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 Restart
(Three Mile Island Nuclear Station, Unit No. 1)	)	

UNION OF CONCERNED SCIENTISTS
PROPOSED FINDINGS OF FACT AND
CONCLUSIONS OF LAW ON UCS
CONTENTIONS NOS. 13 and 14
AND BOARD QUESTIONS 2 AND 6

Ellyn R. Weiss
HARMON & WEISS
1725 I Street, N.W.
Suite 506
Washington, D. C. 20006
(202) 833-9070

DATED: June 12, 1981

Table of Contents

UCS Contention No. 13	page 129
Board Question No. 6	page 166
UCS Contention No. 14	page 195
Board Question No. 2	page 229

UCS Contention No. 13 was accepted for litigation by this Board as follows:

> "The design of TMI does not provide protection against so-called 'Class 9' accidents. There is no basis for concluding that such addicents are not credible. Indeed, the staff has conceded that the accident at Unit 2 falls within that classification. Of the realm of possible accidents, the staff's method of determining which fall within the design basis accidents and those for which no protection is required is faulty in that the design basis accidents for TMI do not bound the credible accidents which can occur. Therefore, there is not reasonable assurance that TMI-1 can be operated without endangering the health and safety of the public and resumption of operation should not be permitted."

314. UCS made it clear that the essence of its contention is that the staff has no technically supportable method for classifying particular accident sequences as either credible or not credible. (Union of Concerned Scientists and Steven C. Sholly Joint Proposed Reply Procedural Findings, 5/18/81, at 14-15).

315. The term "Class 9" accidents is derived from a proposed rule published by the Atomic Energy Commission in 1971. The proposed rule, which has now been withdrawn by the Nuclear Regulatory Commission, set forth a system of classification of potential accidents for use in NRC Staff assessments performed pursuant to the National Environmental Policy Act of 1969. The proposed rule set forth a spectrum of accidents divided into nine classes ranging from trivial in nature to the most severe for the purposes of evaluating environmental risk.

316. Class 9 accidents were characterized in the proposed rule as "involv(ing) sequences of postulated successive failures more severe than those postulated for the design basis for protective systems and engineered safety features." These events, characterized as beyond the design basis, were not explicitly assessed in determining the adequacy of the facility design. For the purposes of analysis pursuant to 10 CFR Part 100, Class 9 accidents were considered as "not credible". (Rosenthal and Check, ff. Tr. 11,158, at 6-7)

317. The design basis is the set of prescribed anticipated operational occurrences and accidents used to assess the way specific systems respond to upset conditions. Design-basis events (DBE's) are events or sequences of events which fall within the design basis. DBE's provide a set of analytic tests of the plant design, consisting of sample challenges to the plant safety systems. These tests are used by the Staff to determine if installed or proposed safety features can cope adequately with the DBE's (Rosenthal and Check, ff. Tr. 11,158, at 4).

318. An explicit list of DBE's is not provided in the Commission's regulations, but must be found on a system-by-system basis for each plant in the Final Safety Analysis Report (FSAR), the Technical Specifications, applicable reference or topical reports, and related design documents (Rosenthal and Check, ff. Tr. 11,158, at 3). The set of DBE's now used by the Staff to test the overall adequacy of the plant design was not developed until the mid-1970's (Rosenthal and Check, ff. Tr. 11,158, at 17-18). A listing of events to be considered is included in Regulatory Guide 1.70, Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants (Revision 2), issued in 1975 (Levy,

ff. Tr. 11,049, at 2). The Board notes in this context that TMI-1 received its operating license in April 1974.

319. The response of each plant to the DBE's is assessed using the requirements stated in the General Design Criteria (10 CFR Part 50, Appendix A) and other standards set forth in the Standard Review Plan and Regulatory Guides. The consequences of DBE's are assessed against the requirements of 10 CFR Part 100; for the purposes of this analysis, DBE's are considered to be "credible" events (Rosenthal and Check, ff. Tr. 11,158, at 5).

320. Since the withdrawal of the AEC's proposed rule by the Commission, the term "Class 9" accident has no formal meaning, but it is in common usage. The Staff uses the phrase "events beyond the design basis" as equivalent to the term "Class 9" (Tr. 11,245-46, Rosenthal).

321. The Staff's use of the design-basis event concept and the manner in which this concept is applied in the licensing and safety review process is quite clear to this Board and would be acceptable if the Staff had a scrutable, technically justifiable method of determining which events are credible (i.e., within the design basis) and which are not credible (i.e., beyond the design basis). It is fundamental that in order to make a reasonable assessment of the safety of nuclear plants one must have knowledge of the likelihood of a particular event or sequence of events. Once one understands the likelihood of an event or sequence,

the consequences of the event or sequence must be understood. Understanding the likelihood and consequences of an event or sequence, one is then in a position to determine, based on appropriate criteria, whether the event or sequence needs to be protected against (and hence should be included within the design basis), or whether no such protection is required (and hence should be excluded from the design basis). The evidence and testimony presented to this Board demonstrates quite clearly that the Staff has no scrutable method for making the determination of credible or not credible.

322. The most widely recognized study which produced probability estimates on various events and sequences of events was WASH-1400, the so-called Rasmussen Report (Reactor Safety Study, October 1975). The NRC, in response to criticisms of WASH-1400, formed a panel to review WASH-1400 (the panel has become known as the Lewis Committee, after its Chairman, Harold Lewis, now a member of the Commission's Advisory Committee on Reactor Safeguards). In "Report of the Risk Assessment Review Group to the U.S. Nuclear Regulatory Commission" (NUREG/CR-0400, September 1978), the Lewis Committee questioned the absolute probability numbers used in WASH-1400, stating:

> "We are unable to determine whether the absolute probability of accident sequences in WASH 1400 are high or low, but we believe that the error bounds on these estimates are, in general, greatly underestimated. This is true in part because there is in many cases an inadequate data base, in part because of an inability to quantify common cause failures, and in part because of some questionable methodological and statistical procedures." (Rosenthal and Check, ff. Tr. 11,158, at 24).

323. In a January 19, 1979 Policy Statement, the Commission withdrew any endorsement of the Executive Summary of WASH-1400 and noted that the Commission "does not regard as reliable the Reactor Safety Study's numerical estimates of the overall risk of reactor accident." Licensing Boards were cautioned not to rely on the probability estimates in WASH-1400 as a basis for their decisions.

324. It became clear in the litigation of UCS Contention No. 13 that the Staff has no numerical estimates of overall plant reliability for TMI-1. The Staff estimated that a year would be required to generate such numbers (Tr. 11,242, Tourtellotte; Tr. 11,242-43, Check). The Staff has no probability numbers, is not attempting to generate such numbers, and therefore does not rely on probability numbers (Tr. 11,165-67, Tourtellotte). The Staff has not evaluated and does not know the probability that an accident beyond the design basis of TMI-1 will occur (NRC Staff Response to Union of Concerned Scientists First Set of Interrogatories, March 7, 1980, answer to Interrogatories 134 and 135, as cited in Union of Concerned Scientists Motion for Summary Disposition of UCS Contention No. 13, which went unchallenged by the NRC Staff). The Staff has no prevent means to reliably estimate the probability that accidents which it deems or deemed incredible will in fact occur, and does not know how many other accidents previously deemed "incredible" are, in fact, credible (Union of Concerned Scientists Motion for Summary Disposition of UCS Contention No. 13, at 3-4).

325. In fact, the Staff acknowledged that prior to responding to this contention, the Staff had not "set down in

sufficient clarify for all to follow" the Staff's method of analyzing and classifying accidents, and that "this was a very appropriate time to reflect and try to set down clearly, if we could, what it is we do and how we do it." (Tr. 11,192, Check). The Staff's testimony makes it clear that the Staff never, prior to this proceeding, had a clearly defined method for classifying accidents as credible or not credible, and that the Staff's testimony represents a post hoc effort at rationalizing, for the purposes of this particular litigation, both the lack of a clearly stated methodology and the actual lack of a technically scrutable method for classifying accidents. There is an inherent evidentiary weakness in such testimony.

326. The Board notes that there were numerous recommendations made by the Lessons Learned Task Force which relate to this very problem, that of classifying accidents. Although the examples which the Board will cite are long-term items, the Staff has clearly turned a blind eye toward them in responding to this contention, and has gone about responding to the contention in a "business-as-usual" framework. Among the recommendations of the Lessons Learned Task Force are the following:

a. That the Staff perform a systematic assessment of the reliability of safety systems in operating plants (NUREG-0585, at A-14).

b. That the number of failures in non-safety equipment that are considered in accident analyses should reflect the expected number of non-safety systems simultaneously exposed during the event under study to conditions for which they were not designed or qualified (NUREG-0585, at A-14).

c. That the use of probabilistic analysis to supplement the "deterministic" analysis normally done in the past be implemented. The Task Force noted, "There remains, however, the possibility that significant event sequences have been overlooked and not included within the current design basis

events, or that the deterministic design requirements are incomplete or inadequate for some events and systems." (NUREG-0585, at 3-1 to 3-2).

d. That the general safety criteria should be revised, including the issue of whether to modify or extend the current design basis (NUREG-0578, at 16-17).

327. According to Staff witnesses, the "method used by the Staff to characterize events or sequences of events as "credible" or "not credible" is "engineering judgment informed by engineering assessment of the performance characteristics of the various systems and components in a nuclear power reactor, and of the kinds of system or component failures that may occur" (Rosenthal and Check, ff. Tr. 11,158, at 16-17).

328. From the Board's perspective, this only states the obvious. Any method of determining which accidents are credible and which are not credible, regardless of whether that method involves probabilistic risk assessment, fault-tree analysis, event-tree analysis, or some combination of these or other methods, ultimately rests on engineering judgment. In the Board's view, it is how that engineering judgment is applied that is the key--how one reaches the determination of what is credible and what is not credible is at the very heart of this issue. The bottom line is that the Staff has no method of making such a determination. It is unusual in writing a decision that a Board relies on exact quotes from the record, but in this instance the Staff's own words speak quite clearly to the problem.

329. The Commonwealth of Pennsylvania's nuclear engineer, Mr. Dornsife, requested the Staff, in cross-examination to describe whether there are any strict criteria or guidance used by the Staff to determine what is or is not a credible event or sequence of events. The responses of the two Staff witnesses were astonishing:

> "There is no numerical safety goal. There is no numerical cutoff between credible and not credible in terms of probabilistic numbers or numbers of failures that would have to occur. There is no definitive test." (Tr. 11,203, Rosenthal).
>
> "And a specific answer to your question is no, there is no guidance given to the Staff which enables it to declare an event or sequence of events credible or not credible." (Tr. 11,203, Check).

330. This testimony alone would be sufficient, or nearly so, to sustain UCS's contention that the Staff has no technically justifiable method of classifying accidents as either credible or incredible. It indicates clearly that there are no criteria used by the Staff in determining whether concededly possible accident sequences are either not "credible", or should be include within the design basis. It should be noted that the total absenc of regulatory criteria raises a question going beyond the issue of the probability or likelihood of particular accidents. Even if all parties agreed that the probability of accident "X" were 10^{-5} or any other number, the question would still remain: should that accident be within or outside the design basis? As to this question -- the definition of "credible" for the purposes of design -- neither the Staff nor the Licensee has presented any evidence.

331. Mr. Dornsife then asked the Staff witnesses if there were any qualitative goals or qualitative criteria which the Staff used in making a determination of whether an event or sequence of events is credible or not credible. The only example which the Staff witnesses could point to was the single-failure criterion. (Tr. 11,204, Check) The Board will return to the single-failure criterion below.

332. An even more telling piece of testimony was given by Staff witness Check:

> "We do not have a process that I could describe for you easily that would spit out an answer, credible or incredible, when we embark on a study of events. . . We described the deterministic, the engineering judgment, the deterministic approach that [we have] employed for the past several decades, and how we have gotten to the point of evaluating certain events and perhaps not others. Now it is a reasonable inference, I suppose, to say well, the Staff believes, and therefore, this event is credible and this event is not. I can see now -- how you can make that judgment, and in fact, I guess that is implied in what we do. . ." (Tr. 11,199, Check).

333. It is quite clear that the Staff has no scrutable method by which it determines whether events or sequences of events are credible or not credible. Returning now to the issue of the use of the single-failure criterion, it became clear as a result of cross-examination that the single-failure criterion is not without its problems. The single-failure criterion grew out of work on electrical components in which the reliability of each of the trains was rather high, and, in such a case, the adoption of single level redundancy was appropriate. However, the Staff adopted the single-failure criterion across the board. The Staff now concedes that perhaps this was the wrong approach (Tr. 11,204-05, Rosenthal).

334. The Staff testified that the single-failure criterion is not appropriate for use in connection with requirements for diesel generators (Tr. 11,205, Rosenthal).

335. As the Board discussed in Finding No. 8, supra., it is fundamental that in order to make a reasonable assessment of the safety of nuclear plants one must have knowledge of the likelihood (i.e., probability) of a particular event or sequence of events The Staff, both technical members and legal counsel, repeatedly told this Board that the Staff does not rely on probability numbers or estimates. Yet, it is quite clear that the Staff implicitly relies on probability, even though actual probability numbers are not generated by means of a calculation or assessment process. The Staf: relies on its "sense of more or less what is probable, what is highl; improbable in an engineer's mind" (Tr. 11,200-01, Check). Thus, whether by engineering judgment, formal risk assessment, or some combination of the two, any attempt to classify accidents as credible or incredible depends fundamentally on the probability of occurrence of the accident in question.

336. As the Staff candidly testified, "There is the implication of an understanding of probabilities in this thing we have called a deterministic approach." (Tr. 11,253, Check). This is self-evident.

337. Moreover, the Staff used its implicit understanding of probabilities in the selection of events or event sequences to be analyzed in safety analyses (Rosenthal & Check, ff. Tr. 11,158, at 20). The Staff testified, however, that it did not use any probability numbers from WASH-140 (Tr. 11,160-61, Rosenthal). The question to be asked, then, is where did the Staff obtain its

"implicit" understanding of probabilities? The Staff is apparently relying on its judgment of probabilities.

338. The Staff used its judgment to arrive at the set of DBE's used to define the design basis (Levy, ff. Tr. 11,049, at 2; Rosenthal and Check, ff. Tr. 11,158, at 4-5, 17, 20). The Staff uses its judgment in the same manner to evaluate operating experience and new failure modes and failure sequences (Tr. 11,248, Check). As the Board will shortly explain, this same process was used in originating the set of requirements which came to be embodied in the TMI Action Plan, and later in NUREG-0737. We shall now consider whether this judgment rests on sound ground.

339. The Staff, in its analysis of what events or sequences of events are credible or not credible, relies on its engineering judgement as supplemented by the Staff's engineering assessment of the performance characteristics of the reactor systems and components and, more importantly in the Board's view, the Staff's engineering judgment of "the kinds of system or component failures that may occur." (Rosenthal and Check, ff. Tr. 11,158, at 16-17). The Staff limits itself to consideration of single failures; failures of accident mitigating systems are considered on the basis of single failures (Rosenthal and Check, ff. Tr. 11,158, at 20); compounding of causally unrelated failures is something the Staff considers to be highly improbable, and does not consider at all. (Tr. 11,201, Check) The single-failure criterion is embodied in the Commission's regulations, regulatory guides, and the Standard Review Plan (See, 10 CFR Part 50, Appendix A, Introduction, GDC 17, GDC 21, GDC 24, GDC 34,

GDC 35, GDC 38, GDC 41, and GDC 44). In spite of a recommendation by the President's Commission on the Accident at Three Mile Island that there be increased attention to the possibility of multiple failures, Staff witness Wermeil could not point to any new requirements that multiple failures be considered in evaluating the emergency feedwater system, for example (Tr. 16,756-57, Wermeil). The witness was aware of a general pursuit of this particular recommendation in other areas, but provided no examples (Tr. 16,757, Wermeil). The Staff has totally eliminated any consideration of the occurrence of two or more random equipment failures as initiating events by, on the basis of Staff judgment, precluding such failures from the design basis (Rosenthal & Check, ff. Tr. 11,158, at 20). In fact, the only criterion which the Staff could name which is used in determinations of whether events or event sequences are credible or not credible is the single-failure criterion (Tr. 11,203, Check).

340. The Staff's use of the single-failure criterion is typically limited by the General Design Criteria of 10 CFR Part 50, Appendix A, to evaluations of safety-grade systems. However, if the Staff's evaluation of the B&W report in the Integrated Control System Reliability Analysis (BAW-1564) is any indication, the Staff is extending this principle to even non-safety-grade systems such as the ICS (Tr. 7005, Joyner; Licensee Ex. 18, at 4-1, 4-2; Tr. 6964, Joyner; Tr. 7240, Thatcher).

341. This over-riding reliance on single failures is not warrante As Oak Ridge National Laboratory observed, "The serious safety problem experienced in operating reactors have, in general, involved multiple failures, or sometimes a single failure compounded by operator error." (Sholly Ex. 2, lt 10) The TMI-2 accident, which according to the Staff was a Class 9 accident (i.e., an accident beyond the design basis) (Rosenthal and Check, ff. Tr. 11,158, at 8), was caused by a common mode failure of redundant trains of high-pressure injection (HPI) resulting primarily from operator error. (Tr. 11,238, Rosenthal) Use of the single failure criterion results in the classification of the TMI-2 accident as incredible.

