UNITED STATES OF AMERICA
NUCLEAR REGULATORY COMMISSION

BEFORE THE ATOMIC SAFETY AND LICENSING BOARD

In the Matter of	)	
	)	
METROPOLITAN EDISON COMPANY, ET AL	)	Docket No. 50-289
(Three Mile Island Nuclear Station Unit 1)	)	
	)	

NRC STAFF TESTIMONY OF JAMES H. CONRAN RELATIVE TO CLASSIFICATION OF SYSTEMS AND COMPONENTS AS IMPORTANT TO SAFETY

(UCS CONTENTION 14)

Q.1 Please state your name and your position with the NRC.

A. My name is James H. Conran. I am an employee of the U. S. Nuclear Regulatory Commission, assigned to the Systems Interaction Branch in the Division of Systems Integration, Office of Nuclear Regulatory Regulation.

Q.2 Have you prepared a statement of professional qualifications?

A. Yes. A copy of that statement is attached to this testimony.

Q.3 Please state the nature of the responsibilities that you have had with respect to Three Mile Island Nuclear Station Unit 1 (TMI-1).

A. Prior to the March 28, 1979 accident at Unit 2, I had no involvement with either of the TMI units. Following the accident at Unit 2, I was assigned for several months to the task of monitoring for NRR the ACRS proceedings related to the TMI-2 accident and the status of recommendations made by the

Committee in that regard. At the end of May 1979 I was assigned as a member of the Lessons Learned Task Force which was chartered to identify and evaluate safety concerns arising out of the TMI-2 accident, and to recommend changes to licensing requirements and the licensing process for nuclear power plants based on lessons learned from that experience. In connection with my Lessons Learned Task Force activity, I was also given lead responsibility for evaluating (and drafting the Commission's response to) the Report of the Ad Hoc Committee of the Illinois Commission on Atomic Energy regarding implications of the TMI-2 accident.

After issuance of the Final Report of the Lessons Learned Task Force, I was assigned as a member of a small staff group charged with implementing approved Short Term Lessons Learned recommendations in the context of the so-called Near Term Operating License plants, (which included Sequoyah Unit 1, North Anna Unit 2, Salem Unit 2 and Diablo Canyon Units 1 and 2), and I participated in the preparation of Safety Evaluation Reports to support those proposed licensing actions. Currently, I am assigned to the Systems Interaction Branch, a new entity in the NRR organization. This branch and function was created at the time of the recent NRR reorganization, specifically in response to lessons learned from the TMI-2 accident; one of the principal functions of the new branch is consideration of the effects of interaction between safety and non-safety systems.

Q.4 What is the purpose of your testimony?

A. The purpose of my testimony is to respond to UCS Contention #14, which states:

"The accident demonstrated that there are systems and components presently classified as non-safety-related which can have an adverse effect on the integrity of the core because they can directly or indirectly affect temperature, pressure, flow and/or reactivity. This issue is discussed at length in Section 3.4, "System Design Requirements," of NUREG-0578, the TMI-2 Lessons Learned Task Force Report (Short Term). The following quote from page 18 of the report describes the problem:

> 'There is another perspective on this question provided by the TMI-2 accident. At TMI-2, operational problems with the condensate purification system led to a loss of feedwater and initiated the sequence of events that eventually resulted in damage to the core. Several nonsafety systems were used at various times in the mitigation of the accident in ways not considered in the safety analysis; for example, long-term maintenance of core flow and cooling with the steam generators and the reactor coolant pumps. The present classification system does not adequately recognize either of these kinds of effects that nonsafety system can have on the safety of the plant. Thus, requirements for nonsafety systems may be needed to reduce the frequency of occurrence of events that initiate or adversely affect transients and accidents, and other requirements may be needed to improve the current capability for use of nonsafety systems during transient or accident situations. In its work in this area, the Task Force will include a more realistic assessment of the interaction between operators and systems.'

The Staff proposes to study the problem further. This is not a sufficient answer. All systems and components which can either cause or aggravate an accident or can be called upon to mitigate an accident must be identified and classified as components important to safety and required to meet all safety-grade design criteria."

