SYSTEMS INTERACTION

AND

SINGLE FAILURE CRITERION

DRAFT REPORT

PREPARED BY

MHB TECHNICAL ASSOCIATES
1723 HAMILTON AVENUE
SAN JOSE, CALIFORNIA 95125

COMMISSIONED BY

STATENS KÄRNKRAFTINSPEKTION

NOVEMBER, 1980

Appendix A

SECTION 2

SOURCES OF BACKGROUND INFORMATION

2.1: INTRODUCTION

This section of the report identifies the major sources of information utilized by MHB during the information gathering portion of this Study. Specifically, in Subsection 2.2, the NRC's past policy for the selection of "design basis accidents" is reviewed, particularly the licensing criterion that certain reactor systems be able to survive any single failure and still accomplish their safety goal or mission.

Several nuclear plant accidents have demonstrated multiple-failures in which different plant systems interact with each other in such a manner that the performance of safety systems is degraded. Some of these past accidents, and the accident sequences, are briefly identified in Subsection 2.3. Finally, a summary of past U.S. reviews of the systems interaction issue is presented in Subsection 2.4 of this Study.

2.2: SELECTION OF DESIGN BASIS ACCIDENTS

Traditionally, the NRC has approached accident and safety analysis on a system-by-system basis, using the "single failure criterion" (See 10 C.F.R. Part 50, Appendix A, Criterion 21 for example). The effect of this is to require "that a system designed "to carry out a specific safety function must be able to fulfill its mission in spite of the failure of any single component within the system, or failure in an associated system that supports its operation."[1/]

Historically, a further assumption in NRC design reviews and licensing was that if reactor plant systems can handle large-scale design basis accidents, they can also handle a spectrum of smaller accidents that are regarded as being "within the design envelope." As a result, emphasis tends to be placed on major failures within a single system. There is inadequate consideration of smaller failures. As both the Kemeny Commission[2/] and the NRC's Special Inquiry Group (Rogovin Report)[3/] have pointed out, the tendency is to assume that if the large failures can be controlled "we need not worry about the analysis of 'less important' accidents," and there is inadequate consideration of what happens if multiple pieces of equipment fail from a common cause.[4/] The Rogovin Report concluded that there is also inadequate consideration of systems interaction--that is, the potential for adverse, accident-causing or accident-contributing interactions between or among different nuclear plant systems.[5/] This lack of consideration is aggravated by the tendency to assign the design and safety analysis of each system (e.g., mechanical, electrical, or nuclear) to a different team of engineering specialists, without ensuring that the work of those teams is sufficiently integrated to enable them to identify or assess adverse interactions between systems.[6]

An historical description of the NRC's policy for the review of "design basis accidents" is summarized by the NRC in the recently published notice of proposed rulemaking for a range of degraded core cooling events.[7] As noted by the NRC, in the Safety Analysis Report the Applicant for a reactor license is required to determine margins of safety for both normal and abnormal operations and to determine "the adequacy of structures, systems, and components provided for prevention of accidents and the mitigation of the consequences of accidents." To assist the Applicant in complying with this regulation, the NRC has published Regulatory Guide 1.70, Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants,[8] which describes the information to be provided in the Safety Analysis Report.

In particular, section 15 of Regulatory Guide 1.70 provides guidance to an Applicant concerning "design basis assumptions acceptable to the NRC for purposes of determining adequacy of the plant design to meet 10 CFR Part 100 criteria." Regulatory Guide 1.70 explains that these design basis assumptions can, for the most part, be found in regulatory guides that deal with radiological releases and suggests use of Regulatory Guides 1.3 and 1.4, Assumptions Used for Evaluation of the Potential Radiological Consequences of a Loss-of-Coolant Accident. Regulatory Guide 1.70 further states that "This analysis should be referred to as the 'design basis analysis.'" Operating events corresponding to design basis assumptions are termed "design basis accidents," and satisfactory analysis conclusions concerning them allow a judgment that the facility can be operated without undue risk to the health and safety of the public.

It should be noted that these events are analyzed primarily for the purpose of establishing the adequacy of engineered safety features, such features being those structures, systems, and components designed into a plant to mitigate the consequences of postulated design basis accidents, and which supplement other plant features designed to meet performance specifications for normal operations and anticipated abnormal conditions.