342. Multiple failures were postulated in the Staff's "Class 9" accident sequence study (NRC Staff Ex. 3, at 7-11). Four of the seven postulated loss of main feedwater sequences led to a loss-of-coolant-accident (LOCA), namely sequences designated as TQ, TP_2, TL, and TLP_2 (NRC Staff Ex. 3, at 13). Of the seven sequences beginning with a LOCA, five of these sequences lead to core melt, namely sequences designated as BH, BP, BRH, BRP, and BD (NRC Staff Ex. 3, at 14). Some of the core melt sequences lead to containment failure, namely sequences designated as BP (NRC Staff Ex. 3, at 16), and any loss-of-feedwater sequences which end with the BP LOCA sequence, namely sequences designated as T_2S_3 (ibid., at 21), T_3S_3 (ibid., at 26), T_5S_3 (ibid., at 31), and T_6S_3 (ibid., at 36). In all such cases, containment failure is caused by failure of post-accident heat removal (PAHR).

343. The Staff explicitly precludes any consideration of

core melt and/or containment failure accidents (including the TMI-2 accident sequence) within the design basis because such events and event sequences involved multiple failures (Tr. 11,246 Rosenthal). The Staff goes even further, however, and concludes that on the basis of the implementation of the measures specified in the Staff's "Class 9" accident report (NRC Staff Ex. 3), the event sequences with close nexus to the TMI-2 accident "are no longer dominant contributors to total risk, but rather represent risks consistent with other contributory risks of the facility as a whole. In this sense, the probability of these event sequences occurring and leading to core melt, with concurrent or consequential containment failure such that Part 100 guidelines are exceeded, is sufficiently low that these event sequences may be considered not 'credible.'" (Rosenthal and Check, ff. Tr. 11,158, at 16) However, since the Staff has not quantified the probability of progressing up or down on the event trees in the Staff's core damage sequence accident report (NRC Staff Ex. 3, at 13-14) (Tr. 11, 250, Rosenthal), the Staff simply has no basis for concluding that this is the case.

344. This conclusion appears to be consistent with Staff practice concerning actual operating experience. As the Staff testified, "As we learn of new potential failure modes and failure sequences we explore them and we evaluate them in the way we had evaluated design basis events. . ." (Tr. 11,248, Check) Board emphasis. Apparently, the Staff has examined the TMI-2 accident sequence, concluded that the proximate cause was a common mode failure of redundant HPI trains caused primarily by operator error (Tr. 11,238, Rosenthal), and therefore concluded

that since the TMI-2 accident involved multiple failures it was beyond the design basis (Tr. 11,246, Rosenthal).

Had the TMI-2 accident not actually happened, but rather had it been predicted on the basis of an analysis, the Staff would have declared this sequence to be beyond the design basis and dismissed it as not credible. As the Staff testified, either it is a design basis accident, or it is not and, therefore, one need not worry about it (Tr. 11,248-49, Check).

345. However, since the TMI-2 accident represents actual operating experience, rather than an analytical result, the Staff was forced by circumstances to do more. Two products of this additional effort are the TMI Action Plan (to which the Board will later address itself) and, as a result of considerable prodding by the Board in this proceeding, the Staff's "Class 9" report, "TMI-1 Potential Core Damage Accident Sequences and Preventive and Mitigative Measures" (June 1980) (NRC Staff Ex. 3). As discussed above, the Staff's core damage accident report revealed that there are several sequences with nexus to the TMI-2 accident which result in core melt, some also involving containment failure (See, Finding No. 26, supra.). As a result, it was necessary for the Staff to attempt to prove that these sequences were not "credible." It undertook to do so by attempting to demonstrate that post-TMI-2 improvements or modifications moved these accident sequences from the realm of the credible to the incredible. The Staff's core damage accident sequences report cites many pages of recommendations and changes proposed by the Staff, most of which correspond to items in the TMI Action Plan. Before addressing the specific recommendations in the core damage sequence report, the Board will address the genesis of the TMI Action Plan.

346. By the Staff's own testimony, the TMI Action Plan arose from the traditional way in which the Staff has done business, i.e., "to consider virtually everything that occurs to us, starting from the reviewer level and having suggestions reviewed internally through several stages of management, having them amplified, having them focused, and then having discussions first with the ACRS and subsequently with the Commission itself, and at each stage learning from the discussions, incorporating the good that came of those discussions, and in that way developing a sound engineering regulatory approach to the problem." (Tr. 11,180-81, Check).

347. Staff witnesses Ross and Capra testified before the Board on Board Question No. 2, which was intimately related to the consideration of accidents beyond the design basis. Board Question No. 2 was stated by this Board as follows:

> "(Tr. 2392) "The Board stated its concern with having an adequate record on the sufficiency of the proposed short-term and long-term actions to protect the health and safety of the public. Without further explanation the question may appear to invite conclusionary testimony of the ultimate factual issues to be decided by the Board. (Commission's August 9, 2979 Order, 10 NRC 141, 148.) This is not what the Board has in mind as a response to the question. Our concerns were expressed in part in the June 23, 1980 memorandum on the Staff's report on TMI-1 accident sequences. To explain further: We assume that the Staff and Licensee may present evidence that each Category A and each Category B recommendation in Table B-1 of NUREG-0578 (Order items ST 8 and LT 3, and that each preventive and mitigative measure identified with respect to a given accident sequence in the Staff's TMI-1 Core Damage Accident Sequence Report will be, at least, sufficient to resolve the related safety problem or accident sequence. However, nowhere have we seen in the

> Restart Report, SER, the Accident Sequence Report, or elsewhere, an explanation as to how the Staff or Licensee has determined that all of the necessary TMI-2 related recommendations have been identified and that all the appropriate accident sequences have been addressed. The Board wants testimony or other evidence which explains, if such be the case, how the Licensee and the Staff have concluded that the NUREG-0578 short- and long-term recommendations, and other subsequent safety recommendations, and the identified accident sequences (with their respective preventative or mitigative measures) are in their totality sufficient to provide reasonable assurance that TMI-2 can be operated without endangering the health and safety of the public. The question is not intended to enlarge the scope of the hearing. The response may be limited to consideration of accidents following a loss-of-feedwater transient."

348. Staff witnesses Ross and Capra made two basic arguments in response to this Board Question. First, the witnesses conclude that because the Action Plan grew out of the collective and comprehensive assessment by persons within and outside the NRC having expertise in many technical disciplines, this provides reasonable assurance that the probable causes of the TMI-2 accident and their associated corrective measures have been completely and adequately identified (Ross and Capra, ff. Tr. 15,555, at 5).

349. Secondly, the Staff concludes that "general agreement" as to the causes of the accident and the areas where improvement should be made provides further assurance that "all significant deficiencies related to the accident have been identified in the Action Plan." (Ross and Capra, ff. Tr. 15,555, at 5).

350. In summary, the Staff bases its assurance that the Action Plan contains all areas needing improvement as a result of the TMI-2 accident on the process that was used to arrive at the Action Plan (Ross and Capra, ff. Tr. 15,555, at 11). The same

holds true for the assurance that surrounds the necessity and sufficiency of the items in the subset of Action Plan items that the Staff has determined are required for implementation by the Licensee prior to restart (Ross and Capra, ff. Tr. 15,555, at 11-12).

351. The Staff further argues, that having used the process of arriving at the Action Plan, and having taken what it describes as a "broad approach" to accidents with nexus to TMI-2, that this "obviated the need for a probabilistic assessment screening to focus on particular sequences." (Rosenthal and Check, ff. Tr. 11,158, at 16).

352. In both cases, in arriving at the set of actions and recommendations that comprise the Action Plan, and in arriving at the set of sequences that comprise the Staff's judgment as to accident sequences with a reasonable nexus to the TMI-2 accident, it is the Board's conclusion that the Staff has exalted form over substance. Nowhere in the record of this proceeding is there evidence that the Staff has undertaken a systematic evaluation of the TMI-2 accident and accident sequences with a reasonable nexus, and evaluated alternative recommendations as to their effectiveness in meeting the concerns raised by the TMI-2 accident, nor is there evidence in this record that the Staff has systematically identified both all the areas which require improvement as a result of the TMI-2 accident, and the necessary degree of improvement. Indeed, once the various investigations of the TMI-2 accident were completed, it was

the NRC Staff which controlled which recommendations were highlighted what measures were presented to the Commission to address these recom at s, and the priority given to these measures and recommendations. The Staff's indelible imprint is found throughout the Action Plan. N where in the record, or elsewhere for that matter, is there the sligh suggestion that the Staff has attempted to have the various investiga bodies (or members thereof) evaluate the specific measures recommende by the Staff to address the concerns raised by the investigators and comment on them.

353. Even the Staff's characterization of what disagreement it i willing to acknowledge regarding the Action Plan displays an attitude favors form over substance. The Staff testified, "Where differences opinion occurred, they most often related to the degree of improvemen required and the best method of achieving that improvement." (Ross a Capra, ff. Tr. 15,555, at 5) The Staff's testimony on this matter co veniently avoids any discussion of disagreements within the Staff and disagreements with persons outside the Commission, as if the substanc of their disagreement (i.e., disagreement over how much improvement i necessary and the best manner in which to achieve that degree or impro ment) made that disagreement somehow unimportant or as if the manner which the disagreement was dealt with somehow was more important than the substance of the disagreement.

354. It is worth noting, in connection with Board Question No. 2 that the Licensee presented no testimony on this key issue, despite an express invitation from the Board to do so. Moreover, Licensee's cros examination of the two Staff witnesses was aimed exclusively at testin the necessity of certain of the Staff's recommendations, while failing address the issue of the sufficiency of the recommendations. (See, Tr 15,637-15,740)

355. The Board now moves to the issue of the sufficiency of the recommendations, i.e., the "fixes" (to use the Staff's term), which were recommended in the Staff's core damage accident sequence report. We must consider whether these measures are sufficient to move TMI-related Class 9 sequences from the "credible" back into the realm of the "incredible." Before addressing the specific recommendations, the Board will address the general approach taken by the Staff in making recommendations for changes to be made as a result of the TMI-2 accident. Past practice has been for the Staff to address accidents at the high-consequence end of the design basis (e.g., a double-ended guillotine break of the RCS) primarily by requiring the installation of emergency safety features (i.e., hardware changes), although the Staff has also employed some procedural measures to mitigate DBE's. Event sequences within the design basis (but not at the high-consequence fringe) have been "fixed" by the Staff primarily by requiring increased surveillance and testing of equipment, improved plant procedures, improved operator training, and some hardware requirements. The goal of these "fixes", according to the Staff testimony, is to reduce the probability and/or the consequences of an event sequence. Selection of the means to implement one or more of the "fixes" is based in part on risk assessment, but predominately on "engineering judgment." (Rosenthal and Check, ff. Tr. 11,158, at 18). For accidents within the design basis, the assumption has presumably been that if operator action or procedures fail, there are engineered plant safety systems to mitigate such events.

356. However, there are no safety systems designed to mitigate accidents beyond the design basis. In addition, the occurrence of a Class 9 accident by definition implies the failure of safety systems

either through mechanical malfunction or operator action. Despite th fact that Staff practice has been to address accidents at the limit o the design basis primarily by requiring hardware modifications, the Board finds upon examination of the "fixes" proposed by the Staff to address the first accident beyond the design basis that most of the "fixes" are related to operator training and procedural modifications The record in this proceeding does not establish the degree of gain i safety, either in terms of reducing the probability of accident sequences of reducing the consequences of the accident sequences, from such procedural and training modifications.

357. In fact, the Staff testified that it could not quantify such gains which occurred principally in the "human regime". (Tr. 11,251, Rosenthal) The Staff was very reluctant to place any quantifiable terms on the probability of operator error, and, indeed, the Staff found it as difficult to correct operator action as it did to place numbers on the probability of operator error. (Tr. 11,235-36, Rosenthal and Check) The Staff testified that it had included operat error in the core damage sequence report, but that the inclusion was implicit since the report did not distinguish the cause of hardware failure (either mechanically - or operator error - induced). Signifi ly, by so considering operator error, the Staff equates the probabilit of and the results of operator error with mechanically-induced hardware failure. There is absolutely no evidence in this record which justifies such an assumption. There is no record in this proceeding of the likelihood and consequences of operator action or inaction.

358. Thus, the Board again arrives at a critical point in the Staff's "methodology" regarding the determination of "credible" and "not credible" accidents and the determination of the sufficiency of the "fixes" proposed to deal with such accidents, and again the Board finds the Staff relying implicitly on probabilities without having probability numbers or actual calculations to back up the Staff's judgment of what the probabilities are. The Staff relies upon its judgment as to the selection of "fixes", again without any apparent systematic consideration of the relative worth of the fixes in improving the safety of the plant or reducing the consequences of the accident sequences. In fact, the Staff acknowledges that not only is the record incomplete from the standpoint of describing the benefits of the proposed "fixes", but the record is also incomplete from the standpoint of describing the potential risks associated with even what is presumed to be an improvement (Tr. 11,189, Check). The issue of the "potential risks associated with even what is presumed to be an improvement" has not been addressed at all in this proceeding by either the Staff or the Licensee.

359. The hardware changes proposed by the Staff are as follows (Rosenthal and Check, ff. Tr. 11,158, at 14-15):

A. Main feedwater
--none

B. Emergency feedwater
--automatic initiation
--modification of EFW control valves
--automatic block loading of motor driven EFW pumps on diesels
--indication of EFW to each steam generator
--indication of EFW supply water
--automatic feed only to good steam generator logic
--future separation of EFW from ICS

C. Primary pressure relief requirement
--raise relief valve setpoint and reduce high-pressure reactor trip setpoint
--anticipatory trip for loss of feedwater and turbine trip

D. Primary system pressure relief and primary system integrity
--testing of relief and safety valves
--direct indication of valve position
--emergency power to relief and block valves and associated instrumentation control

E. Emergency coolant injection (ECI) and Emergency coolant recirculation (ECR)
--subcooling meter
--instrumentation for inadequate core cooling (full implementation by January 1982)

F. Post accident ralioactivity removal (PARR) and post-accident heat removal (PAHR)
--none

360. The Board believes that even for these limited hardware changes as defined by the Staff there are substantial considerations involved which the Staff did not address. First, upon reading the Staff's core damage sequences report (NRC Staff Ex. 3), it became clear that the post-accident radioactivity

removal (PARR) and post-accident heat removal (PAHR) are both crucial functions. PARR removes radioactivity from the containment atmosphere following an accident (via the reactor building spray system); failure of this system does not effect the condition of the core, but does affect the severity of the consequences of the accident (NRC Staff Ex. 3, at 5, 8, 11). PAHR removes core decay heat from the containment to prevent overpressure of the containment (via the reactor building spray pumps or the reactor building air cooler units); failure of PAHR leads ultimately to containment failure in several of the LOCA sequences presented in the Staff report (NRC Staff Ex. 3, at 5, 8, 11, 16, 21, 26, 31, and 36). The Board notes that the Staff has proposed no hardware modifications whatsoever to these systems as a result of the TMI-2 accident, despite their obvious safety significance and impact on the public health and safety. The Staff is apparently relying on procedural changes and operator training to address these concerns, yet the Board cannot find a single reference to any operator training or procedural changes which specifically affect these two vital functions. The Board can find no basis in the record for concluding that the changes proposed by the Staff and the Licensee will improve either the capabilities of these functions or the reliability of these functions by any degree whatsoever.

361. Secondly, not all of the hardware changes associated with Item D in Finding 42, supra., are, in reality, hardware changes. As the Staff testified, certain of such changes must be

considered to be changes in the "human regime", namely the provision of direct indication of valve position. This change does not alter the probability of failure or success of the valve in performing its function, but rather provides more accurate information to the plant operator. The Staff testified that such improvements must be considered as a "human fix" because "you don't know what he [the operator] is going to do with that." The Staff could not quantify the benefit of such improvements (Tr. 11,251, Rosenthal). The Board also notes that the testing of relief and safety valves will not be completed until 10/1/81 (according to the implementation schedule set forth in NUREG-0737 and in Staff Ex. 13, at 10). In addition, block valve testing is not scheduled for completion until 7/1/82 (ibid., at 10). Even these completion dates are not firm (Tr. 21,046, 21,048, 21,136, Silver).

362. Similarly, there are other "hardware" changes which upon second look are clearly within the "human regime". These changes are instrumentation changes which provide additional information to the plant operators, but do not alter in any way the capabilities of plant equipment or the performance of this equipment. Changes in Finding 42, supra., which fall into the realm of changes in the "human regime" within this definition are, in addition to the example above, indication of EFW to each steam generator (Item B), indication of EFW supply water (Item B), subcooling meter (Item E), and instrumentation for inadequate core cooling (Item E).

363. Regarding the "instrumentation for inadequate core cooling" under Item "E" in Finding No. 42, supra., it is not at all clear that the full implementation date of January 1982 will be met, since the Licensee has not made reasonable progress toward identifying or design such an instrument. In fact, it is nearly certain that it will not be met. Licensee is opposed to the installation of any additional instrumentation for the detection of inadequate core cooling, taking the position that the installed instrumentation, together with additior training, is sufficient both for the short-term and the long-term (Keaten et al., ff. Tr. 10,619). The Board understands this to be a consistent position with regards to Babcock and Wilcox NSSS owners.

