

UNITED STATES OF AMERICA
NUCLEAR REGULATORY COMMISSION

BEFORE THE ATOMIC SAFETY AND LICENSING BOARD

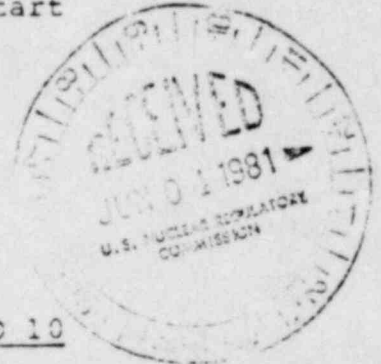
In the Matter of)
)
)

METROPOLITAN EDISON COMPANY, et al.,)

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

Docket No. 50-289
Restart

UNION OF CONCERNED SCIENTISTS
PROPOSED FINDINGS OF FACT AND
CONCLUSIONS OF LAW ON UCS
CONTENTIONS NOS. 1, 2, 3, 4, 5 AND 10



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

Robert D. Pollard
UNION OF CONCERNED SCIENTISTS
1725 I Street, N.W.
Suite 601
Washington, D.C. 20006
(202) 296-5600

DATED: June 1, 1981

DS03
S
0/1

8106050508

G

UCS pursued two contentions asserting that natural circulation cooling at TMI is inadequate to remove decay heat and that reliable forced cooling should be provided by systems which meet the Commission's regulations applicable to systems important to safety.

UCS CONTENTION NO. 1

The accident at Three Mile Island Unit 2 demonstrated that reliance on natural circulation to remove decay heat is inadequate. During the accident, it was necessary to operate at least one reactor coolant pump to provide forced cooling of the fuel. However, neither the short nor long term measures would provide a reliable method for forced cooling of the reactor in the event of a small loss-of-coolant accident ("LOCA"). This is a threat to health and safety and a violation of both General Design Criterion ("GDC") 34 and GDC 35 of 10 CFR Part 50, Appendix A.

UCS CONTENTION NO. 2

Using existing equipment at TMI-1, there are only 3 ways of providing forced cooling of the reactor:
1) the reactor coolant pumps; 2) the residual heat

removal system; and 3) the emergency core cooling system in a "bleed and feed" mode. None of these methods meets the NRC's regulations applicable to systems important to safety and is sufficiently reliable to protect public health and safety:

- a) The reactor coolant pumps do not have an on-site power supply (GDC 17), their controls do not meet IEEE 279 (10 CFR 50.55a(h)) and they are not seismically and environmentally qualified (GDC 2 and 4).
- b) The residual heat removal system is incapable of being utilized at the design pressure of the primary system.
- c) The emergency core cooling system cannot be operated in the bleed and feed mode for the necessary period of time because of inadequate capacity and radiation shielding for the storage of the radioactive water bled from the primary coolant system.

1. Testimony on these contentions was given by the Licensee (Keaten and Jones, ff. Tr. 4588) and the Staff

(Jensen, Natural Circulation, and Jensen, Forced Flow, ff. Tr. 4913).

2. Adequate removal of decay heat following a small break loss-of-coolant accident was discussed in two parts: (1) removal of core decay heat from the fuel rods to the primary system fluid, and (2) removal of the energy from the reactor coolant system. (Keaten and Jones, ff. Tr. 4588, at 3)

3. Adequate removal of decay heat from undamaged fuel rods can be maintained as long as the core remains covered by liquid or two-phase water coolant. If the fuel rods are uncovered to a limited extent and/or for a limited time, cooling of the uncovered portion of the core is provided by the steam rising from the covered portion of the core. (Keaten and Jones, ff. Tr. 4588, at 3)

4. No evidence was presented by the Licensee or Staff to define the "limited" extent of uncovering and/or time for which steam cooling of the uncovered fuel would be adequate. No evidence was presented by the Licensee or Staff to describe the extent of core damage, such as fuel rod swelling, for which adequate core cooling would be maintained, following a period of core uncovering, simply by recovering the core and without forced circulation of the coolant.

5. To prevent excessive reactor coolant system pressure from occurring, the energy added to the coolant must be removed. (Keaten and Jones, ff. Tr. 4588, at 6)

6. The methods available to remove energy from the reactor coolant system are: (1) through the break, (2) through the steam generators and (3) through the pressurizer relief valve and/or safety valves. (Keaten and Jones, ff. Tr. 4588, at 7-8 and Tr. 4696, Jones)

7. For breaks larger than about 0.01 to 0.02 ft², the energy discharged through the break is sufficient to prevent a pressure increase and, therefore, no other method of removing energy from the reactor coolant system is needed. (Jensen, Natural Circulation, ff. Tr. 4913, at 5; Keaten and Jones, ff. Tr. 4588, at 7) The high pressure injection system must operate to replace the coolant lost through the break in order to keep the core covered. (Jensen, Natural Circulation, ff. Tr. 4913, at 4)

8. The second method of removing energy from the reactor coolant system - through the steam generators - requires the availability of feedwater from either the main or emergency feedwater system. The coolant heated in the reactor vessel is circulated to the steam generators where it is cooled by the secondary system feedwater.

The secondary coolant boils and the steam is removed to the condenser or to atmosphere. (Jensen, Natural Circulation, ff. Tr. 4913, at 4) The primary coolant heated in the reactor vessel is circulated to the steam generators by either the reactor coolant pumps or by natural circulation if the reactor coolant pumps are inoperative.

9. The reactor coolant pumps will be inoperative if offsite electrical power is lost (Tr. 4654, Keaten) which is a condition required to be postulated by GDC-17 of Appendix A to 10 CFR Part 50. Even if offsite power is not lost, the reactor coolant pumps are supposed to be shut off if high pressure injection is automatically initiated. (Lic. Ex. 48, at 2.0)

10. Natural circulation of the primary coolant can occur in two ways - liquid or two-phase circulation. The Licensee referred to liquid circulation as natural circulation and two-phase circulation as the boiler-condenser mode. (Keaten and Jones, ff. Tr. 4588, at 7). The Staff uses the term natural circulation to apply to either liquid flow or two-phase flow. (Tr. 4932, Jensen)

11. In either the liquid or two-phase natural circulation process, primary system inventory must be maintained using the high pressure injection system and feedwater flow to the

steam generators must be maintained. (Tr. 4693-4695, Jones)

12. In the liquid natural circulation mode, the primary system, excluding the pressurizer, is basically full of liquid. (Tr. 4682, Jones) In the boiler-condenser or two-phase natural circulation mode, the primary system contains both steam and liquid water. To achieve natural circulation in this condition, the primary system must contain sufficient liquid water to fill the system up to at least the inlet of the reactor coolant pumps. (Tr. 4698, Jones) In addition, the secondary water level must be higher than the primary water level in the steam generators in order to provide a condensing surface for the steam in the reactor coolant system. (Tr. 4933, Jensen)

13. For primary system breaks smaller than about 0.01 to 0.02 ft², steam generation or voiding in the primary system will be sufficient to interrupt liquid natural circulation. (Jensen, Natural Circulation, ff. Tr. 4913, at 6; Keaten and Jones, ff. Tr. 4588, at 7) If makeup from the high pressure injection system is less than the water lost through the break, the water level in the primary system would continue to drop. When the primary water level decreases below the level of the emergency feedwater inlet on the secondary side of the steam generators, the boiler-condenser or two-phase mode of natural circulation

will be established. (Jensen, Natural Circulation, ff. Tr. 4913, at 6)

14. The third method of removing heat from the reactor coolant system - through the pressurizer relief or safety valves - is referred to as the feed-and-bleed mode. Water is injected into the primary system by the high pressure injection system and the decay heat is removed through the pressurizer pilot operated relief valve (PORV) or the safety valves. (Jensen, Natural Circulation, ff. Tr. 4913, at 8-9) Two high pressure injection pumps are needed for some break sizes to assure adequate core cooling in the feed-and-bleed mode. (Jones, ff. Tr. 4589, at 3)

15. During the TMI-2 accident, forced cooling of the core was provided by operation of all four reactor coolant pumps from the start of the accident until about 1 hour and 13 minutes when two were shut off. The remaining two were shut off at approximately 1 hour and 40 minutes. (Tr. 4608, Keaten) At the time the last two reactor coolant pumps were stopped, there was not sufficient liquid water in the primary system to establish two-phase natural circulation. (Tr. 4628, Jones; Tr. 4963, Jensen) The result was a period of core damage which was stopped by the closure of the PORV block valve and the resumed operation of a reactor coolant pump. (Tr. 4678-4680, Jones) A second period of core

damage about 3 hours and 45 minutes after the start of the accident was terminated by the initiation of maximum high pressure injection flow. (Tr. 4680-4681, Jones)

15. Liquid natural circulation did not become established during the TMI-2 accident because steam or a mixture of steam and hydrogen was trapped in the 180° bend of the reactor coolant system hot legs at the top of the steam generators. (Tr. 4616-4617, Jones) The boiler-condenser or two-phase mode of natural circulation was not established because the primary system was being refilled, thereby raising the primary system level above the secondary coolant level in the steam generators, blocking the condensation of steam in primary system. (Tr. 4616, Jones)

16. In summary, in the period from four hours into the accident when maximum high pressure injection was initiated until sixteen hours, when a reactor coolant pump was started, liquid natural circulation was not established because of the void in the hot legs and two-phase circulation was not established because there was too much water in the primary system to expose a steam condensing surface in the steam generator tubes.

18. Under the conditions that prevailed from approximately 4 to 16 hours after the start of the accident, the only way to get natural circulation started was to start a

reactor coolant pump. (Tr. 4617, Jones)

19. Early in this proceeding, Licensee and Staff testified that the addition of high point vents prior to the restart of TMI-1 would provide another way to remove steam or noncondensable gas and restore natural circulation. (Tr. 4617, Jones; Tr. 4942-3, 4992-4993, Jensen; Staff Ex. 1, at C8-63) However, it was disclosed near the end of the hearings that the earlier Licensee commitment and Staff requirement have been changed. It is now stated that the high point vents will not be installed until July 1, 1982, which is after the proposed restart date. (Staff Ex. 14, at 53; Tr. 21, 078, Jacobs.) There is no assurance that this date is firm and will not be further postponed. (Tr. 21, 045-6, 21, 136-40, 21, 144-5, 21,236, Silver and Jacobs.)

20. Furthermore, the TMI-1 emergency procedures rely on restarting the reactor coolant pumps to establish core cooling in the event of inadequate core cooling. (lic. Ex. 48, at 7.0, 23.0-26.0)

21. The Licensee's witnesses testified that after adequate high pressure injection flow was restored, subsequent to core damage, the core was effectively cooled even though natural circulation was not occurring. (Keaten and Jones, ff. Tr. 4538, at 8) Under cross-examination, however, the witnesses testified that their attention had actually centered on the accident up to the time the last reactor coolant pump was initially turned off, at about one hour and forty minutes into the accident. (Tr. 4605, Keaten)

The witnesses also testified, that for about the first three days following restart of one reactor coolant pump, natural circulation might not have been established if the pump had stopped because of the amount of noncondensable gas in the primary system. (Tr. 4654-4655, Keaten)

Finally, the witnesses testified that the first time following the start of the accident when adequate core cooling is known to have been established is at 16 hours when a reactor coolant pump was restarted. (Tr. 4655, Jones) The Staff also testified that in later stages of the TMI-2 accident, after an adequate primary coolant inventory was restored, the core was successfully cooled by natural circulation in spite of the severe flow blockage expected in the damaged core. (Jensen, Natural Circulation, ff. Tr. 4913, at 7). However, under cross-examination, the Staff's witness testified that he did not know when adequate coolant inventory had been restored, and did not know when (whether days or months) natural circulation was restored. (Tr. 4942, 4954, 4963, Jensen) The witness also testified that he did not know, for all times after an adequate coolant inventory was restored, whether the TMI-2 core was successfully cooled by natural circulation. (Tr. 4964-4966, Jensen) Furthermore, the Staff's witness testified that he did not know whether it was necessary to have started

a reactor coolant pump to achieve adequate core cooling during the TMI-2 accident. (Tr. 4977-4978, Jensen)

22. In sum, the Staff's testimony did not attempt to analyze what happened at TMI-2. Instead, a computer analysis was done showing that natural circulation will be effective in cooling the core if emergency feedwater is present and if high pressure injection is not prematurely terminated. These assumptions lead to a conclusion that there would be no core damage, no hydrogen generation and natural circulation would not be lost. (Tr. 4966-4968, Jensen) However, for the situation which prevailed in the TMI-2 accident, the Staff's witness did not know whether it was necessary to provide forced circulation cooling using a reactor coolant pump. (Tr. 5027-5028, Jensen)

23. During the TMI-2 accident, several attempts were made to establish forced cooling of the core before forced cooling was established at 16 hours into the accident. (Tr. 4609-4610) Then an attempt was made to depressurize the primary system so that the low pressure injection system (or residual heat removal system) could be operated. However, system pressure could not be lowered sufficiently. (Tr. 4650-4651, Jones) Finally, at about 16 hours into the accident, a reactor coolant pump was started, removing the void in the hot leg and reestablishing forced circulation

in the primary system and heat removal via a steam generator. (Tr. 4635-4636, Jones) In both instances (attempting to restart a reactor coolant pump and attempting to start the normal shutdown cooling mode of operation of the decay heat removal system), the operators were trying to get the plant into a condition covered by their training and procedures where they would really feel like they knew what was going on. (Tr. 4636, 4652, Keaten)

24. The evidence supports a conclusion that liquid natural circulation is an adequate means of satisfying GDC-34 and GDC-35 for small break loss-of-coolant accidents provided that feedwater is available and the high pressure injection system provides sufficient water to the primary system to prevent the formation of voiding in the 180° bends of the hot legs. (Keaten and Jones, ff. Tr. 4588, at 4,5)

25. However, in light of the TMI-2 accident, it must be assumed that accidents involving sufficient voiding to interrupt natural circulation are credible. If this was not the case, there would be no need for several modifications, such as the high point vents, being required by the Commission.