In the Safety Analysis Report the license Applicant is not required, however, to explicitly analyze accidents more severe than the design basis accidents.[9/] This approach is based on the assumption that such accidents are of sufficiently low probability that mitigation of their consequences is not necessary for public safety. This low probability was thought to result from the "defense in depth" approach that requires conservative design, multiple physical barriers, quality assurance for design, manufacture and operation, and continued surveillance and testing to prevent such accidents.

Furthermore, in reviewing reactor plant designs using the "design basis accident" approach, the NRC does not review all structures, systems, and components but rather reviews, in varying levels of detail, only those considered "safety grade" by the Applicant submitting a Safety Analysis Report. Items considered by the Applicant to be outside the scope of design basis accident analyses are generally not considered to be "safety grade" and are not reviewed by the NRC to see whether they will perform as intended or meet various dependability criteria. This method of classification is based on the notion that things credited in the analysis of a design basis event or specified in the regulations are important to safety and thus are "safety grade" while all else is "non-safety grade." Non-safety grade items do not receive continuing regulatory supervision or surveillance to see that they are properly maintained or that their design is not changed in some way that might interact negatively with other systems. Instead, these items simply receive what attention may be dictated by routine industrial codes and by desires to enchance plan availability.

The accident at Three Mile Island, Unit 2, resulted in core damage more severe than that considered in current design basis events and has shown the need to re-examine these historical approaches to analyzing reactor plant design and plant accidents. The October, 1979, Report of the President's Commission on the Accident at Three Mile Island recommended that in-depth studies be initiated on the probabilities and consequences (on-site and offsite) of nuclear power plant accidents, including the consequences of core meltdown. This report recommended that these studies include a variety of small-break, loss-of-coolant accidents and multiple-failure accidents, with particular attention to human failures.

Similarly, the January, 1980, Rogovin Report, Three Mile Island: A Report to the Commissioners and to the Public, states on page 150 that:

> "....we have come far beyond the point at which the existing, stylized design basis accident review approach is sufficient. The process is not good enough to pinpoint many important design weaknesses or to address all the relevant design issues. Some important accidents are outside or are not adequately assessed within the 'design envelope'; key systems are not 'safety related'; and integration of human factors into the design is grossly inadequate."

2.3: MULTIPLE-FAILURE ACCIDENTS AT OPERATING REACTORS

The TMI-2 accident revealed major shortcomings in many of the procedures upon which NRC has based its approach to safety. First, the accident "involved a sequence of events more severe than those included in current design basis events."[10] Core temperatures exceeded 3500°F.,[11] or more than 1300°F. above the level for which emergency cooling systems are designed. The chemical reaction between water and the zirconium fuel cladding generated five to ten times as much potentially explosive hydrogen as is assumed in the design bases for hydrogen control systems.[12] And indeed, although extensive core damage, with cracking, crumbling, and possible melting and fusing together of fuel pellets and parts of fuel assemblies such as occurred at TMI[13/] was foreseen as a possible event, it was excluded from the design basis since plant safety features were provided to prevent it.[13/] The transport of radioactive gases and liquid into the auxiliary building (through normal leakage in water make-up and let-down pumps and tanks deliberately run to cool the reactor coolant pump seals) also fell outside the design basis.

Second, the TMI-2 accident involved a sequence of several multiple-failures which thus demonstrated the inadequacy of the single failure criterion. In the accident at TMI-2, the combination of closed auxiliary feedwater valves, stuck open pilot-operated relief valves, and misinformation to the operator allowed the failure of adequate feedwater and the partial blowdown to create voids in the primary coolant. The voids in turn produced misleading pressurizer level indications. This resulted in the operator terminating emergency cooling water, which eventually resulted in failure of the fuel. The release of radioactivity was due to the high sump level causing the pump to turn on and pump radioactive waste to the Auxiliary Building where it was released to the environment as a result of additional errors. The radioactivity in the atmosphere fed back through the control room ventilation system thereby raising the levels to the point where special breathing apparatus had to be worn by the operators trying to control the accident. After the accident, the high radiation levels in the containment and the primary loop have continued to make it very difficult to work on the system to perform the necessary maintenance functions. In general, the multiple, interrelated failures involving various systems and their interactions (with and without human intervention) were not foreseen in the safety analyses conducted as part of the licensing process.