364. The Board now turns to the specific "recommendations for improvement" made by the Staff which are claimed to reduce the likelihood of the core damage sequence accidents identified by the Staff, pushing them back to the incredible realm. Table 7 in the Staff's Report (NRC Staff Ex. 3, at 42) lists 14 actions purportedly proposed by the Staff to increase the reliability of the feedwater system by avoiding loss of main feedwater. The Board notes first of all that there have been no hardware changes directed toward decreasing the probability of main feedwater failure. (Rosenthal and Check, ff. Tr. 11,158, at 14) The first recommendation cited by the Staff is the completion of the ICS failure modes and effects analysis. The Board has already dealt at length on the problems inherent in the ICS reliability analysis performed by B&W [See, Proposed Findings of Fact and Conclusions of Law on Plant Design Issues, Steven C. Sholly, 6/1/81]. The Staff also cites items 1-13 on Table 16 (NRC Staff Ex. 3, at 78-79). However, items 1, 3, 11, and 12 are not requirements, having been deleted from TMI

Action Plan requirements in NUREG-0737.* Item 12 has apparently been implemented by the Staff as the SALP program (systematic assessment of licensee performance), but there is no evidence in the record as to the purposes, procedures, or effectiveness of this program and, therefore, the Board can assign this program no weight in evaluating the effectiveness of this recommendation at reducing the probability for loss of main feedwater. Moreover, what little evidence on this matter which is in the record suggests that SALP is a very general program with at best a tangential relevance to reducing the probability of loss of feedwater transients. Item 2 in Table 16 (operational quality assurance program) requires no licensee submittal; additionally, the Staff's evaluation of this matter is not yet complete (NRC Staff Ex. 13, at Enclosure 1). Item 1 (requirement for review of operating experience) is also an area of incomplete Staff review (NRC Staff Ex. 13, at 6). Virtually all of the recommendations with regards to reducing the probability of LOFW transients deal with operator training, review of operating experience, and additional procedural changes. It is unclear what degree of improvement is expected from these changes, and the Staff makes no effort to quantify this improvement. In fact, all the Staff could do was make a general argument that improvements were made, noting however that the degree of improvement could not be quantified "in a manner that is sensible." (Tr. 11,251, Rosenthal) This is an insufficient basis upon which to conclude that otherwise credible accidents are now incredib

---

* These items are:review of operating experience, verification of adequacy of management and technical structure, requirement for onsite safety engineering group, and NRC's systematic evaluation of licensee safety.

365. Table 8 in the Staff's report deals with measures to "Reduce Potential for Failure of Emergency Secondary Heat Removal Function" (NRC Staff Ex. 3, at 46-49). Again, Item 1 on the list is the ICS FMEA. Remarkably, two key measures cited here by the Staff are Items 5 and 7, the IREP program and the resolution of Unresolved Safety Issue A-17. IREP is a program whose benefits, whatever they will be, will accrue at best at some undefined date in the future. There are no plans to include TMI-1 within the IREP program at any time. (Tr. 8709-10, Conran) Regarding systems interaction (A-17), the Board can find no evidence which suggests that any progress is being made in this matter; in any event, this, too, is a long-range matter. TMI-1 is not part of the IREP program and there are now no plans whatever to do any systems interaction study for TMI-1. (Tr. 8685-90, 8709-10, Conran) Manifestly, this Board cannot give any credit for these measures or assume that they contribute anything to reducing the risk of accidents.

366. Table 8 also references numerous items from Table 16 (NRC Staff Ex. 3, at 78-82), which is entitled "Generally Applicable Measures to Reduce the Potential for Safety Functions Failure." The Board was presented with no evidence on the applicability of these measures to preventing emergency feedwater function failure. A number of the recommendations in Table 16 are no longer requirements for TMI-1, despite Staff testimony that <u>all</u> of the recommendations in Table 16 apply to TMI-1. (Tr. 11,275, Rosenthal) Items 3, 11, 12, 24, 25, and 31 in Table 16 are not listed in NUREG-0737, and are therefore not required.*

---

* Item 3 (verification of management and technical capability); Item 11 (requirement for onsite safety engineering group); (continued on next page)

367. Some of the items in Table 16 appear on their face to have at best tangential relevance to avoiding loss of emergency feedwater (i.e., Items 3, 4, 9, 11-13, 21-24, 26, 27, 29, and 30).** The Board has been presented with no

---

** Item 3 (verification of management and technical capability); Item 4 (verification of adequacy of safety review and operational advice); Item 9 (shift manning requirement for emergency situations); Item 11 (requirement for onsite safety engineering group); Item 12 (systematic assessment of licensee safety); Item 13(shift technical advisor); Item 21 (small break analysis); Item 22 (onsite technical support center); Item 23 (onsite operational support center); Item 24 (simulator requirements); Item 26 (revisions to licensing examinations); Item 27 (control room access procedures); Item 29 (requirement for definition of shift supervisor responsibilities); and Item 30 (requirement for review of shift supervisor duties) are not clearly related to emergency feedwater, and the Board was presented with no evidence demonstrating such a relationship in the absence of an obvious link.

(cont) Item 12 (systematic assessment of licensee safety); Item 24 (simulator requirements); Item 25 (long-term program for improving plant emergency procedures); and Item 31 (requirement for plant drills in emergency procedures) are not included in the requirements set forth in NU -0737, and cannot be considered applicable to TMI-1 and cannot be accorded any evidentiary weight whatsoever.

evidence on the degree of improvement expected from these recommendations.

368. Further, the Board notes Licensee's own admission that even the conversion of the emergency feedwater system to safety-grade will not substantially alter the reliability of emergency feedwater since the principal deficiencies are in the environmental qualification of equipment for non-LOCA events (Capodanno, Lanese, and Torcivia, ff. Tr. 5642, at 11). Licensee's own testimony is in conflict on the degree of improvement to be expected from modifications to the emergency feedwater system, since Licensee's Class 9 accident witness Mr. Levy testified that he expected improvements to result in a reduction in frequency of loss of feedwater (and therefore a reduction in demand for emergency feedwater, leading to a reduction in frequency of loss of emergency feedwater) by a factor of 2 to 3 (Levy, ff. Tr. 11,049, at 14). The Board easily resolves this conflict, however, since Mr. Levy's figures are based on WASH-1400 probability results (Tr. 11,130, Levy) and his own probability figures are "based on engineering judgment, on some rather quick assessment of a probability type of calculation, but not, you know, considerable detail type of studies. It was just done on a gross basis, and as indicated there, there are some uncertainties in the numbers." (Tr. 11,091-92, Levy). The Board does not regard Mr. Levy's probability estimates as reliable.

369. In examining each of the Tables purporting to identify measures sufficient to reduce the likelihood of each accident in the Staff's core damage accident sequence report, the Board finds proble similar to those described above. It would appear that the Staff has done little more than compile a list of items which were at some point being considered for implementation on operating reactors, without distinguishing the important from the less important recomme dations, without indicating what degree of improvement is associated with each and even without deleting those items not adopted for implementation. The Staff then claims that these measures, in their undifferentiated entirety, will reduce the probability of TMI-2-rela accident sequences to the realm of being "not credible." For the Board to come to such a conclusion would require a considerable leap of faith.

370. In evaluating the so-called "recommendations" which were proposed by the Staff to mitigate the core damage sequence accidents the Board found numerous examples of recommendations which have sinc been eliminated as requirements, examples of recommendations which bear no obvious relationship to the event for which they are propose as mitigating measures, and recommendations which will not have <u>any</u> short-term benefit.

371. Examples of recommendations which have been eliminated as requirements (not listed in NUREG-0737) include:

a. Table 12, Item 6, IREP.

b. Table 12, Item 8, systems interaction -- resolution of generic safety issue.

c. Table 13, Item 4, correction of welds in safety-related systems.

d. Table 15, Item 7, LOFT research program on ECCS functio

372. Examples of recommendations which are not obviously relate

to the failures for which they are proposed to mitigate include:

a. Table 14, Item 4, correction of defective welds in containment spray, alleged to improve post-accident heat removal.

b. Table 16, Item 3, verify management and technical capability, alleged to improve primary system pressure relief capabilities, protect primary system integrity, prevent emergency coolant injection failure, prevent post-accident radioactivity removal failure, prevent post-accident heat removal failure, and prevent emergency coolant recirculation failure.

c. Table 16, Item 4, verify capability of safety review and operational advice, alleged to improve the same areas as example "b" above (except for prevention of emergency coolant injection failure).

d. Table 16, Item 12, systematic assessment of licensee safety, alleged to improve primary system pressure relief capabilities, protect primary system integrity, prevent emergency coolant injection failure, prevent PARR failure prevent PAHR failure, and prevent ECR failure.

e. Table 16, Item 27, control room access procedures, alleged to prevent PAHR failure, prevent emergency feedwater function failure, prevent ECI failure, and prevent ECR failure.

373. Examples of recommendations which do not have any short-term benefit including:

a. Table 10 and 11, Item 1, safety and relief valve testing program.

b. Table 12, Item 5, long-term ICC instrumentation.

c. Table 12, Item 6, IREP.

d. Table 12, Item 7, LOFT research program on ECCS.

e. Table 12, Item 8, systems interaction study--resolution of Unresolved Safety Issue A-17.

f. Table 16, Item 24, simulator requirements.

g. Table 16, Item 26, revisions to licensing examination.

374. We have found the whole concept of credible vs. incredible as it is used either explicitly or implicitly for purposes of determi the design basis to be an elusive and troubling one. The Board was frankly astonished that the Staff has apparently never been called upon to justify its practice before, nor has it apparently ever attempted to apply anything approaching a rigorous analytic technique to its design basis determinations. The first effort at a justificati of its practice was presented to this Board.

375. In summary, the staff has no quantitative or even clearly elucidated qualitative measure of the likelihood of Class 9 TMI-related accidents before the implementation of the post-TMI-2 improvements. Likewise, it has no measure of the degree of improvement which can be associated with the post-TMI-2 improvements. It knows neither where it started nor where it has progressed to. Perhaps the only hard evidence in this case which reflects directly on the reliability of the staff's judgments with respect to the probability of accidents beyond the design basis is the fact that TMI-2 <u>was</u> such an accident and that the staff judged it to be incredible until it happened. This does not give us grounds for confidence.

376. Despite knowing neither where it started nor where it has progressed to, the Staff asks this Board to accept the proposition that all TMI-related accidents beyond the design basis are now incredible. This record does not support such a finding. Indeed, it would be irresponsible for this Board to make a finding of such great consequence and precedential value on the basis of the evidence before us.

377. In summary, the Board finds:

a. The Staff has no probability numbers for any accident sequence, and does not therefore know the likelihood of any accident sequence.

b. The Staff has no scrutable, technically justifiable method for classifying accidents as credible or not credible.

c. The Staff implicitly assumes an understanding of probabilities, which understanding has no factual or technically justifiable basis.

d. The Staff has made no showing that it has identified all of the credible accident sequences with nexus to the TMI-2 accident.

e. The Staff has made no showing that it has identified all of the necessary and sufficient recommendations for changes which will adequately protect the public health and safety from the consequences of accidents with a nexus to the TMI-2 accident.

378. Moreover, in response to a specific direction from the Board to address the issue of the probability of the TMI-2 accident sequence (and those with close nexus), as embodied in the Board's June 23, 1980, Memorandum on NRC Staff Accident Sequences Report, neither the Staff nor the Licensee attempted a showing even approaching what the Board requested. UCS has prevailed on its Contention No. 13.

379. Based upon all of the foregoing, the Board concludes that the short and long-term actions recommended by the Director of NRR are not sufficient to provide reasonable assurance that TMI-1 can be operated without endangering the health and safety of the public in that they do not ensure against the recurrence of a TMI-2 related accident beyond the design basis for TMI-1.

BOARD QUESTION NO. 6

380. The Board posed a series of questions aimed at determining whether the decay heat removal systems at TMI-1 are sufficiently reliable to permit restart without undue risk to public health and safety. (Board Question 6, Emergency Feedwater Reliability, Tr. 2394-96)

381. We address below the applicable TMI-2 lessons learned, the TMI-1 decay removal methods, the Licensee's testimony, and the Staff's testimony.

EFW Lessons Learned

382. The need for an emergency feedwater system of high reliability is a clear lesson learned from the TMI-2 accident. (NUREG-0578, at 10)

383. In recent design reviews since the issuance of the Standard Review Plan, the auxiliary feedwater system is treated as a safety system in a pressurized water reactor plant. It is required to satisfy the decay heat removal requirements set forth in General Design Criterion 34 of Appendix A to 10CFR Part 50. It also plays a significant role in the mitigation of feedwater

transients, which are anticipated operational occurrences. (Id., at A-30)

384. General Design Criterion 20 of Appendix A to 10 CFR Part 50 requires, in part, that the protection system shall be designed to initiate automatically the operation of appropriate systems to assure that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences.

385. Appendix A to 10 CFR Part 50 defines and explains anticipated operational occurrences as "those conditions of normal operation which are expected to occur one or more times during the life of the nuclear power unit and include but are not limited to loss of power to all recirculation pumps, tripping of the turbine generator set, isolation of the main condenser, and loss of all offsite power.

TMI-1 Methods of Decay Heat Removal

386. In the event of an anticipated operational occurrence such as a main feedwater transient or a loss of all offsite power, the TMI-1 systems initially available for decay heat removal are the emergency feedwater system and the high pressure injection system, in conjunction with the PORV or pressurizer safety valves, operating in the

feed and bleed cooling mode. (Keaten, et al, ff. Tr. 16,552, at 6-8)

387. After the reactor coolant system has been cooled and depressurized to about 250° and 320 psig, the low pressure injection system (also called the decay heat removal system) can be used to continue the cooling process until the conditions of cold shutdown (reactor coolant system average temperature less than 200°F) are reached. (Id., at 5, 9)

Licensee Testimony

388. The Licensee has performed no evaluation to determine the probability of loss of main feedwater at TMI-1. However, the generic data for B&W plants over a two year period for five plants (i.e., 10 unit-years) shows that the frequency of loss of main feedwater was 0.3 per plant-year. The Licensee estimated that the uncertainty attached to this frequency is less than a factor of 10. (Tr. 16,618-20, Keaten) This represents a high probability of loss of main feedwater and a consequently high rate of demand for emergency feedwater.

389. The Licensee also does not know either the probability of failure of the emergency feedwater system or the probability of failure of all decay heat removal system at TMI-1. (Tr. 16,629, Keaten)

390. The Board inquired into the protection provided by the emergency feedwater system in the event there is a loss of steam in the secondary system which results in failure of the turbine-driven pump. (Board Question 6.g.)

391. The Licensee testified that if only one motor-driven pump is available initially, reactor coolant system temperature and pressure would initially increase, possibly resulting in lifting a relief valve. (Keaten, et al, ff. Tr. 16,552, at 7)

392. It must be emphasized that the pertinent lesson learned requirement was that "the auxiliary feedwater system initiation time and capacity and the reactor scram time should be such that the water levels in the steam generators being supplied, following loss of main feedwater flow, remain high enough to provide sufficient heat transfer capability to remove stored and residual heat without causing opening of the primary coolant system relief and code safety valves." (NUREG-0578, at A-30, emphasis added)

393. We conclude that the TMI-1 design does not meet this requirement in that loss of one motor-driven pump does not leave sufficient EFW capacity available to prevent opening of the PORV or safety valves.

394. The Licensee, under cross-examination, agreed that use of the EFW system for decay heat removal relies upon the

operation of other non-safety grade equipment such as the atmospheric dump valves, the turbine bypass valves, and/or the main condenser. (Tr. 16,557-59, Keaten) There is no way to remove decay heat from the steam generators without the use of non-safety grade equipment. (Id.) This introduces an inherent unreliability into the system.

395. The reactor operator is relied upon to manually control steam generator level. Automatic control of steam generator level is provided by the non-safety grade integrated control system, but not at a sufficiently high level for adequate heat removal in the two-phase mode natural circulation. (Tf. 16,561-62, Ross)

396. The Licensee has not done a quantitative reliability analysis of the feed and bleed cooling. (Jones, ff. Tr. 4589, at 3)

397. The feed and bleed cooling mode cannot be used to achieve cold shutdown conditions. (Id., at 2)

398. For some break sizes, a minimum of two high pressure injection pumps are needed for feed and bleed cooling. (Id., at 3)

399. Feed and bleed cooling cannot be terminated unless main or emergency feedwater is restored or the PORV is used to depressurize the reactor coolant system to allow operation

of the decay heat removal system. (Tr. 16,574-75, Ross)

400. There is no method available by which TMI-1 can be taken from hot shutdown conditions at normal temperature and pressure to either cold shutdown conditions or the conditions necessary to allow operation of the low pressure injection system using only safety grade equipment.* (Tr. 16,557-59, Keaten; 16,574-75, Ross; Tr. 16,583-85, Keaten)

401. The Licensee also testified that use of a new vent valve on the top of the pressurizer could be used to depressurize the reactor coolant system in case the non-safety grade PORV fails. (Tr. 16,575-76, Keaten)

402. However, this vent will not be installed prior to the planned restart date in late 1981. (Staff. Ex. 14, at 52-53) Therefore, we can give no credit for it.

403. In the feed and bleed cooling mode, the pressurizer safety valves may have to cycle open and closed, but the Licensee did not know whether the qualification testing of the PORV and safety valves will include such operation. (Tr. 16,580-81, Keaten and Colitz)

404. The Licensee has not reviewed the initial test program for the high pressure injection pumps to determine whether they

---

* Regulatory Guide 1.139, the provisions of which are applied by staff to pending applications, requires a demonstration that the plant can be taken to cold shutdown using only safety grade equipment, assuming a single failure, with only on-site power, from the control room. The Division of Safety Technology has requested the Division of Licensing to develop a plan for implementing this position on operating reactors, but a plan has not yet been proposed for this. (Tr. 8079-8081, Silver)

are qualified for long term operation at a discharge pressure of 2500 psig. Instead, Licensee relies on the original design specification for the pumps and the belief that someone must have looked at the original qualification tests before issuing the feed and bleed operating guidelines. (Tr. 16,582-83, Colitz and Ross) No one who had "looked" was offered or even identified. Under these circumstances, such testimony can be given no weight in the Board's consideration.