26. In addition, no analyses have been performed to determine whether natural circulation is adequate if core damage in excess of 10 CFR 50.46 limits is experienced. There is no evidence in the record to support a finding that liquid natural circulation is an effective means to cool the core in the event of core damage or voiding which interrupts natural circulation. The evidence of the TMI-2 accident indicates otherwise.

27. The evidence does not support a conclusion that the boiler condenser or two-phase mode of natural circulation

is adequate to meet the requirements of GDC-34 and GDC-35. Analyses performed prior to the TMI-2 accident did not rely on the boiler-condenser mode because the smallest break analyzed was 0.04 ft^2 and that break size or greater is capable of removing essentially all the energy.

(Tr. 4691-4692, Jones) The smallest break analyzed after the accident was 0.005 ft^2 . (Tr. 4692, Jones) None of the tests of natural circulation done prior to the accident involved sufficient primary system voiding to interrupt natural circulation. (Tr. 4702, Jones) None of the tests kept the PORV open or in any other way simulated a LOCA. (Tr. 4703, Jones) None of the tests simulated flow blockage which would result from core damage. (Tr. 4702-4703, Jones) None of the unplanned occurrences in operating B&W plants involving natural circulation resulted in voiding sufficient to interrupt natural circulation. (Tr. 4704-4705, Jones) There are no plans to test the boiler-condenser mode on a B&W plant because there is no instrumentation available to control either the secondary or primary water levels accurately and the reactor might be damaged. (Tr. 4687-4688, Jones)

28. In addition, as noted above, the two-phase mode of natural circulation requires that the water level on the secondary side be higher than the water level on the primary side of the steam generators in order to provide a condensing surface. (Tr. 4933, Jensen) However,

post-TMI-2 emergency procedures direct the operators to immediately refill the primary system using the pumps following a LOCA and to keep the pumps in operation until the plant has achieved adequate cooling. (See the discussion of IE Bulletin 79-05A, item 4, Staff Ex. 1 at C2-4 - C2-5.)

29. Moreover, the TMI-1 emergency feedwater system, which is required for either liquid or two-phase natural circulation to be effective, has a probability of failure on the order of

10^{-2} to 10^{-4} per reactor year (Wermeil and Curry, ff. Tr. 16,718, at 35, 37) and is therefore not sufficiently reliable.

30. The evidence does not support a conclusion that feed-and-bleed can be relied on to meet the requirements of GDC-34 and GDC-35. The Staff does not rely for its analyses or findings on heat removal using feed-and-bleed; the Staff relies on heat removal using the emergency feedwater system. (Tr. 5016, Jensen)

31. The February 26, 1980 accident at Crystal River was advanced by the Licensee and the Staff as an event which demonstrated the adequacy of feed-and-bleed cooling. (Jones, ff. Tr. 4589, at 3-4; Jensen, Natural Circulation, ff. Tr. 4913, at 9 - 10) However, on cross-examination, it was established that natural circulation occurred during a portion of the transient, feedwater was provided to one steam generator except for a period of four to five minutes, a bubble was restored in the pressurizer probably by use of the pressurizer heaters and the reactor coolant pumps were restarted. (Tr. 4705-4706, Jones) It was also established under cross-examination that feed-and-bleed cooling was not required in this instance to cool the core because feedwater was restored within twenty minutes. (Tr. 5012, Jensen)

32. The most that can be concluded from this Crystal River accident is that water was fed into and bled from

the reactor coolant system. It cannot be concluded that this demonstrated the adequacy of feed-and-bleed to remove decay heat.

33. We consider it highly significant that the feed-and-bleed mode cannot be used to achieve cold shutdown conditions using safety grade equipment because the primary system cannot be depressurized. Bleed and feed depends on use of the safety valves which the operator cannot control. (Tr. 4984-4985, Jensen; Jones, ff. 4589, at 2)

34. A quantitative reliability assessment of the feed and bleed mode has not been performed. (Jones, ff. 4589, at 3)

35. Although the actions taken by the operator directly related to achieving feed-and-bleed are not complex, the combination of other actions which the operator must take during a LOCA and the decision process that must be followed is complex. (Tr. 4788-4840, Jones; Lic. Ex. 48, at 31.0) The crucial nature of the operator's role in achieving and controlling cooling via bleed and feed introduced another clear element of unreliability.

36. We reach the following conclusion

a. Liquid natural circulation capability at TMI-1 is not a sufficiently reliable method of decay heat removal because:

(1) Voids that can accumulate in the hot legs and interrupt liquid natural circulation cannot be removed because the reactor coolant pumps are not safety grade and therefore cannot be relied upon and high point vents on the hot legs have not been installed, and

(2) The emergency feedwater system is not sufficiently reliable

b. The boiler-condenser or two-phase mode of natural circulation at TMI-1 is not a sufficiently reliable method of decay heat removal because:

(1) There is no method of determining primary system water level,

(2) Post-TMI-2 emergency procedures requiring refilling of the primary system after a break will preclude the establishment of a condensing surface on the primary side of the steam generator tubes,

(3) The effectiveness of the boiler-condenser mode has not been and will not be tested, and

(4) Emergency feedwater is not sufficiently reliable

c. The feed-and-bleed mode of operation at TMI-1 is not a sufficiently reliable method of decay heat removal because:

- (1) Its effectiveness has not been demonstrated,
- (2) Its operation depends on operator action and the requisite actions and decision process are complex,
- (3) Cold shutdown conditions cannot be achieved using feed-and-bleed.

d. No reliable method of forced cooling is provided at TMI-1 because

- (1) The reactor coolant pumps do not meet the Commission's requirements applicable to components important to safety (i.e., safety grade components), and
- (2) The normal shutdown cooling mode of operation of the decay heat removal system cannot be used because primary system pressure will be far above the design pressure of the decay heat removal system.

37. Based on the above, we find that the "short term actions" recommended by the Director of Nuclear Reactor

Regulation (set forth in Section II of the Commission's August 9, 1979, order) are not sufficient to provide reasonable assurance that TMI-1 can be operated without endangering the health and safety of the public and that, therefore, restart cannot be authorized.

UCS Contention No. 3 is as follows:

The Staff recognizes that pressurizer heaters and associated controls are necessary to maintain natural circulation at hot stand-by conditions. Therefore, this equipment should be classified as "components important to safety" and required to meet all applicable safety-grade design criteria, including but not limited to diversity (GDC 22), seismic and environmental qualification (GDC 2 and 4), automatic initiation (GDC 20), separation and independence (GDC 3 and 22), quality assurance (GDC 1), adequate, reliable on-site power supplies (GDC 17) and the single failure criterion. The staff's proposal to connect these heaters to the present on-site emergency power supplies does not provide an equivalent or acceptable level of protection.

38. Direct testimony on this contention was presented by UCS (Pollard, ff. Tr. 8182), the Licensee, (Keaten, et al., Safety Classification, ff. Tr. 7558, at 16-18) and the NRC Staff (Jensen, ff. Tr. 8712).

39. UCS's testimony was that the TMI-2 accident demonstrated the importance of highly reliable decay heat removal capability. Indeed, the accident graphically showed that inability to remove decay heat can lead to severe core damage. (Pollard, ff. Tr. 8182 at 3-3). The Reactor Safety Study found that failures leading to the inability to remove decay heat resulted in a greater probability of core melt than that predicted for large LOCA's. (Id. at 3-10)

40. UCS testified that there is only one proven effective way of removing the decay heat at TMI-1: Water must be circulated through the reactor, the main coolant piping, and the steam generator tubes. The decay heat transferred from the fuel to the reactor coolant is thus transferred to the secondary system through the steam generator tubes. (Pollard, ff. Tr. 8182 at 3-1 - 3-2.)

41. There are two methods of providing circulation of the reactor cooling water at TMI-1: 1) forced circulation using one or more reactor coolant pumps or 2) natural circulation. Both methods of circulation require maintaining reactor coolant system pressure at a level sufficient to prevent boiling of the water. If the pressure drops, steam will form in the reactor coolant system, blocking natural circulation and also preventing operation of the

reactor coolant pumps. (Id.)

42. The pressurizer is used to control reactor coolant system pressure, by use of the pressurizer heaters and pressurizer spray. (Id.) The pressurizer heaters and their associated instruments and controls are not safety-grade and were not previously classified as components important to safety. At the time of the TMI-2 accident, the design of TMI-1 was such that, in the case of a reactor shutdown coupled with loss of off-site power - a condition that must be postulated pursuant to 10 CFR Part 50, App. A, GDC 17 - the pressurizer heaters (and reactor coolant pumps) would be inoperable. (Id. p. 3-2 - 3-3).

43. If the ability to maintain pressure control with the pressurizer heaters is lost, the only way to maintain reactor coolant system pressure is by adding water to the system. This can only be done by operation of the high pressure injection ("HPI") pumps, which constitutes in effect, a challenge to the emergency core cooling system. (Tr. 8184, Pollard.)

44. The NRC's Task Force on the TMI-2 accident concluded that one of the significant lessons learned from the accident is that the maintenance of natural circulation capability is important to safety:

Maintenance of safe plant conditions, including the ability to initiate and maintain natural circulation, depends on the maintenance of pressure control in the reactor coolant system. Pressure control is normally achieved through the use of pressurizer heaters. Experience at TMI-2 has indicated that the maintenance of natural circulation capability is important to safety, including the need to maintain satisfactory natural circulation during an extended loss of offsite power.

(NUREG-0578, at A-2, Emphasis added; Pollard, ff. Tr. 8182 at 3-4).

45. The Lessons Learned Task Force further found that changes to plant design were needed "to increase the availability of the reactor pressurizer for pressure control in the event of loss of offsite power, thus decreasing the frequency of challenges to [the] emergency core cooling system." (NUREG-0578 at 6; Pollard, ff. Tr. 8182 at 3-4 - 3-5.)

46. Thus, the purposes of the plant modifications proposed by the Lessons Learned Task Force are, while interrelated, twofold in focus: 1) to improve the availability of the

pressurizer heaters to control pressure in order to maintain the capability of natural circulation, and 2) to decrease challenges to ECCS. UCS testimony is that both functions are important to safety. (Pollard, ff. Tr. 8182, at 3-4 - 3-5, 3-7, 3-14; Tr. 8706-7)

47. The modifications proposed by the staff and adopted by Order Item 8 call only for modifying the pressurizer heaters to provide the capability of manually connecting some heater banks to the onsite emergency diesel generators. (Pollard, ff. Tr. 8182 at 3-3.) UCS's testimony was that this modification is insufficient to assure the availability of pressurizer heaters when needed, does not achieve the objective of the lesson learned from TMI-2 (Id. at 3-5 - 3-15) and, because the heaters and their instrumentation and controls are not safety grade, poses an additional hazard to public health and safety by potentially endangering the integrity of the plant's emergency power supply. (This latter issue is covered by UCS Contention 4.) If the heaters and their associated instruments and controls were classified as components important to safety and required to meet the applicable General Design Criteria governing diversity (GDC 22), seismic and environmental qualification (GDC 254), automatic initiation (GDC 20), separation and independence (GDC 3 and 22), quality assurance

(GDC 1), on-site power (GDC 17) and the single failure criterion, this would assure their availability, decrease challenges to ECCS and preclude endangerment to the emergency power supply for plant safety systems. (Id.)

48. UCS's testimony was that providing a manual connection between some pressurizer heater banks and the diesel generators is insufficient either to assure the availability of the heaters when needed or to decrease challenges to ECCS. The NRC has developed the requirements contained in 10 CFR Part 50, Appendix A - the General Design Criteria - as essentially the definition of the minimum design, fabrication, construction, testing and performance criteria necessary to assure that a structure, system or component can be relied upon to protect the public. In assessing the adequacy of a plant design, only those systems that meet the GDC can be assumed to function. (Id. at 3-5 - 3-6.)

49. In this case, while certain heaters may be connected to on-site power, failure to meet the other GDC means that, for example, no independence between heater groups has been provided and the heaters must be assumed to be nonfunctional following a safe shutdown earthquake, a steamline break or a loss of coolant accident. (Id. at 3-8 - 3-9) Nor are the heaters or their circuits single

failure-proof. Thus they cannot be considered to be highly reliable.

50. UCS gave examples of the anomalies resulting from the staff and licensee positions. The first concerns the fact that the heaters will not be seismically qualified. The occurrence of a safe shutdown earthquake could - and would, in the opinion of UCS - result in a loss of offsite power. (Id. at 3-9, 3-11). Assuring the availability of the pressurizer heaters to maintain natural circulation during an extended loss of offsite power is the stated purpose of the proposed modification to the heaters. (Id. at 3-4 - 3-5) Yet, for a seismic event likely to cause loss of offsite power, the heaters must be assumed to be inoperable because they are not seismically qualified. (Id. at 3-9 - 3-11)

51. UCS's position is supported by Regulatory Guide 1.139, "Guidance for Residual Heat Removal" which notes that, based upon the findings of the Reactor Safety Study that equipment failures leading to the inability to remove decay heat result in a higher probability of core melt than that predicted for large LOCA's, "a significant safety benefit will be gained by upgrading those systems and equipment needed to maintain the [reactor coolant system] at the hot standby condition for extended

periods or those needed to cool and depressurize the [reactor coolant system] so that the [residual heat removal] system can be operated." (Id. at 3-10).

52. Regulatory Guide 1.139 goes on to state that it is "obvious that the ability to transfer heat from the reactor to the environment after a shutdown is an important safety function..." (Id., emphasis added) Finally, the guide states that the accident conditions in which it is essential to remove decay heat "can conceivably include a safe shutdown earthquake (SSE) and an extended loss of offsite power that may have resulted from that SSE."

(Id.) Thus, the Regulatory Guide lends strong support to the proposition that the ability to remove decay heat and depressurize the reactor are important to safety (and therefore need to be accomplished with safety-grade equipment) and that such equipment must be seismically qualified.