Other accidents such as the Dresden-2 blowdown in June, 1970, the Browns Ferry fire in March, 1975, and the Crystal River loss of non-nuclear instrument power resulting in a partial blowdown in February, 1980, all involved the effects of one system on another, producing more severe consequences than had previously been expected. Also, the NRC reviews of the June 28, 1980, partial failure to scram incident at Browns Ferry-3 disclosed a potential for unacceptable interaction between the control rod drive system and the non-safety-grade control air system. Other recent examples of systems interaction, as described in License Event Reports, are summarized in Appendix A to this report.

The NRC's Lessons Learned Task Force, after reviewing the TMI-2 accident scenario, formed the following conclusion regarding the potential for system interaction:

> "The interactions between non-safety-grade and safety-grade equipment are numerous, varied, and complex and have not been systematically evaluated. Even though there is a general requirement that failure of non-safety-grade equipment or structures should not initiate or

> aggravate an accident, there is no comprehensive and systematic demonstration that this has been accomplished...." 15/

They recommended that comprehensive studies of system interaction be conducted by all license applicants. They further recommend that these studies cover both safety and non-safety systems, under normal, transient, and accident conditions. While the implications of these recommendations for nuclear safety regulation are vast, they do not represent a surprise to the nuclear industry. As evidenced by the information in the following portion of this Study, Subsection 2.4, the systems interaction issue has long been recognized as a high-priority, high-risk potential, unresolved safety issue.

2.4: LONG HISTORY OF SYSTEMS INTERACTION PROGRAM

In November, 1974, the Advisory Committee on Reactor Safeguards (ACRS) first requested that the NRC Staff give attention to the evaluation of safety systems from a multi-disciplinary point of view, in order to identify potentially undesirable interactions between plant systems. The ACRS concern arises because the design and analysis of systems is frequently assigned to teams with functional engineering specialties--such as civil, electrical, mechanical, or nuclear. The question is whether the work of these functional specialties is sufficiently integrated in their design and analysis activities to enable them to identify adverse interactions between and among systems. Such adverse events might occur, for example, because designers did not assure that redundancy and independence of safety systems were provided under all conditions of operation required, which might happen if the functional teams were not adequately coordinated.

In this Study, we will refer to these related deficiencies in accident and safety analysis--the lack of systems interaction analysis, the lack of multiple or "common-cause" failure analysis, and the tendency of the "single-failure criterion" to exclude a large number of potential accident-causing events - as the "systems interaction issue." This issue became extremely significant after the TMI-2 accident, which itself involved not a single failure but rather a series of failures, or domino effect, which included both dependent and independent multiple failures. The Kemeny Commission found that "|t|he accident at TMI-2 was a multiple-failure accident,"[16/] as did the NRC's Special Inquiry Group.[17/] But "|i|n the licensing process, applicants are only required to analyze 'single failure' accidents. They are not required to analyze what happens when two systems fail independently of each other,"[18/] nor to assess possible adverse interactions among systems. As a result, the Kemeny Commission called upon the NRC to emphasize:

> "a systems engineering examination of overall plant design and performance, including interaction among major systems and increased attention to the possibility of multiple failure. 19/

The NRC's Special Inquiry Group also criticized the NRC's safety and accident analysis as inadequate,[20] noting that "one of the obvious lessons" of TMI-2 "is the critical need for overall plant and systems analysis," and, with particular regard to the concentration of engineering design and analysis teams on single specialized systems, that "|t|here is as much or more of a chance that safety matters will 'fall in the cracks' between two or more highly proficient technical groups as there is for a safety error to be made in any of the specific groups."[21]

In addition, in late 1979 the NRC's Advisory Committee on Reactor Safeguards recommended an investigation at the Indian Point nuclear plant of the systems interaction issue as follows:

> "Thus, <u>uncovering the potential for interaction of nonconnected systems will usually require careful, in-situ examination of the physical plant. This examination must consider all features having the potential to damage safety systems, including the safety systems themselves</u>. The physical inspection of the plant could be approached by dividing the plant into 'compartments' following discernable structures--such as walls, ceilings, and floors with appraisable strengths and weaknesses. Doors, stairs, ventilation ducts, piping, and other penetrations would be evaluated for potential influence transport (fire, steam, hot air, etc.). Structures, which act as barriers to the flow of a damaging influence, would be assessed for the adequacy of their resistance to such influences.
>
> "<u>In each compartment the elements of the safety systems, including such extensions as instrument lines and power or control wiring should be identified on a 'train basis</u>.' The physical vulnerability of the safety system elements to nonstandard conditions (temperature, pressure, water, spray, etc.) should

be identified. The characteristics of such systems as influence generators under faulted conditions would have to be assessed if such system elements exist as redundant elements within the identified 'compartment' boundaries.

"The influence potential of all non-safety elements, including such items as sewer and drain lines, combustible gas transport and storage, compressors, and heavy-power circuits and transformers, within the given compartment should be assessed with respect to potential for damaging or disrupting (as with induced electrical noise) critical system(s) within the 'compartment' and the 'compartment' boundary itself.

"The invasion of damaging influences through the barriers or boundaries into the identified compartment would also have to be assessed. This would include consideration of entry of personnel carrying influence generators such as welding equipment.

"Special consideration would have to be given to the identification of convergence of safety functions into single compartments and the degree of convergency within the given space. The study of interactions between nonconnected systems would also have to include the possibility of non-visible interactions, such as the possibly adverse effect of failure of one buried pipe on a neighbor due to scouring. A study of plant drawings would be required in connection with this aspect." (Emphasis added.) 22/

A detailed assessment of the proposed Indian Point Study was not conducted as part of this contract. However, a brief discussion of the current status of the Indian Point investigation is included in Sections 4 and 5 of this report.

As with other "generic" unresolved safety issues, the history of the systems interaction issue has been one of repeated recognition, classification, reclassification, and relisting without much progress. The ACRS felt that at least some types of systems interaction which might lead to a significant degradation of safety could be identified and then dealt with through a study of Licensee Event Reports (LERs), which each reactor owner must make when abnormal incidents occur. However, the ACRS itself concluded in NUREG-0572[23/] that a detailed review of LERs cannot be expected to identify all systems interactions. By far, the bulk of the LERs deal with failure of individual components and equipment, with relatively few cascades of failures--such as the TMI-2 accident--resulting from an initiating event.[24/]

Similarly, in 1975 the NRC-commissioned "Rasmussen Report" (WASH-1400) recognized that the greatest accident risk is posed not by the large single (or so-called "design basis") accidents, but by <u>small</u> loss-of-coolant accidents compounded by <u>multiple</u> failures or human error,[25/] such as the 1970 and 1971 accidents at Commonwealth Edison's Dresden nuclear facility[26/] and the TMI-2 accident. While WASH-1400 was severely criticized as overoptimistic by the NRC's Lewis Committee in 1978,[27/] and the NRC then formally disavowed WASH-1400's overall conclusions about the low risk of nuclear accidents,[28/] its recognition of where the major accident risks lie has not been faulted. Yet the NRC's Special Inquiry Group found that "[t]hese types of potential accident sources have...been all but ignored by the NRC in the regulatory review process."29/

After the systems interaction issue became a high-priority issue in the list of generic unresolved technical issues which was first published in NUREG-0410, NRC contracted with Sandia Laboratories to study it. In December, 1979, Sandia issued its Phase I report, clarifying some of the potential undesirable interaction areas not adequately taken into account in the NRC review process (for details see Section 3 of this Study). In parallel, the NRC's post TMI "Lessons Learned" Task Force concluded nearly a year ago (in NUREG-0585) that the systems interaction issue required prompt and thorough attention during the licensing process.30/

An assessment of multiple-failure and systems interaction for U.S. commercial nuclear power stations has been specifically precluded in the past by the Atomic Safety and Licensing Board ruling, such as follows, that, based on its test of credibility:

> "....mechanisms which depend upon independent simultaneous failure of more than one piece of safety grade equipment also fail the test. Indeed, the single failure criterion embodied in 10 CFR Part 50, Appendix A, supports the view that the Commission does not intend such mechanisms to be examined. In this regard, the Board gives no weight whatever to the fact that a study such as that reported in WASH-1400 may have considered and evaluated such mechanisms; we do not view 'credible' in the present sense as being synonymous with 'worth looking at'." 31/