405. In summary, the Licensee presented no convincing evidence that it had made a serious attempt to assess whether the reliability of the methods for decay heat removal is sufficiently high to justify restart in light of the lessons learned from the TMI-2 accident. Therefore, we must consider whether the Staff's testimony was sufficient to fill the void in the record.

Staff Testimony

406. The Staff testified that it had performed a reliability assessment of the TMI-1 EFW system and concluded that the EFW system with the modifications to be implemented by the time of restart would be sufficiently reliable to allow restart of TMI-1. (Wermiel and Curry, ff. Tr. 16,718, at 1) There was substantial questioning about the basis for this conclusion.

407. The Staff presented reliability estimates of the TMI-1 emergency feedwater system design as it existed in mid-1979 and as it will exist after planned changes are completed. (Id., at 31) In the latter case, the reliability estimate

assumed that all of the long-term modifications had been completed. (Tr. 16,733, Curry)

408. The Staff's analysis used failure rate estimates from WASH-1400. (Wermiel and Curry, ff. Tr. 16,718 at 33-34, Tr. 16,962, Curry)

409. The Staff analyzed three specific plant "transients" that result in the demand for EFW - loss of main feedwater, loss of offsite power coincident with loss of main feedwater, and loss of all AC power coincident with loss of main feedwater. (Wermiel and Curry, ff. Tr. 16,718, at 32)

410. To estimate the probability of EFW failure, the Staff defined failure as failure to provide 460 gpm flow to at least one steam generator within five minutes. (Id., at 31)

411. Given a loss of main feedwater, the Staff estimated the probability of EFW failure to be $8X10^{-3}$ for the mid-1979 design and $4.5X10^{-4}$ for the design after all long-term modifications are completed. (Id., at 35, 37, and Attachment 3)

412. Given a loss of offsite power coincident with loss of main feedwater, the Staff estimated the probability of EFW failure to be approximately the same as given above for the loss of main feedwater. (Id., at 35, 37)

413. For a loss of all AC power, the Staff estimated the probability of EFW failure to be about $6X10^{-2}$ for the mid-

1979 design and about the same for the design after all long-term modifications are completed. (Id.)

414. The Staff also estimated that, for the loss of main feedwater transient, the probability of EFW failure is about $3X10^{-3}$ for the design as it will exist at the proposed restart date. (Tr. 16,738, Curry) The Staff did not present an estimate of the probability of EFW failure for the restart design for the loss of offsite power and loss of all AC "transients." The Staff witness believed that his estimates were accurate within an uncertainty range of a factor of 10. (Tr. 16,965, Curry)

415. These are, of course, relatively high failure rate estimates particularly considering that the demand rate for the emergency feedwater system is also high. This is because EFW is required to remove decay heat for anticipated operational occurrences such as loss of main feedwater and loss of offsite power. Loss of main feedwater has historically occurred at B&W plants at the rate of 0.3 per plant year. (Tr. 16,618-20, Keaten)

416. Thus, while it could conceivably be acceptable to tolerate lower reliability levels for safety equipment which is called upon to function only very rarely, the evidence shows that emergency feedwater is needed perhaps once a year or within that range. Given this demand rate, an EFW failure rate in

the range which the staff presented is intolerable.

417. Moreover, the failure rate is in fact higher than indicated by the staff. The staff witness biased the results of his fault tree analysis by simply assuming that at least one of the diesel generators would function when called upon. That is, he assumed that one diesel generator was available and the probability of failure of the other diesel generator was 10^{-2}. (Tr. 16,971, Curry)

418. UCS requested the Board to take official notice of the diesel generator failure rate estimates used in WASH-1400. The estimate presented in WASH-1400 for failure of a diesel generator to start is $3X10^{-2}$. (WASH-1400, App. III, Section 2, Table III 2-1) We denied this request on the ground that the figures presented in WASH-1400 are not universally accepted. We have reconsidered this ruling.

419. We noted above that the failure rates used by the staff were derived from WASH-1400. We have also found in our review of the record that the Licensee has relied on WASH-1400 component failure rates in calculating accident probabilities. (Eg, Tr. 11,107, 11,130, 11,140, Levy; Levy, ff. Tr. 11,049 at 14,15)

420. In addition, we have reviewed the Appeal Board decision in Florida Power and Light Co. (St. Lucie Nuclear Power Plant, Unit No. 2), ALAB-603, 12 NRC 30 (1980). The issue in that

proceeding centered around the likelihood of total loss of AC power. In that connection, one staff witness on diesel generator reliability used the WASH-1400 demand failure rate of $3X10^{-2}$. (Id., at 47) The Appeal Board noted that this was an appropriate use of WASH-1400. (Id. at n. 60, p. 47) Based upon this figure, they determined that the probability of failure of both diesel generators is in the range of 10^{-3} to 10^{-4}. (Id., at 48)

421. Considering that the Licensee's objections to the Board's taking official notice of the failure rate of diesels was general in nature and presented no facts suggesting that these figures are inaccurate, and considering that the staff has itself used these figures in testimony very recently, we see no reason why they cannot be officially noticed.

422. If the diesel generator failure rate were factored into the staff's analysis, the effect would be to make the probability of failure of emergency feedwater even greater, although the exact magnitude of the change cannot be determined.

423. Judging from the Staff's failure probability estimates for the loss of main feedwater "transient', it can be concluded that relatively little of the improvement in EFW reliability attributable to hardware changes will be incorporated prior to the proposed restart date. (Tr. 16,742-43, 16,746, Curry)

424. The Staff attempted to downplay the significance of the relatively high probability of EFW failure in two ways. First, the Staff claimed that if more time for operator action were considered, i.e., if the definition of EFW failure was changed to allow more than five minutes to deliver flow to at least one steam generator, the estimated reliability of EFW would improve. Second, the Staff claimed that the availability of the bleed and feed cooling mode could be recognized as a backup to EFW for decay heat removal. We now address these two factors to explain why such testimony cannot be given any weight.

425. The Staff acknowledged that it had done no analysis of TMI-1 EFW failure probability for a time interval longer than five minutes. (Tr. 16,744, 16,746, Curry)

426. The Staff opined nonetheless that if a longer period of time were analyzed (i.e., if the definition of EFW failure allowed more time to deliver EFW to the steam generators), operator action could introduce additional failure modes, but that it was more likely that operator action would correct failures. (Tr. 16,749, Curry) However, that testimony was not based on review of the TMI-1 emergency procedures or operator qualification training and is little more than speculation. (Tr. 16,758-9, Wermiel)

427. When the Board (Dr. Jordan) asked the Staff to explain why Westinghouse plants have an order of magnitude higher EFW system reliability than TMI-1 (Wermiel and Curry, ff. Tr. 16,618, at 35,37), the Staff attribu[illegible] this to the difference in the success criterion. That is, since Westinghouse steam generators dry out in the absence of EFW more slowly than TMI-1, much more credit can be given for operator recovery action. (Tr. 17,075-76, Curry)

428. However, B&W did analyze EFW reliability for 5, 15, and 30 minute intervals, and in no case were the reliability estimates as high as the best Westinghouse reliabilities! (Tr. 17,076, Curry) Therefore, this record indicates that, even if the success criteria had been loosened, no great improvement in EFW reliability would be demonstrated.

429. The Staff made no attempt to analyze the longer time periods. (Tr. 17,076-77, Curry)

430. Nevertheless, the Staff's witness still testified that he "suspected" that credit for operator action would improve the reliability sufficiently that in his "judgment" the reliability could 'broach" the high range. (Tr. 17,095, Curry)

431. We find such Staff testimony disturbing. Despite the lack of any supporting analyses whatever and despite contradictory B&W analyses, the Staff apparently would have this

Board rely on its feelings that the reliability of the TMI-1 EFW is not as low as the Staff's own analyses indicated. The evidence does not support such a conclusion.

432. The other line of argument made by the Staff in an effort to mitigate the relative unreliability of EFW was that the feed and bleed cooling mode is available as a backup to EFW for decay heat removal. (Tr. 16,847, Wermiel) However, no analysis of the decay heat removal capability over an extended period of time for the feed and bleed mode has been reviewed by the Staff. (Tr. 16,848, 16,873, Wermiel)

433. Staff witness Jensen testified: "We have not requested nor has Metropolitan Edison provided us with either procedures or analyses for cooldown of the Reactor Coolant System by feed-and-bleed, nor have we performed such evaluations." (Wermiel et al., ff. Tr. 6035 at 6)

434. We will not reiterate all of our previous findings on feed-and-bleed.* One additional point should be noted, however. Use of bleed-and-feed to mitigate anticipated operational occurrences has the effect of transforming such relatively

---

* We have previously determined that feed and bleed is not a reliable method of core cooling. (UCS Proposed Findings on UCS Contentions 1 and 2, parcel. 36)

likely events into loss-of-coolant accidents, since primary system valves must be opened to "bleed" the cooling water. In addition, of course, ECCS must be used for bleed and feed. It seems to us to turn the NRC's regulatory philosophy on its head to rely on bleed and feed for mitigating anticipated operational occurrences when General Design Criterion 14 requires an "extremely low probability" of LOCA's.

435. The Staff also testified that to draw conclusions about the comparative risks of operating various nuclear plants, consideration needs to be given to the integrated response of all plant systems to cope with potential transients, not solely EFW. This integrated response, while clearly affected by the reliability of individual systems, is also a function of systems interactions. (Wermiel and Curry, ff. Tr. 16,618, at 39-40)

436. However, the Staff has not done and is not planning to do, in the foreseeable future, such an integrated relability assessment for TMI-1. (Tr. 16,732, Curry)

437. Furthermore, the Staff has not done a systems interaction study for TMI-1 (Tr. 16,877, Wermiel) and is not planning to do one. (Tr. 16,923, Rowsome)

438. The Staff's witness was unaware of the ACRS recommendation that the Licensee should conduct reliability assessments of the plant and was unfamiliar with any ACRS reports concerning

the methods to be used in systems interaction studies. (Tr. 16,877, 16,883, Wermiel)

439. Studies done on other plants have identified three potential common mode failures for B&W plants that could constrain the reliability with which a plant can deal with a loss of feedwater. These are as follows: (1) a loss of both onsite and offsite AC power; (2) a loss of a NNI (non-nuclear instrumentation) bus which could both cause a loss of main feedwater and prevent automatic flow from the EFW system; and (3) a failure in the steamline break detection circuitry which could result in isolation of feedwater to both steam generators. (Tr. 16,913, 16,921-22, Rowsome)

440. Only the first of these concerns has been corrected at TMI-1. There are plans afoot to address both the other concerns, but not until the first refueling outage after the proposed restart date. (Tr. 16,922, Rowsome)

441. UCS attempted to establish through cross-examination of the Staff that no criteria were used to decide whether any particular change to EFW was necessary as a prerequisite for TMI-1 restart - that the Staff's "requirements" were not requirements at all, but were infinitely flexible and the Staff accepted as the bounds of its "requirements" whatever was practical for the Licensee to accomplish. As discussed below, we conclude that UCS successfully demonstrated this to be the case.

442. The Staff could not identify any requirements applicable to the EFW system that it considered so vital that restart would not be permitted without meeting the requirement. (Tr. 16,835, Wermiel)

443. Even where the Staff acknowledged that a requirement was important enough to safety that TMI-1 should not be permitted to operate for the remainder of its lifetime without complying, the Staff was unwilling to state that failure to meet the requirement would require TMI-1 to shut down. (Tr. 16,836-37, Wermiel)

444. The Staff witness was unfamiliar with the details of compliance with GDC-20, (Automatic initiation of protection systems functions), and did not know whether the initiation circuits for EFW had to be safety grade in order to comply with GDC-20. (Tr. 16,860-63, Wermiel)*

445. The Staff originally rejected the Licensee's proposal to delay installing a fully safety grade EFW system until the first refueling outage following restart. When questioned

---

* Although the Licensee disputed the applicability of GDC 20 (automatic initiation of projection system functions) to the TMI-1 emergency feedwater system (Tr. 5802, Capodamo and Lanese), the Lessons Learned document, NUREG-0578, states: "Recent analyses of primary system response to feedwater transients and reliability of installed auxiliary feedwater systems establish the need for automatically initiating the auxiliary feedwater system, consistent with satisfying the requirements of GDC 20." (Board Exhibit 7 at A-30). The Staff apparently assumed the applicability of the criterion. (Tr. 6058-6062, 16,860, Wermiel; Wermiel and Curry, ff. Tr. 16,718, at 9)

about the reason for this, the Staff could not provide an explanation. In fact, the Staff testified that its original "requirement", that the fully safety grade modification of EFW be installed within 60 days after receipt of the required equipment, never held much weight because equipment delivery could be delayed until the refueling outage occurred. However, the Staff acknowledged that at the time it imposed the 60-day installation requirement, equipment delivery was expected in March 1981. The Staff believes that installation of a fully safety grade EFW system would provide a significant improvement in EFW reliability. (Tr. 16,864-67, Wermiel; Staff Ex. 1, at C8-37)

446. However, the Staff's position is now changed to agree with the Licensee's original proposal which the Staff had previously rejected. The Licensee "commits" to installation of the safety grade EFW system by the first refueling after restart. The Staff finds this acceptable based on the good-faith effort of the Licensee to obtain the required equipment and the fact that some other B&W plants have similar problems. (Staff Ex. 14, at 38)

447. The Staff witness did not know whether the EFW system was seismically qualified or even if it has to be seismically qualified prior to restart. (Tr. 16,894-96, Wermiel)

448. The Staff witness did not know if compliance with GDC-19, with respect to control of EFW if access to the main control room is lost, was required prior to restart and did not evaluate the TMI-1 design to determine the extent of compliance. (Tr. 16,896-99, Wermiel)

449. We conclude, based on the Staff testimony described above, that the Staff's conclusion that the TMI-1 EFW system is sufficiently reliable to allow restart has no credible basis.

450. In fact the staff did no plant-specific analysis of TMI-1 as it will be at the time of restart in order to determine whether it is safe enough to restart. (Tr. 21,117-19, Silver) It simply attempted to ascertain whether TMI-1 was moving on approximately the same schedule as other similar B&W reactors. (Tr. 21,042-44, 21,049-50, Silver; Staff Ex. 14, at 3)

451. This Board is required to determine whether the short-term measures recommended by the Director of NRR are "necessary and sufficient" to assure that TMI-1 can be safely restarted. This record is abundantly clear that the staff has equated "sufficiency" with practicality. That is, whatever can be done by restart is sufficient for restart. (Tr. 21,044-21,050, Silver) While we do not doubt that considerations of practicality have a place in the setting of regulatory

requirements, it must be a secondary place to considerations of safety. "Safety first" is a principle which the Commission has espoused from its inception. [Power Reactor Development Corp. v. International Union of Electrical Radio and Machine Workers, 367 U.S. 396,402 (1961)]

452. What is most troubling here is the total absence of any objective criteria on the staff's part for determining that the set of measures in place at restart are sufficient to ensure safety.

453. In addition, this record shows that virtually every post-restart deadline is waivable, nothing is so important to safety as to make a deadline firm and there is no assurance that any deadlines falling later than June 30, 1981 will not be changed. (Tr. 21,045-46, 21-136-37, Silver; Tr. 21,236, Jacobs) Under these circumstances, there is no assurance that the long-term modifications, which include upgrade of EFW initiation and control to safety-grade, will be accomplished expeditiously. Indeed, the record indicates that certain components required for the upgrade will not be available for two years. (Staff Ex. 14 at 37; Tr. 21,052-53, Silver) We note that this would appear to fall later than the next refueling outage after restart, suggesting that the modifications would not be made until the succeeding refueling outage.

454. The Staff and Licensee argue that TMI-1 restart should be permitted despite the fact that EFW will not be safety grade. The following is a summary of the improvements which all parties concede are required to the emergency feedwater system but which will not be accomplished by restart.

455. Cavitating venturis to protect against steam generator overfill (and a resulting overcooling accident) will not be installed. The purchase order was expected to have been issued in May 1981. (Staff Ex. 14, at 36,38) The Staff had no explanation for why the purchase order had not been issued earlier and could identify no specific problems to account for the delay. (Tr. 21,264-65, Jacobs)

456. The existing automatic circuits for opening the EFW control valves on an automatic initiation of EFW are derived from the Integrated Control System which is not safety grade and therefore the automatic circuits do not meet the single failure criterion. (Staff Ex. 1, at C8-36) This violates the short term requirement that the automatic initiation circuits shall be designed so that a single failure will not result in the loss of auxiliary feedwater system function. (Staff Ex. 1, at C8-34) Nevertheless, the Staff argues that manual control of EFW flow can be used in lieu of the required automatic control. (Staff Ex. 1, at C8-37)

457. The Staff reports that the Licensee "commits" to the installation of redundant control and block valves by the first refueling after the proposed restart date. (Staff Ex. 14, at 38) The Staff did not investigate whether an earlier schedule is possible, and does not know the delivery date of the valves or the type of valves to be used. (Tr. 21,265-67, Jacobs)

458. Automatic initiation of EFW from low steam generator level detection is not installed and the Staff has no estimate of how long it will be before it is installed. (Staff Ex. 14, at 37; Tr. 21,267-68, Jacobs)

459. Safety grade steam generator level instrumentation qualified to IEEE Std 323 (1974) will not be installed prior to the proposed restart date. (Staff Ex. 14, at 37)

460. The water supply for the EFW system comes from the condensate storage tank but the existing condensate storage tank level instrumentation is not safety grade (Staff Ex. 14, at 37) and both existing instruments are powered from the same power supply (Tr. 17,003, Wermiel) and, thus, do not meet the single failure criterion. Thus, we cannot find that the EFW system provides an equivalent level of protection to a safety-grade system.