53. Another logical anomaly resulting from the Staff and Licensee position is that the heaters and their instruments and controls are not qualified to operate in the environment following a small loss-of-coolant accident, the very sequence involved in the TMI-2 accident. (Id. at 3-11)

54. Nor does the testimony demonstrate that providing a connection between some heater banks and the on-site

power supply contribute significantly to meeting the staff's stated goal of reducing challenges to ECCS. As noted above, there are many events for which the heaters must be assumed to be inoperable.

55. When the heaters are lost, a challenge to the HPI system results. (Tr. 8184, Pollard)

56. There is no dispute among the parties that natural circulation is the "preferred" and "normal" mode of removing decay heat and that use of the pressurizer heaters is the "normal" method of pressure control during natural circulation. (Brazill in Keaton et al., ff. Tr. 7558 at 16, 17; Tr. 8031, Keaten.) The Licensee's position, however, is that the ability to maintain natural circulation is not "essential" to core cooling because core cooling can be accomplished by bleed and feed using the HPI system. (Id. at 16). Moreover, the Licensee states that natural circulation can be accomplished without the pressurizer heaters by maintaining pressure with the makeup or HPI system while the reactor coolant system is solid. (Id. at 14). Both the makeup and HPI system use the HPI pumps so both involve a challenge to ECCS. (Tr. 8184, Pollard) Licensee

concludes that operation of the pressurizer heaters and associated controls is not "essential to safety." (Brazill, in Keaton et al., ff. Tr. 7558 at 17.)

57. As we concluded above in connection with UCS contentions 1 & 2, bleed and feed is not a satisfactory substitute for a safety-grade mode of core cooling. No analysis has been made to support a determination that it meets such criteria as fire protection (GDC 3), independence (GDC 22) or the single failure criteria, either alone or in combination with use of the other plant systems. It is clear that neither system alone is safety-grade. (Id. at 3-13.) The Staff has not relied on bleed and feed nor analyzed it in detail. The Staff has seen no analysis of how the primary system could be depressurized in bleed and feed. (Tr. 4984-5, Jensen) No demonstrations proving the effectiveness of bleed and feed alone to cool the core have been made. (supra., paras. 30 - 32)) Nor can the plant be brought to cold shutdown with the bleed and feed mode using only safety-grade equipment. (supra., para. 33)

58. Nor are the alternative modes for maintaining natural circulation satisfactory substitutes for use of the pressurizer to control pressure. Both require operating the reactor coolant system in the solid mode, one controlling pressure by adding water to the system

with the makeup pump and the other with the HPI pumps. The latter is functionally the same as bleed and feed except that the equipment is used for pressure control rather than core cooling per se. (Brazill in Keaten et al., ff. Tr. 7538 at 14).

59. As has been noted above, the HPI and makeup system both use the high pressure injection pumps and while one of the three pumps is normally used for makeup, the plant is permitted to operate with only two HPI pumps operable. (Tr. 8311-8314, Pollard) Therefore, these two alternatives are one in reality. Either involves a challenge to the ECCS, (Tr. 8184, Pollard) the second in all cases and the first in some unknown number of cases. Simply because there is a way to control pressure using ECCS pumps does not mean that that is adequate. One of the principal reasons for upgrading of the pressurizer heaters advanced by the Staff is to reduce the frequency of challenges to ECCS which may go beyond the previously understood and accepted design basis. That in itself is a safety function. (Tr. 8199-8202, 8306, Pollard).

60. Perhaps more importantly, there are serious safety disadvantages associated with attempting to cool the plant in a solid water condition which have been ignored by the

licensee. It is extremely difficult to control reactor coolant system ("RCS") pressure in the solid mode while making any changes whatever to the plant condition.

(Tr. 8183, Pollard) Very small changes in temperature can result in large pressure fluctuations. (Id.; see also Tr. 8060, 8083-5, Brazill.) If the pressure decreases too rapidly, there is a risk of flashing to steam in the RCS, creating bubbles which can interrupt natural circulation. (Id.) If the pressure increases too rapidly, a challenge to the non-safety-grade PORV and/or safety valves can result. At low temperatures there is also a risk of exceeding the pressure/temperature limits on the reactor vessel. This has happened even with plants in a cold shutdown condition. (Id.) UCS's witness knew of no case where a commercial plant has been taken from hot to cold shutdown in a solid water condition throughout. (Tr. 8187, Pollard). None of the other witnesses knew of such an example either. (Tr. 8055-6, Brazill and Keaten; Tr. 8726-7, Jensen). Cooling down in a solid water condition would take the full attention of at least one operator and possibly others to avoid fluctuations in the temperature or inventory of the RCS, to stay within the pressure/temperature limits on the reactor

vessel and to maintain the required subcooling margin. (Tr. 8189, Pollard) We find that these are substantial safety disadvantages which preclude finding that solid water operation is a satisfactory substitute for natural circulation using the pressurizer heaters to control pressure.

61. Moreover, there are other important safety-related advantages of using what the licensee concedes to be the preferred and normal mode of removing decay heat. The operator is fully familiar with this mode and trained in it. (Tr. 8185, Pollard). This supports upgrading the heaters to full safety-grade for precisely the same reason that the staff has required upgrading the emergency feedwater system to full safety-grade, as explained in its letter to all Licensees of October 21, 1980. While the staff recognizes in that letter that alternative ways for removing decay heat may be available, it is requiring emergency feedwater to be fully upgraded because use of the steam generators to remove decay heat is the first choice and therefore "should satisfy the same standards applied to other safety-related systems in the plant." (Tr. 8185-6, Pollard.)

62. Using precisely the same reasoning, we conclude

that the pressurizer heaters are important to safety and should be fully safety-grade. Nor are the pressurizer heaters for TMI-1 essentially safety-grade. For example, they do not meet the single failure criterion, the cables are not separated at all beyond the terminal box and do not meet IEEE Std. 279 or 308, the terminals and connections for the heater circuits are subject to moisture, there is no evidence that the heaters have been tested or that a limiting condition of operation has been placed on the plant requiring operability of the heaters which have been provided with the connection to the diesels, and the connection to the diesels is manual rather than automatic. (Tr. 8192-8, Pollard.) These examples are not exclusive, since neither the staff nor licensee provided an analysis of the measures required to make the heaters safety-grade.

63. A fundamental disagreement existed between UCS and the licensee concerning the meaning of "important to safety" in this context or the showing required to demonstrate that proper functioning of a system or component is "important to safety." The licensee took the position that only those systems and components required

to mitigate a design basis accident are important to safety - the rest are "niceties." (Tr. 7573-4). This is reflected in the licensee's use of the phrase "essential to safety" in discussing the role of pressurizer heaters, rather than "important to safety." That is, since the consequences of failure of pressurizer heaters can be mitigated by use of ECCS, they are not important (or "essential", in licensee's terminology) to safety and need not be safety-grade, irrespective of the fact that the operators are taught to cooldown using pressurizer heaters and are familiar and comfortable with this mode of operation. (Tr. 7573-5). In addition, the licensee simply does not agree with the Lesson's Learned Task Force that the TMI-2 accident demonstrated a need to decrease the number of demands for operation of the emergency core cooling system.* The licensee's witness, Mr. Keaton, did not even agree that ECCS ought to be actuated very rarely (Tr. 7744) and, while first stating that he was

* The full statement from NUREG-0578 at A-2 is as follows:
"The frequency with which the high pressure emergency core cooling system is operated may exceed the previously understood and accepted design basis. Therefore, there is a need to consider the upgrading of those pressurizer heaters and associated controls required to maintain natural circulation at hot standby conditions in order to achieve greater reliability and decrease the number of demands for operation of the emergency core cooling system." Tr. 7743

unaware of any quantitative criteria limiting the frequency of use of ECCS, later agreed that there are design basis limitations on the number of times a vessel may undergo rapid cooling. (Tr. 7743-4) He did not know what that design basis limitation is for TMI-1. (Tr. 7744)

64. We find that the licensee's interpretation is overly restrictive, particularly in light of the lessons to be learned from the TMI-2 accident and the NRC's current position on emergency feedwater systems, discussed above. It is not disputed by UCS that there are ways to remove decay heat from the RCS without use of the pressurizer heaters. (Tr. 8241-3, Pollard.) However, as noted above, these alternatives have serious safety disadvantages - a proposition which the licensee did not refute. We believe that the ability to remove decay heat by maintaining natural circulation in the preferred and normal mode is important to safety and that the pressurizer heaters are required to control pressure in that mode.*

* We also note that the Licensee's witness had not even reviewed the plant procedures or training for TMI-1 to determine the extent to which the operators are instructed to rely upon pressurizer heaters. His testimony dealt solely with system capability. (Tr. 8033-4, Brazill). In light of the crucial part which the operators' actions had in the TMI-2 accident, such a narrow view of the scope of analysis required to demonstrate that safety is assured is unreasonably restricted.

(Tr. 8199, Pollard.)

65. The NRC Staff witness on this subject, the same Mr. Jensen who testified with respect to UCS Contentions 1 and 2, addressed himself only to the question of whether the plant can be cooled down after pressurizer failure.

(Tr. 8724, Jensen) In concluding that the pressurizer heaters are not important to safety, he assumed that everything else in the plant was normal and that no accident conditions such as a small break LOCA existed. (Id.) Thus, he did not consider even the conditions present during the TMI-2 accident.

66. He did agree that the capability of maintaining natural circulation is important to safety and that pressure control is important to achieving the conditions necessary for natural circulation, (Tr. 8727, Jensen), but generally echoed the licensee's position that pressure control for natural circulation can be maintained by use of the HPI system. (Jensen, ff. Tr. 8712 at 5) In view of the witness's testimony that the primary purpose of the staff's required modification of the heaters is to prevent unnecessary actuation of ECCS because the plant is only designed for a limited number of rapid cooldowns (Tr. 8713-4, Jensen), his conclusion that pressure control by use of

the HPI system is perfectly acceptable is questionable.

67. Moreover, we were troubled by answers to one line of questions. Dr. Jordan read the following passage in NUREG-0578: (Tr. 8731)

There is a need to consider the upgrading of those pressurizer heaters and associated controls required to maintain natural circulation at hot standby conditions to a safety-grade classification*.

* To place the quotation in context, we reproduce below the entire paragraph on p. A-2 of NUREG-0578:

Maintenance of safe plant conditions, including the ability to initiate and maintain natural circulation, depends on the maintenance of pressure control in the reactor coolant system. Pressure control is normally achieved through the use of pressurizer heaters. Experience at TMI-2 has indicated that the maintenance of natural circulation capability is important to safety, including the need to maintain satisfactory natural circulation during an extended loss of offsite power. Without the availability of pressurizer heaters, it may be necessary to operate the high-pressure emergency core cooling system to maintain satisfactory natural circulation conditions. The frequency with which the high-pressure emergency core cooling system is operated may exceed the previously understood and accepted design basis. Therefore, there is a need to consider the upgrading of those pressurizer heaters and associated controls required to maintain natural circulation at hot standby conditions to a safety-grade classification in order to achieve greater heater reliability and to decrease the number of demands for operation of the emergency core cooling system. However, the required number of pressurizer heaters required to maintain natural circulation during transition to cold shutdown needs further evaluation, in the longer term. In the short term, designs should be upgraded to provide the operator with the capability to maintain natural circulation at hot standby through the use of pressurizer heaters when offsite power is not available.

68. Dr. Jordan then asked the witness if that consideration was made by the staff and, as a result of the consideration, the staff decided against upgrading the heaters and controls to safety-grade. The witness answered, "Well, I guess that is my testimony." (Tr. 8731, Jensen). On cross-examination, it was later brought out that the witness was saying that his testimony, prepared for the TMI-1 Restart hearings, constituted itself the sole consideration given by the staff to the question specifically cited by NUREG-0578 and raised by UCS's contention: the need to consider upgrading the heaters and controls to safety-grade.

69. We do not find it credible that the brief testimony presented by this witness, who addressed himself solely to the question of pressurizer failure in an otherwise normally functioning plant, who was unfamiliar with the specific sequence of events involved in the TMI-2 accident (Tr. 4952-3, 4954, 4963, 4965-4968) , who did not participate in the preparation of NUREG-0578 (Tr. 4918, Jensen) and whose experience is almost entirely in the area of computer modelling, constitutes a thorough or serious consideration commensurate with the importance of the question reserved by the Lessons Learned Task

Force.

70. In sum, the Staff presented no persuasive reasoning beyond that presented by the licensee.

71. Based upon the foregoing, we find that the short 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 insofar as they do not require upgrading of pressurizer heaters and associated controls to fully safety-grade. Such upgrading is necessary to provide reasonable assurance that TMI-1 can be safely operated.

UCS Contention No. 4

Rather than classifying the pressurizer heaters as safety-grade, the staff has proposed simply to add the pressurizer heaters to the on-site emergency power supplies. It has not been demonstrated that this will not degrade the capacity, capability and reliability of these power supplies in violation of GDC 17. Such a demonstration is required to assure protection of public health and safety.

72. Testimony on this contention was presented by UCS (Pollard, ff. Tr. 9607), the Licensee (Torcivia and Shipper, ff. Tr. 9098), and the Staff (Fitzpatrick, ff. Tr. 9700).

73. In accordance with the Commission's August 9, 1979, Order and Notice of Hearing, Item 8, the Licensee was required to design TMI-1 to provide the capability to supply electrical power from the onsite emergency power source to a predetermined number of pressurizer heaters and associated controls necessary to establish and maintain natural circulation at hot standby conditions. (Staff, Ex. 1, at C8-3) The objective of this modification has

been discussed above in connection with UCS Contention No. 3, above.