The Board limited the scope of this contention to the core cooling system. (First Special Prehearing Conference Order, December 18, 1979).

Q.5 How is the term "... components important to safety ..." defined in the Commission's regulations?

A. The term "... structures, systems, and components important to safety ..." is defined in the introductory paragraph to the General Design Criteria (Appendix A to 10 CFR Part 50) as those "... structures, systems, and components that provide reasonable assurance that the facility can be operated without undue risk to the health and safety of the public." From this context, it is clear that the expression "... important to safety ..." is meant to apply generally to all structures, systems, and components addressed in the General Design Criteria (GDC). The term is used consistently in that sense throughout the GDC, and in other parts of the regulations as well (e.g., see dicussion below).

Q.6 Is the term "... safety-grade ..." defined in the regulations?

A. That term is not defined explicitly in the regulations. The term is widely-used, however, in the context of the safety review process. The meaning of the term, as most commonly used by the staff in that context, is inferred from the language of the regulations, as follows:

(a) General Design Criterion 1 introduces the notion of different quality levels for plant features with differing safety roles and varying degrees of importance to safety. Specifically, GDC-1 requires application of "... quality standards commensurate with the importance of the safety function to be performed ..." for structures, systems, and components important to safety.

(b) Appendix A to 10 CFR Part 100 implements the concept established in GDC-1 (i.e., gradations in quality levels corresponding to relative safety importance) by identifying explicitly a select

sub-class of structures, systems, and components (out of the broad class "important to safety") that are required for the performance of specific, critical safety functions (e.g., safe shutdown, accident prevention and consequence mitigation, etc.). Specifically, Sec. III.c of Appendix A to 10 CFR Part 100 defines the Safe Shutdown Earthquake (the most severe seismic event analyzed for a nuclear power plant), and requires that "... certain structures systems, and components (important to safety) ..." be designed to remain functional for that event. Those "certain" plant features, and the critical safety functions they must perform, are further identified in Sec. III.c as: "... those necessary to assure:

(1) The integrity of the reactor coolant pressure boundary,

(2) The capability to shut down the reactor and maintain it in a safe shutdown condition, or

(3) The capability to prevent or mitigate the consequences of accidents which could result in potential offsite exposures comparable to the guideline exposures of this part."

Very high quality standards must, of course, be applied to plant features required for such purposes, in order to assure their availability when called upon and very high reliability in service. Such considerations are the origin of the term "safety-grade"; and the staff applies that term only to the structures, systems and components required to perform the specific critical safety functions identified above. (Frequently, the term "safety-grade, systems or components" is shortened to "safety systems or components." These two terms are used interchangeably in the following testimony).

Q.7 Would you summarize from the preceding, the relationship between the terms "important to safety" and "safety-grade"?

A. (1) The term "important to safety" applies generally to the broad class of structures, systems, and components addressed in the General Design Criteria.

(2) "Safety-grade" structures, systems and components are a sub-class of all those "important to safety."

(3) All structures, systems, and components encompassed by the term "important to safety" (including the "safety-grade" sub-class) are necessary to meet the broad safety goal articulated in Appendix A to 10 CFR Part 50 of the regulations (i.e., provide reasonable assurance that a facility can be operated without undue risk to the health and safety of the public).

(4) Only "safety-grade" structures, systems and components are required for the critical accident prevention, safe shutdown, and accident consequence mitigation safety functions identified in Sec. III.c of Appendix A to 10 CFR Part 100.

Q.8 Has the staff identified those structures, systems and components which must be safety-grade?

A. Yes. They are listed in detail in Regulatory Guide 1.29. The specific purpose of Reg. Guide 1.29 was to identify all structures, systems and components of nuclear power plants that should be designed to withstand the effects of the Safe Shutdown Earthquake (designated Seismic Category I). Because of the manner in which the term safety-grade was derived in the preceding discussion, however, the list of Seismic Category I plant features identified in Reg. Guide 1.29 should also be the listing of all "safety-grade" structures, systems, and components in a plant.

