done using a SPAR model for the plant illustrated in Figure 4.5-1. Therefore, not all initiating events are reflected; other things being equal, CDF results will be higher for models addressing more initiating events (such as remaining internal events initiators, and external events).

"Functional Unreliability" was evaluated from the sum of the frequencies of LOOP core damage (CD) sequences involving failure of both EFW (including SUFP if credited in a particular option) and FAB (if credited in a particular option). This saved construction of a specialized event-tree model focusing on this function alone. As a result, blackout sequences are included in the evaluation, and the full SPAR model treatment of AC recovery therefore is implicitly credited in the functional unreliability quoted, based on these sequences. According to the intent of Alternative 3, crediting recovery in this way would create a regulatory stake in the efficacy of those recovery measures, if one did not already exist.

Results obtained from solving the model's fault trees for EFW and FAB (conditional on LOOP) are also provided. Using these results corresponds more directly to the approach taken in implementing the TMI action plan. The fault-tree numbers on Table 1 do not reflect the sequence-specific AC recovery actions credited in the full sequence models, or the competition between core damage due to unmitigated RCP seal failure, and that due to failure of decay heat removal.

Comparison of Functional Unreliabilities Across Options

The bare-EFW option (~6E-4) conspicuously fails to achieve the target (< 1E-4). The options satisfying the DFC all achieve the target, though the EFW+SUFP option (no FAB) suffers in comparison to EFW + FAB and EFW + SUFP + FAB. As expected, the option that takes credit for everything obtains the best result.

Comparison of CDFs Across Options

The bare-EFW option (>4E-4/yr) again conspicuously fails to achieve the target (< 1E-4/yr). The other options again pass, but this time, EFW+FAB is less satisfactory than the other two.

Again, as expected, the option that takes credit for everything obtains the best result.

The functional unreliability results discussed above were conditional on LOOP. In comparing overall CDFs for these options, the effects of different EFW/SUFP/FAB configurations on other initiators are being examined as well, or at least those reflected in the SPAR model, such as transients and small LOCAs. The

results on this table confirm the expectation (based on years of licensing experience) that satisfying an ambitious target for LOOP also drives up the plant's ability to respond to many other initiating events.

Table 4.5-5
Example: Characteristics of Different Options for Satisfying Requirements on Post-Trip Decay Heat Removal

		CDF (events /yr)	Functional Unreliability	BIRNBAUMS (events /yr) (Evaluated over Full Model)			
		Target: < 1E-4	Target: < 1E-4	TDP FTS	MDP FTS	Op-SUFP	Op-FAB
Satisfy SFC only	EFW Only	4.45E-04 (above target)	6.86E-04 (above target)	2.79E-02	1.44E-02	NA	NA
Satisfy DFC	EFW + SUFP, but no FAB	4.71E-05	7.00E-05	4.06E-04	1.80E-04	3.81E-04	NA
	EFW + FAB, but no SUFP	7.83E-05	3.77E-05	2.70E-03	4.82E-04	NA	3.84E-04
	EFW, SUFP, FAB	4.140E-05	1.88E-05	7.33E-05	2.55E-05	3.69E-05	6.39E-06

Key:

CDF	Core Damage Frequency	EFW	Emergency Feedwater	FAB	Feed and Bleed	TDP FTS	Turbine-driven EFW pump Failure to Start
MDP FTS	Motor-driven EFW pump Failure to Start	SUFP	Startup Feedwater Pump	Op-FAB	Operator action to initiate Feed and Bleed Cooling	Op-SUFP	Operator action to align & actuate Startup Feedwater Pump

Operational Considerations

Finally, it is instructive to examine selected importance measures evaluated within each of the options.

Table 4.5-1 also presents Birnbaum measures for selected basic events calculated for each option over all sequences, not just LOOP. The Birnbaum importance measures for the EFW pumps in the bare-EFW option are very high (> 1E-2/yr), meaning that very little is backing up these trains relative to their challenge frequencies. Even if these trains were extremely reliable, CDF still would be extremely sensitive to any change in their performance. Therefore, licensing based on the bare-EFW option would be difficult to justify, even setting aside the DFC requirement, because to achieve the desired low functional unreliability and the desired low CDF, there would be a need to commit to phenomenal levels of reliability performance. (That is, extremely low failure probabilities would have to be claimed for basic events in the EFW fault tree.) Operating experience is not, in general, consistent with those levels of reliability performance. Therefore, commitment to those levels of unreliability would be difficult to justify, validate, or monitor meaningfully. These observations are essentially a restatement of the considerations that led to the TMI action plan in the first place.

Comparison of Birnbaums for the other options suggests a significant benefit for the EFW+SUFP+FAB option, depending on its implementation. The Birnbaums of the EFW pumps are significantly lower in this option than in the others. This means that significantly greater latitude should be available in performance monitoring because the plant's CDF is less sensitive to these parameters. Moreover, although the measure tabulated is for fail-to-start, the result shown strongly suggests that significantly greater latitude also would also be available in evaluating configuration-based completion times for maintenance on these components.

Results

This example examined one safety function for one initiating event. Several configurations were considered; it was shown that those satisfying the redundancy target (the DFC) also satisfy the high-level and functional unreliability targets. For comparison, a configuration satisfying only the SFC was examined; it did not meet either the unreliability target or the CDF target.

This example does not clearly illustrate the potential for reducing burden, although it shows how flexibility is available to the licensee in deciding what to credit, based on how performance targets then will be established. To see how this alternative might lessen burden, a function would have to be considered that is challenged very infrequently but is currently required to satisfy the SFC. To determine the overall net benefit of this alternative, it is necessary to carry an example through all functions and all initiating event categories.

Safety Implications

The overall safety implications of the alternative would need to be assessed in light of its comprehensive application, examining all functions and all initiating event categories. That said, the example treated here shows that the bare-ESW case satisfies the SFC, but does not satisfy the redundancy guidelines contemplated in Alternative 3, the functional unreliability target, the CDF target, or the guideline in the TMI action plan.

The present evaluation considers failure modes not treated in implementing the TMI action plan, such as CCF contributions, and uses modern failure probabilities rather than the numbers used in NUREGS-0611 and NUREGS-0635. Nevertheless, it is significant that the bare-ESW configuration is found wanting, while the significantly enhanced configurations all satisfy the targets. This outcome is not driven by the

simplification of the present example because a more complicated example would present more possibilities for going beyond the SFC (more bleed and feed options, for example).
The Alternative 3 framework also provides a logic-model-based approach to identify where special prevention measures may need to be taken (CCF prevention, for example).

Burden Implications

As was the case for safety implications, the overall burden implications of the alternative would need to be assessed in light of its comprehensive application, examining all functions and all categories of initiating events.

Because this plant is licensed and operating, some of the burdens imposed as a result of this alternative would relate to the regulatory implications of taking credit for items that may not already be part of the safety case, such as PORVs, or the operator's action to initiate FAB.

Other burdens would relate to the need for more analysis of the new safety case. If FAB were credited, the associated success paths to a regulatory standard of T/H evaluation would need to be validated, and the provisions for operator action based on the findings. The present intention is not to revert to deliberately and significantly conservative T/H evaluations, as done in traditional safety analysis, but rather to apply careful T/H evaluation, and to understand when actions must occur, and what entry conditions are essential for success.

In terms of the licensee's benefit, looking only at the function examined in the example, increased operational flexibility is available if SUFP and FAB are credited, in addition to EFW. This has two aspects: (1) It is much easier to achieve a performance target if performance is spread over redundant and diverse trains, which reduces regulatory concerns when temporary issues of performance issues affect individual trains; (2) the conditional CDF associated with on-line maintenance decreases, potentially allowing increased completion times.

Other licensee benefits would be expected to result from an application that included infrequently challenged functions, where requirements would be reduced from current levels.

Methodology Implications

A methodological requirement not necessarily clarified in the present example is the need to explore the whole problem at once (all initiators, all functions) to gain the right perspective on the burden implications. This example was based only on one function (post-trip decay heat removal) for one category of initiating events (frequent). Including other initiating events, such as various LOCAs, would require bringing HPI into the safety case, whether or not FAB is credited. Thus, the incremental cost of taking credit for FAB in DHR is less than it would be if HPI were not already a safety system. Other functions that are needed in other initiating events might entail a need to include PORVs in the safety case. Thus, even though the DFC sounds like an increase above the SFC, it does not necessarily translate into a significant increase in SSCs credited. However, it may lead to SSCs being credited in contexts that are not presently analyzed. These new success paths require validation.

Logic modeling ground rules would need to be established to support implementation of this alternative. Logic models need to be developed in such a way as to support evaluation of the DFC requirement. Ground

rules for what to credit may be in order. For example, some models incorporate basic events corresponding to certain recovery actions, but it might prove inappropriate to credit certain of them against the DFC target. Since part of the alternative is aimed at identifying areas where "enhanced prevention" is appropriate, guidelines on modeling of passive failures and CCF events might be warranted.

Because the present alternative assigns "enhanced prevention" to cross-cutting failure events, more flexibility is available in dealing with the issue of what a passive failure is, or how certain electrical failures ought to count against the rule. Furthermore, licensees would commit to low probabilities of certain events; treatment and regulatory oversight (inspections and monitoring) would be predicated on that commitment.

5. SUMMARY

5.1 Motivation

This report summarizes work performed in response to the Commission's Staff Requirements Memorandum of March 31, 2003 that directs the NRC RES staff to "pursue a broader change" to the SFC. The Commission directed that "The staff should pursue a broader change to the single-failure criterion (SFC) and inform the Commission of its findings." To support a response to this directive, a study was undertaken to develop risk-informed alternatives to the SFC. This report summarizes the background of the existing SFC and presents the approach used to develop risk-informed, performance-based alternatives to it. Four alternatives, including the current SFC, are discussed. The work reported here applies to the current generation of U.S. nuclear power plants.

A single failure is defined as "...an occurrence which results in the loss of capability of a component to perform its intended safety functions...", and includes any additional failures that are consequences of the single failure. The SFC requires that specific plant-safety functions are designed with redundant means to ensure that the safety functions can be accomplished, assuming a single failure. The intent of the SFC is to promote high reliability of safety functions important to safety, and to help ensure that, in the event of a single failure, adequate safety margins are maintained.