Thus, the systems interaction issue has been a known, unresolved safety issue since at least 1974, when the ACRS requested that the NRC Staff give attention to it. It was a Category A high-priority generic technical issue in NUREG-0410, published in January, 1978.[32/] It was classed as a "potential high risk" issue in the NRC's 1978 risk-based evaluation of unresolved safety issues.[33/] It was one of the top twenty unresolved safety issues listed in the NRC's January, 1978, Report to the U.S. Congress.[34/] In fact, in the Denton/Steering Committee "point value" NRC manpower allocation directives, no issue had a higher point value.[35/] It is part of the TMI Action Plan (as "Task" II.C.3), with a priority 1 classification and a point value indicating that it was again determined to be of high safety significance for the Action Plan as well.[36/]

In summary, the systems interaction issue has been recognized again and again as a high-priority, high-risk-potential, unresolved safety issue. It is directly applicable to all nuclear power stations. At least three different possible approaches to the issue have been suggested: a "fault-tree" approach, as in WASH-1400 (Section 3 of this Study); a physical plant inspection of interaction possibilities, as the ACRS suggested for the Westinghouse-designed Indian Point nuclear plant; and a site-specific analysis based on a single initiating event (e.g., an earthquake) as the ACRS requested be performed for the Diablo Canyon plant in California (Section 5 of this Study).

2.5: SUMMARY

Safety systems for commercial nuclear power stations are designed based on the criterion that they must be able to survive any single failure and still accomplish their safety goal or mission. This has resulted in a level of redundancy and, in some cases, diversity, to make systems capable of complying with the single failure criterion. However, several accidents, including TMI-2, have shown that there are serious safety implications from failures in one system which affect or interact with other systems to cause additional complicating failures. Detailed plant-specific studies appear needed to assess the potential safety improvement available through reduction in system interactions by careful consideration of multiple-failures.

SECTION 2

LIST OF REFERENCES

1/ Rogovin Report, page 147.

2/ The Need for Change: The Legacy of TMI, Report of the President's Commission on the Accident at Three Mile Island (U.S. Government Printing Office, Washington, D.C., October 1979), pages 9, 19-20, 52. This is hereafter referenced "Kemeny Report."

3/ Rogovin Report, pages 147-148.

4/ Kemeny Report, pages 9, 19-20, 52.

5/ Rogovin Report, pages 119, 148, 150.

6/ Rogovin Report, page 119.

7/ Advance notice of proposed rulemaking "Consideration of Degraded or Melted Cores in Safety Regulation," Federal Register, Vol. 45, No. 193, October 2, 1980, pages 65474 to 65476.

8/ Regulatory Guides are available from the U.S. Nuclear Regulatory Commission, Washington, D.C., 20555.

9/ There are other design requirements which would presuppose events where significant core damage and release of radioactive material has occurred. For example, radioactive source terms of Technical Information Document TID-14844,"Calculation of Distance Factors for Power and Test Reactor Sites," which imply a major reactor accident, are used to judge design adequacy of various engineered safety features and certain other plant systems and components. TID-14844 is available from National Technical Information Service, U.S. Department of Commerce, Springfield, Virginia 22151.

10/ NUREG-0585, TMI-2 Lessons Learned Task Force - Final Report U.S. Nuclear Regulatory Commission, Washington, D.C., October, 1979, page 3-1.

11/ Rogovin Report, Vol. II, page 18.

12/ NUREG-0683, Draft Programmatic Environmental Impact Statement for TMI-2 Decontamination and Disposal of Radioactive Wastes, 1980, U.S. Nuclear Regulatory Commission, Washington, D.C., page S-1.

13/ NUREG-0578, TMI-2 Lessons Learned Task Force Status Report and Short-Term Recommendations, 1979, U.S. Nuclear Regulatory Commission, page 16.

14/ Ibid 13.

15/ Ibid 10, page 3-3.

16/ Kemeny Report, page 52.

17/ Rogovin Report, page 148.

18/ Kemeny Report, pages 19 to 20.

19/ Kemeny Report, page 63.