74. In mandating this connection of a substantial non-safety grade load (126 KW in this case) to emergency power supplies, the Lessons Learned Task Force recognized that the modification must not result in endangering the safety-grade emergency power supplies which provide on-site power for the plant's engineered safety features:

Careful attention should be given to assure that the capacity, capability and reliability of the emergency power source (diesel generators) is not degraded as a result of implementing the capability to supply selected pressurizer heaters from either the offsite power source or the emergency power source when offsite power is not available.

(NUREG-0578, p. A-3, Tr. 9549)

75. In order to ensure that the emergency power supplies are protected against the effects of a fault in the non-safety-grade pressurizer heater circuits, the pressurizer heater motive and control power interfaces with the emergency buses is required to be accomplished through devices that have been qualified in accordance with safety grade requirements. (Staff Ex. 1, at C8-3)

76. This latter requirement was clarified as follows:
"The Class IE interfaces for main power and control power are to be protected by safety-grade circuit breakers.

(See also Reg. Guide 1.75.)" (Staff Ex. 1, at C8-6; see also NUREG-0737, at 3-86)

77. Therefore, the design of TMI-1 is required to meet the provisions of Regulatory Guide 1.75. (Pollard, ff. Tr. 9607, at 4-8; Tr. 9641-9645, Pollard; Tr. 9337-9339, Torcivia)

78. At TMI-1, a 480 volt circuit breaker is used as the isolation device between the Class IE and non-Class IE portions of the circuits. The terms "Class IE" and "non-Class IE" are equivalent to "safety grade" and "non-safety grade." (Pollard, ff. Tr. 9607, at 4-5; UCS Ex. 30, at 2.1-6, Am. 18; Tr. 9118, Torcivia)

79. Regulatory Guide 1.75 specifies that interrupting devices actuated only by fault current are not considered to be acceptable isolation devices. (UCS Ex. 29, at 1.75-2)

80. In the "Basis" for this Regulatory Position, Regulatory Guide 1.75 considers and rejects the protection of Class IE circuits from faults in the non-Class IE circuits using breaker or fuse coordination because the main breakers are in series with the fault and could experience momentary currents above their setpoints. (Id.) Thus, the fault could affect the entire circuit at the same time.

81. Therefore, circuit breakers are only acceptable as isolation devices if they are tripped open by a signal other than one derived from the fault current or its effects. With such a design, the downstream non-safety circuits would already be isolated from their safety grade power source and a subsequent fault in the non-safety circuits could pose no threat to the safety grade power source. (Pollard, ff. 9607, at 4-7; Tr. 9615-9618, Pollard; UCS Ex. 1, at 1.75-2)

32. The technical basis for the unacceptability of coordinated isolation devices actuated by the fault current or its effects can be briefly explained. As noted above, the effects of a fault can be felt on the entire circuit at once. In the past, coordinated breakers have failed to work as intended to protect emergency power supplies. The accuracy and reliability of devices which operate on fault current are not high, either with respect to the reliability of the device to trip at the intended set point or to operate in conformance with designed time delays. (Tr. 9652, Pollard) It should also be noted that there are no plans to test this arrangement by loading the diesel generators and then simulating a fault in the pressurizer heater circuits by imposing a

bolted line-to-line fault. (Tr. 9653, Pollard)

83. At TMI-1, the main feeder circuit breakers used as the isolation devices between the non-safety grade pressurizer-heaters and the safety-related buses can be tripped open by an automatic safety features actuation signal, low bus voltage, overcurrent trip elements and manually. (Torcivia and Shipper, ff. Tr. 9098, at 4, 5 and Figure 1.)

34. None of these methods of opening the main feeder circuit breaker satisfied the requirements of Regulatory Guide 1.75.

85. The overcurrent trip is specifically rejected by Regulatory Guide 1.75. (UCS Ex. 29, at 1.75-2)

36. The low voltage trip depends upon an effect of the fault current. (Pollard, ff. Tr. 9607, at 4-6; Tr. 9422-9424, Torcivia; document ff. Tr. 9424). Thus, the low voltage trip is specifically rejected by Regulatory Guide 1.75 since the reduced voltage is caused by the fault current. (UCS Ex. 29, at 1.75-2)

37. The Staff attempted to argue that the low voltage condition was a result of the fault and not a result of the fault current and therefore not precluded by Regulatory Guide 1.75. (Tr. 9704-9709, 9725-9731, Fitzpatrick)
We find that line of argument to be without merit. At

best, it is a semantic argument that ignores the objectives of the Regulatory Guide provisions to prevent the upstream safety grade circuits from experiencing the fault current even momentarily. Thus, it is irrelevant whether the trip device senses the fault or the fault current (or an effect of the fault current).

88. An accident signal, such as the automatic safety features actuation signal, is given as an example of an acceptable trip signal in Regulatory Guide 1.75. (UCS Ex. 29, at 1.75-2) The Licensee claimed that using this signal to trip the main feeder breaker made the circuit breaker an isolation device that meets the requirements of Regulatory Guide 1.75. (Tr. 9344, Shipper)

89. However, that signal does not make the main feeder breaker an acceptable isolation device in this instance because it is incapable of protecting the safety grade power supply against a pressurizer heater fault. (Pollard, ff. Tr. 9607, at 4-7)

90. To explain why the ES signal is not acceptable under these circumstances, we recall that the requirement to provide an onsite power supply for pressurizer heaters was for the purpose of maintaining natural circulation capability during a loss of offsite power event without

use of the emergency core cooling system. (NUREG-0578, at A-2)

91. During a loss of offsite power without a LOCA, an automatic safety features actuation signal will not be generated. (Tr. 9615-9616, Pollard)

92. Therefore, following connection of the pressurizer heaters to the onsite power supply, the signal will not trip the main feeder breaker in the event of a heater fault. (Id.)

93. Furthermore, even if an automatic safety features actuation signal were generated, that signal would be bypassed at the time the heaters were connected to the onsite power supply. Thus, when the heaters are connected to the emergency power supply, there is no ES signal available to isolate a fault in the heaters from endangering the emergency power supply. (Tr. 9617, Pollard)

94. Therefore, although the provision of the safety feature actuation signal to trip the main feeder breaker is required to prevent the pressurizer heaters from becoming part of the diesel generator loading sequence, (Staff Ex. 1, at C8-6) it does not make the main feeder breaker an acceptable isolation device within the provisions of Regulatory Guide

1.75 because the signal would either not be present or would be bypassed during the time the heaters are connected to the safety grade onsite power supply.

95. No party argued that the provision of a means to manually trip the pressurizer heater circuit breakers satisfied the requirements of Regulatory Guide 1.75.

96. The pressurizer heater circuits also contain distribution circuit breakers downstream of the main feeder breakers. These distribution breakers are equipped with thermal magnetic overload trip elements to open the breaker if a fault exists in the pressurizer heater. (Torcivia and Shipper, ff. Tr. 9098, at 5)

97. However, this trip depends on sensing the fault current (Tr. 9103, Torcivia) and is therefore also specifically rejected by the provisions of Regulatory Guide 1.75 (UCS Ex. 29, at 1.75-2) In addition, the Licensee takes no credit for the distribution breakers because of their location in an area of the plant that is not seismically qualified. (Tr. 9112, 9120, Torcivia)

98. We conclude that the design of TMI-1 does not provide safety grade interfaces between the pressurizer heaters and the emergency power supplies because the main feeder breakers do not meet the provisions of Regulatory Guide

1.75 pertaining to isolation devices.

99. The Licensee acknowledges that a fault in the non-safety grade pressurizer heater circuits could result in loss of the safety grade power supply bus to which the heaters are connected. (Pollard, ff. Tr. 9607, at 4-7 to 4-8; UCS Ex. 30, at 2.1-76 Am. 18; Tr. 9119-9120, Torcivia)

100. Amendment 18 to the Restart Report contained the following statements:

The undervoltage relays will initiate tripping of the 480-volt ES circuit breaker feed to the pressurizer heaters and thereby remove any endangerment caused by that circuit.

(Emphasis added)

Taking into account the single failure criterion*, faults on the BOP system will at most cause the loss of one 480-volt ES system.

(Emphasis added)

(Tr. 9623-5; UCS Ex. 30)

101. These statements were later replaced by Amendment 22 to the Restart Report by the following sentences:

The design prevents a malfunction fault on the pressurizer heaters from causing unacceptable influences on the ES system.

(Emphasis added)

The design prevents a malfunction fault on the pressurizer heaters from causing unacceptable influences on the ES system as described above.

(Emphasis added)

(Id.)

* As will be discussed below, we also conclude that represents an incorrect interpretation of the single failure criterion.

102. Although the effect of these changes is to obscure the fact, it is clear that a fault in the pressurizer heater circuits can cause the loss of one 480-volt ES power supply.

103. The Staff also evidenced concern that the isolation between the non-safety grade heater circuits and the safety grade power supply is not adequate.

104. The Staff mandated the requirement that only one heater bank may be connected at any given time to an emergency power supply. (Staff, Ex. 1, at C8-8)

105. The concern expressed by the Staff was that, if two heaters were simultaneously connected to the two redundant onsite emergency power supplies, the required independence of the two power supplies could not be assured because of inadequate electrical separation within the pressurizer heater circuits. (Staff, Ex. 1, at C8-7) The result could be the loss of both bus IP and bus IS, the two redundant emergency power supplies.
(Tr. 9819, Fitzpatrick)

106. It is apparent that, if the proposed isolation devices could be relied upon to protect the emergency power supply, there would be no concern about or need to prohibit the energizing of both heater groups simul-

taneously. (Pollard, ff. Tr. 9607 at 4-8 - 4-9; Tr. 9622-9625, Pollard). The staff's concern arises from the fact that at some points there is no physical separation whatever between the cables for the non-safety grade pressurized groups. (Tr. 9816-7, Fitzpatrick). Thus, a failure could clearly affect both heater groups. But, it is obvious that even such a failure affecting both heater groups could not threaten the emergency power supply if the isolation device between the heaters and the ES power supplies were effective.*

107. The Staff testified that its actions in precluding the simultaneous connection of both heater groups were "prudent", although not required. Putting aside for the moment the question of the applicability of the provisions of Regulatory Guide 1.75, the inference is clear that even the staff is unwilling to place its reliance on these isolation devices to protect the emergency power supplies.

* Following this reasoning, IEEE Std. 384-1974 does not require physical separation between non-safety-grade circuits so long as the non-safety-grade circuits are separated from the safety-grade power supplies by acceptable isolation devices. (Tr. 9818, Fitzpatrick)

108. The Staff, in tacit recognition that the TMI-1 design does not provide an acceptable isolation device, argued that the provisions of Regulatory Guide 1.75 do not apply following the transient associated with starting and loading the diesel generator. (Tr. 9701-9703, 9710-9719, 9724, Fitzpatrick)

109. As noted above, during such transients when the pressurizer heaters are connected to the diesels, an ES actuation signal will either not be present (for a loss of offsite power event) or will have been bypassed. Supra, paras. 91-93)

Thus, when the heaters are connected to the emergency power bus, there is no ES signal available to isolate a fault in the heaters from endangering the emergency power supply. The only "isolation devices" available are those which trip when sensing the fault current or its effects.

110. The Staff argued that after the automatic loading of the diesel generator was completed, Regulatory Guide 1.75 ceased to apply and it is therefore acceptable to rely on the coordination of the overcurrent protection devices. The Staff suggested that support for this proposition can be found in the fact that it has traditionally allowed any of the nonsafety loads to be reconnected to

the emergency power supply after the ES loads have been sequenced on. (Tr. 9767-9768, Fitzpatrick)

111. The Staff argued that if the requirements of Regulatory Guide 1.75 were applied after the stabilization period, (defined as the 25 seconds or so requiring for sequenced loading of the diesels,) this would preclude any connection of non-safety loads to the safety buses. (Tr. 9772, Fitzpatrick)

112. That testimony was incorrect because, as both the Licensee and UCS testified, there are isolation devices available that meet the requirements of Regulatory Guide 1.75. (Tr. 9620, Pollard; Tr. 9225-7, Torcivia)

113. Moreover, the witness's definition of "stabilization" - the point at which the diesels are loaded - (Tr. 9710, Fitzpatrick) bears no relationship whatever to the condition of the plant as a whole and the need for the operation of the safety systems powered by the diesels. (Tr. 9712-14, Fitzpatrick). The witness agreed that "one" purpose of requiring isolation between non-safety equipment and emergency power supplies is to ensure the integrity of the power supplies to the engineered safety features. (Tr. 9713, Fitzpatrick) However, his interpretation of the scope of Reg. Guide 1.75 would permit that integrity to be threatened at the very time when the engineered

safety features are needed to protect public health and safety. The Staff provided no technically supportable justification for this result and we reject it.

114. We note in this connection that the record indicates that this is the first time the staff has ever required the provision of a connection between a non-safety component or system and a plant's safety-grade emergency power supplies. (Tr. 9694, Pollard)

Perhaps this explains the apparent inability of the Staff to recognize that the fundamental safety purpose reflected in the provisions of Reg. Guide 1.75 would be thwarted were this design to be accepted.

115. When questioned by Dr. Jordan as to whether circuit breakers are exceedingly reliable devices, so reliable that they can be used as isolation devices, the Staff witness stated that he believed them to be reliable and that the Staff has traditionally put faith in them.

(Tr. 9775-9776, Fitzpatrick) No further reasoning nor evidence of reliability was offered by the Staff.

116. We conclude that the Staff's testimony does not support the argument that Regulatory Guide 1.75 provisions can be disregarded after the stabilization period of the emergency power supply. There remains the need to insure

that the connection of the non-safety grade pressurizer heaters to the emergency power supply does not result in loss of the emergency power supply.

117. We have found above that the requirements of Regulatory Guide 1.75 apply to TMI-1 and that the design does not meet those requirements. This means that the isolation devices (i.e., the main feeder breakers) are not safety grade. Therefore, as explained below, a single failure could result in loss of redundant safety grade emergency power supplies in violation of the requirements of General Design Criterion 17 of Appendix A to 10 CFR Part 50.