Q.9 Is the term "... core cooling system ..." defined in the regulations?

A. To my knowledge, that term is not defined explicitly in the regulations. From the context in which it is applied in the specification of this contention, however, the staff considers that term to encompass those primary, secondary, and auxiliary systems used to remove heat from the core and transfer it to the heat sink, both in normal operation and under accident conditions.

Q.10 Referring now to the first sentence of the contention,

(a) Can non-safety systems and components directly or indirectly affect the temperature, pressure flow and/or reactivity, and

(b) Can non-safety systems and components, therefore, have an adverse effect on the integrity of the core?

A. (a) The staff stipulates that non-safety systems and components can directly or indirectly affect core reactivity and primary coolant temperature, pressure and flow. It follows, therefore, that (at least in general) failure or off-normal operation of non-safety systems and components can cause or aggravate an accident, but

(b) That does not establish that failure or off-normal operation of non-safety systems and components <u>alone</u> can have an adverse effect on the integrity of the core, as strongly implied by the wording of the contention. (In the TMI-2 accident sequence, failure of non-safety components, <u>coupled with improper operation of installed safety systems</u>, led to core damage.)

Q.11 Do you have any clarifying or amplifying comments regarding the second paragraph of the contention, i.e., the quote excerpted from NUREG-0578?

A. The staff acknowledges that non-safety systems and components were used in the mitigation of the TMI-2 accident; but it is important to note and emphasize, in the discussion of this contention, that resort was made to use of non-safety systems and components in the accident mitigation role, only after improper operation of installed safety systems had resulted in severe core damage and other outside-design-basis conditions (e.g., voiding in the primary coolant and hydrogen generation, which may have blocked natural circulation, thus creating the need for forced cooling).

Q.12 Referring now to the last sentence of the contention, what is the staff's position regarding the statement that "All systems and components which can either cause or aggravate an accident or can be called on to mitigate an accident must be identified and classified as components important to safety and required to meet all safety-grade design criteria"?

A. We believe that, in the sense that the term "important to safety" is defined and used consistently in the regulations (see response to Q.5 above), such systems and components would already be regarded (i.e., classified) as important to safety. But, as further established in the responses to Q.6 and Q.7 above, all components important to safety need not be safety-grade. Only components required for the specific critical safety functions delineated explicitly in the response to Q.6 above need to meet safety-grade design criteria.

Q.13 More specifically, if a given non-safety system or component is known to have contributed to an accident, or is known to have been relied upon to recover from an accident (as was the case at TMI-2), how does the staff decide whether-or-not the safety classification of the system or component should be changed and whether-or-not that system or component should be made safety-grade?

A. The test applied by the staff, in deciding whether a given non-safety system or component should be upgraded to safety-grade, is not just whether it could cause or aggravate or be called upon to mitigate an accident. The final determination (regarding whether-or-not to upgrade) is based upon consideration of the following questions (decision criteria), which derive directly from the definitions and discussions developed in the responses to Q.5 through Q.10:

(a) will the failure or off-normal operation of the non-safety system or component in question, in and of itself, degrade the capability of installed safety systems such that those safety systems cannot mitigate accident consequences and assure adequate safety,*

(b) will the effects of failure or off-normal operation of the non-safety system or component in question alone exceed the capability of installed safety systems to mitigate accident consequences and assure adequate safety, if installed safety systems are operated properly so that full credit can be taken for their functioning to design capability throughout the accident sequence,*

*Assuming single failure in the installed safety systems in accordance with the Single Failure Criterion.

(c) is a non-safety system or component that may be called upon actually required to mitigate accident consequences and assure adequate safety, if installed safety systems are operated properly so that full credit can be taken for their functioning to design capability throughout the accident sequence.*

If the staff determines, either by careful analysis or actual experience, that the answer to any of these questions, in all of its aspects, is yes, then:

(i) the system or component in question would be upgraded to safety-grade, or

(ii) the design of the facility and/or the capability of the installed safety systems would be improved such that the answer is no to all three questions.