The SFC was incorporated as a set of requirements in the U.S. Code of Federal Regulations in the early days of the nuclear-power industry. The SFC is set out in NRC documents in two major contexts: (1) System design requirements, largely associated with the General Design Criteria (GDC) of 10 CFR 50 Part A that require designing safety-related systems to perform safety functions to mitigate design-basis initiating events, assuming a single failure, and, (2) the guidance on analyzing design-basis accidents in Chapter 15 of Regulatory Guide 1.70 and of the Standard Review Plan, directed towards demonstrating adequate design margins based upon defined acceptance criteria. Additional SFC guidance is found in NRC regulatory guides and other NRC documents, and in industry consensus standards accepted for use by the NRC. The requirements and guidance are reviewed in this report.

The GDC specify safety functions to which the SFC is to be applied, and also provide additional constraints and assumptions to be incorporated in single failure analysis of specific safety functions and safety systems. The delineated safety functions include plant protection, electric power, residual heat removal, emergency core cooling, containment heat removal, containment atmosphere cleanup, and cooling water systems. While passive failures of electrical components are encompassed in single-failure analysis, generally only active failures of fluid system components are included. The NRC staff's positions on passive failure were developed and used in the licensing process, but the regulations still state that the "...conditions under which a passive component in a fluid system should be considered in designing the system against a single failure are under development."

The SFC is, in part, a surrogate for system reliability for nuclear plant safety systems that is intended to advance high system reliability. Several regulations, guidelines and programs, including quality-assurance requirements, technical specifications, testing, inspection and maintenance requirements, act in concert with the SFC to promote such reliability. The qualitative SFC, however, has not always led to the design of safety systems whose reliabilities were judged commensurate with the frequency of safety challenges to the plant. Consequently, on the basis of risk considerations, the SFC was supplemented by regulatory guidelines and regulations for some safety systems. These, in turn, entailed plant modifications and licensee programs

to either improve system reliability or to demonstrate that the system design was otherwise adequate to cope with postulated initiating events. Other actions by the NRC led to improvements to address phenomena such as common-cause failure, whose impacts on plant safety are not mitigated by a redundant safety function design. Additional measures were adopted to supplement the SFC, including the Reactor Oversight Process tracking of safety-system availability. In combination with such measures, regulations, guidelines and programs, the SFC requirement of redundant design of safety systems has contributed to maintaining an adequate level of safety in operating U.S. nuclear power plants.

On the other hand, application of the SFC sometimes has led to redundant system elements which, while providing an acceptable safety margin, have minimal impact on risk, based on risk assessment studies, as demonstrated in this report. While maintaining adequate safety margins is a major safety objective, the benefits of assuming the worst single failure for all design-basis accidents, may sometimes impose unnecessary constraints on licensees.

Such risk insights suggest alternatives to the SFC might be constructed that relate more directly to quantitative functional or system reliability than does the current one, while simultaneously maintaining appropriate defense-in-depth and adequate safety margins. These alternatives would require system reliability to be commensurate with the frequency of challenges to the safety systems, and require reliability designs that addresses common-cause failure, system dependencies, spatial dependencies, and multiple independent failures, which the current SFC does not incorporate. In addition, alternatives may be considered that could require risk-informing the choice of accident sequences selected for design-basis analysis. A study of potential risk-informed alternatives was conducted to address these and other issues related to the SFC.

5.2 Alternative Development Process

A process was devised to develop and evaluate potential risk-informed alternatives to the current SFC, together with a process flowchart to guide implementation of the process; it is presented in Section 3.2 of this report. The effort began with a study of the background of the existing SFC, and the development of an understanding of the criterion's original intent NRC policy documents were used, including the Strategic Plan [USNRC, 2004a], the PRA Policy Statement [USNRC, 1995], the Risk-Informed Regulation Implementation Plan [USNRC, 2003b], Guidance for Performance-Based Regulation [USNRC, 2002c], and the White Paper on Risk-Informed and Performance-Based Regulation [USNRC, 1999a], together with risk-informed perspectives such as those described above, to gather a set of desired attributes of risk-informed SFC alternatives.

These attributes, discussed in Section 3.2.3, include the desirability to (1) address functional reliability quantitatively, and relate it to the frequency of challenges and to plant risk, (2) maintain defense-in-depth, (3) risk-inform application of the worst single-failure assumption in design-basis safety analyses, and, (4) use performance-based regulatory approaches as much as possible. In addition, the alternatives should be amenable to effective implementation, coherent with other risk-informed regulatory initiatives and consistent with security programs underway at the NRC.

The existing SFC was compared with the attributes, and potential modifications of it were delineated. The potential modifications then were used to develop risk-informed alternatives that address both the GDC reliability context of the SFC, and the worst single-failure DBA analysis context of the criterion.

Each alternative has two elements: (1) Risk-Informing Approach: A combination of qualitative and quantitative risk and/or reliability guidelines that establishes the levels of performance that the regulator wants the function or system to achieve to satisfy regulatory objectives, and, (2) Implementation: A discussion of steps that would be required of both the NRC and the licensee to implement the Risk-Informing Approach. These alternatives were examined with knowledge of the ongoing efforts of the NRC and the nuclear licensees, including risk-informing the large break LOCA related to 10 CFR 50.46, and the "special treatment" work related to 10 CFR 50.69.

5.3 Risk-Informed Alternatives

A relatively large number of potential risk-informed alternatives were devised that satisfied at least some of the attributes. When they were compared with each other, they demonstrated many similarities. This allowed focusing and merging them into four alternatives, including the current implementation of the SFC, that demonstrate the range of possible approaches to risk-informing the SFC.

Table 5.3-1 summarizes the alternatives developed in response to the Commission directive to "pursue a broader change to the SFC." The current approach is listed, along with the four alternatives resulting from the work described here. The set of risk-informed alternatives demonstrates a range of possible approaches to pursuing changes to the SFC. They demonstrate concepts to risk-inform the SFC. Other alternatives, involving different combinations of the basic concepts, may be constructed.

The Baseline Alternative would continue current practices associated with implementing the SFC in its reliability and DBA analysis contexts. The current approach to implementation of the SFC is embodied in the General Design Criteria, the Standard Review Plan, other NRC guidelines, and industry consensus standards. Specific issues, such as AFWS reliability and risk-informing 10 CFR 50.46, related to the SFC, have been and would continue to be dealt with on a case-by-case basis. Retaining this approach is the Baseline Alternative. A possible change that could be pursued without altering basic SFC practice, is to develop a way to resolve the passive failure issue for fluid systems. This Baseline Alternative would not address fundamental issues with the SFC arising from the lack of risk-informed considerations, as discussed in Sections 2.7 and 5.1 of this report.

Alternative 1 recognizes that in the current application of the SFC to DBA analysis, risk-insignificant accident sequences involving an initiating event and a single failure typically are included in the plant design basis. In contrast, some multiple-failure sequences involving an initiating event and multiple independent failures, whose risk-significance can be on the order of that of single-failure sequences, may not be included in the design basis. This alternative would risk-inform the selection of accident sequences that are included. The risk-significance of specific accident sequences would be determined using a plant's PRA, and the NRC would develop risk-significance measures and guidelines for the licensee's use. For each initiating event, a licensee would identify all its single- and multiple-failure success paths, and from its PRA and the risk-significance measures and guidelines, develop a complete list of accident sequences to be included into its design basis. Some single-failure sequences that are now part of its current design basis may be removed based upon their risk-significance, while some multiple-failure sequences that are now excluded may be added. Any plant change resulting from adopting the alternative must satisfy RG 1.174. An example application of Alternative 1 illustrates the potential for removing from the design basis an operationally-limiting, low-frequency DBA event sequence that includes an initiating event with a single system failure. It demonstrates how the alternative could offer an opportunity for revising the DBA analysis, so providing more operational or performance flexibility.

Table 5.3-1 Comparison of Risk-Informed Alternatives

	BASELINE ALTERNATIVE (CURRENT APPROACH) Retain Current SFC	ALTERNATIVE 1 Risk-Inform Application of SFC to DBA Analysis	ALTERNATIVE 2 Risk-Inform Application of SFC Based on Safety Significance	ALTERNATIVE 3 Generalize and Enhance the SFC
Risk-Informed Approach	The original motivation for the SFC was to promote high reliability of safety-related systems, and to provide an adequate safety margin in the event of a single failure in the safety system in response to a design-basis event. Specific licensing issues relating to the SFC arise periodically, providing the opportunity to reconsider application of the SFC from a risk-informed point of view. This alternative would risk-inform the regulatory framework by refining the scope of application of the SFC in selected areas, but would not change the current regulatory structure for implementing the SFC. Risk-informing the current SFC would be considered in the context of specific licensing issues as they arise (e.g., redefining LBLOCA). Aspects of Alternatives 1-3 could be considered for application to a particular issue. A position would be developed on single passive failures in fluid systems to replace the footnote now included in 10 CFR Part 50 Appendix A definitions.	Safety-insignificant single failure event sequences are sometimes included in the plant design basis, while some safety-significant multiple failure sequences are not. This alternative would risk-inform the selection of such sequences used in DBA thermal hydraulics analysis. Risk-inform event sequences postulated in DBA thermal-hydraulics analysis: (1) Permit the removal from the design basis of sufficiently unlikely single-failure sequences that are non-risk significant. (2) Require adding sequences of multiple failure events to the design basis when their frequency exceeds that of any single-failure sequence postulated for the same initiating event. Criteria for quantitative frequency would be established for removing and adding event sequences to the design basis.	The intent of the SFC, in part, is to promote high safety-related system reliability. However, sometimes the SFC is not applied in manner commensurate with the safety-significance of the safety system. Risk-inform application of the SFC such that a system's reliability is commensurate with its safety-significance. Categorizing the systems would be consistent with 10 CFR 50.69. Sub-alternatives are identified for the desired degree of relaxation of the level of defense-in-depth required for systems of low safety significance (RISC 3): (1) Alternative 2a proposes that redundant safety-related trains may be removed from service, leaving the system with a single train. (2) Alternative 2b proposes that one train would remain as safety-related, and reclassifying the redundant trains as non-safety-related. (3) Alternative 2c proposes that all trains would remain as safety-related. The regulatory requirements for one of them remain the same; the redundant trains can encompass operational flexibility.	Current practice, which applies the SFC to selected postulated events (and classifies the credited equipment accordingly), imposes burden that is incommensurate with SSC safety significance as analyzed in risk models. Alternative 3 generalizes the SFC and supplements it with reliability targets to better align safety resources to safety needs. Instead of requiring sufficient redundancy to withstand a single failure in plant's response to selected postulated events (current practice), Alternative 3 requires more redundancy and diversity in response to frequent events, and less for infrequent events. Where redundancy targets are not met, the alternative recommends enhancing the treatment of SSCs to compensate for the lower redundancy. Qualitative redundancy criteria are supplemented by quantitative targets on functional unreliability, and by integrated checks on CDF and LERF. Licensees determine which plant features to credit to address the targets, and how much credit they take for those features. Implementation (including monitoring) is informed by licensee choices.