118. The single failure criterion requires, in part, that a safety system be capable of performing its safety function in the event of any single failure within that safety system concurrent with all failures of non-safety grade components whose failure adversely affects the system. (Pollard, ff. Tr. 9607, at 4-2 to 4-3)

119. Applying this requirement to the TMI-1 design, an electrical fault in the pressurizer heaters can and must be assumed because the heaters are non-safety grade components. (Pollard, ff. Tr. 9607, at 4-3) The main feeder breaker can and must be assumed to fail to interrupt the fault before the emergency power supply is lost because

it is a non-safety grade isolation device. (Pollard, ff. Tr. 9607, at 4-3 to 4-4.)

120. The other redundant emergency power supply is assumed failed by the single failure. (Pollard, ff. Tr. 9607 at 4-4) In other words, failure of one diesel generator is the "single failure" in safety-grade equipment.

121. The result is that the onsite power supply is unable to perform its safety function because both redundant divisions have been lost, one as the result of a single failure and the other as a result of a fault in the non-safety grade heaters connected to it without the use of a safety grade isolation device. (Id.)

122. Even if the connection of the pressurizer heaters itself causes the loss of only one 480 volt ES bus, rather than an entire diesel generator, this is equally unacceptable in combination with the postulated single-failure loss of the other diesel generator, since the safety functions being performed by the other equipment powered by that 480 volt ES bus could be critical at the time of failure of the bus. (Tr. 9682-5, Pollard). Neither the Licensee nor the Staff attempted to argue that loss of one diesel generator plus loss of one 480 volt ES bus on the other diesel generator would be acceptable.

123. The Licensee and Staff apparently concluded that the requirements of the single failure criterion were met on the basis that, if only one heater bank is connected to the emergency power supply, a heater failure and the resultant loss of only one emergency power supply will leave the redundant emergency power supply operable. (Pollard, ff. Tr. 9607 at 4-9) This reasoning depends entirely upon the argument that the isolation devices protecting the diesel generators from failures originating in the pressurizer heater circuits are safety grade and thus their failure cannot be assumed. (Tr. 9334-9339, Torcivia and Shipper)

124. That reasoning is incorrect because, as discussed above, the heater fault and isolation device failure must be assumed concurrent with a single failure in the redundant emergency power supply because the heaters and isolation devices are not safety grade components. (Pollard, ff. Tr. 4907, at 4-10)

125. The Licensee agreed that, if the isolation device does not meet the provisions of Regulatory Guide 1.75, it cannot be classified as safety grade for the purpose of performing the failure analysis. (Tr. 9339, Torcivia) As we have found above, the isolation devices do not

meet Reg. Guide 1.75. Thus, they are not safety-grade and their failure must be assumed.

126. Well after litigation of this contention was completed, the Licensee provided for the record a large number of revisions to various emergency procedures. (Tr. 16,569 - 16,572) without drawing the Board's or the parties' attention to any particular changes therein. In their proposed findings, UCS brought to our attention the fact that a change in the pertinent procedure was made to direct the operators not to connect the pressurizer heaters to the emergency power supply if only one diesel generator is available. (Lic. Ex. 50, at 12.0) There was no testimony presented by the Staff or Licensee on the purpose of this change. At first glance, this appears to resolve the question of whether the design meets the single failure criterion. However, we see two problems which preclude such a finding.

127. First, it is obvious from the foregoing discussion and finding that connecting the non-safety grade heaters to the emergency power supply, even if both diesel generators are available, increases the probability of failure of the power supply to which the heaters are connected. Thus, contrary to the lessons learned requirement, the capability, capacity and reliability of the emergency

power supply is degraded by the connection of the pressurizer heaters. It is no solution to specify that such degradation will be permitted only when both emergency power supplies are available.

128. Second, administratively prohibiting the connection of the heaters to the emergency power supply if only one diesel is available is contrary to the intent of the lessons learned requirement. The lessons learned requirement is to provide the capability to supply power from the emergency power supply to the heaters in order to maintain natural circulation capability. (Staff Ex. 1, at C8-3) This was clarified to mean explicitly that redundant capability to provide emergency power to the heaters must be provided. (Staff, Ex. 1, at C8-6) Thus, if one diesel generator fails, there must be provided a redundant capability to power the heaters from the other diesel generator. The Licensee cannot be permitted to violate this aspect of the lessons learned requirement to compensate for a design that does not provide an acceptable isolation device between the heaters and the emergency power supply.

129. Finally, the Licensee argued that, even if a heater fault did result in tripping of the main bus breaker and the consequential loss of power to an ES bus, it would be simple to restore power by operating a switch in the

control room. (Tr. 9107, 9687, Torcivia). This testimony was subsequently changed to indicate that contrary to the witness's original testimony, two switches have to be operated - one locally at the main breaker and one in the control room.* (ff. Tr. 21,099, Torcivia) No testimony was provided on how long this would take.

130. Even if it were a "simple matter" to restore power to the emergency power supply bus, such a design is not acceptable. First, no analysis has been done to determine the length of time the emergency bus may be deenergized and the effect of the safety systems being deenergized for that period of time.

131. The plant safety analysis assumes continuous operation of safety systems - nothing in this record remotely suggests that it is acceptable to interrupt the operation of ECCS, for example, for some unknown period of time. Second, to rely upon the operator to correct the effects of an inadequate design in the manner suggested violates the Commission's longstanding policy of defense-in-depth.

* While the Licensee changed the portions of the transcript where its witness gave incorrect answers on this subject, it never moved to similarly change several other places in the record where counsel for the Licensee asked UCS's witness questions and made statements to the Board premised upon the same incorrect information: Tr. 9648, 9685-6).

132. An applicant may not avoid meeting the requirements which assure the integrity of emergency power on the grounds that, if lost, it can subsequently be restored. This is analogous to arguing that the requirements governing physical separation of circuitry for redundant safety systems can be waived on the grounds that a fire threatening such circuitry could be extinguished. (Tr. 9692-9694, Pollard)

133. During cross-examination of UCS by the Commonwealth, the question arose whether it is ever acceptable to connect any non-safety grade equipment to a safety grade power supply. (Tr. 9677, 9678)

134. UCS testified that there is no general prohibition against connecting any non-safety load to a safety grade bus. (Tr. 9677, Pollard)

135. However, the connection of the pressurizer heaters to the emergency power supply is unique in several respects.

136. This is the first time NRC has required non-safety equipment to be connected to a safety grade power supply. (Tr. 9694, Pollard)

137. Emergency procedures has been developed instructing the operators to search for ways to permit connection of the heaters. (Tr. 9694-9695, Pollard)

138. The pressurizer heaters are a significantly greater load than other non-safety loads which can be powered from

the emergency onsite power supplies. (Tr. 9695, Pollard)
139. Other non-safety loads are connected to the emergency power supplies generally only after a long period of time after the accident begins or after some other malfunction (other than loss of offsite power) occurs. (Id.)

140. In addition, once the non-safety loads are shed (i.e. disconnected) from the safety grade bus, they generally are not reconnected. (Tr. 9696, Pollard)

141. UCS concluded that, given the design proposed for TMI-1, the provision to connect the heaters to the emergency power supply is a detriment to safety. That is, in addition to failing to achieve the objective of reducing challenges to the ECCS, a fault in the pressurizer heaters, by causing the loss of an emergency power supply bus, could result in making some portion of ECCS unavailable. (Tr. 9697, Pollard)

142. We have been called upon in the course of ruling on this contention to consider varying interpretations of the requirements and applicability of Regulatory Guide 1.75. In particular, the NRC Staff argued that the provisions of the Regulatory Guide ceased to apply after the point at which the engineered safety features have been automatically loaded onto the diesel generators. (Tr. 9701-

9703, 9710-9714, 9761 ff. Fitzpatrick) The Licensee argued similarly that the isolation provisions do not apply when the pressurizer heaters are connected to emergency power, after the sequenced loading, when the ES signal is no longer present. (Tr. 9496-7, Shipper) We have found that such a narrow interpretation of Regulatory Guide 1.75 - the only regulatory guidance directed toward protecting emergency power supplies from failures in non-safety-grade equipment - would have the effect of permitting those vital power supplies to be endangered. We cannot believe that such a result was intended.

143. We have also given the appropriate weight to the fact that UCS's witness on this subject was unusually well qualified and experienced in precisely this area, in comparison to the other witnesses. Mr. Pollard was NRC's representative on the IEEE Committee which developed IEEE Std. 384-1974, which is endorsed by Reg. Guide 1.75, and participated in the development of the Reg. Guide. (Pollard, ff. Tr. 9607 at 4-5) By contrast, the Licensee's witnesses were not involved in either effort. (Tr. 9500, Torcivia and Shipper)* In addition, the only previous experience either of the Licensee's witnesses had in designing an

* The Staff's witness was not specifically asked about his participation in either effort and there is no evidence he did participate. (Fitzpatrick, Professional Qualifications, ff. Tr. 9700; Tr. 9786, Fitzpatrick)

isolation device to meet Regulatory Guide 1.75 was Mr. Torcivia's involvement in the Forked River plant, which utilized a high impedance transformer, a device which clearly does meet Reg. Guide 1.75 (Tr. 9620-22, Pollard; Tr. 9225-7, Torcivia) as an isolation device. (Tr. 9497-8, Torcivia and Shipper). Moreover, neither of the Licensee's witnesses knew of any previous cases where an isolation device like the one proposed here has been used to protect the emergency power supply from non-safety-grade loads. (Tr. 9341, Torcivia and Shipper)

144. The record is clear that the are acceptable isolation devices which meet Reg. Guide 1.75 which are available and in use. (Tr. 9225-7, Torcivia; Tr. 9620, Pollard.) The Licensee testified that high impedance transformers were used in the Forked River plant. (Tr. 9497-8, Torcivia) In addition, there are other ways of protecting the emergency power supply and achieving the objective of increasing the availability of the pressurizer heaters for natural circulation. The first, of course, is to upgrade the pressurizer heaters to safety grade. They could then be connected to the emergency power supply like any other safety load without any concern for isolation. This is the option urged by UCS. Another possibility is

to add a small onsite power supply just for the heaters.
(Tr. 9621-2, Pollard)

145. Considering all of the evidence, we conclude that the manner in which the TMI-1 pressurizer heaters are to be connected to the on-site emergency power supply will unacceptably degrade the capacity, capability and reliability of the emergency power supply. When considered in connection with our findings on UCS Contention No. 3, above, it is clear that the appropriate solution is to upgrade the pressurizer heaters and their associated circuitry to the level of safety grade. This will achieve the primary objective of the lesson learned, ensuring the availability of the heaters to control pressure during natural circulation, without risking any loss of the emergency power supply or portions thereof. After upgrading, the heaters can be connected to the emergency power supplies without any requirement whatever for isolation devices. By contrast, the effect of this proposed modification is to degrade the reliability of the emergency power supply while, at the same time, failing to ensure that the non-safety-grade heaters are available when needed. Thus, the salutary objective of the lesson flowing from the TMI-2 accident is not met and the result would appear to be an overall detriment to plant safety. (Tr. 9680-9684, Pollard)

146. Even if we had not concluded that the pressurizer heaters are important to safety pursuant to UCS Contention No. 3, we would still find this modification unacceptable because of the risk it poses to the integrity of the emergency power supply. In that case, we would have required the isolation devices between the non-safety grade pressurizer heaters and the emergency power supply to meet the requirements of Regulatory Guide 1.75 as we have interpreted those requirements.

147. Based upon the foregoing we find that the short 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 the proposed provision of a connection between the non-safety grade pressurizer heaters and the emergency power supply will unacceptably degrade the capacity, capability and reliability of the emergency power supply.

UCS Contention No. 5

Proper operation of power operated relief valves, associated block valves and the instruments and controls for these valves is essential to mitigate the consequences of accidents. In addition, their failure can cause or aggravate a LOCA. Therefore, these valves must be classified as components important to safety and required to meet all safety-grade design criteria.

148. Testimony on this contention was given by UCS (Pollard, ff. Tr. 9027), the Licensee (Correa, et al., ff. Tr. 8746), and the Staff (Jensen, ff. Tr. 8821).

149. As a result of the TMI-2 accident, the Commission ordered certain improvements or upgrading of the pilot operated relief valve (PORV), the block valve and the instrumentation and controls for these valves. UCS concludes that, considering the lessons learned from the TMI-2 accident, the Commission's requirements are necessary, but not sufficient to provide adequate protection for the public. (Pollard, ff. Tr. 9027, at 5-1).

