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

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

W200300050

OAR in ADAMS? (Y or N) Y ADAMS ACCESSION NO.: PGK ML051950610 TEMPLATE NO. SECY-012
Publicly Available? (Y or N) N DATE OF RELEASE TO PUBLIC: _____ SENSITIVE? N
To receive a copy of this document, indicate in the box: "**C**" = Copy without attachment/enclosure "**E**" = Copy with attachment/enclosure "**N**" = No copy
*See previous concurrence.

OFFICE	*RES/PRAB		*RES/PRAB		*RES/PRAB		*RES/PRAB		*RES/DRAA	
NAME	DWatkins		JLane		HHamzehee		DLew		CAder	
DATE	7/ /05		7/ /05		7/ /05		7/ /05		7/ /05	
OFFICE	*TECH ED		*RES/DSARE		*RES/DET		*D:NSIR		*D:NRR	
NAME	PGarrity		FEltawila		RBarrett		RZimmerman		JDyer	
DATE	7/13/05		7/13/05		7/6/05		7/1/05		7/5/05	
OFFICE	*NMSS		*OGC		*OCFO		D:RES		EDO	
NAME	JStrosnider		STreby		JFunches		CPaperiello		LReyes: **MJV Acting For**	
DATE	7/11/05		7/12/05		7/5/05		7/15 /05		8/2/05	

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: (15) Permit removal of sufficiently unlikely, non-risk-significant single-failure sequences from the design basis. (16) 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: (17) Alternative 2a proposes that redundant safety-related trains may be removed from service. The system would then comprise a single train. (18) Alternative 2b proposes that one train would remain safety-related, but the redundant trains could be reclassified as non-safety-related. (19) 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: (20) top-level risk targets for CDF and LERF (21) lower-level functional reliability targets commensurate with challenge frequency (22) 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.**	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."	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.	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: **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.**	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.	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.	Performance Monitoring: Monitoring would confirm that assigned performance targets are actually met.

Attachment 2