461. The Staff was unable to specify or even reliably estimate the date by which the emergency feedwater system upgrade will

be completed and the record indicates that the ultimate date will depend entirely upon considerations of expediency. (Tr. 21,264-21,321, Silver, Jacobs and Jensen, particularly 21,318-21, Silver)

Board Conclusions

462. The Board has considered the state of this record on emergency feedwater reliability in light of the Appeal Board's decision in Florida Power and Light Co. (St. Lucie Nuclear Power Plant, Unit No. 2), ALAB 603, 12 NRC 30 (1980) We note at the outset that the probability of emergency feedwater system failure is far greater than the guideline values in Section 2.2.3 of the Standard Review Plan for designating a particular event a design basis accident - 10^{-7} per year calculated "realistically" or 10^{-6} per year calculated "conservatively." While, as the Staff points out, Section 2.2.3 applies on its face to external hazards such as hazardous materials (Wermiel et al., ff. Tr. 6035 at 10), we have been presented with no convincing reason why these valves cannot or should not be used as a starting point in determining the risk level acceptable for other situations, as the Appeal Board used them in St. Lucie, supra at 45. Moreover, neither the Licensee nor the Staff have presented to us any alternative, objective criteria for use in considering the reliability of the emergency feedwater system.

463. There is, in addition, at least one significant difference between the situation presented in ALAB-603 and the current record which strengthens our view that it is appropriate here to use objective, quantitative reliability criteria. In ALAB-603, the Appeal Board specifically found that GDC 17, the pertinent General Design Criterion governing the reliability of offsite power, was met by the Applicant. (Id. at 44) In the case of the TMI-1 EFW system, at least some of the GDC defining a safety-grade emergency feedwater system will not be met at restart, particularly GDC 13 (instrumentation and control) and GDC 20 (automatic initiation) (Tr. 6058-6063, Wermiel). Also, the cavitating venturis required in order to provide 10 minutes for operator action to mitigate overcooling will not be installed at restart. (Tr. 6062-6, Wermiel) See the discussion, supra paras. 454-461.

464. Thus, this is not simply a situation where a quantitative reliability assessment indicates a need to go beyond current regulatory requirements. The quantitative reliability assessment in combination with the non-safety-grade status of the emergency feedwater system at restart demonstrate an overall level of system reliability at restart which is unacceptable. We add that in our view, the record also does not justify a finding that the system will be acceptably reliable even after the fuel upgrade. In the latter case, after emergency feedwater

is safety-grade this situation is more directly analogous to St. Lucie. We note that the record shows, perhaps surprisingly, that safety-grade emergency feedwater systems are not historically significantly more reliable than others. (Tr. 6106-7, Lantz)*

465. Another difference between St. Lucie and this case which appears pertinent to us is that the issue under consideration there - the extent to which "station blackout" should be considered in plant licensing - was the subject of a staff "Task Action Plan." (Id at n. 55, p. 46) Indeed, in accepting review of the issues presented by ALAB-603, the Commission limited its review to only two "generic" issues: 1) the generic implications of using the SRP §2.2.3 guideline valves for determining design basis events and 2) the appropriateness of designating station blackout as a design basis accident given the pendency of the staff

---

* Board Question 6C asked for "the experience in other power plants with failures of safety-grade emergency feedwater systems..." The Licensee apparently misconstrued the question, since it presented statistics only for B&W plants, without distinguishing between those which have safety-grade EFW systems and those which do not. (Capodanno et al., ff. Tr. 5642 at 5-6) Only one of the plants - Davis Besse - has a safety grade system. (Tr. 5745-6, Capodanno) The Staff testified that, considering only safety-grade emergency feedwater systems, there have been 8 instances of EFW unavailability in 200 reactor years. Considering all PWR's, there have been 9 instances in 280 reactor years. (Tr. 6093, 6107, Lantz) These statistics are likely to understate the problem, since LER's are notoriously hard to interpret. In addition, no statistics on emergency feedwater system success on demand are maintained so the Staff's statistics came only from surveillance testing data. (Wermiel et al., ff. Tr. 6035 at 3-4)

review of the subject in its Task Action Plan. (Florida Power & Light Co. (St. Lucie Nuclear Power Plant Unit No. 2), CLI-80-41, 12 NRC 650, 652-3 (1980). ALAB-603 was left in force with respect to its plant-specific treatment of St. Lucie. At least as to the latter question, neither the Staff nor Licensee drew our attention to any ongoing program directed toward considering the reliability of emergency feedwater systems (or decay heat removal systems) or the extent to which loss of emergency feedwater following a loss of main feedwater should generically be considered a design basis event.

466. The record in this case demonstrates that total loss of feedwater should be considered a design basis event for TMI-1 in light of the relatively high probability of loss of emergency feedwater and the high rate of demand for emergency feedwater to remove decay heat in the event of such anticipated operational occurrences as loss of main feedwater (and loss of offsite power).

467. We make this ruling not by simply applying in some mechanistic way the Standard Review Plan guidelines, although we note that the probability of emergency feedwater failure as calculated by the Staff is not even close to the SRP values of 10^{-7} and 10^{-6} per year for design basis events. This record as a whole provides insufficient basis for this

Board to find reasonable assurance that the TMI-1 emergency feedwater system is sufficiently reliable to remove decay heat when needed.

468. Based upon the foregoing, we conclude that:

1. This record does not establish that the TMI-1 emergency feedwater system provides a sufficiently reliable means of decay heat removal to permit operation of the facility.

2. This record does not establish that the bleed-and-feed cooling mode is a sufficiently reliable means of decay heat removal either as a substitute for or in addition to emergency feedwater. In addition, reliance on bleed-and-feed for decay heat removal is fundamentally inconsistent with the principle that the primary reactor coolant system should be breached extremely rarely.

3. This record does not establish that the means of removing decay heat for TMI-1 are sufficiently reliable to permit operation of the plant.

469. The foregoing findings apply both to the condition of the plant at restart and after the planned restart improvements are completed. The only effort at a reliability analysis, that done by the Staff, showed surprisingly little improvement attendant upon the longer-term modifications.

470. On the basis of this record and in the absence of any other objective criteria for judging the reliability of the TMI-1 decay heat removal systems, we conclude that the following must be shown in order to establish that TMI-1 is safe enough to operate:

1) that the combination of the probability of demand for decay heat removal and the probability of failure of emergency feedwater* is less than 10^{-6} per year; and

2) that the plant can be taken from hot standby to cold shutdown with only safety-grade equipment, and

3) that the capacity of emergency feedwater has been increased so that in the event of an anticipated operational occurrence, a single failure in the emergency feedwater system (e.g. loss of the turbine-driven pump) will not result in opening or the primary system relief or safety valves. **

471. Based upon all of the foregoing, the Board concludes that the short and long-term actions recommended by the Director of NRR are not sufficient to provide reasonable

---

* Feed and bleed cannot be relied upon because it transforms an anticipated operational occurrence into a LOCA. There are no other decay heat removal systems at TMI which can be used at normal operating temperature and pressure.

** An alternative to this may be the addition of a limiting conditi for operation requiring all three EFW pumps to be operable. Currently, plant operation is permissible with only two pumps operable. Thus, a single failure could leave only one motor-driven pump operable, resulting in opening of a relief or safety valve. (Supra, para. 391)

assurance that TMI-1 can be operated without endangering the health and safety of the public.

UCS CONTENTION 14

UCS Contention 14 was admitted as follows:

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 3.2, "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 systems 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 safety-grade design criteria.

472. Direct testimony on this contention was presented by UCS (Pollard, ff. Tr. 8091), the Licensee (Keaten and Brazill, ff. Tr. 7558) and the Staff (Conran, ff. Tr. 8372, voir dire, Tr. 8314-8371).

473. In summary, UCS's testimony explained the significance in nuclear safety regulation of the distinction between safety-grade and non-safety-grade systems and components and described how the TMI-2 accident demonstrated three types of shortcomings in past practice: 1) certain systems previously classified as not safety-related are, in fact, important to safety; 2) some systems known to be important to safety do not meet all of the criteria applicable to such systems and 3) the design basis for judging the capability of safety systems has not been properly specified.

474. UCS maintains that despite NRC's general requirement that fa of non-safety grade equipment should not initiate or aggravate an accident, there is currently no comprehensive and systematic analysis done to demonstrate that this requirement has been met. In other words, the elaborate structure for ensuring diverse and redundant safety systems to mitigate accidents remains

vulnerable to unforeseen failures of non-safety equipment, or adverse systems interactions, just as during the TMI-2 accident. In the aftermath of the accident, no systematic effort has been made to identify and correct this problem. Therefore, UCS proposes that all systems currently classified as non-safety-related which can in fact either cause or aggravate an accident or be called upon to mitigate an accident should be identified and required to meet safety-grade criteria so as to preclude adverse interactions. (Pollard, ff. Tr. 8091, at 14-1 to 14-9)

475. UCS's testimony described the manner in which the NRC's licensing process depends upon assessing whether the plant's structures, systems and components can be relied upon to protect public health and safety in the event of occurrence of any of the selected design basis accidents or anticipated operational occurrences. The Commission has developed a set of regulations that define the minimum requirements for design, fabrication, construction, testing and performance which must be met if a structure, system or component is relied upon to protect the public. These requirements are set forth in the General Design Criteria of Appendix A to 10 CFR Part 50, industry standards such as IEEE Std. 279, which are incorporated in 10 CFR §50.55a, and other sections of 10 CFR Part 50. (Id. at 14-3)

476. The introduction to the General Design Criteria provides as follows:

> Pursuant to the provisions of §50.34, an application for a construction permit must include the principal design criteria for a proposed facility. The principal design criteria establish the necessary design, fabrication, construction, testing, and performance requirements for structures, systems, and components important to safety; that is, 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.
>
> (App. A, 10 CFR Part 50, introduction, emphasis added)

477. As the language quoted above indicates, UCS testified that commission policy has been to apply the requirements of the GDC to systems variously referred to as safety-related, safety-grade or important to safety. It is assumed that only safety-grade systems are available to function during a design basis event. Non-safety-grade systems are, by contrast, assumed to be unavailable and therefore, their functioning is not credited in evaluating the protection available to mitigate such events. (Id. at 14-3 to 14-4)

478. As additional support of this description of the licensing process, UCS cited the following language from the NRC's advance notice of proposed rulemaking. "Consideration of Degraded or Melted Cores in Safety Regulation" September 26, 1980:

> 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' where 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 damaged in some way that it might interact negatively with other systems. Instead, these items simply receive what attention may be dictated by routine industrial codes and by desires to enhance plant availability."

(Emphasis added)

479. The language from the Commission quoted above confirms both that the terms "important to safety" and "safety grade" are used interchangeably (..."things credited in the analysis of a design basis event or specified in the regulations are important to safety and thus are 'safety grade'...) and that all other equipment is classified as non-safety grade and receives cusory NRC review, if any.

480. Further confirmation can be found from the Lessons Learned Task Force itself, which described the classification system and noted that the present classification scheme does not adequately recognize that non-safety systems can (and did at TMI-2)

cause accidents and can (and did at TMI-2) be used in accident mitigation in ways not considered in the plant's safety analysis. (The full quote from P.A-18 of NUREG- 0578 is contained in the text of UCS contention 14)

481. While we may appear to be belaboring this initial question concerning NRC's safety/non-safety classification scheme and its implications, the discussion is necessary because, surprisingly, NRC's witness disputed UCS's description of the licensing process. This dispute will be treated in some detail later.

482. The Board returns now to the substance of UCS's testimony. Examples were provided of the three types of shortcomings of the current safety/non-safety destinction which were demonstrated by the TMI-2 accident. First, under the rubric of improper classification of systems, UCS noted that several systems that had been previously classified as non-safety (or not "important to safety") were used to mitigate the accident. These include the reactor coolant pumps, which were used at vaious times to accomplish core cooling, the pressurizer level instruments, the PORV and its associ block valve and the auxiliary (or emergency) feedwater system. None have been reclassified as important to safety.[1/] (Id. at 14-4 to 14-6) We note in addition that the failure of another non-safe

1/ Discussion of the specific role during the accident of the POR and its block valve and the emergency feedwater system are contain in the Board's findings on UCS contention 5 and Board question 6, respectively.

system - the demineralizer - started the chain of events which led to the accident. Much of the litigation of this contention centered around this aspect of the contention and the general question of whether adequate steps have been taken to identify and eliminate adverse systems interaction and to recognize the role that so-called non-safety systems have in maintaining plant safety.

483. The second category covered systems conceded to be important to safety which failed to meet all requisite criteria. One example is that the protection system signals used to initiate ECCS were not derived from direct measurements of the desired variable - reactor vessel water level. (Id. at 14-6)

484. The third general area in which the accident highlighted pertinent shortcomings, according to UCS, was the inadequate determination of the severity of the design basis event for which safety grade systems must provide protection. For example, the safety analysis for TMI assumed no significant core damage or radioactivity in the primary system. Hence, it was assumed that the low-pressure Decay Heat Removal (DHR) System could be used to remove decay heat. However, during TMI-2, the DHR system could not be used because its leak rate and radiation shielding were inadequate to prevent excessive radiation exposure and because the primary system could not be depressurized to the point at which DHR can function. (Id. at 14-6 to 14-7)

485. UCS testified that the above demonstrated that the licensing review of TMI-1, while based on a fundamental dis-

tinction between "safety" and "non-safety" equipment, was not adequate to identify all systems which are important to safety, to define the design basis for such equipment, or to identify and prevent adverse interactions between non-safety and safety equipment which can compromise the ability of safety systems to perform their necessary functions. The Lessons Learned Task Force conceded as much:

> 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." (NUREG-0585, p.3-3)

(Id. at 14-7 to 14-8)

486. UCS notes, finally, that the Staff has agreed in this litigation that systems currently classified as non-safety-related can affect the core because they can directly or indirectly affect temperature, pressure, flow, and/or reactivity. (Id. at 14-8)

487. Having demonstrated that the lessons to be learned from the TMI-2 accident include that the current safety/nonsafety classification scheme does not adequately identify all systems important to safety or identify and correct all potentially adverse systems interactions, UCS turns to the

measures which have been proposed by the Staff to respond to this issue. At the time that UCS's testimony was written, it appeared as if one long-term requirement had been imposed addressed to this question, requiring the Licensee to "evaluate the interaction of non-safety and safety grade systems ... to assure that any interaction will not result in exceeding the acceptance criteria for any design basis event." (NUREG-0585, at A-14, Recommendation 9). It was recommended that this study be completed within one year. (Id.) During the course of this proceeding it became apparent that even this recommendation of the Lessons Learned Task Force will not be implemented. There are no plans to do any systems interaction review for TMI-1 and TMI-1 is not included in the IREP program. (Infra, para. 525)

488. This is despite the fact that the ACRS letter on TMI-1 of December 11, 1980 stated as follows:

> In accordance with our previous recommendations, we believe that the Licensee should conduct reliability assessments of the plant as modified. Such assessments should accelerate the acquisition of potentially significant safety information and would expedite the development of the basis for further changes, should they be necessary. They would also provide the Licensee with additional technical insight into the safety of the plant. In addition, we believe the Licensee should examine the plant from the standpoint of systems interactions that may degrade safety. Although both

> of these studies should be conducted on a timely basis, their completion should not be a condition for restart.
>
> (Staff Ex. 14, App. C)

489. While the ACRS did not consider completion of such studies to be a necessary condition for restart, it can fairly be inferred from its letter that at least committment to "timely completion" of such studies should be a restart condition.

490. In response to the ACRS, the Staff merely describes the so-called IREP program, intended as a "proving ground for procedural guidelines" for Licensees and states that it does not "feel" that TMI-1 need be included in the program. Beyond this bald statement of its feelings, the Staff states no reason why TMI-1 can be safely operated nor makes any substantive response to the ACRS's concerns. The record is quite clear that the studies specifically called for by the ACRS will not be performed at all, much less on a "timely basis."

491. The essence of UCS's contention is a simply-stated question. Given that the accident demonstrated that systems presently classified as non-safety and receiving little or no NRC review can cause accidents and/or be called upon to mitigate them, and given that there are no present

plans to identify and upgrade these systems and/or to preclude interactions between safety and non-safety systems, what is the basis for finding reasonable assurance that the plant is safe enough to operate?

492. Before proceeding to discuss the positions taken by the Staff and Licensee, the Board notes that there was virtually no substantive cross-examination done of UCS's witness by either the Licensee or the Staff. Other than posing its usual series of questions about whether the safety concerns expressed by UCS were unique to TMI-1 or covered other plants as well, the Licensee pursued only one issue: are there circumstances where the Staff can and should mandate a partial upgrade of non-safety equipment without going all the way to full safety grade? While noting that past NRC practice in implementing the GDC prior to this case has not encompassed partial upgrade, Mr. Pollard stated that such partial upgrading might be justified from an engineering standpoint if it were based upon the results of technical analyses assessing the degree of improvement to safety gained by the partial upgrade, comparing that with the degree of improvement to be gained by full upgrade and establishing that the partial upgrade causes no adverse effects on plant safety. (Tr. 8123, Pollard.) No such analyses have been done in this case. (Tr. 8613-8621, Conran)

NRC Staff Testimony

493. The Staff testimony on this subject was presented by James Conran, ff. Tr. 8372. UCS did an extensive voir dire of Mr. Conran, culminating in an objection to his testimony on the grounds that the witness was not qualified to present it, that his experience with the agency was very largely in unrelated areas, that his experience with the systems interaction issue was tangential at best and that he had no direct experience with TMI-1, nor knowledge of the TMI-1 plant systems. (Tr. 8365-8369) This objection was overruled by the Board and the evidence was admitted. However, the matters raised on voir dire and in cross-examination do substantially affect the weight that can be attached to Mr. Conran's testimony. We treat those now.