Table 5.3-1 Comparison of Risk-Informed Alternatives (continued)

	BASELINE ALTERNATIVE (CURRENT APPROACH) Retain Current SFC	ALTERNATIVE 1 Risk-Inform Application of SFC to DBA Analysis	ALTERNATIVE 2 Risk-Inform Application of SFC Based on Safety Significance	ALTERNATIVE 3 Generalize and Enhance the SFC
Implementation Approach	Initial Licensing Changes: The NRC would identify a regulatory issue that could involve some aspect of the SFC, e.g., system reliability or DBA analysis margins. Licensees would submit appropriate information in accordance with the revised requirements. The position on passive failures in fluid systems would be developed considering industry standards, and worked through the rulemaking process.	Initial Licensing Changes: The NRC would issue new regulations or guidelines for modifying DBA analysis requirements. The licensee would delineate all possible single-and multiple-event sequences, and, on the basis of event sequence frequency, would propose which single-failure paths are to be removed and which multiple-failure paths are to be added. Any proposed changes to the plant based on Alternative 1 would be reviewed using RG 1.174 guidelines.	Initial Licensing Changes: The NRC would develop a new regulation, which could be an expanded version of 10 CFR 50.69, that would include the approach to risk-informing the SFC. The GDC that are related to the SFC also may have to be modified. The licensee would use the plant's PRA, and could make physical or operational changes to the plant's systems as long as the changes meet the guidelines in RG 1.174.	Initial Licensing Changes: The NRC would replace or change the current regulations. The Agency would define the targets for CDF and LERF, functional unreliability, and redundancy and diversity. The licensee would establish train-level reliability targets satisfying the above, and identify areas needing enhancement. These changes based on Alternative 3 would be reviewed using RG 1.174 guidelines.
	Programmatic Activities: Changes to current activities, such as the Maintenance Rule, ISI, IST, and QA,. would be considered for the particular activity and issue.	Programmatic Activities: No changes considered at this time.	Programmatic Activities: Each sub-alternative risk-informs these activities to some extent. For example, sub-alternative 2c allows operational flexibility, such as relaxation of AOTs, STIs, ISI and IST.	Programmatic Activities: Programmatic activities, such as IST, would be informed by the licensee's choices made to satisfy the targets (e.g., might need to be extended to some systems). A basis for the heightened SSC treatment for systems without target redundancy would need to be addressed.
	Performance Monitoring: Performance monitoring requirements would be considered as appropriate for changes in SFC requirements. They could include current approaches or those being developed in the ROP, or augmented for the particular issue if new targets or goals are developed.	Performance Monitoring: Monitoring would be required of industry data on the frequency of rare initiating events, such as large pipe breaks; also, periodic revision by experts would be needed. Plant-specific monitoring programs would be appropriately adapted to verify PRA models and the data used for DBA selection.	Performance Monitoring: Monitoring would be required of the reliability of safety-significant systems. Each sub-alternative proposes a different type of monitoring of safety-related non-safety-significant systems (see Section 4.4.2.2).	Performance Monitoring: Monitoring would confirm that assigned performance targets are met.

Alternative 2 considers that the redundancy requirement of the SFC is a qualitative surrogate for system reliability. It considers risk-informing the application of the SFC such that system reliability is considered directly, and is commensurate with the safety-significance of the system. The alternative is related to the NRC and industry's work on 10 CFR 50.69. With the categorization framework of 10 CFR 50.69, licensees would use a risk-informed process for classifying systems. Alternative 2 holds that regulatory requirements on systems should be commensurate with a system's safety-significance, and so the SFC should be applied in a manner that accounts for it. For safety-significant, safety-related systems (RISC-1 category), Alternative 2 would require application of the SFC based upon GDC requirements and other NRC and industry guidelines. For non-safety-related safety-significant systems (RISC-2 category), Alternative 2 would require, in addition to current requirements, an increase in the level of regulatory requirements by monitoring the system's performance in maintaining the current reliability. For low safety-significant, safety-related systems (RISC-3 category), Alternative 2 would relax the regulatory requirements, and further, offer three sub-alternatives. For a low safety-significant safety-related system with redundant trains: a) Alternative 2a would not require redundancy, so one safety-related train remains in service and the redundant train(s) can be removed from service, b) Alternative 2b suggests that the system could be comprised of one safety-related train and the redundant train(s) would be re-classified as non-safety-related, c) Alternative 2c proposes that all trains would remain as safety-related ones; the regulatory requirements for one of them remain the same, while the redundant trains would have additional operational flexibility. RISC-4 systems are non-safety-related ones that have low safety significance; any current regulatory requirements would be expected to be maintained for them. Alternative 2 would require the licensee to monitor the reliability performance of all safety-significant systems, including the non-safety-related ones. A plant's PRA of a quality necessary for the application would be used for the safety-significance determinations. Any changes resulting from this alternative would have to be shown to comply with RG 1.174. The major advantages of Alternative 2 are that it would require that system reliability is commensurate with safety-significance, and that regulatory requirements, including the SFC, would be applied according to the system's safety-significance. An example application of Alternative 2 illustrates the potential for relaxing SFC requirements for safety-insignificant safety-related systems, and ensuring or maintaining safety by requiring monitoring of safety-significant non-safety-related systems.

Alternative 3, like Alternative 2, recognizes that the redundancy requirement of the SFC is a qualitative surrogate for system reliability. However, rather than modifying the SFC as does Alternative 2, this alternative considers replacing the SFC with a framework involving a combination of top-level risk targets (e.g., CDF), function reliability targets that are commensurate with the system's challenge frequency, and guidelines for using redundancy and diversity that also depend on challenge frequency. The NRC would establish these targets and guidelines on a plant-type basis, and the licensee would use them, along with a plant PRA, to set up lower-level train reliability targets. The licensee would track the compliance of the trains' performance with those targets. The major advantages of Alternative 3 are that it would require that system functional reliability be commensurate with the frequency of challenges to that system, and also require reliability performance monitoring at the train level to track compliance with functional reliability targets, thereby providing a coherent approach to regulatory oversight. Arguably, Alternative 3 is the most complex of those discussed here, and would involve considerable efforts from the NRC and the licensees. Rulemaking would be required, since the GDC's current single-failure requirements would not be applicable. Instead, system redundancy requirements would be subsumed into the overall functional reliability framework. An illustrative example of Alternative 3 demonstrates the generalization and enhancement of the SFC, and shows how, for a specific plant, options for combining existing systems may address all the alternative's targets.

Table 5.3-2 summarizes the advantages and disadvantages of the three alternatives. Alternatives 1-3 offer concepts for risk-informing the SFC based upon the Commission's directive to "pursue a broader change" to it. All were based upon desired attributes for risk-informed alternatives that were developed during this study. They would entail efforts by the NRC and industry to implement the risk-informed changes to the SFC. The "Baseline Alternative" retains the current SFC's regulatory structure, but recognizes that opportunities for risk-informing it may arise in the future in the context of specific regulatory issues.

5.4 Concluding Observations

Scope of Application of the SFC

Alternatives 1, 2, and 3 each, in different ways, change the scope of application of the SFC in the regulatory process. Alternative 1 changes the consideration of the worst single active failure in accident analysis, provided that the subsequent event sequence has very low frequency. Alternative 2 applies the SFC within systems, but only to ones deemed "safety significant." Alternative 3 applies the SFC and variations on it to key safety functions, depending on the frequency at which those functions are challenged, and the consequences of their failures. Examples of how Alternatives 1, 2 and 3 could be applied in practice are presented in Sections 4.3, 4.4, and 4.5 of the report, respectively.

Range of Possible Alternatives

Alternatives 1, 2, and 3 illustrate a range of features that may be used to define alternative variations. For example, alternatives to the SFC could vary according to the degree of their continued reliance on structuralist requirements, the degree to which they apply rationalist requirements, and the levels at which they use risk information. All apply an integrated risk evaluation (e.g., change in core damage or large early release frequency); in addition, Alternative 1 incorporates probability at the event sequence level; Alternative 2 applies importance measures at the system level; and, Alternative 3 suggests functional reliability goals. All alternatives could include developing a position on single passive failures in fluid systems to replace the footnote now in 10 CFR Part 50 Appendix A definitions.

Table 5.3-2 Comparison of Pros and Cons of Risk-Informed Alternatives

	BASELINE ALTERNATIVE (CURRENT APPROACH) Retain Current SFC	ALTERNATIVE 1 Risk-inform Application of SFC to DBA Analysis	ALTERNATIVE 2 Risk-inform Application of SFC Based on Safety Significance	ALTERNATIVE 3 Replace SFC with Risk and Safety Function Reliability Guidelines
Pros	• The major benefit of this alternative is that it would not involve revising all existing regulations that include the SFC. Instead, it would consider changes to the SFC requirements in the context of other regulatory issues that may arise in the future (as 10 CFR 50.46 is being examined, including the requirements for the single-failure assumption).	• This alternative could result in additional predicted margin, which could be used to justify plant changes consistent with RG 1.174's guidelines. • Alternative 1 appears consistent with ongoing efforts, including LOCA redefinition, risk-informing design-basis LOCA-LOOP assumptions, and developing a framework for licensing advanced reactors. • The frequency-based logic of Alternative 1 could be applied to more generally risk-inform DBA selection, including LOCA-LOOP assumptions, selecting design-basis initiators, and, potentially, the inclusion of safety-significant success paths.	• Alternative 2 provides a framework (for both the NRC and licensees) indicating the importance of systems to safety. In general, classifying systems provides a framework for assigning regulatory requirements to them according to their safety significance. Alternative 2 thereby relates the requirements of the SFC to a system's safety significance. •This alternative proposes performance-monitoring of system reliability for non-safety-related but safety-significant (RISC-2) systems. Hence, Alternative 2 encompasses non-safety systems which are not addressed by the SFC. • This alternative extends the scope of 10 CFR 50.69 to risk-inform the SFC.	• Alternative 3 would drive the plant's risk profile towards desirable characteristics: - the overall level of risk would be commensurable with the QHOs, - the risk profile would be balanced in that no single family of sequences would be dominant, - vulnerabilities would be addressed, and, - these outcomes would not be completely limited by traditional PRA "quality" issues. • The licensee's performance targets would directly inform the implementation measures, including regulatory oversight, and residual uncertainties would be partly resolved through supplementary requirements on redundancy and diversity.