In some instances (as has been the case for some of the non-safety components which were involved in the TMI-2 accident sequence and recovery process), even though none of the decision criteria above that would require upgrading are met, the staff may decide as a prudent measure to require upgrading of the system or component in question, but not to full safety-grade. This might be done, for example, in order to improve the availability and reliability of the component in question, and thereby provide increased safety margins or greater flexibility for dealing with potential future accident situations (either within the current design basis or like TMI-2, and irrespective of how such conditions might come about).

*Assuming single failure in the installed safety systems in accordance with the Single Failure Criterion.

Q.14 Were any of the decision criteria set forth in the answer to Q.13 (that would require upgrading to safety-grade) met for any of the non-safety systems or components which either contributed adversely to or had to be called upon to mitigate the TMI-2 accident?

A. No. The severe effects produced in the TMI-2 accident (e.g., serious core damage; voiding in the primary coolant and hydrogen gas generation which may have blocked natural circulation; dispersal of large amounts of radioactive fission products in the primary coolant; etc.) did not result from non-safety system or component failure alone. If operator action had not interfered with the proper functioning of the installed safety systems to their design capability, the safety systems could have accommodated the effects of the non-safety component failures that occurred, and still have prevented the serious core damage and other outside-design-basis effects that resulted. And if the core damage and other outside design-basis effects which occurred had been prevented, it would not have been necessary to call upon non-safety components to assist in accident mitigation and recovery (e.g., long term maintenance of core flow and cooling with RCP's and steam generators).

Q.15 Is there a need, then, for any of the non-safety systems or components that contributed to the TMI-2 accident, or that were called upon in the accident recovery process, to be made safety-grade?

A. No. Reliance can still be placed, in future TMI-1 operations, on the capability of safety systems currently provided in the TMI-1 design to assure adequate safety, <u>without resort to the general upgrading of non-safety systems and components which would be required by the contention</u>,

if proper operation of installed safety systems is assured such that full credit can be taken for the functioning of those systems to design capability.*

Q.16 What has been done to provide increased assurance that installed safety systems will be operated properly at TMI-1, in view of what happened in that regard in the TMI-2 accident?

A. The staff has specified a number of corrective measures (described in NUREG-0680, "TMI-1 Restart SER," and in a letter dated 8/28/80 from Director, ONRR, to All Power Reactor Applicants and Licensees) in the aftermath of TMI-2, to better assure that operators will not interfere with the proper functioning of installed safety systems in the future. These corrective measures fall into three general categories:

(a) improved analyses of anticipated transients and accidents, and improved procedures for operators based on those analyses,
(See NUREG-0680 at C1-12, C2-4, C2-9, C2-16, C2-17, C2-18, C2-47, and D2-1 for details)

(b) improved instrumentation (e.g., sub-cooling meter, improved indication of PORV and safety valve position, improved AFW flow indication, etc.), to better monitor and understand critical plant parameters, and to better recognize the need for safety system operation if the occasion arises,
(See NUREG-0680 at C1-5, C8-11, C8-14, C8-38, and D3-1 for details)

*Assuming single failure in installed safety systems, in accordance with the Single Failure Criterion.

(c) improved operator training to better cope with anticipated and unanticipated plant conditions,

(See NUREG-0680 at C1-6, C1-7, C1-16, C2-4, C2-5, C2-9, C2-10, C2-12, C2-16, C2-17 and C8-47 for details. Also see ltr, dated 3/28/80, Denton to All power Reactor Applicants and Licensees)

The staff believes that satisfactory compliance with these requirements will provide the improved assurance needed that installed safety systems will be operated properly, so that full credit can be taken for their effective functioning as required to assure adequate safety.

Q.17 Has the staff required upgrading of <u>any</u> of the systems or components that either contributed to the TMI-2 accident or were called upon in the accident recovery process? Has upgrading to full safety-grade been required? Explain the staff's rationale for whatever action was taken in each case.