150. Briefly, the requirements incorporated in the Commission's August 9, 1979, Order are as follows:

- (1) The motive and control components of the PORV and the PORV block valve shall be capable of

being supplied from either offsite power or the emergency power source when offsite power is not available. (Staff Ex. 1, at C8-8; NUREG-0578, at A-5);

(2) The PORV and associated control circuitry shall be tested to demonstrate its qualification to operate under expected operating conditions for design basis transients and accidents. (Staff Ex. 1, at C8-10; NUREG-0578, at A-8); and

(3) The PORV shall be provided with a positive indication in the control room derived from a reliable valve position detection device or a reliable indication of flow in the discharge pipe. (Staff Ex. 1, at C8-11; NUREG-0578, at A-10)

151. The purposes or objectives of these requirements are as follows:

(1) To reduce the frequency of challenges to emergency core cooling components and systems, NUREG-0578, at 6, A-3 to A-4);

(2) To limit the lifting frequency of the safety valves, (NUREG-0578, at A-3); and

(3) To aid the operator in diagnosing a failure and in taking corrective action. (NUREG-0578, at A-10)

152. It should be emphasized that the above requirements were portrayed as the first steps toward improving the reliability of the PORV and block valve pending a longer term decision on whether the PORV and the block valve should be designated as equipment important to safety and required to meet all safety grade design criteria, whether reliability criteria for valves in the primary coolant boundary are needed and whether the man-machine interface in the control room needs significant improvement. (NUREG-0578, at 6, 7, and A-3 to A-4)

153. USC argued that the PORV, block valve and associated controls have at least six specific safety-related functions and, therefore, this equipment should be classified as important to safety and required to meet all applicable safety grade criteria. (Pollard, ff. Tr. 9027, at 5-18)

154. The PORV is electrically controlled and, therefore, the pressure at which the PORV is signalled to open can be easily adjusted. During normal plant operation, the TMI-1 PORV is set to open at a reactor coolant system pressure of 2450 psig. In addition to this automatic mode of operation, the reactor operator can command the PORV to open at any pressure by manually controlling the electrical signal to it. (Pollard, ff. Tr. 9027, at 5-2 to 5-3)

155. In contrast, the safety valves were operated directly by reactor coolant system pressure. The reactor operator cannot control the safety valves at all and their opening pressure set point cannot be changed during plant operation. The safety valves are set to open at 2500 psig. (Pollard, ff. Tr. 9027, at 5-3)

156. The PORV has associated with it a block valve which is located between the PORV and the pressurizer. The block valve is manually controlled by the reactor operator. The operator can close the block valve to stop the flow of primary coolant through the PORV or prevent the PORV from opening. (Pollard, ff. Tr. 9027, at 5-3 to 5-4)

157. The safety valves have no block valves associated with them and, therefore, the reactor operator cannot terminate a loss of coolant through a safety valve if it fails to reclose. (Id. at 5-4)

158. It is important to place this contention in context by recalling the relevant lessons learned from the TMI-2 accident. Section 2 and the corresponding section of Appendix A of NUREG-0578, TMI-2 lessons learned Task Force Status Report and Short-Term Recommendations, July, 1979* contain the short-term

* NUREG-0578 was not formally introduced into evidence by any of the parties although it was referred to frequently throughout the testimony. Since this document formed the basis of the requirements adopted by the Commission in its Order of August 9, 1979, the record would be incomplete without including it in full. Therefore, the Board adopts NUREG-0578 as Board Exhibit 7.

requirements recommended by the NRC staff lessons learned Task Force and adopted by the Commission's Order of August 9, 1979, concerning the pressurizer PORV, block valve and safety valves.

159. The language which we will quote below makes it clear that the role of the non-safety-grade PORV during the TMI-2 accident - in both contributing to the accident and being called upon during recovery from the accident - raised three fundamental interrelated safety concerns:

- 1) Because a stuck-open PORV can result in challenging ECCS, it raises the question of whether the frequency with which safety systems are called upon to function for reactor coolant system pressure or volume control may exceed their generally understood and previously accepted design basis.

- 2) Because the PORV (and other equipment) previously classified as non-safety-related contributed to the accident and were used in its recovery, the question raised is the need to expand the applicability of existing reliability criteria to include such equipment.

- 3) Because a failed-open PORV results in a direct violation of the integrity of the reactor coolant system pressure boundary; an obvious question is raised concerning conformance with GDC 14, 15 and 30,

requiring an "extremely low probability" of abnormal leakage, rapidly propagating failure and gross rupture.

160. Sections of the pertinent language of NUREG -0578 follow :

2.1.1 Emergency Power Supply Requirements for the Pressurizer Heaters, Power-Operated Relief and Block Valves, and Pressurizer Level Indicators in PWRs.

A general lesson learned from our review of the TMI-2 accident is that the frequency with which some safety systems, such as the high-pressure safety injection system (part of the Emergency Core Cooling System provided pursuant to General Design Criterion 35 of 10 CFR Part 50, Appendix A), are called upon to function for reactor coolant system pressure or volume control may exceed their generally understood and previously accepted design basis. Other actions pursuant to the Bulletins and Orders applied to B&W reactors have been aimed at increasing the overall performance reliability of the plants for feedwater transients. This, in turn, decreases the reliance on high-pressure safety injection. Work is also under way in this area by the B&W Task Force in its review of Westinghouse and Combustion Engineering reactors. Over the long term, additional work is likely to be required

in a general review of the frequency of challenges to safety systems based on past operating experience, possibly in the development of acceptable numerical criteria for past and future designs:

For the short term, the Lessons Learned Task Force recommends that the specific changes described below be made in current PWR designs to increase the availability of the reactor pressurizer for pressure control in the event of loss of offsite power, thus decreasing the frequency of challenges to emergency core cooling systems. In some designs, loss of pressurizer heaters due to a loss of offsite power requires the use of the high-pressure emergency core cooling system to maintain reactor pressure and volume control for natural circulation cooling. Similarly, in some designs the inability to close the power-operated relief valve upon loss of offsite power could result in additional challenges to the high-pressure emergency core cooling system. Finally, proper functioning of the pressurizer level instrumentation is necessary to maintain satisfactory pressure control for natural circulation cooling using the pressurizer heaters.

A generic question raised by TMI-2 is the need to expand the applicability of existing reliability criteria to equipment not previously included in the licensing interpretation of equipment designated as "important to safety."

The existing criteria for safety equipment include the single-failure criterion, diversity criteria, and other so-called "safety grade" design criteria, such as seismic and environmental qualifications. Pending longer term decisions on the need for new safety classifications for such equipment, we recommend that the emergency power supply changes described below be a first required step in that direction. (NUREG-0578, Bd. Ex. F at 6-7, emphasis added)

* * *

2.1.2 Performance Testing for BWR and PWR Relief and Safety Valves

The TMI-2 accident sequence included a failure of a power-operated relief valve to close. This and other operating experience raise a significant question about the performance qualification of two types of valves in the primary coolant boundary; safety and relief valves. The Task Force recommends that programs be promptly initiated and completed prior to July 1981 to establish the functional performance capabilities of PWR and BWR safety and relief valves for normal, transient, and accident conditions. The Task Force is continuing to consider whether there is a need to provide reliability criteria for these and other valves in the primary coolant boundary in implementation of General Design Criterion 14.

(Id. at 7, emphasis added)

* * *

Power Supply for Pressurizer Relief and Block Valves

The purpose of the power-operated relief valve (PORV) is to limit the lifting frequency of the ASME Code safety valves by relieving at a lower set point. The PORV is also used to prevent overpressurization of the reactor coolant system during operation at low temperatures, an operational mode when the nil ductility transition temperature (NDTT) becomes a consideration for structural integrity of the primary coolant pressure boundary.

* * *

The relatively high frequency of AOOs places a reliability demand on the operation of the PORVs and associated equipment that is higher than originally envisioned. Also, the operation of some components and systems provided for emergency core cooling have been challenged more times than was previously expected as a result of AOOs. Therefore, there is a need to consider the upgrading of the PORVs, block valves, and the associated control and power equipment to a safety-grade classification to achieve greater valve reliability and to minimize the number of challenges to the operation of the emergency core cooling components and systems. However, the merits and degree of upgrading of all pressure-relief equipment associated with the pressurizer requires further evaluation, which should be accomplished on a longer term basis. In the short

term, the design should be upgraded to provide the operator with the capability to control the operation of the PORVs and associated block valves when offsite power is not available. This capability is essential to mitigate the consequences of transients caused by or resulting from the loss of offsite power.

In addition to the PORVs and associated block valves, there are other valves whose failure to open or close under certain conditions may affect the integrity of the reactor coolant pressure boundary. These valves, as well as the associated control and power equipment, should be evaluated by the NRC staff on a long-term basis to determine whether they should be upgraded to safety-grade classifications or become the subject of specific numerical reliability criteria.

(Id. at A-3 - A-4, emphasis supplied)

* * *

TITLE: Performance Testing for BWR and PWR Relief and Safety Valves (Section 2.1.2)

1. INTRODUCTION

General Design Criteria 14, 15, and 30 of Appendix A to 10 CFR 50 require that the reactor coolant pressure boundary be designed, fabricated, and erected to the highest quality standards and be tested to ensure an extremely low probability of abnormal leakage, rapidly propagating

failure, and gross rupture. These criteria also require that the design conditions of the reactor coolant boundary not be exceeded during any condition of normal operation, including anticipated operational occurrences.

Proper operation of reactor coolant system relief and safety valves is vital for conformance to these design criteria. The inability of a sufficient number of these valves to open could lead to a violation of the integrity of the reactor coolant system pressure boundary. The failure of one or more of these valves to close results in a direct violation of the reactor coolant system pressure boundary integrity.

(Id. at A-6, emphasis added)

* * *

Solid-water or two-phase flow through the relief and safety valves can greatly increase the dynamic forces on valve internals, piping, and supports over those that would be expected from saturated steam flow conditions. Present ASME qualification requirements for safety valves include only flow under saturated steam conditions. Because the safety analyses have not given credit for the pressure-relief capability of the power-operated relief valves, the ASME Code also does not address qualification requirements for these valves.

To date, there have been a number of instances of improper operation of relief and safety valves. These examples include valves opening below set pressure, valves opening above set pressure or failure to open, and valves failing to reseat when open. The failure of the power-operated relief valve to reseat was a significant contributor to the TMI-2 sequence of events.

It is not clear whether these past instances of improper operation resulted from inadequate qualification of the valve or from a basic unreliability of the valve design.

(Id. at A-7, emphasis added)

* * *

TITLE: Direct Indication of Power-Operated Relief Valve and Safety Valve Position for PWRs and BWRs Section 2.1.3.2)

I. INTRODUCTION

General Design Criterion 14 of Appendix A to 10 CFR 50 requires that the reactor coolant pressure pressure boundary be designed, fabricated, erected, and tested to have an extremely low probability of abnormal leakage, rapidly propagating failure, and gross rupture. Although the application of this criterion has emphasized the integrity of passive components in the reactor coolant

system, such as the reactor vessel and the piping, this criterion should also apply to the valves that provide isolation for the system. Failure of relief and safety valves to close has been the cause of events that result in small break LOCAs. Unambiguous indication of the position of the valves can aid the operator to detect a failure and take proper corrective action.

(Id. at A-9, emphasis added)

161. Additional conclusions concerning the reliability of the PORV (and safety valves) and their relationship to plant safety were made by the staff as a result of the generic evaluation of small break LOCA accident behavior in B&W plants, NUREG-0565. (Bd. Ex. 4)* A review of available B&W operating data** disclosed 10 instances of failure of a PORV to close in 31 reactor years and 162 challenges. Six of the PORV failures were prior to initial operation. (Bd. Ex. 4 at 3-1 3-3) These statistics translated into a probability of 0.3 events per B&W reactor year for a LOCA caused by PORV failure and a probability of 0.13 per B&W reactor year of a LOCA from PORV failure after plant startup. (Id.)

162. The staff concluded on the basis of these statistics

* The findings of NUREG-0565 and their significance were addressed in UCS's direct testimony (Pollard, ff. Tr. 9027 at 5-6) and at Tr. 9066, 9076-7, 9079-80, Pollard)

** This data did not include all PORV openings, since records are only kept of those occurring during a transient involving a reactor trip. (Bd. Ex. 4 at 3-3). In addition, no information has been provided on the number of inadvertent PORV openings due to control failures, although there have been some. (Tr. 9066, 9077-8, Pollard.)

that the probability of a small break LOCA caused by valve failure in a B&W plant was "considerably higher" than the probability of a small break LOCA caused by pipe rupture. (Id., at 3-3)

163. These statistics, of course, predate the post-TMI-2 modifications which required inverting the set point of the PORV and the reactor trip and adding additional reactor trip signals. The staff expressed its belief that these changes have reduced the frequency of PORV challenges (Id. at 3-6) and experience since the accident bears this out. We note, however, that these modifications do nothing to reduce the rate of inadvertent PORV openings from control system failures or the rate at which PORV's, once opened for any reason, will fail to reclose.

16' The staff found that it was not possible to make a quantitative judgment of the expected frequency of future PORV actuations and therefore called for additional analyses directed toward answering this question. (Id. at 3-6) This was endorsed by the Commission in NUREG-0737 and translated into the requirements contained in Items II. K.2.14 (Lift Frequency of PORV and Safety Valves) and II.K.3.7 (Evaluation of Power Operated Relief Valve Open Probability During Overpressure Transient) (Staff Ex. 12, at II.K.2.14-1 ff.) In brief, the Licensee is required to demonstrate that the PORV will lift in less than 5% of overpressure transients. This demonstration has not yet been made, although

it is a requisite to restart. (Id. at II.K.2.14-3, Tr. 21,325, Jacobs) Nor was any evidence introduced in this hearing that the frequency of PORV actuation is less than 5% of overpressure transients.

165. Finally, while acknowledging that the frequency of PORV actuations has been reduced, the staff in NUREG-0565 found that it should be reduced still further by the installation of a system to automatically isolate the PORV by closing the PORV block valve after RCS pressure has decreased. (Bd. Ex. 4 at 3-7) This was adopted in modified form by the Commission; automatic PORV isolation need be implemented if the analyses required by Item II.K.2.14 and II.K.3.7, discussed above, show that it is necessary. Because the staff "do[es] not find the licensee's analysis under Item II.K.3.2 acceptable," (Staff Ex. 12 at II.K.3.1-2) it has not been able to determine whether automatic PORV isolation is required for TMI-1.

166. Against this backdrop, we consider the positions of the parties.

167. UCS identified the following as the primary safety-related functions of the PORV and the PORV block valve:

- (1) The PORV is part of the reactor coolant pressure boundary.
- (2) The PORV is used to limit the number of times the safety valves are called upon to open.
- (3) The PORV is used to prevent overpressurization of the reactor coolant system at low temperatures when the integrity of the reactor vessel becomes the limiting consideration.
- (4) The block valve serves to reduce the challenge rate to the ECCS because the inability to isolate an open PORV would require ECCS to function.
- (5) The PORV is used to "bleed" cooling water during the "bleed and feed" cooling mode.
- (6) The PORV is essential to depressurize the reactor coolant system in order to utilize the low pressure injection system during conditions of inadequate core cooling. (Pollard, ff. Tr. 9027, at 5-4 to 5-5)

163. We will address these functions seriatim except that those numbered (1) and (4) are addressed together since they are addressed to the common objective of reducing the challenge rate of the ECCS.

