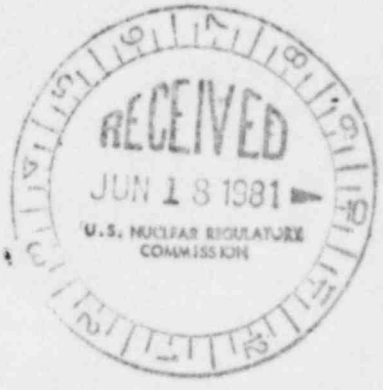
US Department of Energy
ARGONNE NATIONAL LABORATORY
9700 South Cass Avenue, Argonne, Illinois 60439
Telephone 312/972-4639

47-1345

May 27, 1981



Dr. David Okrent
Advisory Committee on Reactor Safeguards
Energy and Kinetics Department
5532 Boelter Hall
School of Engineering & Applied Science
University of California
Los Angeles, California 90024

Dear Dr. Okrent:

Subject: Revision of General Design Criteria

As a general approach to the revision of the General Design Criteria for Light Water Reactors, the following is recommended:

1. Review each of the existing criteria listed in Appendix A of 10CFR50.

2. Review the recommendations which have been issued since the TMI-2 accident and revise or supplement the existing criteria.

3. Review the unresolved safety issues and decide whether the general design criteria can be modified prior to complete resolution of an issue.

4. Review the regulatory guides and branch technical positions and decide whether these documents contain recommendations that should be included in the general design criteria.

5. Review the general design criteria used in other countries, compare them with US criteria, and decide whether US criteria should be modified.

6. Rulemaking hearings scheduled for the near future on:
   a. Emergency planning
   b. Hydrogen Control
   c. Siting
   d. Degraded core cooling
   e. Minimum engineered safety features

   will affect the General Design Criteria.

Decide whether:

(1) To issue new criteria prior to the rulemaking hearings or

(2) To wait until the rulemaking hearings are completed before issuing a complete set of revised criteria.

7. Coordinate the activity of revising the LWR General Design Criteria with the activity of the ACRS Subcommittee on Advanced Reactors which is reviewing general design criteria for Liquid Metal Fast Breeder Reactors.

8. Establish a plan to obtain early industry input into the revised criteria before they are issued in final form.

With respect to item 6 above, I would not recommend delaying the issuance of revised general design criteria by waiting for rulemakings to be completed.

The following specific recommendations for revision to the general design criteria are based on recommendations transmitted to you by W. W. Libarkin, ACRS, by memorandum dated January 26, 1981 and modified by me:

I. A natural circulation dedicated residual heat removal system which is independent of the secondary system shall be provided. This system shall be designed 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 design conditions of the reactor coolant boundary are not exceeded. The system shall be capable of operation over the full range of primary system temperature and pressure. It shall keep the reactor core within specified limits for at least 24 hours without replenishment of consumable materials (fuel, water, lubricants, etc.) and there shall be sufficient consumable material on site for at least seven days of continuous operation.

The backup residual heat removal system shall be dedicated to this purpose only and shall have its own dc power supplies and shall be independent of all ac power and other plant systems. It shall be protected against impacts from both externally and internally generated missiles as well as from the effects of crashing aircraft. The backup system shall be spacially and systemically separated from other heat removal systems so that no single credible event could incapacitate all systems. It shall have such redundancy in components and features, and suitable interconnections, leak detection and isolation capabilities to assure that the system's function can be accomplished assuming a single failure of passive or active components and multiple active component failures for those credible events where common mode failure could result from adverse environmental conditions, extreme plant conditions, or maintenance errors of a generic nature.

The dedicated residual heat removal system shall have components arranged in such a way as to meet the standards of testability for systems important to safety.

The dedicated residual heat removal system is an Engineered Safety Feature and shall be automatically actuated after a normal reactor scram or a backup reactor shutdown if an Anticipated Transient Without Scram should occur. The system shall be designed for the system to be activated on loss of dc power.

Unambiguous operating procedures shall be provided to define the conditions which allow the dedicated heat removal system to be deactivated and allow residual heat to be removed via the secondary system.

Comment: The definition of "single failure" appears in 10CFR50, Appendix A and is used in Criteria 17, 21, 34, 35, 38, 41, and 44. The requirement that a single failure be considered in the design of a system important to safety intuitively implies that the system reliability will be improved. On a relative basis this is true. A two-train system will be more reliable than a single-train system, but application of the single failure criteria does not guarantee that even a two-train system will provide the required degree of reliability. Therefore, the single failure criteria should be supplemented. The following modification to Criteria 17, 21, 34, 35, 38, 41, and 44 is recommended:

II. The system shall be designed for high functional reliability and inservice testability commensurate with the safety functions to be performed. Redundancy and independence designed into the system shall be sufficient to ensure that (1) no single failure results in loss of the system function and (2) removal from service of any component, train, or channel does not result in loss of the required minimum redundancy. The acceptable reliability of operation of the system shall be demonstrated by using probabilistic assessment methods. Weak points of system design, including vulnerability to common mode failures, should be detected and corrected as practical. Relative probabilistic assessment should be used to decide on system options, to optimize maintenance procedures, and to determine appropriate maximum allowable repair times in redundant systems.

The system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant trains or channels do not result in loss of the system function, or shall be demonstrated to be acceptable on some other defined basis. Design techniques such as physical separation, barrier protection, functional diversity or diversity in component design, and principles of operation, shall be used to the extent practical to prevent loss of the system function.

Comment: It is recommended that Criterion 17, Electric Power Systems, be supplemented by adding an additional criteria for dc power systems.

III. Direct Current Electric Power Systems. When direct current power is used by systems or components important to safety, the dc electrical system shall:

(1) Provide sufficient stored power for n hours of operation of all systems or components important for safety without any support from other electrical systems.

(2) Have sufficient redundancy and diversity that minimum safety functions will not be lost due to a single failure while one segment of the ac power supply is out of service for maintenance or repair.

(3) Be designed so that one portion of the system cannot be disabled by inadvertent connection to a faulted portion of the system.

(4) Be controlled so that components important to safety are not compromised by either over or under voltage when powered from either the charger or the battery either separately or combined.

(5) Be used exclusively for safety-related functions.

(6) Have redundant supply paths protected against external events such that a single external event will not prevent the operation of the minimum safety functions.

(7) Have sufficient testability to verify the performance of the required safety functions.

Sincerely,

Walter C. Lipinski

Walter C. Lipinski
Senior Electrical Engineer
Reactor Analysis and Safety Division

WCL/at

cc: R. Savio, ACRS
Max Carbon, ACRS