A. Examples of non-safety systems or components for which the staff has specified upgrading, but not to full safety-grade, include:

(1) emergency power supplies for pressurizer heaters

(See NUREG-0680 at C8-3; also see Testimony of Jensen re: UCS Contention 3)

(2) emergency power supply for PORV and block valves

(See NUREG-0680 at C8-8; also see Testimony of Jensen re: UCS Contention 5)

(3) improved position indication for PORV and safety valves

(See NUREG-0680 at C8-11)

(4) automatic initiation of AFW system, short term (long term requirement is to provide safety-grade initiation)

(See NUREG-0680 at C8-34)

(5) AFW Flow indication

(See NUREG-0680 at C8-38)

The detailed rationale for staff actions taken in this regard, and further information regarding applicability, status, and actual plant changes required in each of these areas with respect to TMI-1, is contained in the references cited for each of the individual items identified above.

Q.18 Does the staff have any long term plans or programs for evaluating possible safety effects of non-safety systems or components generally, and for reassessing the appropriateness of current non-safety classifications, in view of the lessons learned from the TMI-2 accident?

A. Yes. That was an explicit objective of Recommendations 9 (Review of Safety Classifications), 7.1 (Control Room Reviews), and 7.2 (Plant Safety Status Display) of the Lessons Learned Task Force Final Report (NUREG-0585) and at least an implicit, partial objective of Recommendation 2.1.9 (Analysis of Design and Off-Normal Transients and Accidents) of the Short Term Lessons Learned Task Force Report (NUREG-0578). Commission-approved action plans describing the programs for carrying out these recommendations and objectives, are contained in the overall NRC TMI-2 Action Plan (NUREG-0660), principally in individual action items

II.C.1, II.C.2, II.C.5, I.C.1, I.D.1, I.D.2 and I.D.3. (See also related or complementary action items I.E.1, I.E.2, I.E.3, II.E.3.2, II.F.3, II.F.4, II.F.5, and II.G).

TECHNICAL QUALIFICATIONS INFORMATION

JAMES H. CONRAN

SYSTEMS INTERACTION BRANCH

DIVISION OF SYSTEMS INTEGRATION

OFFICE OF NUCLEAR REACTOR REGULATION

Education: B. S. in Physics, 1960, The Colorado College, Colorado Springs, Colorado. Post-graduate and Professional Courses in Physics and Solid-State Electronic Engineering; University of Kansas 1962-1963. Professional Courses in Fault-Tree Analysis 1972 and 1980.

Experience: U. S. Nuclear Regulatory Commission/U. S. Atomic Energy Commission Washington, D. C., 1973 to Present

- Principal Systems Engineer, Systems Interaction Branch, Division of Systems Integration, Office of Nuclear Reactor Regulation. Responsible for development of systems interaction analysis methods, systems integration review methods, and corresponding regulatory guidance; systems integration review of operating license and construction permits; and review of operating experience and systems interaction effects.

- Senior Project Manager on special assignment for one year to the Lessons Learned Task Force and follow-on implementation activities. Responsible for identification and evaluation of safety concerns arising out of TMI-2 accident, and recommendation of changes to licensing requirements and safety licensing process; liaison with the Bulletins and Orders Task Force and ACRS on TMI-2 accident review matters, follow-on implementation of Lessons Learned Task Force recommendations to Near-Term Operating License Applications;

development of Near-Term Construction Permit Lessons Learned licensing requirements; and participation in the formulation of the overall NRC TMI-2 Action Plan (NUREG-0660).

- Senior Project Manager, Standardization Branch, Division of Project Management, Office of Nuclear Reactor Regulation. Responsible for management and coordination of safety review of applications for standard design approvals, and development of standardization policy.

- Senior Nuclear Engineer, Reactor Systems Safety Branch, Division of Engineering Standards, Office of Standards Development. Involvement in development of quality assurance standards and Regulatory Guides for nuclear material processing facilities, protection-of-informants policy studies, and special safeguards-related investigations and hearings.

- Systems Engineer and Senior Safeguards Analyst, Requirements Analysis Branch, Division of Safeguards, Office of Nuclear Material Safety and Safeguards. Responsible for comprehensive studies of adequacy of safeguards for existing licensed nuclear facilities (including nuclear materials processing facilities and power reactors), and development of applicable safeguards regulations and other regulatory guidance.