169. The PORV is part of the reactor coolant pressure boundary. GDC-14 of Appendix A to 10 CFR Part 50 requires that the reactor coolant pressure boundary shall be designed, fabricated, erected, and tested so as to have an extremely low probability of abnormal leakage, of rapidly propagating failure, and of gross rupture. (Pollard, ff, Tr. 9027, at 5-6 to 5-7)

170. Inadvertent opening of the PORV or a stuck open PORV causes a loss of coolant accident requiring operation of the ECCS unless the block valve can be closed. (Pollard, ff. Tr. 9027, at 5-4; Correa, et al, ff. Tr. 8746, at 3; Jensen, ff, Tr. 8821, at 4)

171. Since a single failure in the circuitry associated with the PORV could result in inadvertent opening of the PORV, UCS argued that the PORV should be safety grade and meet the single failure criterion and IEEE Std. 279. (Pollard, ff, Tr. 9027, at 5-12)

172. Similarly, because the PORV might stick open whether opened intentionally or inadvertently, the block valve and its associated controls should be classified as safety grade and meet IEEE Std. 279. (Id)

173. In each of these two instances, UCS argued that the requirement for safety grade classification was necessary to accomplish the goal of reducing challenges to the ECCS.

174. The Licensee and Staff opposed this contention by arguing that if the PORV was open and the block valve could not be closed, the ECCS would safely mitigate the loss of coolant accident. (Correa et al., ff. Tr. 8746 at 2; Jensen, ff. Tr. 8821 at 4)

175. UCS responded to this line of argument by noting first that the Commission's regulations require both an extremely low probability of a LOCA (e.g., GDC-14) and ECCS protection against a LOCA. (e.g., GDC-35, 36, and 37). (Pollard, ff. Tr. 9027, at 5-6 to 5-7) The fact that an accident can be mitigated does not excuse the licensee from meeting the GDC requiring that the plant be designed and built so as to have an "extremely low probability" that an accident will occur. This is a cornerstone of the defense-in-depth philosophy which rightly pervades the regulation of nuclear plants.

176. Moreover, an important lesson learned from the TMI-2 accident is the necessity to reduce the frequency of occurrence of plant conditions which require the operation of ECCS. (Pollard, ff. Tr. 9027, at 5-11)

177. As noted above, a general lesson learned from the TMI-2 accident is that the frequency with which some safety systems such as ECCS are called upon to function

- may exceed their generally understood and previously accepted design basis. Therefore, the Lessons Learned Task Force recommended specific changes to decrease the frequency of challenges to ECCS. (NUREG-0578, at 6)
178. In our view, it is self-evident that if the frequency with which ECCS is called upon to function may be greater than its design basis, then reducing the frequency of such challenges is a function that is itself important to safety.
179. The Staff testified that the reason the PORV and block valve are being upgraded is that the "repeated unnecessary challenges to these systems [i.e., the ECCS and the safety valves] is undesirable." (Jensen, ff. Tr. 8821, at 5)
180. To the extent that this implies that reducing ECCS challenges is a good idea but not required for safety, we reject it on two grounds. First, if the PORV is open and the block valve cannot be closed, the result is a need for ECCS to function to provide core cooling. Its actuation in such circumstances can hardly be referred to as "unnecessary." Similarly if the PORV fails to open and halt the rise in system pressure, the safety valves must function. Such challenges cannot be labeled unnecessary.
181. Second, if the ECCS is being challenged in ways and at a frequency greater than it is designed for by failures of the PORV and block valve, the situation is far more

than merely "undesirable." The ECCS provides critical protection relied upon for the public health and safety. Maintaining the rate and type of challenge to such a safety system to a level unquestionably within its design basis is required for safety.

182. UCS also emphasized that the Staff's failure to require the PORV and the block valve to be safety-grade and meet the single failure criterion and IEEE 279 is fundamentally inconsistent with the reasoning behind the requirements placed on the reactor coolant system high points vents that are required to be installed. (Pollard, ff. Tr. 9027, at 5-8 to 5-9) With respect to these vents, the Staff has taken the following position:^{1/}

Since these vents form a part of the reactor coolant pressure boundary, the design of the vents shall conform to the requirements of Appendix A to 10 CFR Part 50, General Design Criteria. In particular, these vents shall be safety grade, and shall satisfy the single failure criterion and the requirements of IEEE-279 in order to ensure a low probability of inadvertent actuation. (Staff Ex. 1, at C8-60, Emphasis added)

183. These requirements applicable to the vents were restated and clarified in NUREG-0737 as follows:

. . . the vents must not lead to an unacceptable increase in the probability of a loss-of-coolant accident. . .

^{1/} These are the current requirements of the high point vents.

Since the reactor coolant system vent will be part of the reactor coolant pressure boundary, all requirements for the reactor pressure boundary must be met, and, in addition, sufficient redundancy should be incorporated into the design to minimize the probability of an inadvertent actuation of the system.

The probability of a vent path failing to close, once opened, should be minimized; this is a new requirement. Each vent must have its power supplied from an emergency bus. A single failure within the power and control aspects of the reactor coolant vent system should not prevent isolation of the entire vent system when required. (NUREG-0737, at 3-55 to 3-57, Emphasis added)

184. It is significant that neither the Licensee nor the Staff offered any reason why the same logic and hence the same regulatory requirements should not apply to the PORV and block valve which, like the to-be-installed high point vents, pose a risk of breach of the reactor coolant pressure boundary - a LOCA requiring ECCS operation - by inadvertent actuation or failure to close after appropriate actuation. Indeed, the past history of PORV failures indicates that they pose a demonstrable risk as compared to the high point vents, where the risk is more speculative. Hence, there is arguably more reason to apply the safety-grade criteria to the PORV and block valve. Indeed, the staff witness agreed that, considering the instances in which these valves have failed to reseal, the PORV does not have an extremely low probability of abnormal leakage. (Tr. 8848, Zudans) We concur.

185. We concur further with UCS's view that the reasoning behind the staff's treatment of the high point vents applies

with equal force to the PORV and block valve.

186. Based upon the foregoing, we find that the PORV serves a function important to safety in ensuring that the challenge rate to ECCS is kept within the design basis for that critical safety system. We find in addition that the PORV is part of the reactor coolant pressure boundary and hence governed by the regulations requiring an extremely low probability of abnormal leakage and rupture. (E.g. GDC 14, 15 and 30) A single failure can cause a breach in the integrity of the pressure boundary. This in combination with the relatively high rate of PORV's failing to reseal constitutes a violation of the criteria for the pressure boundary. In order to perform its safety function and to maintain the integrity of the pressure boundary, the PORV should be safety grade.

187. The second function of the PORV, which UCS identified as a basis for its position that the PORV circuitry should be safety grade, is the function of reducing the number of times the safety valves are required to open. (Pollard, ff. Tr. 9027, at 5-9 to 5-10)

188. The Staff agreed that one function of the PORV is to prevent the pressurizer safety valves from being opened for mild transients. (Jensen, ff. Tr. 8821, at 3; see also NUREG-0578, at A-3) This is because the safety valves have no block valve and cannot be isolated if

- they should stick open. (Jensen, ff. Tr. 8821, at 3)
189. IE Bulletin 79- 05B, issued to all Licensees after the TMI-2 accident required modifications to reduce the likelihood of automatic actuation of the PORV during anticipated transients without resulting in increasing the frequency of pressurizer safety valve situation for these transients. (Pollard, ff. Tr. 9027 at 5-9; see also Staff Ex. 1 at C2-11)
190. The resulting modifications made at TMI-1 were to lower the high pressure SCRAM set point to 2300 psig, raise the PORV opening set point to 2450 psig and add new reactor SCRAM signals to shut down the reactor in the event of turbine trip or loss of feedwater. (Pollard, ff. Tr. 9027, at 5-10)
191. UCS testified that these modifications are not sufficient to assure that the PORV will open instead of the safety valves because the control circuitry for the PORV is not safety grade, and of course, not single failure-proof. A single failure can prevent the PORV from opening, creating a challenge to the safety valves. Reducing the pressure difference between the PORV and safety valve set points from 145 psi^{2/} to only 50 psi makes it even more

^{2/} This is apparently incorrect. The Licensee testified that the PORV set point before the charge was 2255 psig. Thus, the difference between the PORV and safety valve set points before the modifications was 245 psi. (Correa, et al, ff. Tr. 8746, at 3)

important to require the PORV and its controls to be of the highest reliability. (Pollard, ff. Tr. 9027, at 5-10)

192. No testimony was presented by the Licensee or Staff evaluating the challenge rate to the safety valves or the extent to which the modifications made to the set points and reactor trips have affected that challenge rate. No response was provided to UCS's point that reducing the differential between the PORV and safety valve set points to only 50 psi suggests a possible increase in safety valve challenges.
193. The Licensee testified that as a result of the changes to the PORV set point and the high pressure SCRAM set point, actuation of the PORV is now not expected during operational transients if feedwater is available. (Correa, et. al., ff. Tr. 8746, at 3)
194. This change alone may sufficeintly reduce the probability of actuation of both the PORV and the safety valves during operational transients to resolve UCS' concerns. However, we note that the Staff has not completed its review of NUREG-0737 items II.K.2.14, Lift Frequency of PORV and Safety Valves, and II.K.3.7, Evaluation of Power-Operated Relief Valve Open Probability During Overpressure Transient. (Staff Ex. 12, at II.K.2.14-1 to II.K.2.14-3)

195. We therefore conclude that, prior to restart of TMI-1, either one of the following two requirements must be satisfied:

- (1) The PORV and its control circuits must be classified as safety grade and meet all applicable criteria including the single failure criterion and IEEE Std 279 to assure that the PORV can fulfill its function of limiting the frequency of challenges to the safety valves.
- (2) It must be demonstrated that both the probability of challenges to the safety valves and the probability of the safety valves failing to reclose are acceptable (i.e., NUREG-0737 items II.K.2.14 and II.K.3.7 are resolved) assuming that the PORV fails to open.

196. The basis for requiring the assumption that the PORV does not open is that it is not safety grade and the Commission's practice is not to give credit for non-safety grade equipment when evaluating the adequacy of safety systems.

197. We recognize that if option 2 above is used to justify restart, other aspects of these findings still require the PORV to be safety grade.

198. UCS testified that the use of the PORV to prevent overpressurization of the reactor coolant system at low temperatures is an

additional safety function of the PORV. (Pollard, ff.Tr.9027, at 5-10 to 5-11)

199. At low temperatures, the steel of the reactor vessel is susceptible to cracking (i.e. brittle fracture). Until the reactor vessel walls are above the nil ductility transition temperature, the reactor coolant system pressure must be limited to a few hundred pounds per square inch. Since reactor pressure vessel rupture is an accident beyond the capability of ECCS to mitigate, it is extremely important to maintain the integrity of the vessel. (Id.)
200. The PORV is used during low temperature operations to protect against overpressurizing the reactor vessel. This function, the third safety-related function identified by UCS cannot be performed by the safety valves because their opening pressure set point - 2500 psig - is far above the permissible pressure limit and cannot be changed by the operator. (Id.)
201. UCS's position is supported by NUREG-0578 which states that "[t]he PORV is also used to prevent overpressurization of the reactor coolant system during operation at low temperatures, an operational mode when the nil ductility transition temperature (NDTT) becomes a consideration for structural integrity of the primary coolant pressure boundary. *** The NDTT protection mode can also be selected, in which case the PORV opens in the event a preselected low-pressure setpoint is reached or [sic] reactor temperatures are w the NDTT limit." (NUREG-0578, at A-3)

202. The Licensee confirmed that this description is applicable to TMI-1. (Tr. 8755-8756, Jones) The Staff and Licensee agreed that the PORV is used to prevent reactor coolant system overpressure during low temperature operation, but argued that this function of the PORV is only a backup to reactor operator action. (Jensen, ff. Tr. 8821, at 3; Tr. 8755-8756, Jones) UCS testified that it is incorrect to refer to this function of the PORV as a backup to the operator because under some plant conditions, the only way to limit overpressure is by use of the PORV. (Tr. 9031-9033, Pollard)

203. During cross-examination by UCS, the Licensee agreed that, if the plant is in cold shutdown condition with the reactor coolant system solid, the PORV "may" serve a safety function in relieving the overpressure. (Tr. 8979, Jones)

204. Nevertheless, the Licensee still attempted to maintain that the operator has the capability to terminate an overpressure event and the PORV is just a backup. (Id)

205. We find this assertion to be without merit. Operator action can be relied on only if adequate time is available. In the case of the primary system in a solid condition, i.e., without a bubble in the pressurizer, that operator does not have time to act. (Tr. 8976, Jones) Furthermore, a technical specification requires that the PORV shall not

be taken out of service nor shall it be isolated from the reactor coolant system unless the high pressure injection pumps are disabled, the reactor vessel head is removed, or the average primary coolant temperature is above 320°F. (Tr. 9015, Jones)

206. This specification would appear to define plant conditions where either overpressurization has a low probability of occurrence or the primary system temperature is above the nil ductility transition temperature. In either case, the plant conditions are such that the low temperature overpressure protection provided by the PORV is not needed. One can reasonably infer that under all other conditions of low temperature operation, the PORV is needed for safety, otherwise there would be no prohibition against taking it out of service.

207. We conclude that the low temperature overpressure protection provided by the PORV is important to safety and, therefore, the PORV and the associated instrumentation and controls used to provide this protection must meet the criteria applicable to safety grade equipment.

208. UCS testified that since the bleed and feed cooling mode has been devised with reliance on the PORV and since all applicable procedures and operator training have been directed toward use of the PORV, the PORV should be safety grade. (Pollard, ff. Tr. 9027, at 5-16) This is the fifth safety function of the PORV identified by UCS.