20/ Rogovin Report, pages 148 to 151.

21/ Rogovin Report, page 119.

22/ ACRS letter to NRC, October 12, 1979.

23/ NUREG-0572, Review of Licensee Event Reports (1976-1978), U.S. Nuclear Regulatory Commission, Washington, D.C., September, 1979, pages 3-3, D-9 to D-12, D-19 to D-22.

24/ Ibid 23.

25/ WASH-1400 (NUREG-75/014), Reactor Safety Study - An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, U.S. Nuclear Regulatory Commission, Washington, D.C., October, 1975. The NRC's Special Inquiry Group said that WASH-1400 "shows that the greatest risk of an accident comes not from the design basis accidents, such as the large loss-of-coolant accident, but from small loss-of-coolant accidents and relatively routine transients compounded by multiple failures or human error, having a higher probability of occurring than a large pipe break." Rogovin Report, page 148. The Kemeny Commission agreed. Kemeny Report, page 32. Both groups agreed that TMI-2 was an accident of this type, and the Kemeny Commission added (page 32) that "based on WASH-1400....such accident should have been expected."

26/ Kendall, et al, The Risks of Nuclear Power Reactors, Union of Concerned Scientists, Cambridge, Massachusetts, August, 1977, Appendix B.

27/ NUREG/CR-0400, Risk Assessment Review Group Report to the U.S. Nuclear Regulatory Commission, U.S. Nuclear Regulatory Commission, Washington, D.C., September, 1978.

28/ Nuclear Regulatory Commission Statement of Policy, Federal Register, January 18, 1979.

29/ Rogovin Report, page 148.

30/ Ibid 10, page 3-3.

31/ ASLB Memorandum and Order, May 25, 1977, Black Fox Station, NRC Docket Nos. 50-556 and 50-557, page 5.

32/ NUREG-0410, NRC Program For The Resolution Of Generic Issues Related To Nuclear Power Plants, U.S. Nuclear Regulatory Commission, Washington, D.C., January 1978.

33/ Taylor, et al, Summary Report On A Risk Based Categorization Of NRC Technical and Generic Issues, preliminary draft issued by NRC, page 1. In addition, see NUREG-0510.

34/ NUREG-0510, Identification of Unresolved Safety Issues Relating to Nuclear Power Plants, Report to Congress, U.S. Nuclear Regulatory Commission, Washington, D.C., January, 1979.

35/ See NRC Document SECY-79-76 (January 30, 1979), a memorandum from Harold R. Denton, Director, Office of Nuclear Reactor Regulation, to the NRC Commissioners. In addition, see memorandum from Harold R. Denton to Roger S. Boyd, et al, January 23, 1979 (attached to SECY-79-76).

36/ NUREG-0660, NRC Action Plan Developed as a Result of the TMI-2 Accident, Vols. I, II, U.S. Nuclear Regulatory Commission, Washington, D.C., May 1980.

UNITED STATES OF AMERICA
NUCLEAR REGULATORY COMMISSION

THE ATOMIC SAFETY AND LICENSING BOARD

In the Matter of	)	
	)	
COMMONWEALTH EDISON COMPANY	)	Docket Nos. 50-237-SP
	)	50-249-SP
(Dresden Station, Units 2 and 3)	)	(Spent Fuel Pool Modification)
	)	

CERTIFICATE OF SERVICE

I hereby certify that I have this 10th day of December, 1980, served copies of the foregoing Intervenor's Response to Applicant's Motion to Strike by depositing same in the U.S. Mails, first-class, postage prepaid, to the following:

John F. Wolf, Esq.
3409 Shepherd Street
Chevy Chase, Maryland 20015

Dr. Linda W. Little
5000 Hermitage Drive
Raleigh, North Carolina 27612

Dr. Forrest J. Remick
305 East Hamilton Avenue
State College, Pennsylvania 16801

Atomic Safety and Licensing Board Panel
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

Docketing and Service
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

Richard Goddard
Office of the Executive Legal Director
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

Philip P. Steptoe, Esq.
Isham, Lincoln & Beale
Suite 4200
One First National Plaza
Chicago, Illinois 60603

Mary Jo Murray

MARY JO MURRAY
Assistant Attorney General
Environmental Control Division
State of Illinois