Table 5.3-2 Comparison of Pros and Cons of Risk-Informed Alternatives (continued)

	BASELINE ALTERNATIVE (CURRENT APPROACH) Retain Current SFC	ALTERNATIVE 1 Risk-inform Application of SFC to DBA Analysis	ALTERNATIVE 2 Risk-inform Application of SFC Based on Safety Significance	ALTERNATIVE 3 Replace SFC with Risk and Safety Function Reliability Guidelines
Cons	•This alternative would not afford the opportunity for placing SFC in context of quantitative risk measures, nor for reexamining the DBA worst single failure aspect of the criterion. •Improvement of coherence between programs would be limited.	• **Alternative 1 requires PRAs of a quality that the NRC must first establish.** • **The implementation of Alternative 1 is expected to require the NRC and industry's effort** to establish regulatory guidance and possible rulemaking.	• Alternative 2 requires PRA models of adequate quality. • Implementing Alternative 2 is expected to require effort by the NRC and industry to develop regulatory guidance and possible rulemaking.	• Alternative 3 would require rethinking and modifying the regulatory framework and the plant licensing basis, on the part of both the NRC and the licensee. This would entail an effort to change regulations and develop regulatory guidance.

Continued Reliance on Structuralist Requirements

Alternatives 1, 2, and 3 all retain elements of "structuralist" guidance. In effect, all of them continue the current practice of partly judging a design by what failures it can tolerate and still meet safety objectives. None of them rely entirely on quantifying risk metrics to establish a design's acceptability. Alternatives could have been developed that apply reliability targets without structuralist elements, but the present report does not include such ones. Depending on the details of formulation, they probably would have scored poorly on the "defense-in -depth" attribute, and would be considered "risk-based" rather than "risk-informed."

Increased Reliance on Risk Perspective to Reduce Excessive Requirements

While all of the alternatives retain structuralist elements, they also moderate the application of the SFC by applying quantitative analysis to rationalize not applying it in areas where its burden is not justified by a safety benefit. Alternative 1 would eliminate low-probability events as failures that must be postulated in applying the SFC. Alternative 2 reduces requirements on systems that are not safety significant. Alternative 3 does not apply the SFC where the challenge frequency is sufficiently low.

Increased Reliance on Risk Perspective to Address Potential Gaps in SFC Coverage

In selected areas, the alternatives may go beyond the SFC in imposing requirements. Thus, Alternative 1 requires considering multiple-failure scenarios in design-basis analysis, if they lie above a frequency cutoff.

Alternative 2 contemplates increased regulatory attention to systems that are non-safety-related but safety-significant. Alternative 3 suggests allowing for more than one failure in functions that are challenged frequently, and also supplements this structuralist element with functional reliability targets.

Work to Move Forward

The major focus of this study was to identify potential alternative risk-informed approaches to the SFC. Example applications of each alternative were carried out; the findings are discussed in this report. Additional examples or pilot activities would give a better understanding of the potential usefulness of such alternatives, including approaches to implementation, and the implications on resources required for their further development and implementation.

In Alternatives 1 and 2, the approaches are based on low assessed event probabilities. Work would be needed to both create a basis for assessing the requirements for implementation implied by the approach, and establish protocols for making licensing decisions. A new regulation would require an acceptable rationale to reasonably assure that certain event probabilities are low, and that they would remain so, and that if the probabilities change, what licensing actions need to result. Additionally, some relationships between the safety analyses and plant equipment classification cut across regulations. Rather than working with assessed probabilities directly in licensing decisions, Alternative 3 employs reliability targets defined relative to top-level safety objectives. The development of regulatory protocols and rationale apply to an even greater extent to this alternative.

In summary, care will be needed to make sure that the ramifications of these changes are considered. A detailed deliberation of these alternatives would need to be informed by practical trial applications, including a consideration of implementation methods.

The staff believes that, while a wide range of alternatives have been evaluated, additional stakeholder involvement and further evaluation will be necessary to assess the practicality of implementing any alternative. In fact, stakeholder input may result in other viable alternatives meriting consideration. Therefore, the staff does not recommend one alternative over another at this time. As directed in a staff requirements memorandum dated May 9, 2005, the Office of Nuclear Regulatory Research plans to work with the Office of Nuclear Reactor Regulation to develop a formal program plan to make a risk-informed, performance-based revision to 10 CFR Part 50. The staff could include any follow-up activities to risk-inform the SFC in this formal program plan.

6. REFERENCES

AEC 1965, General Design Criteria, AEC H-252, November 1965 [citation from Okrent, 1981].

AEC 1967, General Design Criteria, AEC-172, July 1967 [citation from Okrent, 1981].

ANSI/ANS 1981, "Single-Failure riteria for Light Water Reactor Safety-Related Fluid Systems," American National Standard, American Nuclear Society, ANSI/ANS-58.9-1981.

CFR 2004, U.S. Code of Federal Regulations, Title 10, Part 50, Appendix A, Criterion 34.

CFR 2004, U.S. Code of Federal Regulations, Title 10 CFR Part 50, Appendix A, GDC 35.

CFR 2004, U.S. Code of Federal Regulations, Title 10, Part 50, Appendix A, Definitions and Explanations.

Haskin, F.E.,*et al.*, 2002, "Perspectives on Reactor Safety," Section 2.4 of NUREG/CR-6042 Rev. 2, SAND 93-0971, March 2002.

IAEA 1990, Safety Series No. 50-P-1, "Application of the Single-Failure Criterion - A Safety Practice," Vienna, 1990.

IEEE 1971, IEEE Std 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations," 1971.

IEEE 1991, IEEE Std 603-1991, "IEEE Standard Criterion for Safety Systems for Nuclear Power Generating Stations," June 1991.

IEEE 2000, IEEE Std 379-2000, "IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Systems," Section 6.3.2, p. 8, 2000.

King, T. *et al.*, 2000, "Framework for Risk-Informed Changes to the Technical Requirements of 10 CFR 50," Attachment 1 to SECY-00-198 (USNRC, 2000).

Nuclear Energy Institute, "10 CFR 50.69 - SSC Categorization Guideline," NEI 00-04 Final Draft, April 2004.

Okrent, D. 1981, "Nuclear Reactor Safety: On the History of the Regulatory Process," The University of Wisconsin Press.

Powers, D. 1999, "The Role of Defense in Depth in a Risk-Informed Regulatory System," Letter, Powers to Jackson, May 19, 1999.

Sorenson, J.N. 1999, *et al.*, "On the Role of Defense in Depth in Risk-Informed Regulation," Proceedings International Topical Meeting on Probabilistic Safety Assessment, PSA '99, Risk Informed, and Performance Based Regulation in the New Millenium,", Vol. 1, 408-413, August 1999.

Sorenson 2002, NUREG-1755, "Some Observations on Risk-Informing Appendices A and B to 10 CFR Part

50," ACRS, 2002.

USNRC 1975, "Reactor Safety Study - An Assessment of Accident Risks in US Commercial Nuclear Power Plants," NUREG-75/014.

USNRC 1976a, "Staff Discussion of Fifteen Technical Issues Listed in Attachment to November 3, 1976 Memorandum from Director NRR to NRR Staff," NUREG-0138.

USNRC 1976b, "Staff Discussion of Additional Technical Issues Received by Responses to the November 3, 1976 Memorandum from Director NRR to NRR Staff," NUREG-0153.

USNRC 1977, SECY-77-439, "Single-Failure Criterion," August 1977.

USNRC 1978, Regulatory Guide 1.70, "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants, LWR Edition," Rev. 3, November 1978.

USNRC 1978, "Regulatory Guide 1.70, Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants, LWR Edition, Revision 3", Chapter 15, November 1978.

USNRC 1979, "Staff Report on the Generic Assessment of Feedwater Transients in Pressurized Water Reactors Designed by the Babcock & Wilcox Company," NUREG-0560.

USNRC 1980a, "Clarification of TMI Action Plan Requirements," NUREG-0737.

USNRC 1980b, "Generic Evaluation of Feedwater Transients and Small Break Loss-of-Coolant Accidents in Westinghouse-Designed Operating Plants," NUREG-0611.

USNRC 1980c, "Generic Evaluation of Feedwater Transients and Small Break Loss-of-Coolant Accidents in Combustion Engineering-Designed Operating Plants," NUREG-0635.

USNRC 1981a, "Standard Review Plan," NUREG-0800, Rev. 2, Chapter 15, July 1981.

USNRC 1981b, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," NUREG-0800, Section 10.4.9 Rev. 2.

USNRC 1984, "A Prioritization of Generic Safety Issues," NUREG-0933.

USNRC 1985, "Loss of Main and Auxiliary Feedwater Event at the Davis-Besse Plant on June 9, 1985," NUREG-1154.

USNRC 1991, "Foundation for the Adequacy of the Licensing Basis", NUREG-1412.

USNRC 1995, "Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities: Final Policy Statement," Federal Register, Volume 60, Number 158, p. 42622, August 1995.

USNRC 1996, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," NUREG-800 Draft Report for Comments, June 1996.

USNRC 1998, “Regulatory Guide 1.174, An Approach for Using Probabilistic Risk Assessment In Risk-Informed Decisions On Plant-Specific Changes to the Licensing Basis,” July 1998.

USNRC 1999a, “Staff Requirements - SECY-98-144 - White Paper on Risk-Informed and Performance-Based Regulation,” March 1, 1999.

USNRC 1999b, “Recommendations for Reactor Oversight Process Improvements,” SECY 99-007.

