UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
WASHINGTON, DC 20555 - 0001

June 10, 2005

The Honorable Nils J. Diaz
Chairman
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

SUBJECT: DRAFT COMMISSION PAPER ON "RISK-INFORMED ALTERNATIVES TO THE SINGLE FAILURE CRITERION"

Dear Chairman Diaz:

During the 523rd meeting of the Advisory Committee on Reactor Safeguards, June 1-3, 2005, we reviewed the draft Commission Paper, "Risk-Informed Alternatives to the Single Failure Criterion." During our review, we had the benefit of discussions with the NRC staff and the documents referenced.

CONCLUSIONS AND RECOMMENDATIONS

1. The staff has conducted a useful review of the role of the single failure criterion in the current regulatory system, defined desirable attributes of risk-informed alternatives, and developed some potential alternatives to the single failure criterion.

2. We concur with the staff that it is premature to select any particular alternative at the present time.

3. Additional input from stakeholders should be sought to determine if there is sufficient benefit to justify the resources that will be required to proceed with development of a risk–informed alternative.

4. We concur with the staff that any follow-up activities to risk-inform the single failure criteria should be included and prioritized in the program plan being developed for a risk-informed, performance-based revision to 10 CFR Part 50.

DISCUSSION

In response to a Staff Requirements Memorandum (SRM), dated March 31, 2003, the staff and its contractors have prepared a report, "Technical Work to Support Evaluation of a Broader Change to the Single Failure Criterion," that examines risk-informed alternatives to the single failure criterion. Although the Commission directive was associated with General Design Criterion (GDC) 35 and the emergency core cooling system (ECCS) acceptance criteria, the staff has examined alternatives to the single failure criterion that could apply to all safety (and non-safety) functions of the plant.

Single failure criterion requirements are part of the GDC. They are also addressed in the guidance for the analysis of some of the Design-Basis Accidents (DBAs) in Chapter 15 of Regulatory Guide 1.70 and the Standard Review Plan. The intent of the single failure criterion requirements is to achieve high safety system reliability through redundancy. The search for the most limiting single failure leads to a systematic study of design weaknesses and has generally resulted in robust designs.

However, it is evident from operating experience and risk analyses that the single failure criterion has not always succeeded in assuring adequate reliability. Common-cause failures, multiple independent failures, failures of support systems, multiple failures caused by spatial dependencies, and multiple human errors may not be mitigated by redundant system design alone. The NRC has imposed additional requirements for diversity and redundancy to increase system reliabilities through the station blackout rule, the anticipated transient without scram rule, and the post-Three Mile Island accident requirement to increase the availability of the auxiliary feedwater systems of pressurized water reactors.

The requirements for redundancy imposed by the single failure criterion may result in unnecessary burden with little risk benefit. Studies carried out by the staff with the Standardized Plant Analysis Risk (SPAR) models to examine the effect of system and functional redundancy on core damage frequency (CDF) showed that the impact of the redundancy of different systems on CDF varied by two orders of magnitude. Reducing redundancy in some cases led to large increases in CDF, and in others to virtually no change in CDF. Similarly, the single failure requirements in the analysis of some DBAs sometimes focus attention on events with very low frequency that may in fact have low risk significance.

Currently, changes in single failure criterion requirements are considered in the context of specific licensing issues as they arise (e.g., large-break loss-of-coolant accident (LBLOCA) redefinition). One of the alternatives the staff has considered is to continue with this current approach, which focuses resources on the most important issues. In the draft Commission Paper, this is referred to as the “baseline alternative.” A related topic, the LOCA/loss-of-offsite power requirement, is already being dealt with as a separate issue.