- Senior Safeguards Analyst, Special Safeguards Study Project, Office of Special Studies. Responsible for management, coordination, and technical review and evaluation of contractor studies relating to safeguards issues identified in GESMO (plutonium recycle) proceedings; development of recommendations regarding the Reference

Safeguards System concept.

- Senior Staff Assistant/Project Engineer, Advisory Committee for Reactor Safeguards. Senior project leader responsible for: coordinating activities of ACRS project subcommittees, ACRS consultants, Regulatory Staff, and applicants in support of ACRS licensing reviews; preparation of reports for ACRS use identifying areas requiring detailed evaluation or resolution of deficiencies.

U. S. Atomic Energy Commission, Albuquerque Operations Office (ALOO), 1970 - 1973

- Reactor and Criticality Safety Engineer, Reactor and Criticality Safety Branch, Division of Operational Safety. Responsible for: inspection and evaluation for criticality safety of all the facilities within the ALOO complex (e.g., weapons design and research laboratories , weapons production in plants, weapons test sites) that support the U. S. Nuclear weapons program, and all pertinent activities therein (e.g., research reactor and critical assembly operation, uranium and plutonium processing weapons assembly, packaging and transportation of fissle materials, etc.); and safety review of reactor and critical assembly instrumentation , control, protection, and electric power systems; including proposed modifications.

San Francisco Bay Naval Shipyard, Vallejo, California, 1967 - 1970

- Nuclear Power Engineer, Test Engineering Branch, Nuclear Power Division. Qualified for Shift Test Engineer position; responsible for preparation of detailed test procedures and direction of on-board shift testing operations involved in the acceptance testing

(pre-operational flushing and hydrostatic testing, systems tests, initial criticality and power range testing, and sea trial) of naval nuclear propulsion systems (new construction, refuel and overhaul).

- Electronic Engineer, Refueling Engineering Branch, Nuclear Power Division. Qualified for Assistant Refueling Director position; responsible for direction of dockside and on-board shift refueling operations for naval nuclear propulsion systems (refuel and overhaul)

Western Electric Company, Kansas City Manufacturing Works, Lee's Summit, Missouri, 1960 - 1967

- Product Planning and Design Engineer, Test Planning Engineer, and Test Equipment Design Engineer. Responsible for planning and direct engineering support in the production and testing of radio and voice frequency telephone carrier systems; design of major production test equipment; and trouble-shooting problems encountered in the production testing and field application of the telephone communications equipment manufactured at the Kansas City Works.

OUTLINE

This testimony of James H. Conran contains the NRC Staff's response to UCS Contention 14.

The purpose of this testimony is to demonstrate that, contrary to the assertions made in the contention, all systems or components of the core cooling system which can either cause or aggravate an accident or can be called upon to mitigate [the consequences of] an accident need not be required to meet safety-grade design criteria.

Conclusions to be drawn from this testimony:

-- NRC regulations do not require that all components and systems that are classified as "important to safety" be designated safety-grade" and designed and qualified to very high standards.

-- Only those systems and components required to perform safety functions are designated safety-grade.

-- Those critical safety functions are identified in Section III(c) of Appendix A to 10 C.F.R. 100.

-- Those systems and components which must be safety-grade are identified in Regulatory Guide 1.29.

-- That failure or off-normal operation of certain non-safety components and systems could cause or aggravate an accident or that certain non-safety components and systems could be called upon to mitigate the consequences of an accident does not mean that those components and systems must be classified, designed and qualified as safety-grade.

-- Whether a non-safety system should be upgraded to safety-grade is determined by applying certain decision criteria set forth in the testimony.

-- Application of those decision criteria indicates that none of the non-safety systems or components which contributed adversely to or were called upon to mitigate the consequences of the TMI-2 accident need be classified as safety grade.

-- The Staff is reassessing the appropriateness of current non-safety classifications of systems and components in view of the lessons learned from the TMI-2 accident.