USNRC 2000a, “Framework for Risk-Informed Changes to the Technical Requirements of 10 CFR 50,” Office of Nuclear Regulatory Research, Division of Risk Analysis and Applications, PRA Branch, Draft, Rev. 3, August 2000.

USNRC 2000b, “Staff Requirements - SECY-00-191, High Level Guidelines for Performance-Based Activities,” September 2000.

USNRC 2000c, “Development of Risk-Based Performance Indicators: Program Overview,” March 2000.

USNRC 2001, “Transmittal of Directive 6.3, The Rulemaking Process”, DT-01-14, Office of Administration, July 2001 (Revised).

USNRC 2002a, Memorandum to Samuel J. Collins, Director, Office of Nuclear Reactor Regulation-Transmittal of Technical Work to Support Possible Rulemaking on a Risk-Informed Alternative to 10 CFR 50.46/GDC35, July 31, 2002.

USNRC 2002b, "Some Observations On Risk-Informing Appendices A and B to 10 CFR Part 50," Advisory Committee on Reactor Safeguards, NUREG-1755, January 2002.

USNRC 2002c, “Guidance for Performance-Based Regulation,” NUREG/BR-0303, December 2002.

USNRC 2002d, “An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis,” Regulatory Guide 1.174, Revision 2.

USNRC 2003a, Staff Requirements – SECY-02-0057, Update to SECY-01-0133, “Fourth Status Report on Study of Risk-Informed Changes to the Technical Requirements to 10 CFR Part 50 (Option 3) and Recommendations on Risk-Informed Changes to 10 CFR 50.46 (ECCS Acceptance Criteria),” March 31, 2003.

USNRC 2003b, Regulatory Guide 1.53, “Application of the Single-Failure Criterion to Safety Systems,” Rev. 2, November 2003.

USNRC 2003c, Memorandum to W. D. Travers (EDO) from A. L Vietti-Cook, “Staff Requirements – COMNJD-03-0002 - Stabilizing the PRA Quality Expectations and Requirements,” December 18, 2003.

USNRC 2003d, “Update of the Risk-Informed Regulation Implementation Plan,” SECY-03-0044, March 2003.

USNRC 2004a, “USNRC Strategic Plan FY2004-FY2009,” NUREG-1614, Vol. 3, August 2004.

USNRC 2004b, "Draft Rule Language for Proposed Rulemaking - Risk-Informed Revision to Emergency Core Cooling System Requirements (10 CFR 50.46)", NRC Website, http://ruleforum.llnl.gov/cgi-bin/library?source=*&library=ECCS_risk_lib&file=*&st=risk, October 2004.

USNRC 2004c, "Code of Federal Regulations," Title 10, Parts 1-50, January 2004.

USNRC 2004d, "Draft Rule Language for 50.46 ECCS LOCA Redefinition Rule.," October 14, 2004.

USNRC 2004e, Staff Requirements Memorandum, SECY-04-0037, "Issues Related to Proposed Rulemaking to Risk Inform Requirements Related to Large Break Loss of Coolant Accidents (LOCA) Break Size and Plans for Rulemaking on LOCA with Coincident Loss of Offsite Power, " July 1, 2004.

USNRC 2004f, Letter from NRC to Catawba Nuclear Station, Units 1 and 2, Subject - Issuance of Amendments RE: SGTR Licensing Basis, September 24, 2004.

Appendix A
Calculations Demonstrating the Influence of Redundancy on Core Damage Frequency

The risk of a nuclear power plant was evaluated to illustrate the current implementation of the SFC. Section A.1 discusses the assessments of the implementation of the SFC, the results, and the insights obtained.

A.1 Evaluations for the Current Implementation of the SFC

The single-failure criterion provisions contained in the General Design Criteria and in the systems sections of the Standard Review Plan result in redundant design of safety functions. These functions are implemented by safety systems; each system may have redundancy, or redundancy may be achieved by two or more single-train safety systems.

Redundancy is a well-known way to increase the reliability of a system and of the functions to which the system contributes to fulfill. In this way, the redundancy in safety functions (systems) contributes to reducing the risk of a plant. To gain quantitative insights of the impact of such redundancy on risk, the redundant trains of each system were made unavailable in the plant's SPAR model, and the corresponding impact on CDF was calculated.

The following evaluations were made for a PWR and a BWR plant for the current implementation of the SFC:

- Type 1. The redundancy of each safety-related system (one system at a time) was removed, and the increase in CDF was determined and compared with the base case. That is, a safety-related system having two or more trains was changed to a single-train system; the updated CDF then was obtained. The non-safety-related systems were retained in the model.

- Type 2. The redundancy of major functions (one function at a time) was removed, and the increase in CDF compared with the base case. For example, if a function uses several safety-related systems, each of which has two redundant trains, then each system in this function was changed to a single-train system; the updated CDF then was obtained. The non-safety-related systems were kept in the model.

- Type 3. The same calculations as in the first point above were made but credit was not given to the non-safety-related systems. In this way, the impact on CDF due to removing redundancy of the safety-related systems was obtained without the mitigating contribution of the non-safety-related systems.

- Type 4. The same calculations as in the second point above were conducted, but credit was not given to the non-safety-related systems in the model. Hence, the impact on CDF was obtained due to removing redundancy of major functions, without the mitigating contribution of the non-safety-related systems.

In each of the four types of calculations, when a safety-related system has redundancy, the redundancy is reduced, taking into account the system's success criteria. For example, the Standby Liquid Control (SLC)

of the BWR plant has a success criteria of 1 out of 2 (1/2) pumps. Then, one pump was made unavailable in the SPAR model, so the SLC only has one pump available. If the plant had been designed with just one pump of SLC, then common- cause failure (CCF) would not be postulated for this pump. For this reason, the CCF contribution was also removed for the components of each system whose redundancy was reduced.

Also, using this same example, if the plant had been designed with just one pump (train) of SLC, then this train might have been designed, operated, and maintained to achieve a higher reliability than that associated with the train remaining after one pump was made unavailable in the SPAR model. However, for illustrating the current implementation of the SFC, it is assumed that the reliability of that remaining train after one pump was made unavailable stays constant in the calculations.

A.1.1 Evaluations for the BWR Plant for the Current Implementation of the SFC

The BWR/4 with a Mark I containment selected for the evaluations is the commonest type of BWR in the United States. Most of them have Mark I containments. In general, the BWR chosen is representative of plants that are designed with two independent high pressure injection systems (High Pressure Coolant Injection (HPCI) and Reactor Core Isolation Cooling (RCIC)). The associated pumps are each powered by a steam-driven turbine. These plants also have a multiloop core spray system and a multimode residual- heat removal system that can be aligned for low-pressure coolant injection, shutdown cooling, suppression-pool cooling, and containment spray function. In particular, the chosen BWR represent plants with four core spray pumps, and four AC divisions per unit.

The original SPAR model for the BWR plant yielded a CDF = 1.19E-5/yr. However, four 18-inch lines would be required to successfully vent containment in an ATWS, but only a single 6-inch line for other accidents. The original SPAR model only credits one vent path for other accidents. This conservatism was removed from the model by requiring only one of the four 18-inch lines for successful venting in non-ATWS sequences. With this modification, the CDF is equal to 1.15E-5/yr. This is the base-case CDF used in this study. The results of each of the four types of calculations are described next.

A.1.1.1 Evaluations Type 1 for the BWR Plant for the Current Implementation of the SFC

The redundancy of each safety-related system (taking one system at a time) was removed, and the increase in CDF compared with the base case determined. That is, a safety-related system having two or more trains was changed to a single-train system; the updated CDF then was obtained. These calculations are conducted keeping the non-safety-related systems in the model.

The first step for this type of calculation, identifying which systems are safety-related, was carried out using the information contained in relevant documents, such as the BWR plant's notebook for the Significance Determination Process (SDP) and Individual Plant Examination (IPE), as well as the engineering judgment of the working team. The following systems of the selected BWR were identified as safety-related and are included in the SPAR model: High Pressure Coolant Injection (HPCI), Reactor Core Isolation Cooling (RCIC), Safety Relief Valves/Automatic Depressurization System (SRVs/ADS), Residual Heat Removal (RHR), Core Spray (CS), Standby Liquid Control (SLC), Containment Venting (CV), Control Rod Hydraulic System (CRD), High Pressure Service Water (HPSW), Reactor Building Closed Cooling Water (RBCCW), Emergency Service Water (ESW), AC Power, Emergency Diesel Generators (EDGs), and DC Power.

Table A.1 gives the results of the sensitivity calculations. Starting from the left side, the first column is the safety-related system that was evaluated, except for the bottom row that is the base case. The second column is the system's success criterion; in general, it is a function of the initiating event, but the criterion that appeared to be applicable to all initiating events was considered, except where noted. Given the system's success criterion, the third column is the number of components that were made unavailable in the SPAR model to reduce the system's redundancy. For example, the success criterion of Core Spray (CS) is 2/4 pumps, so two pumps were made unavailable, leaving just two to mitigate accidents. The fourth column is the point estimate CDF per year for each case. The systems in the table are sorted by descending CDF. The fifth column is the point estimate ΔCDF, i.e., sensitivity-case CDF minus base-case CDF, per year for each case. Finally, the sixth column is the point estimate ratio of the sensitivity-case CDF to the base-case CDF for each case.

Many of the values of CDF, ΔCDF, and ratio of the sensitivity-case CDF to the base-case CDF in this subsection are rounded to one significant decimal. This implies that for a given calculation, the ΔCDF may be greater than zero even if the CDF for one case appears to be the same as the CDF for the base case. For example, the Control Rod Hydraulic System (CRD) has a CDF in Table A.1 that is 1.2e-05/yr, which appears to be the same as the CDF for the base case. However, the ΔCDF for this system is 2.4e-07/yr because the CDF resulting from reducing the redundancy of the CRD is larger than the base-case CDF. For the same reason, the ratio of the sensitivity-case CDF to the base-case CDF may be somewhat larger than 1.0 even though the ratio shown in the tables is 1.0.

The HPCI and RCIC can be used to inject water to the vessel. However, since each of them is a single-train system, redundancy cannot be removed, so sensitivity evaluations were not carried out for these systems. Containment Venting (CV) has a success criteria of 4/4 venting paths after ATWS; since redundancy cannot be removed, evaluations were not carried out for this system either.