494. At the time his testimony was prepared, Mr. Conran had worked for the AEC/NRC for seven years, during which time he held 7 different jobs. His positions with the ACRS and the Commission from 1973 through August, 1978 were in the area of safeguards of special nuclear material. (Tr. 8323-8334, Conran) While his job from July, 1977 to August 1978 was in the Office of Standards Development, which was developing quality assurance standards for nuclear material processing facilities, "by far the greater percentage" of Mr. Conran's time was spent

continuing his safeguards work. (Tr. 8333-8334, Conran)*

495. From August, 1978 to May, 1979, Mr. Conran served as a project manager in the Standardization Branch - the first apparent contact he had with the licensing of reactors. However, Mr. Conran performed no reviews of any plant systems himself during this 10 months; he "coordinated" the review of others of the "balance of plant" design and "assembled them into" the Staff safety review. (Tr. 8342-7, Conran) It is apparent that his duties were managerial rather than technical.

496. Moreover, the review of the two standardized design applications under his jurisdiction was suspended before either of the Staff safety evaluations were even published. (Tr. 8347-8, C

497. Mr. Conran was then assigned for one year to the TMI-2 Lessons Learned Task Force. He monitored the activities of the ACRS so that they could be coordinated with Staff work without duplication. (Tr. 8348-9, Conran) He was not assigned to any of the subgroups with responsibility for particular substantive safety issues and wrote no part of the Lessons Learned Report. (Tr. 8353, 8349-50, Conran) He wrote no

---

* The field of "safeguards" is related to protecting special nuclear material from fuel cycle facilities which may be capable of being fabricated into nuclear weapons, from diversion into the hands of unauthorized persons. (See, e.g. 10 CFR Parts 70 and 73) There is little if any apparent overlap between safeguards work and the work involved in reviewing commercial nuclear plant safety systems for the purpose of licensing pursuant to 10 CFR Part 50.

internal memoranda or draft portions of the report of the Lessons Learned Task Force. (Tr. 8357) Indeed, Mr. Conran conceded that his qualifications with respect to the systems interaction issue are no greater than his qualification for any of the safety issues raised by the TMI accident. (Tr. 8356)

498. After the publication of NUREG-0578, it appears that Mr. Co was not involved in work related to TMI-1 until he was assigned to present the testimony on this contention. (Tr. 8618, 8320,836 Conran) That assignment was made in mid-September, 1980. His testimony was filed approximately two weeks later. (Tr. 8320, Conran) Obviously, such a schedule does not permit much time to review the status of the case and the relevant documents, to deliberate upon the issues and to draft the testimony.

499. It would appear from his statement of professional qualifications that Mr. Conran might have acquired expertise in the area of systems interaction when he was assigned to the new Division of Systems Interaction in approximately March or April of 1980. (Tr. 8325, Conran) However, in the "early months" he was assigned to the budget rather than substantive work. (Tr. 8379, Conran) Considering that his assignment began in April, that the early months were devoted to developing the budget, and that he was assigned to present this testimony in mid-September and produced it in little over two weeks, precious

little time could possibly have been devoted to considering the substance of the systems interaction issue generally, not to mention the specifics of TMI-1.

500. While Mr. Conran has held a number of positions at AEC/NRC and we do not question his intelligence, there is little evidence that he has acquired direct experience in the areas pertinent to our inquiry here. As discussed above, he has apparently never had personal responsibility for the review of any safety system for any operating nuclear power generating facility. (Tr. 8431, Conran) (Nor, or course, has he designed such systems). Moreover, he can hardly be classified as an expert in the systems interaction issue. The great bulk of his direct regulatory experience is in the safeguards field. His testimony indicated heavy reliance on conclusions of other people or work which he assumed had been done by other people. (Tr. 8489-92, 8545, 8547-9, 8554, 8555-9, 8607, 8614-15, 8616-18, 8620, Conran)

501. Moreover, there is another aspect of his testimony which troubles the Board greatly and reflects poorly on the evidentiary weight which can be attached to it. That is, the testimony purports to present a discussion of past and current staff practice concerning the classification of plant systems and the definition of "important to safety" and "safety grade" but the evidence indicates that these were developed solely for the purpose of this litigation and only then circulated through the rest of the staff which was directed to

conform its testimony to Mr. Conran's construction. (Tr. 8318, Conran)

502. Other staff witnesses whose testimony was filed earlier than Mr. Conran's, Mr. Jensen for example, used the terms "important to safety" and "safety grade" in a manner which conforms to UCS's use of the terms rather than Mr. Conran's. Mr. Conran refers to these as "careless." (Tr. 8319, 8523-8524, Conran) Moreover, the Commission and the Lessons Learned Task Force also use the terms interchangeably, (supra, paras 479 - 480).

503. The Board believes that the record indicates, at least with respect to the portion of Mr. Conran's testimony which attempts to draw a distinction between the terms "important to safety" and "safety grade" with important regulatory implications that the testimony is largely a post-hoc attempt for purposes of this litigation to construct a facially logical explanation of staff practice which will support the Staff's conclusions in opposition to the contention. Such post-hoc constructs have little weight.

504. We now proceed to the substance of the Staff testimony, Conran ff. Tr. 8372. He began by asserting that there is an important regulatory distinction between the plant systems covered by the phrase "structures, systems and components

---

* The substance of the testimony will be discussed in detail below.

important to safety" and those which are "safety grade." That is, he claimed that the two phrases are not essentially interchangeable. According to Mr. Conran, only systems and equipment which perform "critical safety functions" (a term nowhere used in the regulations, Tr. 8530-1, Conran) need be safety grade, while other equipment "important to safety" need not be. Regulatory Guide 1.29, which deals with protection from earthquakes, is said to contain a list of all "safety grade" equipment. Thus, Mr. Conran challenges UCS's assertion that when a system is determined to be "important to safety", it has been required to meet the applicable GDC which form the definition of "safety grade." (Conran, ff. Tr. 8372 at 4-6)

505. Mr. Conran goes on to testify that there is no need to fully upgrade any non-safety grade equipment which either contributed to or was used in mitigation of the TMI-2 accident. He states that three criteria are used by the Staff in deciding whether such upgrading is required:

1. Will the failure of the non-safety component in and of itself degrade the capability of safety systems so that they cannot mitigate accidents?

2. Will the effects of failure of the non-safety system alone exceed the capability of properly-operated safety systems?

3. Is the non-safety system actually required to mitigate an accident assuming safety systems are properly operated? (Id., at 8 - 10)

506. According to Mr. Conran, if "by careful analysis or actual experience," the answer to any of these questions is yes, upgrading may be called for. (Id. at 10) However, he states that none of the TMI-1 non safety systems were used until after improper operation of safety systems had caused core damage. (Id. at 8) Nor did failure of non-safety systems cause the core damage. (Id. at 11) Hence, his criteria for upgrade are not met.

507. Mr. Conran then states that even though upgrade is not called for by application of his criteria, the Staff may decide to require partial upgrading "as a prudent measure", (Id. at 10) as it did with the PORV, pressurizer heaters and emergency feedwater. (Id. at 13-14) No criteria for the exercise of this prudence are offered.

508. The Board will deal with these three topics seriatim.

Important to Safety/Safety Grade Distinction

509. Mr. Conran was cross-examined extensively with regard to his assertion that the phrase "structures, systems and components important to safety" in the introduction to Appendix A to 10 CFR Part 50 is an extremely broad category and only equipment with "critical safety functions" need be safety grade and meet the applicable General Design Criteria. Mr.

Conran was asked to identify equipment which is in his view not "important to safety." He identified the office building, rest room and water cooler. (Tr. 8404-6, Conran) He admitted that the term "critical safety function" is used nowhere in the regulations, but is rather his own term. (Tr. 8530, Conran)

510. We note that Mr. Conran's definition of the terms "important to safety" and "safety grade" can be found nowhere in any AEC or NRC documents, regulations or regulatory guides. UCS's witness, who served as a member of the AEC and NRC licensing staffs and as a licensing project manager for 6 1/2 total years, has never seen these definitions nor heard them used in any NRC proceeding nor heard them in discussion with any NRC staff member. (Tr. 8099, Pollard) As discussed above, after Mr. Conran developed his testimony, it was circulated to staff members who were directed to conform their testimony to these definitions. (Tr. 8319, Conran) The above combine to lead us to conclude that Mr. Conran's definitions were developed solely for the purpose of this case and have not appeared before in NRC practice.

511. Mr. Conran states that Regulatory Guide 1.29 contains a list of all safety grade equipment. He derives this from reasoning that, since Reg. Guide 1.29 lists equipment that is

required to perform what he believes are "critical safety functions" after an earthquake, this list of equipment contains, ergo, all equipment that need be safety grade. (Conran, ff. Tr. 8372 at 4-5). While this has a veneer of logic, it does not stand up to scrutiny.

512. First it must be pointed out that Reg. Guide 1.29 never states that the listing of systems and equipment contained therein constitutes a list of all safety grade equipment. (Tr. 8537-8, Conran) Nor does any other NRC document so state. Indeed, the parties were asked earlier in the proceeding if such a listing existed and stated that it did not.*

513. Moreover, GDC 2, which is the genesis of Reg. Guide 1.29 explicitly requires that "structures systems and components important to safety be designed to withstand the effects of natural phenomena such as earthquakes..." (Tr. 8096, Pollard; Tr. 8531-2, Conran) Thus, one must conclude that the listing of equipment in Reg. Guide 1.29, which bounds the coverage of GDC 2, is a listing of equipment "important to safety." This reinforces the proposition that "important to safety" and "safety grade" are indeed interchangeable.

514. We were also disturbed by a circular and self-serving

---

* [N.B. We have not yet been able to locate the transcript reference to this, and are still attempting to search for it.]

element in Mr. Conran's testimony. According to the witness, a system or component could be "important to safety" within the meaning of the introduction to the GDC yet not be required to meet any of the specific GDC or Regulatory Guides, including even the quality assurance provisions of Appendix B to 10 CFR Part 50. The explanation offered is that, although the system or component is important to safety within the meaning of GDC 1, its level of importance is not enough to cause any specific requirements to apply. (Tr. 8409-8426, particularly 8419, Conran) Such an interpretation renders the phrase "important to safety" virtually meaningless as a regulatory concept since no regulatory consequences whatever flow from it. This provides an additional reason for the Board to discount the testimony.

515. Finally, the witness stated that his understanding and definitions had been applied during the licensing of TMI-1. (Tr. 8411, Conran) Yet there is equipment listed or covered by listings in Reg. Guide 1.29 which is <u>not</u> safety grade for TMI-1, including the PORV and emergency feedwater system. (Tr. 8537-42, Conran) Mr. Conran testified that he doesn't know enough about the "details of the system" to know whether non-safety components are listed in Reg. Guide 1.29. (Tr. 8633, Conran; see also Tr. 8692-6, Conran) Since this goes to the heart of his testimony, we cannot treat it lightly.

If Reg. Guide 1.29 is not even a listing of all safety-grade equipment (and none other), the "logical" construct built by Mr. Conran falls completely.

516. Finally, we discerned from the witness's demeanor and use of language the sense that he was sometimes improvising.* We conclude based upon all of the foregoing that Mr. Conran's argument that equipment "important to safety" has not been (and need not be) treated as safety-grade must be rejected.

517. Before leaving this section, we wish to emphasize that because a system or component is important to safety, that does not mean that all the GDC apply, nor does UCS so argue. Certain of the criteria apply only to certain types of systems e.g. the ECCS need not meet the criteria for containment heat removal. (Tr. 8096-7, Pollard) Moreover, the design basis for certain systems will determine whether particular GDC apply. For example, systems needed only after an earthquake need not meet fire protection requirements. (Id.) However, once a system is determined to be important to safety, and its design basis established, it must meet the applicable GDC. That is what makes a system safety grade. (Tr. 8096-

---

* See e.g., Tr. 8413-14 (he has not considered what equipment is not "important to safety"); 8411-12 (his "impression" is that his definitions were used during TMI-1 licensing); Tr. 8419 (he hasn't been able to construct a logical definition of safety-related); Tr. 8419 (it "occurs" to him that "it may be" that something important to safety within the meaning of GDC 1 might not be sufficiently important to call for the application of any specific regulatory requirements); Tr. 8489-92 (he consulted a colleague by telephone overnight since he was "taken aback" by some of the wording of the regulations)

8101, Pollard)

Criteria for Upgrading

518. We now proceed to the criteria for upgrading proposed by the Staff witness. (Supra, para. 505) Essentially, these criteria would require as a requisite to upgrading a showing that failure of a non-safety system by itself would cause core damage or that use of a non-safety system was required to mitigate an accident assuming properly-operated safety systems. Since the witness believes that non-safety equipment was used only after improper operation of safety systems resulted in core damage, he does not believe upgrading of these (or other) non-safety systems is required. (Conran, ff. Tr. 8372 at 11)

519. However, on cross-examination it became clear that the witness could not support this statement. He does not know, for example, whether pressurizer heaters or the reactor coolant pumps were used before core damage occurred. (Tr. 8603, Conran) In fact, the reactor coolant pumps were used for 1 hour and 40 minutes at the very outset of the accident before core damage occurred. (Supra para. 15) It was apparent that the witness had no basis for claiming that non-safety systems were used only after improper operation of safety systems resulted in core damage. (Tr. 8603-8604)

520. Moreover, to the extent that the testimony implies that "careful analysis" was done by the Staff to determine whether any non-safety grade equipment should be upgraded, it is inaccurate. Mr. Conran himself never did such an analysis. (Tr. 8547, Conran) He thought that "someone like Mr. Jensen might be involved in that sort of thing." (Id.) When specifically asked what analysis was done by anyone on the Staff of the TMI systems to enable the Staff to determine whether any TMI-1 non-safety systems meet his criteria for upgrading, the only thing he could point to was the B&W computer analyses of transients and accidents discussed in Mr. Jensen's testimony on UCS Contentions 1 and 2. (Tr. 8551-8554, Conran) There is nothing in the description of that work that suggests that it is directed toward identifying adverse systems interactions or addresses itself to the criteria for upgrading put forth by Mr. Conran. (Tr. 8555-8566, Conran, See also Tr. 8103-8107, Pollard)

521. Based on the foregoing, even if Mr. Conran's criteria for upgrading systems to safety grade are the correct criteria, there is no evidence that they have been applied properly to TMI-1.

522. Finally, with respect to the issue of whether non-safety grade equipment should be partially upgraded as an exercise of "prudence", the witness was questioned on what

bases the Staff used to determine what aspects of the system or equipment should be modified - in other words, what GDC should be applied and which ignored in the partial upgrade? He stated that a "judgment had to be struck as to whether the additional reliability that might be gained by that was necessary." (Tr. 8613, Conran)

523. However, there is no indication that anyone on the Staff ever did the review necessary to exercise that "judgment" or even determined what would be needed to make the particular equipment fully safety grade, what would be gained in reliability and what the cost would be. (Tr. 8614, 8619-20, Conran) Mr. Conran knew of no such analysis. He testified that this is because of the "circumstances under which these kinds of judgments were made," that they were "hot coal items". (Tr. 8614, Conran) Apparently the decisions had to be made very quickly on what to include in NUREG-0578, allowing little time for analysis (Id.)

524. However, even after NUREG-0578 was completed, when there clearly was time for more thought, no such analyses have been done. (Tr. 8614, 8619-20, Conran) It is apparent that the Staff does not know "whether the additional reliability that might be gained" by making the PORV or other equipment safety grade is "necessary," or desirable. Although it claims to have exercised judgment, the Staff is not in possession of

the basic facts necessary in order to exercise judgment.* Hot coal or not, the perceived need to make decisions quickly does not justify the inability to support those decisions.

525. We close by dealing with the implication in the testimony that the systems interaction problem will be dealt with in the longer-term for TMI-1, suggesting that there is no need for the Board to mandate action now. (Conran, ff. Tr. 8372 at 1 15). Mr. Conran lists a series of long-term actions. In fact, the only one specifically addressed to systems interaction is Recommendation 9 of NUREG-0585. (Tr. 8678, Conran) That recommendation was not implemented. There is no existing requirement for any systems interaction study for TMI-1. (Tr. 8685-8689, Conran) TMI-1 is not part of the IREP program (Tr. 8709-10, Conran). While Mr. Conran personally disagrees

---

* Nor did the witness know in what ways either the pressurizer heaters or PORV are non-safety grade. He never looked at the current design <u>because</u> the Staff had already decided that these components did not need to be safety grade. (Tr. 8684-8687, Conran) The reasoning reflected in these answers seems curiously backward to us. How could the Staff decide what measures were needed to improve the reliability of these components without first endeavoring to determine the ways in which they are vulnerable to failure?

with this omission and still strongly favors a specific systems interaction study (Tr. 8689-8690, 8703, Conran), this curiously does not seem to affect his judgment about the propriety of allowing T.I-1 to operate without even a committment to do such a study.

526. The Board has described this Staff testimony and the pertinent cross-examination in an unusual degree of detail in order to clearly indicate why we have concluded that it is not reliable. In short, the testimony did not withstand close scrutiny.