The staff’s Alternative 1 attempts to risk-inform DBA analyses. Sequence frequencies, obtained using probabilistic risk assessment (PRA) models and data, would be used to determine the failure events to be postulated in DBA analyses. Both removals and additions to the current set of design-basis sequences would be possible. Failure events associated with sequences with sufficiently low frequency would no longer have to be postulated. Eliminated failure events could include both initiating events and the assumed single failure postulated in current DBA analyses. The licensee would be required to demonstrate using the plant PRA that the collective frequency of design-basis sequences excluded from DBA analyses is small. Plant changes proposed based on Alternative 1 would have to be consistent with Regulatory Guide 1.174 guidelines.

Alternative 2 would risk-inform the application of the single failure criterion to safety systems based on their safety significance. A risk-informed process would be defined to categorize the safety significance of all plant systems. Taking advantage of current categorization processes, this alternative would expand on the 10 CFR 50.69 approach. Various reductions in the requirements for redundancy for RISC–3 (safety-related, low safety significance) components would be considered.

Alternative 3 is a more systematic approach to evaluating reliability requirements that recognizes the importance of diversity as well as redundancy in assuring high reliability. It would provide quantitative measures of the reliability that has been achieved. More redundancy and diversity would be required in response to more frequent events, and less in response to infrequent events. Licensees would choose target reliability values for each safety function (typically at the train level), and would show that these targets satisfy the functional objectives and the top-level objectives (CDF and large early release frequency). Each safety function would be analyzed using the PRA to show that the function-level reliability target is met. Methods would have to be developed to define the concept of "noncompliance" with set reliability targets. This is a generic challenge for performance-based requirements.

The resources required for Alternatives 1, 2, and 3 are more substantial than proceeding with the current approach, but more systematic approaches could lead to a greater coherency in requirements. As the staff has noted, other alternatives are possible, and not all the technical and implementation difficulties with these alternatives have been addressed. For example, Alternatives 2 and 3, which focus on the role of the single failure criterion in increasing reliability, may have to address the resulting impact on the role of the single failure criterion in DBAs. Thus Alternatives 2 and 3 may not be independent of Alternative 1 or some variation of it. Because of the preliminary nature of the work, the staff does not recommend any particular alternative at the present time. We concur with the staff that such a selection would be premature.

The staff has carried out this effort in response to the SRM without sufficient input from stakeholders. Before further work is performed, the staff should seek additional stakeholder input to determine if there is sufficient benefit to justify the resources that will be needed to proceed with development beyond that needed for the baseline alternative. As directed in the SRM dated May 9, 2005, the Office of Nuclear Regulatory Research will 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. We agree with the staff that any follow-up activities to risk-inform the single failure criterion should be included and prioritized in this program plan.

Sincerely,

/***RA***/

Graham B. Wallis
Chairman

REFERENCES:

1. Memorandum dated May 19, 2005, from Charles E. Ader, Director, Division of Risk Analysis and Applications, RES, to John T. Larkins, Executive Director, ACRS, Subject: Transmittal of Draft Commission Paper Entitled, “Risk-Informed Alternatives to the Single Failure Criterion,” (Pre-Decisional For Internal ACRS Use Only).

2. Memorandum dated May 6, 2005, from Charles E. Ader, RES, to John T. Larkins, Executive Director, ACRS, Subject: Transmittal of Draft Report Entitled, “Technical Work to Support Evaluation of Broader Change to the Single Failure Criterion,” (Pre-Decisional For Internal ACRS Use Only).

3. Staff Requirements Memorandum dated March 31, 2003, from Annette L. Vietti-Cook, Secretary, to William D. Travers, EDO, Subject: Staff Requirements - SECY-02-057 - 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).”

4. Regulatory Guide 1.174, Revision 1, November 2002, An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis.

5. 10 CFR § 50.69 Risk-Informed categorization and treatment of structures, systems and components for nuclear power reactors.

6. Memorandum to L. Reyes, EDO, from A. Vietti-Cook, SECY, dated May 9, 2005, Subject: Staff Requirements - Briefing on RES Programs, Performance, and Plans, 9:30 am, Tuesday, April 5, 2005, Commissioners’ Conference Room, One White Flint North, Rockville, Maryland (Open to Public Attendance) [Refer to: M050405]