The following insights can be obtained from the results in Table A.1:

1. For the systems at the top of the table, such as the RHR, DC Power, and AC Power, removing redundancy causes a large increase in CDF. This can be seen, for example, with the ratios of the sensitivity-case CDF to the base-case CDF that are from about 100 to more than 300 for these three systems. They illustrate the extent to which the redundant design of safety-related systems has contributed to reducing the risk of a nuclear power plant (NPP). In discussions of possible changes to the single-failure criterion, it is useful to understand the positive impact that redundant system design has had on lowering risk.

2. For the systems at the bottom of the table, such as the CS, SLC, SRVs/ADS, and RBCCW, removing redundancy causes a negligible increase in CDF. This can be seen, for example, with the ratios of the sensitivity-case CDF to the base-case CDF that are about 1 for these four systems. These results illustrate the extent to which the redundant design of safety-related systems may be imposing unnecessary burden on the licensees. If a safety-related system is not risk (safety) significant, then the provisions of the SFC, including redundant design, may be unnecessarily burdensome.

   On the other hand, the findings in Table A.1 derive from an internal-events level-1 PRA model. Possibly redundancy may still be required to mitigate external events and/or protect from other events in addition to core damage, such as containment breach that usually is measured by parameters such as large early release frequency (LERF).

3. Three of the four systems that have the largest impact on CDF when their redundancy is removed, namely, DC Power, AC Power, and EDGs, are support systems. In other words, these systems do not directly mitigate an accident, but support those that directly do. Even though the initiating event contribution resulting from, for example, a loss of DC bus, is not included, these systems are risk significant.

   In general, for those support systems whose loss causes an initiating event, the impact on CDF is expected to be larger than that given in Table A.1.

Table A.1 BWR Plant - Evaluations Type 1 for the Current Implementation of the SFC

Safety-related system	Success criterion	Number of components made unavailable	Pt. Est. CDF /yr	Pt. Est. ΔCDF /yr	Ratio Case / Base case
Residual Heat Removal (RHR)	1/4 pumps	3 pumps	3.5e-03	3.5e-03	3.1e+02
DC Power	2/4 buses	2 buses	3.3e-03	3.3e-03	2.3e+02
AC Power	2/4 buses	2 buses	8.6e-04	8.5e-04	7.5e+01
Emergency Diesel Generators (EDGs)	1/4 EDGs	3 EDGs	6.8e-04	6.7e-04	5.9e+01
Emergency Service Water (ESW)	1/2 pumps	1 pump	1.4e-05	2.8e-06	1.2e+00
High Pressure Service Water (HPSW)	2/4 pumps	2 pumps	1.2e-05	4.6e-07	1.0e+00
Control Rod Hydraulic System (CRD)	1/2 pumps	1 pump	1.2e-05	2.4e-07	1.0e+00
Core Spray (CS)	2/4 pumps	2 pumps	1.2e-05	6.1e-08	1.0e+00
Standby Liquid Control (SLC)	1/2 pumps	1 pump	1.2e-05	1.8e-08	1.0e+00
Safety Relief Valves/Automatic Depressurization System (SRVs/ADS)	It varies[1]	Valves powered from one division[1]	1.2e-05	0.0e+00	1.0e+00
Reactor Building Closed Cooling Water (RBCCW)	1/2 pumps	1 pump	1.2e-05	0.0e+00	1.0e+00
Base case	Not applicable	Not applicable	1.2e-05	0.0e+00	1.0e+00

Note 1: Success criteria of this system depends on the initiating event. For the sensitivity case, the valves fed from one division of motive power were made unavailable.

A.1.1.2 Evaluations Type 2 for the BWR plant for the current implementation of the SFC

The redundancy of major functions (one at a time) was removed, and the increase in CDF was compared with the base case. For example, if a function uses several safety-related systems, and each system has two redundant trains, then each was changed to a single-train system; the updated CDF then was obtained. These calculations kept the non-safety-related systems in the model.

Four major functions to mitigate accidents were identified: Reactivity Control, Preserve RCS Integrity, Residual Heat Removal, and Containment Heat Removal. The systems used to fulfill each function were identified, and their redundancy was eliminated.

The function "Reactivity Control" is implemented using the Reactor Protection System (RPS), including the CRD, and the SLC. However, SPAR does not model the RPS in detail, and the CRD is modeled as an alternative means to inject water to the vessel, but not in its function to insert the control rods into the vessel. Therefore, the SLC is the only system that controls reactivity and whose redundancy is included in the SPAR model.

The function "Preserve RCS Integrity" was considered to be fulfilled by the SRVs/ADS because this system protects the RCS from pressure transients, such as the one resulting after an ATWS.

The function "Residual Heat Removal" was considered to be satisfied with the systems that provide coolant to the vessel, as well as the RHR in its modes of low pressure coolant injection (LPCI), shutdown cooling (SDC) and suppression pool cooling (SPC). Accordingly, the systems used by this function are SRVs/ADS, RHR, CS, CRD, and HPSW. The HPCI and RCIC can also inject water to the vessel. However, since each of them is a single-train system, redundancy cannot be removed, so they were not included in the evaluations. The SRVs/ADS can depressurize the RCS so the low-pressure system can provide makeup to the vessel. The CRD and HPSW also can provide makeup to the vessel.

The function "Containment Heat Removal" was considered to be satisfied by RHR in the SPC, SDC, or containment spray modes. CV was not included because, as explained above, no redundancy can be removed.

Table A.2 gives the results of the sensitivity calculations. Starting from the left side, the first column is the major function evaluated, except for the bottom row which is the plant's base case. The second column is the safety-related systems that have redundancy and are used by each function. The redundancy in each system was removed according to the system's success criterion and number of components that were made unavailable is indicated in Table's A.1's second and third columns, respectively. The third column of Table A.2 is the point estimate CDF per year for each case. The functions in the table are sorted by descending CDF. The fourth column is the point estimate ΔCDF, i.e., sensitivity-case CDF minus base-case CDF, per year for each case. Finally, the fifth column is the point estimate ratio of the sensitivity-case CDF to the base-case CDF for each case.

Table A.2 BWR Plant - Evaluations Type 2 for the Current Implementation of the SFC

Major function	Safety-related systems that have redundancy and that are used by function	Pt. Est. CDF /yr	Pt. Est. Delta CDF /yr	Ratio Case / Base case
Residual Heat Removal	SRVs/ADS, RHR, CS, CRD, and HPSW	3.8e-03	3.8e-03	3.3e+02
Containment Heat Removal	RHR	3.5e-03	3.5e-03	3.1e+02
Reactivity Control	SLC	1.2e-05	1.8e-08	1.0e+00
Preserve RCS Integrity	SRVs/ADS	1.1e-05	0.0e+00	1.0e+00

Base case	Not applicable	1.1e-05	0.0e+00	1.0e+00

The following insights are gained from the results in Table A.2:

- The CDF increases substantially when redundancy is removed for some functions, such as Residual Heat Removal and Containment Heat Removal. This increase is illustrated with the ratios of the sensitivity-case CDF to the base-case CDF that are about 330 and 310 for these two functions. The findings again highlight the extent to which the redundant design of safety-related systems has contributed to reducing the risk of an NPP.

- For the two other functions, Reactivity Control and Preserve RCS Integrity, removing redundancy causes a negligible increase in CDF. This can be seen, for example, with the ratios of the sensitivity-case CDF to the base-case CDF that are about 1 for these functions. As discussed previously, the function Reactivity Control is represented only by the SLC that, in turn, is only used to mitigate an ATWS. Similarly, if the valves of the SRVs/ADS that are associated with one division of motive power are made unavailable, it compromises only the function of protecting from pressure transients after an ATWS. Since the ATWS has a low frequency of occurrence, the reduction in redundancy of the SLC (function Reactivity Control) and SRVs/ADS (function Preserve RCS Integrity) gives a negligible increase in CDF.

  These results also demonstrate the extent to which the redundant design of safety-related systems may be imposing unnecessary burden on the licensees.

A.1.1.3 Evaluations Type 3 for the BWR plant for the current implementation of the SFC

These are the same evaluations as for Type 1 (Subsection A.1.1.1), but credit is not given to the non-safety-related systems in the model. In this way, the impact on CDF due to removing redundancy of the safety-related systems can be obtained without the mitigating contribution of the non-safety-related systems.

The first step in carrying out these calculations was to identify non-safety-related systems that directly mitigate accidents (usually called front-line systems); they were the Power Conversion System (feedwater cycle), and Condensate System. The second step was to obtain an updated base-case CDF without their contribution. This CDF is 2.7E-05/yr.

Table A.3 shows the results of the sensitivity calculations. Starting from the left side, the first column is the safety-related system evaluated, except for the bottom row which is the plant's base case. The redundancy in each system was removed according to the system's success criterion and number of components that were made unavailable, indicated in Table's A.1's second and third columns, respectively. The second column of Table A.3 is the point estimate CDF per year for each case. The systems are sorted by descending CDF. The third column is the point estimate ΔCDF, i.e., sensitivity-case CDF minus base-case CDF, per year for each case. Finally, the fourth column is the point estimate ratio of the sensitivity-case CDF to the base-case CDF for each case.

Without the contribution of the non-safety-related systems, the CDF is 2.7E-05/yr, and the original one is 1.2e-05/yr. The difference between these two values is 1.6e-05/yr, and their ratio is about 2.4. This means that non-safety-related systems make a significant contribution to reducing the CDF (risk) of the plant.