Licensee's Testimony

527. The Licensee offered only two pages of testimony on this contention. (Keaten et al, ff. tr. 7558 at 14-16) Its position is a simple one. The Licensee asserts that the TMI-2 accident did not demonstrate a weakness in t[illegible] "inherent design capabilities of safety systems to respond to accidents, including those caused by failure of non-safety systems. If HPI had not been throttled, everything would have been fine; hence there is no need to consider the issues raised by UCS.

528. This position simply ignores the implications of the TMI-2 accident as they are elucidated by the Lessons Learned Task Force and referenced by UCS. Perhaps the clearest statement of the pertinent lessons learned is contained in Section 3.2 of NUREG-0578 (referenced in the text of the UCS contention). First, there is the paragraph quoted in the UCS contention. This paragraph, none of which was disputed by the Licensee, established that the failures of non-safety equipment contributing to the accident and the use of non-safety systems in ways not considered previously in safety analyses, raises issues not adequately recognized by the

NRC's present classification scheme . In particular, the accident indicates: 1) requirements may be needed to reduce the frequency of events that initiate transients and accidents and 2) requirement may be needed to improve the capability of currently classified non-safety systems to operate during transients and accidents.

529. The Licensee made no response whatever to either of these issues. The accident has caused no change in the Licensee's thinkin with regard to potential systems interactions. (Tr. 7703-4, Keaten In fact, Mr. Keaten stated that it is "absolutely acceptable" for the failure of non-safety systems to cause challenges to safety systems without even knowing the acceptable frequency of such chall (Tr. 7582-3 Keaten) This is fundamentally inconsistent with a major theme of the lessons learned. (See Supra , paras. 45-46, 55-59, 63, fn. at p 37, 151, 159, 160 (quoting §2.11 of NUREG-0578), 176-181)

530. The Licensee's position is, in essence, tha[illegible]e core dam at TMI-2 occurred because of improper operator action, and improved ator training will preclude a repetition, no further attention need given to the other safety issues which the analyses of the accident tified and articulated. If this were acceptable, most of the lesson learned requirements would be purely gratuitous. We reject the invitation to put on blinders.

531. A prime illustration of the narrowness with which the Licensee approached the safety implications of the TMI-2 accident is the curious way in which Mr. Keaten "rebutted" UCS's testimony that an important lesson learned was the importance of the emergency

feedwater system. (Tr. 7569-70). Mr. Keaten professed to be able to understand how such a conclusion could be drawn from th accident. (Id.)

532. This testimony is mystifying in light of the finding of the Lessons Learned Task Force that "the need for an emerger feedwater system of high reliability is a clear lesson learned from the TMI-2 accident" (Tr. 7764-5, Keaten) and our findings Board Question 6. It indicates the Licensee's inability or unw l. ness to consider objectively the meaning of the TMI-2 accide

533. Even within the four corners of Licensee's testimony, statements are made which cannot be supported.

534. For example, it is stated that while equipment needed "to provide the greatest assurance of protection for the most severe plant accidents" is designed and constructed "to the hig standards", other plant systems are still "designed to less stringent but still rigorous standards.' However, each time he was questioned about a particular piece of non-safety grade equ the witness could not identify any NRC requirements which appli these, professing an unfamiliarity with what went on in the lic process for TMI-1 or TMI-2. (Tr. 7688-9, 7693-4, Keaten) Thus his statement is little more than a soothing platitude. The Bo can make no assumptions about the quality or reliability system classified as non-safety grade.

535. Another aspect of this issue is the use of non-safety instrumentations to determine whether and how the operator shou perform safety functions. The Licensee conceded that non-safet

equipment - the pressurizer level instruments - were the only instrumentation available to determine primary coolant inventory. When they were lost, the operators had to resort to filling the system full, letting it drain down through the leakages in the system and do a calculation of pressurizer level as a function of time and an uncertainty analysis of that calculation. (Tr. 7578-9 Keaten)

536. The witness agreed that is is important to know primary system inventory, but the pressurizer level instruments will not be made safety grade. (Tr. 7579, Keaten)

537. The witness also agreed that the non-safety grade incore thermocouples were used to indicate the condition of the core. (Tr. 7585-6, Keaten) There are suggestions that their readings we not believed at least partially because they were not safety grade (Tr. 7588-7592, Keaten)

538. Moreover, both the incore thermocouples and the pressuriz level instruments are relied upon today in the plant emergency procedures to indicate to the operator when HPI can be throttled. (Tr. 7592, 7654) In the case of the incore thermocouples, the witn could identify no other instrumentation which the operator can use during a LOCA to determine the temperature in the downcomer. (Tr. 7623, Keaten)

539. The pressurizer level instruments are used to tell the operator when HPI should be throttled to avoid exceeding the temperature-pressure limits on the reactor vessel, (Tr. 7654, Keate a function which the witness agreed is important to safety. (Tr. 7596, Keaten).

540. It is thus apparent that the TMI-1 operators are directed to perform important safety functions depending upon non-safety grade instrumentation.

Board Conclusions

541. Based upon the foregoing, the Board concludes that the analyses of the TMI-2 accident clearly showed that systems presently classified as non-safety, and hence receiving little or no NRC review can cause accidents and be used to mitigate accidents in ways not originally considered in the plants safety analysis. The present NRC classification system does not adequately recognize either of these kinds of effects that non safety systems can have on the safety of the plant.

542. The Board concludes further that while the Staff has recognized the need to consider upgrading non-safety systems to reduce challenges to safety systems and to improve the capability of non-safety systems to operate during accidents and transients, the Staff has no program or plan whatever to take the first required step in this process - the undertaking of a comprehensive study to identify potential systems interactions at TMI-1.

543. Even as to the non-safety equipment specifically involved in the TMI-2 accident (e.g. PORV, pressurizer level instruments) the Staff made only a hasty and ill-documented effort to determine whether and to what extent they need be upgraded. Insufficient basi was presented to justify the Staff's decisions.

544. It is simply unacceptable to acknowledge that an unresolv safety problems exists and then to act as if this plant can be operated without restriction having taken no steps nor even commit to any future steps directed toward resolving that problem.

545. We find a direct analogy between this situation and that presented in Virginia Electric and Power Co. (North Anna Nuclear Power Station, Units 1 and 2), ALAB-491, 8 NRC 245 (1978). There, the unresolved safety issues in question were those identified by the ACRS and the Staff in its Tack Action Plans. The Appeal Board stated:

> Of course, these 'unresolved' issues cannot be disregarded in individual licensing proceedings simply becaus they also have generic applicability; rather, for an applicant to succeed, there must be some explanation why construction or operation can proceed even though an overall solution has not been found.
>
> * * *
>
> Where operation of a facility is involved, similar analysis is necessary; but as to certain issues, the justification for giving an applicant the green light can obviously be more difficult to come by. For example, the reason often given for allowing construction activity is that there is still time to find a solution and build it into the plant's designs. At the operating license state, that reason is not available. But there may be one or more other justifications for permitting the plant to operate. The most common one is that a solution satisfactory for the particular

facility has been implemented, a restriction on the level or nature of operation adequate to eliminate the problem has been imposed; or the safety issue does not arise until the later years of plant operation.

(8 NRC at 248)

546. No such justification has been suggested to this Board sufficient to allow us to authorize unrestricted operation of TMI-1 despite the existence of this safety problem. Nor, as the Appeal Board indicated, does the problem go away because it is generic. The fact that other plants are subject to the same problems and uncertainties is no reason to ignore the issue when it comes to us in a case within our jurisdiction.

547. We are also influenced by the fact that the ACRS recommended "timely completion" of systems interaction studies for TMI-1, a recommendation that the Staff chose to reject, without, in our opinion, apparent justification.

548. It is the Board's opinion that TMI-1 should not be permitted to operate until the completion of a comprehensive engineering analysis which identifies potential interactions between non-safety and safety systems and

1) non-safety systems which can cause or aggravate an accident are either upgraded or their potential adverse effects are effectively isolated from safety systems and

2) non-safety components and systems (including instru-

mentation) which are called upon in the mitigation of accidents and transients are upgraded to safety grade.

549. Based upon all of the foregoing, the Board concludes that the short and long term actions recommended by the Director of NRR are not sufficient to provide reasonable assurance that TMI-1 can be operated without endangering the health and safety of the public.

BOARD QUESTION NO. 2

550. The Commission ordered that the subjects to be considered in this proceeding were to include a determination of whether the short-term and long-term actions recommended by the Director of Nuclear Reactor Regulation are necessary and sufficient to provide reasonable assurance that TMI-1 can be operated without endangering the health and safety of the public. (Order and Notice of Hearing, August 9, 1979, at 12) In this section of our findings, we discuss the latter issue - whether the modifications to TMI-1 are sufficient to justify restart.

551. The Commission in its August 9, 1979 Order provided the Board with the discretion to determine, subject to Commission review, what matters must be resolved prior to restart. In this regard, the Commission subsequently expressed its belief that TMI-1 should be grouped with reactors which have received operating licenses, rather than with reactors with pending operating license applications. However, the Commission emphasized that it expected the Board to find to the contrary when the record so dictates. (CLI-81-3, at 7)

552. Prior to the start of the evidentiary hearing, the Board informed the parties of its concerns as to the adequacy of the

proposed actions for TMI-1 and the type of evidence that would be very important in support of a position that the proposed actions are necessary and sufficient. (Memorandum on NRC Staff Accident Sequences Report, June 23, 1980)

553. We noted that the TMI-2 accident has been identified as having a probability (Kemeny report, p. 32) so high as to be likely within 400 years. We stated that we would inquire as to the basis for any claims that the proposed actions will reduce the probability by several orders of magnitude. (Id., at 2)

554. We also noted that in the past when the Staff has identified a particular accident as being of concern, they have required that the probability be reduced to less than 10^{-6}/yr. (Id.)

555. Without telling the Staff what we would require in the nature of evidence, we stated that evidence to the effect that all accident sequences (with a nexus to the TMI-2 accident) will each have a probability of less than 10^{-6}/yr would be very important in support of a position that the proposed actions are necessary and sufficient. (Id.)

556. We subsequently posed the following Board Question 2:

"The board stated its concern with having an adequate record on the sufficiency of the proposed short-term and long-term actions to protect the health and safety of the public.

Without further explanation the question may appear to invite conclusionary testimony of the ultimate factual issues to be decided by the board. (Commission's August 9, 1979 Order, 10 NRC 141, 128). This is not what the board has in mind as a response to the question. Our concerns were expressed in part in the June 23, 1980 memorandum on the staff's report on TMI-1 accident sequences. To explain further: We assume that the staff and licensee may present evidence that each Category A and each Category B recommendation in Table B-1 of NUREG-0578 (Orders items ST 8 and LT 3), and that each preventative and mitigative measure identified with respect to a given accident sequence in the staff's TMI-1 Core Damage Accident Sequence Report will be, at least, sufficient to resolve the related safety problem or accident sequence. However, nowhere have we seen in the Restart Report, SER, the Accident Sequence Report, or elsewhere, an explanation as to how the staff or licensee has determined that all of the necessary TMI-2 related recommendations have been identified and that all the appropriate accident sequences have been addressed. The board wants testimony or other evidence which explains, if such be the case, how the licensee and the staff have concluded that the NUREG-0578 short- and long-term recommendations, other subsequent safety recommendations, and the identified accident sequences (with their respective preventative or mitigative measures) are <u>in their totality</u> sufficient to provide reasonable assurance that TMI-1 can be operated without endangering the health and safety of the public. The question is not intended to enlarge the scope of the hearing. The response may be limited to consideration of accidents following a loss-of-feedwater transient." (Tr. 2392)

557. Testimony on this Board question was presented by the Staff. (Ross, ff. Tr. 15,555) The same testimony was adopted by Staff witness Capra. (Tr. 15,554, Capra) The testimony was prepared in October 1980 (Tr. 15,549, Cutchin) and was introduced into evidence on March 18, 1981 (ff. Tr. 15,555), five days before the issuance of CLI-81-3 on March 23, 1981. The significance of these dates is discussed later.

558. Basically, the thrust of the Staff's direct testimony was that those Action Plan* items which are both applicable to TMI-1 and required to be implemented prior to restart, provide the most significant improvements in safety and are sufficient to allow TMI-1 to restart. (Ross, ff. Tr. 15,555, at 3, 12)

559. The Staff defines this subset of Action Plan items as the combination of the "short-term actions" required by the Commission's August 9, 1979 Order and the items identified in NUREG-0694 as being necessary prior to issuance of a fuel load or full power license. (Id., at 12)

560. The Staff provided no basis for its conclusion that

---

* NRC Action Plan Developed as a Result of the TMI-2 Accident, NUREG-0660, May 1980, Revised August 1980.

this subset of Action Plan items is sufficient to allow restant.

561. We discuss below the Staff's claim that those Action Plan items which are applicable to TMI-1 and required to be implemented prior to restart, provide the most significant improvements in safety and are sufficient to allow restant. First we examine those Action Plan items which the Staff claims are not applicable to TMI-1. Then we discuss the evidence concerning the Staff basis for deciding which Action Plan items (of those which the Staff identified as applicable to TMI-1) should be required to be implemented prior to restant.

562. The staff testified that of the 279 items in the Action Plan, "186 Action Plan items do not apply to TMI-1 at this time." (Ross, ff. tr. 15,555, at 7, emphasis added)

563. The largest group of these items, 126 items, are claimed by the staff to be not applicable to TMI-1 at this time because the items either do not apply to licensees/applicants or the items may ultimately lead to new requirements, but in a manner not yet determined. (Id.)

564. The Staff also claimed that 7 other Action Plan items are plant specific and do not apply to TMI-1. (Id.)

565. The Staff identified the specific Action Plan items which it considered to be not applicable to TMI-1. (Id., at table 1)

We examined the nature of some of these "NA" and "plant specific" items to evaluate the validity of the Staff's testimony that the most significant improvements in safety will be achieved without implementing these items at TMI-1 prior to restant.

566. The Staff identifies Action Plan items II.C.1, II.C.2, and II.C.3 as "plant specific" and item II.C.4 as "NA." (Id.)

567. The II.C series of four Action Plan items generally are directed toward reliability engineering and risk assessment. The objective is to identify high risk accident sequences at individual plants and determine regulatory initiatives to reduce these high-risk sequences. Reliability requirements and the single failure criterion will be improved. Requirements for station blackout and "nonsafety" systems important to risk will be developed. Consideration will be given to improving the "systems-interaction" issue in regulatory requirements. (NUREG-0660, at II.C-1)

568. Item II.C.1. is an interim reliability assessment program (IREP) which consists of a pilot study of a single plant (Crystal River Unit 3, which has a B&W reactor) followed by a study of six plants. These studies are expected to provide information necessary to develop: generic requirements to reduce high-risk accident frequency or consequences; improvements to the single failure criterian; requirements for "nonsafety-grade" equipment important to risk reduction; requirements needed to assure high reliability of engineered safety features and support systems;

improvements to the resolution of generic safety issues (black-out, d-c power, systems interactions, ATWS, etc.); improvements in the limiting conditions for operation; improvements in operator training and in plant operating, maintenance, and emergency procedures; requirements to address the B&W reactor sensitivity issue; requirements to address incidents of excessive feedwater flow; and improvements in the focus of safety research programs. (NUREG-0660, at II.C-3)

569. Item II.C.2 is a continuation of item II.C.1 which plans IREP studies on all remaining operating plants. (Id., at II.C.-5)

570. Item II.C.3 is a systems interaction study for purpose of coordinating and expanding work on unresolved safety issue A-17. (Id., at II.C-6)

571. Item II.C.4 involves using reliability engineering techiques to complement quality assurance and provide a disciplined approach to systems engingeering and the development of procedures for startup, operating, maintenance and emergency procedures. (Id.,at II.C-

572. The record in this proceeding shows that th se four Action Plan items have an important relationship to safety and that the Staff's basis for not requiring their resolution prior to restant is not based upon an assessment of the risk to public health and safety.

573. The Board (Dr. Jordan) questioned the Staff about its view of the importance of the IREP program with respect to identifying system interactions that could be critical and possibly overlooked

in the absence of a study of TMI-1. (Tr. 15,615)

574. The Staff testified that no system interactions studies are being scheduled very soon for TMI-1. The Staff is trying to develop a policy on what is a good method for studying systems interaction and the extent to which all licensees should be required to conduct such studies. (Tr. 15,616, Ross)

575. Experience with a systems interaction study at Diablo Canyon identified in excess of 600 systems interactions. (Tr. 15,617, Ross)

576. At Crystal River Unit 3, false signals to the integrated control system resulted in the control rods being withdrawn, the pressurizer spray valve opening, the PORV opening, and feedwater being cut back - all because the incoming information to the integnated control system was rendered false by a power failure. (Tr. 15,800, Ross)

577. The IREP study at Crystal River Unit 3 failed to identify those accident mechanisms which could precipitate the initiating event and at the same time degrade the reliability of the safety system called upon to respond to that event. (Tr. 16,911 Rowsome)

578. At Rancho Seco, another B&W plant, a failure of the non-nuclear instrumentation power supply precipitated a loss of feedwater and also comprised the autostart of the emergency feedwater system. (Tr. 16,913, Rowsome)

579. The Staff testified that the limited case of the analysis of the emergency feedwater system at TMI-1 was not as broad as

the typical IREP studies that have been done. A typical IREP study would be more intensive or of greater depth in the sense that such a study would include all of the support systems of the emergency feedwater system. An IREP study would be capable of detecting common cause vulnerabilities that might link the initiating event with the emergency feedwater failure through the support systems. A study of only the EFW system cannot do this. (Tr. 16,919, Rowsome)

580. The Staff has identified three potential common made linkages that could constrain the reliability with which a plant can deal with a loss of feedwater. Only one of these has been corrected at TMI-1. (Tr. 16,920-22, Rowsome)

581. The staff testified that these are several different ways to identify common cause failures. Progress has been made in modeling seismically-induced failures, fire and floods. Models for failures in similar equipment due to common design, manufacture and maintenance have been developed. The Staff also testified that use of these will be a good technique for investigating interactions between safety and nonsafety systems. (Tr. 16,914, Rowsome)

582. The sole basis advanced by the Staff for not requiring a reliability assessment and systems interaction study prior to restart of TMI-1 is that they have not made up their minds yet on the best methodoly to apply and the criteria to be used in judging the results. (Tr. 15,618, Ross; Tr. 16,915, 16,923, Rowsome)

583. When asked specifically why the Staff believes that a reliability assessment and a systems interaction study are not required prior to restart or, alternatively, why the items resolved are sufficient to allow restart, the Staff provided no credible answer. The Staff could only reiterate the process by which the Action Plan was developed and their future plans which may eventual lead to a requirement for such studies. (Tr. 15,622-30, Ross)

584. The Staff classifies Action Plan items II.E.2.1, II.E.2.2, and II.E.2.3 as "NA" - action item does not apply to licenses or the item may ultimately lead to new requirements, but in a manner not yet determined by the Staff. (Ross, ff.tr. 15,555 at Table 1 and Figure 1)

585. The three items involve the emergency core cooling system. The Action Plan states that the objectives are to: decrease reliance on the emergency core cooling system (ECCS) for other than loss-of-coolant accidents; ensure that the ECCS design-basis reliability and performance are consistent with operational experience; reach better technical understanding of ECCS performance; and ensure that the uncertainties associated with the prediction of ECCS performance are properly treated in small-break evaluations. (NUREG-0660, at II.E.2-1)

586. We can divine no basis, and the Staff supplied none, for concluding that these items need not be resolved prior to restart, especially in the face of the lesson learned that the frequency

with which some safety systems such as ECCS are called upon to function for reactor coolant system pressure or volume control may exceed their generally understood and previously accepted design basis. (NUREG-0578, at 6)

587. The Staff also classified Action Plan items II.E.3.2, II.E.3.3, II.E.3.4, and II.E.3.5 as "NA" items. (Ross, ff.tr. 15,555, at Table 1)*

588. The objective of these Action Plan items is to improve the reliability and capability of nuclear power plant systems for removing decay heat and achieving safe shutdown conditions following transients and under postaccident conditions. (NUREG-0660, at II.E.3-1)

589. Item II.E.3.2 involves a study using deterministic and probabilistic methods to identify design weaknesses and possible decay heat removal system modifications that could be made to improve the capability and reliability of these systems under all shutdown conditions. (Id.)

590. Item II.E.3.3 envisions a coordinated effort to evaluate shutdown heat removal requirements in a comprehensive manner which is required to permit a judgement of adequacy in terms of overall system requirements. (Id., at II.E.3-2)

---

* Item II.E.3.1, Reliability of Power Supplies for Natural Circulation is the subject of UCS Contentions 3 and 4.

591. Item II.E.3.4 involves a research project to study the usefulness of installing an additional decay heat removal system in existing plants to improve the overall operational reliability of decay heat removal and to produce system performance and safety design criteria for decay heat removal systems. (Id.)

592. Item II.E.3.5 involves issuing a revision to Regulatory Guide 1.139, "Guidance for Residual Heat Removal to Achieve and Maintain Cold Shutdown", which includes requirements for reaching cold shutdown using safety-grade equipment. (Id., at II.E.3-3)

593. The Staff testified that its current position is that plants should be capable of going to cold shutdown with safety grade equipment, but implementation of that "position" varies from plant to plant. (Tr. 8079, Silver)

594. The Staff does not, at this time, have a requirement that operating plants must implement this position. Even though deficiencies have been identified, the Staff has not issued backfit orders. (Tr. 8080, Silver)

595. TMI-1 is not capable of achieving cold shutdown conditions using only safety grade equipment. (Supra., para 400)

596. The Staff provided no basis for concluding that these Action Plan items pertaining to decay heat removal do not need to be resolved prior to restart.

597. We have decided that it is unnecessary to set forth here a discussion of the substance of each of the Action Plan items which the Staff classifies as not applicable at this time to

TMI-1. The discussion above is sufficient to illustrate that the main reason the Staff classsifies these items as not applicable at this time is that the new requirements that may result from resolving the "not applicable" items have simply not yet been determined. This, of course, does not provide a basis for concluding that the Action Plan items completed to date are sufficient to allow TMI-1 to restart.

598. We also find that the Action Plan itself contradicts the Staff's testimony that the "NA" items would not provide the most significant safety improvements.

599. The Action Plan contains a priority ranking for each of its items. The priority ranking system assigned a maximum of 210 possible points of which only 100 involved an assessment of the Safety significance of the item. The remainder of the points involved the cost of implementation, the length of time required for implementation, and whether the item involved hardware or human element improvements. (Tr. 8101-02, Pollard; NUREG-0660, at Table B.1)

600. With respect to the assessment of safety significance, the Action Plan assigned 100 points to items with "high" safety significance and 50 and 0 points to those items with "medium" and "low" safety significance. (NUREG-0660, at Table B.1)

601. Of the 126 Action Plan items which the Staff classifies as "NA" (i.e., item does not apply to licensees or the item may ultimately lead to new requirements, but in a manner not yet determined by the Staff), approximately 30 items have a "high" safety significance and approximately 40 have a "medium" safety

significance assigned in the Action Plan. (Compare Ross, ff. tr. 15,555, Table 1 with NUREG-0660 Table B.3)

602. Since the Staff has not yet determined the extent to which these Action Plan items may result in new requirements, we cannot determine the basis, if any, for the Staff's conclusionary testimony that the Action Plan items applicable to TMI-1 will provide the most significant safety improvement and, therefore, give no weight to that testimony.

603. We now turn to a discussion of the record with respect to the Staff's basis for deciding which of the Action Plan items it classifies as applicable to TMI-1 should be required to be implemented prior to restart.

604. As we noted above, the thrust of the Staff's direct testimony was that those Action Plan items which are both applicable to TMI-1 and required to be impleted prior to restant are sufficient to allow restart. (Ross, ff. tr. 15,555, at 3,12)

605. The Staff defined this subset of Action Plan items as the combination of the "short-term actions" required by the Commission's August 9, 1979 Order and the items identified in NUREG-0694 as being necessary prior to issuance of a fuel load or full power license. (Id., at 12)

606. The Staff noted that the Commission's August 9, 1979 Order specifying which items were "short-term" and which were "long term" was issued prior to the completion of many of the TMI-2 accident investigations and development of the Action Plan. (Id., at 8) Thus, it cannot be claimed that the Commission itself was in a position to decide on the merits which actions were sufficient to

allow restart. To the contrary, the Commission directed this Board to determine the issue subject to Commission review.

607. The Staff also testified that the remainder of the Action Plan items applicable to TMI-1 which will not be implemented prior to restart, will be required to be completed on a schedule consistent with that specified in NUREG-0737 for operating reactors. (Id., at 12)

608. The Board inquired into the bases for delaying certain items until after restart. The Staff's basis for determining whether the dates proposed for TMI-1 are acceptable focused more on expediency than on an assessment of the risk to public health and safety.

609. Action Plan item I.C.1, "short-term accident analysis and procedures revision", includes requirements to perform analyses of transients and accidents, prepare emergency procedure guidelines, upgrade emergency procedures and conduct operating retraining. "Emergency procedures are required to be consistent with the actions necessary to cope with the transients and accidents analyzed." (NUREG-0660, at I.C-2 to I.C-3)

610. The original schedule for these requirements was to analyze transients and accidents by early 1980 and implement the emergency procedures and retraining within three months after the emergency procedure guidelines were established. (Id., at I.C-3)

611. The Staff modified this "dealine" to the first refueling outage after January 1, 1982 for the training and procedures resulting from the transient and accident evaluation. (Tr. 15,584, Capra)

612. As an "interim approach" to compensate for not completing this item, the Staff is relying on Action Plan item I.C.8, which is a pilot monitoring program of selected emergency procedures. (Tr. 15,587-88, Capra)

613. However, review of procedures at licensed plants has disclosed difficiencies. The Staff has gone through procedures with operators and found instances where the operator could not physically follow the procedure because controls were too far apart. On other occasions the operator literally did not know what to do next. (Tr. 15,732-33, F ss)

614. Nevertheless, the Staff is not reviewing any more than four selected emergency procedures at TMI-1. (Tr. 15,588, Capra) Furthermore, there appears to have been only a cursory review of the selected emergency procedures and no check on subsequent revisions to the procedures. (Tr. 16,771-775, Wermiel) Such a situation neither compensates for not completing item I.C.1 nor provides a basis for concluding that what has been accomplished to date is sufficient to allow restart.

615. There are several items not being required prior to restant solely because of equipment delivery problems. The Staff was quite candid under examination in stating that if the licensee cannot buy a necessary piece of equipment prior to restart, the

staff approved a deadline for implementing the Action Plan item consistent with the time when the equipment could be purchased. (Tr. 15,676, Ross)

616. The Staff also testified that in deciding what was "necessary" prior to restart, their decision was "tempered" by their perception of what is "possible." (Tr. 15,677-78, Ross)

617. The Staff further testified that this concept of "necessity" depends not only upon "possible" and "feasibility", but also on the "pragmatics" of balancing safety against the generation of electricity. (Tr. 16,681-82, Ross)

618. In other instances the Staff, to a large degree, simply considered what the licensee planned to do anyway - this is, without the Staff requiring that something be done. (Tr. 15,683-84, Ross)

619. Among the Action Plan items which the Staff proposes not to require prior to restart because of equipment procurement problems are the following:

(1) Item II.B.1, installation of reactor coolant system high point vents (Tr. 15, 597-99, Ross and Capra);

(2) Item II.B.3, post-accident sampling (Tr. 15,602, Ross);

(3) Item II.E.4.2, containment isolation dependability (Tr. 15,607-09, Ross and Capra);

(4) Item II.F.1, additional accident monitoring equipment (Tr. 15,609-10, Ross); and

(5) III.D.3.3, inplant radiation monitoring to measure iodine accurately (Tr. 15,612-15, Ross and Capra)

620. All of these five items were classified as either "high" or "medium" safety significance items in the Action Plan. (NUREG-0660, at Table B.3)

621. In summary, the record indicates that the Staff has no basis for deciding whether the items which have been completed are sufficient to allow restart. The Staff has taken two approaches. For those items where the requirements for improved safety are known but not implemented, the Staff has simply postponed the deadline without providing a reasoned basis for concluding that the health and safety of the public will not be endangered. For those items where the Staff has not yet determined what requirements are necessary to resolve the lesson learned from the TMI-2 accident, the Staff simply describes its ongoing research and evaluation plans to resolve the item.

622. This latter approach is analagous to the Staff's earlier treatment of generic unresolved safety problems. This practice was specifically rejected by the Appeal Board in River Bend and North Anna.* It also was a subject of the Report by the President's Commission on the Accident at Three Mile Island:

> "NRC's primary focus is on licensing and insufficient attention has been paid to safety.***/ T_7 he evidence

---

* See the discussion supra at paras 544 - 546. Having identified safety problems which remain unresolved does not absolve the Staff or Licensee from demonstrating why the plant can be safely operated pending resolution of these safety problems, wheter generic or not.

indicates that the labeling of a problem as 'generic' may provide a convenient way of postponing decision on a difficult problem". (Kemeny, at 20)

623. "The [President's] Commission believes that the agency must improve on prior perfromance in resolving generic and specific safety issues." (Kemeny, at 64)

624. The Staff has done no plant - specific analysis of TMI-1 to determine whether the plant is safe enough to restart. (Tr.21,117, 21,120-1 Silver; Tr. 21,154, Jacobs) Despite the fact that the Staff recognizes that license conditions must be imposed by the Board, and that only two weeks remained for submitting the Staff's proposed findings, the Staff had not yet determined even what license conditions it would propose to the Board and seemed to have given no thought to the question until it was raised on cross-examination. (Tr. 21,442-3, 21,260-3, Silver)

625. The Staff appears to be operating on the simple proposition that if other plants are being permitted to continue to operate with similar defets to TMI-1, ergo, TMI-1 can restart. (Tr. 21,080, Silver)

626. We were frankly astonished to hear that items which were listed by the Staff as "required" prior to restart, were not, in fact, required. They appear on the list simply because the current implementation dates in NUREG-0737 happen to fall before the projected restart date. If the 0737 dates slip beyond restart, those items will not be required by the Staff. No evaluation was made of any of the items to determine whether they are necessary for safety-

for TMI-1. (Tr. 21,217 - 321, Silver)

627. Moreover, all deadlines are considered amendable by the Staff. Nothing is seen as so important to safety that it should be a hard and fast requirement. (Tr. 21,045-8, Silver) The Staff states that all deadlines beyond June 30, 1981 are subject to reconsideration and the Staff doesn't know whether any are firm. (Tr. 21,236, 21,136, Silver)

628. While the Staff stated that it would require a justification or "explanation" before allowing extensions of deadlines for completion of requirements, it has already allowed such a waiver of committment as to the installation of the high point vents with no apparent justification. (Tr. 21,282-5, 21,297, 21-312-13, Silver and Jacobs) Thus, the Board cannot rely on the promise that good cause will be required to justify an extension.

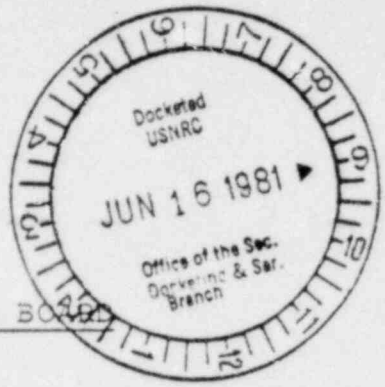
629. We are unable to discern any coherent logic behind the Staff's position that there is reasonable assurance that this plant is safe enough to restart (Staff Ex. 14 at 3) or that the measures recommended by the Director of NRR are sufficient to permit operation. In fact, the Board cannot tell from this record what are "requirements" for restart. Nor can we rely on Licensee "committments" to fill this void, since it is quite clear that such committments are unenforceable, are routinely permitted to be changed as NUREG-0737 deadlines are changed, and simply march in lockstep with NUREG-0737. (Tr. 21,282 - 21,294, Silver) They have no independent force whatever.

630. On the basis of the foregoing, the Board concludes that this

record does not establish that there is reasonable assurance the the TMI-1 is safe enough to restart or that the short and long-term measures recommended by the Director of NRR are sufficient to provide reasonable assurance that TMI-1 can be operated without endangering the health and safety of the public.

UNITED STATES OF AMERICA

NUCLEAR REGUALTORY COMMISSION



BEFORE THE ATOMIC SAFETY AND LICENSING BOARD

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

I hereby certify that copies of "Union of Concerned Scientists Proposed Findings of Fact and Conclusions of Law on UCS Contentions Nos. 13 and 14 and Board Questions 2 and 6 have been mailed postage pre-paid this 12th day of June, 1981 to the parties listed below.

SERVICE LIST

Ivan W. Smith, Esquire (5)
Chairman
Atomic Safety and Licensing
Board Panel
U. S. Nuclear Regulatory
Commission
Washington, D. C. 20555

Dr. Walter H. Jordan
Atomic Safety and Licensing
Board Panel
881 West Outer Drive
Oak Ridge, Tennessee 37830

Dr. Linda W. Little
Atomic Safety and Licensing
Board Panel
5000 Hermitage Drive
Raleigh, North Carolina 27612

James R. Tourtellotte, Esq.
Office of the Executive
Legal Director
U.S. Nuclear Regulatory
Commission
Washington, D. C. 20555

John A. Levin, Esquire
Assistant Counsel
Pennsylvania Public Utility Commission
Post Office Box 3265
Harrisburg, Pennsylvania 17120

Robert Adler, Esquire
Assistant Attorney General
505 Executive House
Post Office Box 2357
Harrisburg, Pennsylvania 17120

Walter W. Cohen, Esquire
Consumer Advocate
Office of Consumer Advocate
14th floor, Strawberry Square
Harrisburg, Pennsylvania 17127

Docketing and Service Section
Office of the Secretary
U.S. Nuclear Regulatory Commission
Washington, D. C. 20555

Jordan D. Cunningham, Esquire
Fox, Farr & Cunningham
2320 North Second Street
Harrisburg, Pennsylvania 17110

Mrs. Louise Bradford
TMI ALERT
315 Peffer Street
Harrisburg, Pennsylvania 17102

Steven C. Sholley
Union of Concerned Scientists
1725 I Street, N.W., Suite 601
Washington, D. C. 20006

Gail Bradford
ANGRY
245 West Philadelphia St.
York, Pennsylvania 17404

Marjorie M. Aamodt
R.D. 5
Coatesville, Pennsylvania
19320

George F. Trowbridge, Esq.
Shaw, Pittman, Potts & Trowbridge
1800 M Street, N.W.
Washington, D. C. 20036

William S. Jordan, III, Esquire
Harmon & Weiss
1725 Eye Street, N.W., Suite 506
Washington, D. C. 20006

Chauncey Kepford/Judith Johnsrud
Environmental Coalition on Nuclear Power
433 Orlando Avenue
State College, Pennsylvania 16801

Marvin I. Lewis
6504 Bradford Terrace
Philadephia, Pennsylvania 16801

Attorney General of New Jersey
Attention: Thomas J. Germine, Esq.
Deputy Attorney General
Division of Law - Room 316
1100 Raymond Boulevard
Newark, N. J. 07102

Ellyn R. Weiss