Table A.3 BWR plant - Evaluations Type 3 for the Current Implementation of the SFC

Safety-related System	Pt. Est. CDF /yr	Pt. Est. Delta CDF /yr	Ratio Case / Base case
Residual Heat Removal (RHR)	3.5e-03	3.5e-03	1.3e+02
DC Power	3.3e-03	3.3e-03	1.2e+02
AC Power	8.3e-04	8.1e-04	3.1e+01
Emergency Diesel Generators (EDGs)	7.0e-04	6.7e-04	2.6e+01
Emergency Service Water (ESW)	3.0e-05	2.8e-06	1.1e+00
High Pressure Service Water (HPSW)	2.8e-05	8.8e-07	1.0e+00
Control Rod Hydraulic System (CRD)	2.7e-05	2.7e-07	1.0e+00
Core Spray (CS)	2.7e-05	9.6e-08	1.0e+00
Standby Liquid Control (SLC)	2.7e-05	2.6e-08	1.0e+00
Safety Relief Valves/Automatic Depressurization System (SRVs/ADS)	2.7e-05	0.0e+00	1.0e+00
Reactor Building Closed Cooling Water (RBCCW)	2.7e-05	0.0e+00	1.0e+00
Base case	2.7e-05	0.0e+00	1.0e+00

A.1.1.4 Evaluations Type 4 for the BWR Plant for the Current Implementation of the SFC

These are the same evaluations as for Type 2 (Subsection A.1.1.2), but credit is not given to the non-safety-related systems in the model. In this way, the impact on CDF due to removing redundancy of the major functions can be obtained without the mitigating contribution of the non-safety-related systems.

The updated CDF without the contribution of the non-safety-related systems of 2.7e-05 / year, described in Subsection A.1.1.3, is applicable to these evaluations.

Table A.4 gives the results of the sensitivity calculations. Starting from the left side, the first column is the major function evaluated, except for the bottom row which is the base case. The second column is the safety-related systems that have redundancy and are used by each function. The redundancy in each system was removed according to the system's success criterion and number of components that were made unavailable, indicated in Table's A.1's second and third columns, respectively. The third column of Table A.4 is the point estimate CDF per year for each case. The functions in the table are sorted by descending CDF. The fourth column is the point estimate ΔCDF, i.e., sensitivity-case CDF minus base-case CDF, per year for each case. Finally, the fifth column is the point estimate ratio of the sensitivity-case CDF to the base-case CDF for each case.

Table A.4 BWR Plant - Evaluations Type 4 for the Current Implementation of the SFC

Major function	Safety-related systems that have redundancy and that are used by function	Pt. Est. CDF / year	Pt. Est. Delta CDF / year	Ratio Case / Base case
Residual Heat Removal	SRVs/ADS, RHR, CS, CRD, and HPSW	3.8e-03	3.8e-03	1.4e+02
Containment Heat Removal	RHR	3.5e-03	3.5e-03	1.3e+02
Reactivity Control	SLC	2.7e-05	2.6e-08	1.0e+00
Preserve RCS Integrity	SRVs/ADS	2.7e-05	0.0e+00	1.0e+00
Base case	Not applicable	2.7e-05	0.0e+00	1.0e+00

The insights obtained from Table A.4 are the same as those discussed in Subsections A.1.1.2 and A.1.1.3.

A.1.2 Evaluations for a PWR for the Current Implementation of the SFC

The PWR selected for evaluations is a Westinghouse four-loop plant with large dry containment; these are the commonest type of PWR in the United States. Containment cooling is assumed not to be required for preventing core damage. This assumption was used in developing the SDP notebooks for this type of plant.

The SPAR model for the PWR plant yielded a CDF = 7.72e-5/yr. The results of each of the four types of calculations are described next.

A.1.2.1 Evaluations Type 1 for the PWR plant for the Current Implementation of the SFC

The redundancy of each safety-related system (one system at a time) was removed, and the increase in CDF compared with the base case was determined. That is, a safety-related system having two or more trains was changed to a single-train system; the updated CDF then was obtained. These calculations retained the non-safety-related systems in the model.

The first step for this type of calculation is to identify which systems are safety-related using information contained in relevant documents, such as the PWR plant's SDP notebook and IPE, as well as the engineering judgment of the working team. The following systems of the PWR plant were identified as safety-related and are included in the SPAR model: Accumulators (ACS), Auxiliary Feedwater (AFW), Chemical and Volume Control System (CVCS), pressurizer PORVs, pressurizer safety valves, Residual Heat Removal (RHR), Safety Injection System (SI), Component Cooling Water (CCW), Essential Service Water System (ESW), AC Power, Emergency Diesel Generators (EDGs), and DC Power.

Table A.5 gives the results of the sensitivity calculations. Starting from the left side, the first column is the safety-related system that was evaluated, except for the bottom row which is the plant's base case. The second column is the system's success criterion; in general, this criterion is a function of the initiating event, but the criterion that appeared to be applicable to all initiating events was considered, except where noted. Given the system's success criterion, the third column is the number of components that were made unavailable in the SPAR model to remove the redundancy of the system, as described for the BWR plant. The fourth column is the point estimate CDF per year for each case, sorted by descending CDF. The fifth

column is the point estimate ΔCDF, i.e., sensitivity-case CDF minus base-case CDF, per year for each case. Finally, the sixth column is the point estimate ratio of the sensitivity-case CDF to the base-case CDF for each case.

The AFW has three pumps, two motor-driven, and one turbine-driven. Since the latter is the only one that is available in station blackout scenarios, this pump was not removed in the sensitivity evaluations. The success criteria of the AFW was considered to be 1/2 motor-driven pumps.

The Chemical and Volume Control System (CVCS) has two centrifugal charging pumps (CCPs) and one positive displacement pump (PDP). Any of the three pumps can provide injection to the seals of the reactor coolant pumps (RCPs). On the other hand, only the CCPs are credited for injection to the vessel. Accordingly, the success criteria for these pumps is 1/3 pumps for RCP seal injection and 1/2 CCPs for injection to the vessel. Table A.5 presents an "overall" success criteria for 1/3 pumps. The sensitivity evaluation for these pumps was carried out by removing one CCP and the PDP; the remaining CCP can be used for RCP seal injection and injection to the vessel.

The CVCS also has two boric-acid transfer pumps; however, the SPAR model does not include them.

The success criteria of the pressurizer safety valves and PORVs after an ATWS is 3/3 pressurizer safety valves and 2/2 PORVs. In addition, the success criteria of the pressurizer PORVs for feed-and-bleed is 2/2 PORVs after transients. Since the success criteria of the pressurizer safety valves and PORVs requires using all these valves, they were not considered to have redundancy. Therefore, no sensitivity evaluations removing redundancy were carried out for these valves.

The plant has four vital 125-volt DC buses. The loss of either one of two buses triggers an initiating event, and the loss of either one of the other two buses does not. For the purpose of the sensitivity evaluations for this plant, the latter two were considered.

Each steam generator (SG) has 1 atmospheric relief valve (ARV) and 5 safety valves. The SPAR model does not include the latter.

The following insights can be obtained from the results in Table A.5:

1. For the systems at the top of the table, such as the CCW and AC Power, removing redundancy results in a large increase in CDF. This can be seen, for example, with the ratios of the sensitivity-case CDF to the base-case CDF that are about 10 or more for these two systems. These results illustrate how much the redundant design of safety-related systems has contributed to reducing the risk of a nuclear power plant.

2. For the systems at the bottom of the table, such as the Accumulators and ARVs, there is a negligible change in the CDF after removing redundancy. Accordingly, these are systems that may be imposing unnecessary burden on the licensees. If a safety-related system is not risk (safety) significant, then the provisions of the SFC, including redundant design, may be inappropriately heavy.

3. When their redundancy is removed, the five systems with the largest impact on CDF are support systems, namely, CCW, AC Power, EDGs, ESW, and DC Power. In other words, these are systems that do not directly mitigate an accident, but support those that directly do. Even though the

initiating event's contribution due to, for example, a loss of CCW, is not included in these evaluations, these systems are risk significant.

In general, for those support systems whose loss causes an initiating event, the impact on CDF is expected to be larger than the one in Table A.5.

Table A.5 PWR Plant - Evaluations Type 1 for the Current Implementation of the SFC

Safety-related System	Success criteria	Number of components unavailable	Pt. Est. CDF / year	Pt. Est. Delta CDF / year	Ratio Case / Base case
Component Cooling Water (CCW)	1/4 pumps	3 pumps	1.1e-03	9.9e-04	1.4e+01
AC Power	1/2 buses	1 bus	7.9e-04	7.1e-04	1.0e+01
Emergency Diesel Generators (EDGs)	1/2 EDGs	1 EDG	3.1e-04	2.4e-04	4.1e+00
Essential Service Water System (ESW)	1/2 pumps	1 pump	3.5e-04	2.7e-04	4.5e+00
DC Power	1/2 buses	1 bus	6.2e-04	5.4e-04	8.1e+00
Auxiliary Feedwater (AFW)	1/2 motor-driven pumps	1 pump	8.8e-05	1.1e-05	1.1e+00
Residual Heat Removal (RHR)	1/2 pumps	1 pump	1.9e-04	1.1e-04	2.4e+00
Chemical and Volume Control System (CVCS)	1/3 pumps	2 pumps	1.5e-04	6.8e-05	1.9e+00
Safety Injection System (SI)	1/2 pumps	1 pump	8.2e-05	5.2e-06	1.1e+00
Accumulators (ACS)	2/4 accumulators	2 accumulators	8.2e-05	5.0e-06	1.1e+00
Secondary PORVs (ARVs)	1/4 valves	3 valves	7.7e-05	0.0e+00	1.0e+00
Base case	NA	NA	7.7e-05	0.0e+00	1.0e+00

A.1.2.2 Evaluations Type 2 for the PWR plant for the Current Implementation of the SFC

The redundancy of major functions was removed, one function at a time, and the increase in CDF compared with the base case. For example, if a function uses several safety-related systems, and each system has two redundant trains, then each system in this function was changed to a single-train system; the updated CDF then was obtained. The non-safety-related systems were retained in the model.

Four major functions to mitigate accidents were identified: Reactivity Control, Preserve RCS Integrity, Residual Heat Removal, and Containment Heat Removal. The systems used to fulfill each function were identified, and their redundancy was eliminated, as described below.

The function "Reactivity Control" is implemented using the Reactor Protection System (RPS). If the RPS fails to scram the reactor, then the operators at the plant can start emergency boration using the CCPs and the boric- acid transfer pumps. However, the SPAR model does not model the redundancy in the RPS. In addition, the SPAR models emergency boration by an operator's action, so this does not include the CCPs and the boric- acid transfer pumps. Hence, no redundancy could be removed for the function "Reactivity Control."

The function "Preserve RCS Integrity" was considered to be satisfied by the pressurizer safety valves and PORVs because they protect the RCS from pressure transients, such as that after an ATWS. Since the success criteria of the pressurizer safety valves and PORVs requires using all these valves, it was considered that they do not have redundancy. Accordingly, no sensitivity evaluations involving removing redundancy were carried out for the function "Preserve RCS Integrity."

For Westinghouse plants with large dry containment, containment cooling is assumed not to be required for preventing core damage. Therefore, the function "Containment Heat Removal" was not evaluated.

The function "Residual Heat Removal" was considered to be accomplished by the AFW, primary PORVs, secondary PORVs (ARVs), CVCS, SI, and RHR. Again, no redundancy was removed for the primary PORVs because their success criteria require using all of them. Hence, redundancy was removed for the systems AFW, ARVs, CVCS, SI, and RHR. The redundancy in each system was removed according to the system's success criterion and number of components that were made unavailable, indicated in Table's A.5's second and third columns, respectively. The resulting point estimate CDF is 2.9E-4 per year. The point estimate ΔCDF, i.e., sensitivity-case CDF minus base-case CDF, is 2.1E-4 per year. Finally, the point estimate ratio of the sensitivity-case CDF to the base-case CDF is 3.7.

The CDF increases substantially when redundancy is removed for the function Residual Heat Removal, as illustrated by the ratio of the sensitivity-case CDF to the base-case CDF that is 3.7. This result illustrates the extent to which the redundant design of safety-related systems has contributed to reducing the risk of a nuclear power plant.

A.1.2.3 Evaluations Type 3 for the PWR Plant for the Current Implementation of the SFC

These are the same evaluations as for Type 1 (Subsection A.1.2.1), but they did not give credit to the non-safety-related systems. In this way, the impact on CDF due to removing redundancy of the safety-related systems can be obtained without the mitigating contribution of the non-safety-related systems.

The first step was to identify non-safety-related systems that directly mitigate accidents (usually called front-line systems); they were the Condensate and Main Feedwater (MFW) systems. The Condensate system was not found in the SPAR model, so the only non-safety-related system made unavailable was the MFW. The second step was to obtain an updated base-case CDF without the contribution of the MFW. This CDF is 7.78e-05 / year.

Table A.6 gives the results of the sensitivity calculations. Starting from the left side of the table, the first column is the safety-related system evaluated, except for the bottom row which is the base case of the plant. The redundancy in each system was removed according to the system's success criterion and number of components that were made unavailable, indicated in Table's A.5s second and third columns, respectively. The second column of Table A.6 is the point estimate CDF per year for each case. The systems in the table are sorted by descending CDF. The third column is the point estimate ΔCDF, i.e., sensitivity-case CDF minus base-case CDF, per year for each case. Finally, the fourth column is the point estimate ratio of the sensitivity-case CDF to the base-case CDF for each case.

Table A.6 PWR plant - Evaluations Type 3 for the Current Implementation of the SFC

Safety-related System	Pt. Est. CDF /yr	Pt. Est. Delta CDF /yr	Ratio Case / Base case
Component Cooling Water (CCW)	1.1e-03	9.9e-04	1.4e+01
AC Power	8.1e-04	7.3e-04	1.0e+01
Emergency Diesel Generators (EDGs)	3.1e-04	2.4e-04	4.0e+00
Essential Service Water System (ESW)	4.3e-04	3.6e-04	5.6e+00
DC Power	7.4e-04	6.7e-04	9.6e+00
Auxiliary Feedwater (AFW)	9.6e-05	1.8e-05	1.2e+00
Residual Heat Removal (RHR)	1.9e-04	1.1e-04	2.4e+00
Chemical and Volume Control System (CVCS)	3.5e-04	2.7e-04	4.5e+00
Safety Injection System (SI)	8.3e-05	5.2e-06	1.1e+00
Accumulators (ACS)	8.3e-05	5.0e-06	1.1e+00
Secondary PORVs (ARVs)	7.8e-05	0.0e+00	1.0e+00
Base case	7.8e-05	0.0e+00	1.0e+00

The following insights were gained from the results in Table A.6:

- The CDF without the mitigating contribution of the non-safety-related system MFW is 7.78e-05/yr. The original base-case CDF is 7.72e-05/yr. The difference between these two values is 6.0e-07/yr, and their ratio is about 1, so the contribution of the MFW in reducing the CDF (risk) is relatively small.

- The ordering of the systems in Table A.6 is the same as the ordering in Table A.5. On the other hand, the impact on CDF of removing the redundancy of the motor-driven pumps of AFW increases when the MFW is not available, from a ratio of base-case CDF to sensitivity-case CDF of 1.1 (from table A.5) when MFW is available, to a ratio of 1.2 when it is not (Table A.6). This is because there are fewer pumps (redundancy) available to provide feedwater to the steam generators.

A.1.2.4 Evaluations Type 4 for the PWR Plant for the Current Implementation of the SFC

These are the same evaluations as for Type 2 (Subsection A.1.2.2), but credit is not given to the non-safety-related systems Hence, the impact on CDF due to removing redundancy of the major functions without the mitigating contribution of the non-safety-related systems is obtained.

The updated CDF without the mitigating contribution of the non-safety-related system MFW of 8.03e-05/yr, described in Subsection A.1.2.3, is applicable to these evaluations.

As before, four major functions to mitigate accidents were identified: Reactivity Control, Preserve RCS Integrity, Residual Heat Removal, and Containment Heat Removal. However, as discussed in Subsection A.1.2.2, "Evaluations Type 2 for the PWR plant for the current implementation of the SFC," no redundancy

could be removed for the functions "Reactivity Control" and "Preserve RCS Integrity." In addition, for Westinghouse plants with large dry containment, containment cooling is assumed not to be required for preventing core damage. Therefore, the function "Containment Heat Removal" was not evaluated.

The function "Residual Heat Removal" was considered to be accomplished by the AFW, primary PORVs, secondary PORVs (ARVs), CVCS, SI, and RHR. Again, no redundancy was removed for the primary PORVs because their success criteria require using all of them. Hence, redundancy was removed for each of the systems AFW, ARVs, CVCS, SI, and RHR according to the system's success criterion and number of components that were made unavailable, indicated in Table's A.5s second and third columns, respectively. The resulting point estimate CDF is 3.0E-04 per year. The point estimate ΔCDF, i.e., sensitivity-case CDF minus base-case CDF, is 2.2e-04 per year. Finally, the point estimate ratio of the sensitivity-case CDF to the base-case CDF is 3.8.

The CDF increases substantially after removing redundancy for the function Residual Heat Removal, as illustrated with the ratio of the sensitivity-case CDF to the base-case CDF, that is 3.8. This finding verifies the important contribution made by the redundant design of safety-related systems in reducing the risk of a nuclear power plant.

The impact on CDF of removing the redundancy of the function Residual Heat Removal increases when MFW is not available from a ratio of base-case CDF to sensitivity-case CDF of 3.7 when MFW is available, to a ratio of 3.8 when it is not. This increase is because fewer pumps (redundancy) are available to supply feedwater to the steam generators.

Appendix B
Previous Reviews of the Single-Failure Criterion

SECY-77-439 [USNRC, 1977]

In SECY-77-439, the NRC Office of Nuclear Reactor Regulation prepared a paper for the Commission on the subject of the SFC. The purpose of the paper was "To inform the Commission of the present status and future use of the Single-Failure Criterion as a tool in the reactor safety review process." The paper reviews the SFC concept, its implementation in regulatory and other documents, discusses its application to several safety functions and safety systems, presents a number of problems associated with its application, and reviews the Reactor Safety Study (RSS) [WASH-1400] from the point of view of the impact of redundant safety systems.

The SFC is viewed in this paper as a tool to advance high system reliability through the provision of redundancy in systems that are designed to perform a safety function. The paper concludes that "...the Single Failure-Criterion has served well in its use as a licensing review tool to assure reliable systems as one element of the defense-in-depth approach to reactor safety." In its review of the numerical assessments of the RSS, the author of the paper concludes that "...component and system redundancy, has made an important and necessary contribution to the overall reliability of nuclear power plant systems..." The RSS results demonstrated that as a result of adequate system redundancy, other issues related to system reliability were important contributors to accident sequences leading to core meltdown. Common cause failure, system dependencies, operator error, downtimes resulting from test, repair and maintenance, were judged to be important by the RSB. These issues are not addressed by the SFC and, as discussed previously, they were the subject of significant staff regulatory actions. The need for an integrated systems approach to these issues is noted.

The issues of single passive failures in fluid systems is addressed. The paper notes that on the basis of licensing review experience it was judged in most cases that the probability of passive failures in fluid systems was sufficiently small that such failures need not be assumed as a source of single failure, although in a small number cases it has been imposed. The issue was still under study.

The paper recognizes the limitations of the SFC from the point of view that it does not address important issues related to system reliability. The paper expressed the view that "...the Single-Failure Criterion should continue to be applied subject to resolution of specific problem areas currently defined and under study[11], pending any long-term wide-scale incorporation of reliability and risk assessment methodology into the licensing process."

[11]These refer to issues that NRC staff raised with respect to a implementation of the SFC: While passive failures in fluid systems were judged of sufficiently small probability so that they could be ignored as an additional failure to the initial failure, some such failures were imposed (long term LOCA recovery). Passive-type valve failure had been observed, but changes in safety criteria were judged not warranted. However, these failure modes were being studied. Consideration was being given to human error as the source of single failure. NRC activities were being initiated to study the role of human reliability as a factor in safety.

ACRS Report: NUREG-1755 [Sorenson, 2002]

This report is an examination of Appendices A and B of 10 CFR 50 from the point of view of identification of risk-informed change to their provisions. Several options for risk-informing the General Design Criteria are discussed, some of which relate to the SFC.

The author recognizes that the objective of the SFC is to help achieve high safety system reliability. One option that is discussed proposes that PRA methods be used to establish quantitative reliability provisions for safety functions. The designer could use redundancy as one design tool to achieve the required reliability. However, the safety system design would not be required to satisfy the SFC as long as the reliability goal is achieved.

Two additional risk-based options are discussed. A second option proposed for risk-informing the GDCs is that they address only the risk significant systems, structures and components, where the risk significance would be evaluated with respect to CDF and LERF risk metrics. A third option that is discussed proposes that the GDCs be replaced with "high-level regulatory objectives (such as the Commission's safety goals) and risk acceptance criteria." While these options for change to the GDCs have implications with respect to the SFC, the implications are not discussed in the report.