209. In our findings on UCS Contentions 1 and 2, we concluded that the bleed and feed cooling mode has not been demonstrated to be a reliable mode of core cooling. This would suggest that there is no need to upgrade the PORV to safety grade for the sole purpose of using it during this cooling mode. However, if bleed and feed is nevertheless found to be an acceptable and necessary cooling mode, we find that the PORV must be upgraded not only for the reasons advanced by UCS relating to emergency procedures and operator training, but also for the purpose of limiting challenges to the safety valves.
210. No party contested the fact that the TMI-1 Emergency Procedures instruct the operator to use the PORV, but there is testimony that, if the non-safety grade PORV is not available, the safety valves can be used to perform the bleeding function. (Tr. 8761, Jones). The bleeding function may require repeated opening and closing of the valves (Pollard, ff. Tr. 9027 at 5-14 and 5-15). During bleed and feed, the valves would be called upon to relieve steam, two-phase and solid water flow. (Tr. 4884-5) However, the safety valves have never been qualified to operate under these conditions.
211. The Staff has not even evaluated the nature of the demands that would be placed upon the safety valves during the bleed and feed mode - either the number of times they would be called upon to operate or the flow quality they

would be required to relieve. (Tr. 8920, see also Tr. 8930-33, Zudans and compare with Tr. 9012-3, Urquhart) The current valve testing program does not appear to be directed towards resolving this question since the test facility cannot simulate the rapid repressurization associated with bleed and feed. (Tr. 8920-2)

212. In the absence of testing or reliable analyses (and considering that the safety valves are not equipped with block valves and cannot be isolated) there is no basis for concluding that the safety valves can be relied upon to perform during bleed and feed conditions which would clearly make demands beyond the qualification of the valves.^{3/}

213. The record suggests that even if the TMI-1 safety valve successfully passes the on-going EPRI testing program, that will not establish its qualifications to perform the bleeding function since, as noted above, the staff has not evaluated the demands placed on the valve during bleed and feed and the tests do not appear to be directed toward simulating such demands.

214. The PORV is clearly the bleeding path stipulated by the plant procedures and included in the operators' training. After the TMI-2 accident, the staff observed accurately

^{3/} "Solid water or two-phase flow through the relief and safety valves can greatly increase the dynamic forces on valve internals, piping, and supports over those that would be expected from saturated steam flow conditions. Present ASME qualification requirements for safety valves include only flow under saturated steam conditions." NUREG-0578, Bd. Ex. 7 at A-7. See also Tr. 8841-4, Zudans and Jensen.

that "[t]his method of decay heat removal [bleed and feed] requires the use of the emergency core cooling system (ECCS) and the power-operated relief valves (PORVs) in the pressurizer." (Pollard, ff. Tr. 9027 at 5-14) We believe that that observation was and is accurate. If bleed and feed is to be relied upon, as the Licensee urges us,^{4/} the PORV serves a function important to safety and must meet safety-grade criteria.

^{4/} E.g. Keaten and Jones, ff. Tr. 4588, at 7, 8, 10-11. See also Jensen, Natural Circulation, ff. Tr. 4913 at 8-9.

215. Finally, UCS identified the use of the PORV to depressurize the reactor coolant system during conditions of inadequate core cooling as another safety function which requires that the PORV be upgraded to safety grade. (Pollard, ff. Tr. 9027, at 5-16 to 5-17)

216. The TMI-1 emergency procedures instruct the operator to open the PORV and leave it open in the event of inadequate core cooling. This action is intended to depressurize the reactor coolant system to allow operation of the low pressure injection system and thereby restore core cooling. (Pollard, ff. Tr. 9027, at 5-16 to 5-17; Lic. Ex. 48, at 28.0)

217. This depressurization function cannot be performed by the safety valves because they will not open below 2500 psig and they are not controllable by the operator. (Pollard, ff. Tr. 9027, at 5-17)

218. Use of the letdown line to depressurize the system might be precluded because of the high level of radioactivity in the reactor coolant system after core damage. (Pollard, ff. Tr. 9027, at 5-17; UCS Ex. 4, at 6.0)*

219. After litigation of this contention was completed, the Licensee amended the TMI-1 emergency procedure referenced by

* There are two Emergency Procedures for TMI-1 covering inadequate core cooling. EP 1202-6B, Attachment 3 is, in different versions, UCS Ex. 6 and Licensee Ex. 48. EP 1202-39 is, in different versions, UCS Ex. 4 and Licensee Ex. 51

UCS, UCS. Ex. 4. The revised procedure, still directs the operator to open the PORV to depressurize the reactor coolant system if feedwater is not available and, if main or emergency feedwater is available, to use letdown flow to help control reactor coolant pressure, but the fact that letdown flow may be prohibited by high activity was deleted from the procedure. (Lic. Ex. 51, at 4.0, 5.0)

220. This change to the emergency procedure does not, of course, change the fact that use of letdown flow to control reactor pressure may be prohibited because of high activity.

221. The Staff also testified that one function of the PORV is to give the operator a means of depressurizing the primary system that is independent of the steam generators. (Jensen, ff. Tr. 8821, at 3)

222. The Licensee testified that the PORV is only an additional means of depressurizing the primary system which has a smaller impact than use of the steam generators. (Tr. 8761-8762, Jones)

223. The Licensee also testified that it was acceptable to rely on non-safety grade equipment in this instance because a situation involving inadequate core cooling is not part of the design basis for TMI-1. (Tr. 8762-8763, Jones)

224. The first argument by the Licensee implies that depressurization using the steam generators is an independent method of

depressurization which does not call for use of the PORV. This implication is contradicted by the TMI-1 emergency procedures.

225. The procedures call for the operator to depressurize the steam generator(s) as rapidly as possible to 400 psig or as far as necessary to achieve a 100° F decrease in secondary saturation temperature. At the same time, the operator is directed to use the PORV, as necessary, to maintain RCS pressure within 50 psi of steam generator pressure. (Lic. Ex. 48, at 26.0 - 27.0)

226. Thus, even if the primary system is being depressurized via the steam generators, the PORV is still used to keep primary system pressure within 50 psi of steam generator pressure. Thus, the PORV is needed in conjunction with use of the steam generators.

227. Furthermore, in another section of the emergency procedures for inadequate core cooling, the operator is directed to both depressurize the steam generator(s) and open the PORV and, following depressurization, to control reactor coolant system pressure below 150 psig using the PORV. (Lic. Ex. 48, at 28.0)

228. The Licensee's second argument is that use of non-safety grade equipment is acceptable because a situation involving inadequate core cooling is beyond the design basis for TMI-1.

(Tr, 8762-3, Jones) This argument ignores the lessons learned from the TMI-2 accident and the other requirements that have been imposed on TMI-1 for accidents previously considered to be beyond the design basis.

229. The Lessons Learned Task Force described the TMI-2 accident and the general issues it raised as follows:

"At Three Mile Island, some of the safety systems were challenged to a greater extent or in a different manner than was anticipated in their design basis. Many of the events that occurred were known to be possible, but were not previously judged to be sufficiently probable to require consideration in the design basis. Operator error, extensive core damage, and production of a large quantity of hydrogen from the reaction of zircalloy cladding and steam were foreseen as possible events, but were excluded from the design basis, since plant safety features are provided to prevent such occurrences. The Task Force will consider whether revisions or additions to the General Design Criteria or other requirements are necessary in light of these occurrences. A central issue that will be considered is whether to modify or extend the current design basis events or to depart from the concept. For example, analysis of design basis accidents could be modified to include multiple equipment failures and more explicit consideration of operator actions or inaction, rather than employing the conventional single-failure criterion. Alternatively, analyses

of design basis accidents could be extended to include core uncover or core melting scenarios. Risk assessment and explicit consideration of accident probabilities and consequences might also be used instead of the deterministic use of analysis of design basis accidents."

(NUREG-0578, at 16-17) emphasis added

230. TMI-1 is being required to install high point vents in the reactor coolant system (Staff Ex. 1, at C8-60) and instrumentation to detect inadequate core cooling. (Id., at C8-14 to C8-21) The venting system is required to be safety grade. (Id., at C8-60) The saturation meter used to detect the approach to inadequate core cooling conditions is required to be safety grade. (Id., at C8-17)

231. The Licensee is being required to upgrade plant radiation shielding to provide adequate personnel and equipment protection after an accident in which significant core damage occurs. (Id., at C8-33)

232. These measures clearly assume the occurrence of an accident beyond the design basis for TMI-1 when it was licensed and yet the new equipment being installed is required to be safety grade.

233. The Licensee offers no reasoning or technical justification for why systems or components necessary to mitigate accidents beyond the pre-TMI design basis, but with a clear connection to the TMI-2 accident, should not be safety grade. It merely invokes the incantation that such events are beyond the design basis. In the aftermath of the TMI-2 accident, which, as the quoted language from NUREG-0578 indicates, exceeded the design basis in many ways, we find the incantation unpersuasive. This is particularly so in light of the fact that other measures discussed above ordered by the Director of NRR to mitigate events beyond the design bases are required to be safety grade. No reason has been offered to this Board why the PORV should be treated differently.

234. We have concluded that the functions performed by the PORV are important to safety and should be performed by safety-grade equipment. In addition, there is a relatively high probability of the PORV failing open and a single failure can cause inadvertent actuation of the PORV. In light of this, the PORV in its present state constitutes a violation of the criteria requiring that the plant be designed and built so as to have an extremely low probability of abnormal leakage or rupture of the reactor coolant pressure boundary.* (GDC 14, 15 and 30)

* Because the block valve is also non-safety grade, it cannot be relied upon to perform the safety function of isolating the PORV. (Pollard, ff. Tr. 9027 at 5-10; Tr. 9061, Pollard) Two pieces of non-safety grade equipment do not compensate for lack of a safety-grade system or provide equivalent protection.

For this latter reason alone, we would conclude that the PORV and its block valve must conform to the requirements of Appendix A to 10 CFR Part 50. In particular, the valves must be safety grade and satisfy the single failure criterion and the requirements of IEEE Std. 279 in order to ensure a low probability of inadvertent actuation and a high probability of isolating the PORV should it stick open.

235. Although it is, of course, up to the Licensee to propose a design which meets these requirements, we have given some thought to the nature of the changes that may be needed.

236. With a few exceptions, the record is unclear on the current status of the PORV and block valve. It is established that a single failure can inadvertently open the PORV (Tr. 8769, Correa) The circuitry for the PORV does not meet the single failure criterion. (Tr. 8770-1, Correa) There was testimony that the block valve is environmentally and seismically qualified and that the PORV is seismically qualified. (Tr. 8768, Correa) However, at the most, the the environmental qualification would have been in accordance with the general criteria in effect at the time the plant was licensed. The witnesses could only recall that temperature and radiation were addressed. (Tr. 8994-8, Urquhart) The

Commission recently held that these older environmental qualification criteria "cannot serve as the standard against which qualification is to be judged" and has ordered all operating plants to meet new, much stricter standards. Petition for Emergency and Remedial Action, CLI-80-21, 11 NRC 707, 711 (May 22, 1980.)

237. Licensees are to demonstrate compliance with the environmental qualification criteria by responding to IE Bulletin 79-01B which requires them to provide detailed qualification information on all safety-related electrical equipment. (Id. at 712-714) While the staff has not yet completed its review of the Licensee's submission in response to the IE Bulletin, UCS's witness testified that his review of the material indicated that neither the PORV nor block valve are included on the Licensee's master list of equipment for which qualification is to be demonstrated. (Tr. 9063, Pollard) Neither the Licensee nor the Staff suggested otherwise. This would mean that the Licensee has no intention of demonstrating that the valves can survive the accident environment. Omission of the valves from their response to IE Bulletin 79-01B would be consistent with the Licensee's position that they are not safety-related.
238. Therefore, even from the standpoint of environmental qualification alone we cannot find that the block valve or

PORV is the "equivalent" of safety-grade. And the record is clear that the valves are not single-failure proof and do not meet IEEE Std. 279. Thus, there are no grounds for believing that the valves currently possess a level of reliability equivalent or even particularly close to that provided by a safety-grade system.

239. In addition to meeting the criteria for environmental and seismic qualification for the valves and their associated circuitry and controls, it will be necessary for the valves to meet the single failure criterion. It appears to the Board that, if the existing PORV and block valve (and circuitry) are both upgraded to safety-grade, it will not be necessary to install additional valves to meet the single failure criterion, since one could not then postulate a failure of both pieces of safety-grade equipment.* However, we are not in a position now to make a definitive statement on that.

240. Based upon the foregoing, we find that the short 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 the evidence shows that the PORV and block valve must meet safety-grade requirements so as to ensure their relia-

* See our discussion of the manner in which the single failure criterion is applied, supra para

bility to perform safety-related functions and to ensure an extremely low probability of violating the integrity of the reactor coolant pressure boundary.

UCS CONTENTION NO. 10

The design of the safety systems at TMI is such that the operator can prevent the completion of a safety function which is initiated automatically; to wit: the operator can (and did) shut off the emergency core cooling system prematurely. This violates §4.16 of IEEE 279 as incorporated in 10 CFR 50.55 (a) (h) which states:

The protection system shall be so designed that, once initiated, a protection system action shall go to completion.

The design must be modified so that no operator action can prevent the completion of a safety function once initiated.

241. The Board limited this contention to the core cooling and containment isolation systems. (First Special Prehearing Conference Order, at 20)

242. UCS further narrowed this contention in two ways. First, it was limited to automatically initiated safety functions, i.e., manually initiated safety functions were not addressed. Second, the phrase, "no operator action," was limited to operator actions involving the equipment

normally used by the operator to terminate the safety function. (Tr. 6544, Pollard)

243. Testimony on this contention was given by the Union of Concerned Scientists (Pollard, ff. Tr. 6410), the Licensee (Clark, et al, ff. Tr. 6225), and the Staff (Sullivan, ff. Tr. 6602).

244. During the TMI-2 accident, operator intervention in the automatic operation of the high pressure injection (HPI) system was premature and had a significant effect on the extent of damage to the reactor. (Pollard, ff. Tr. 6410, at 10-1; Sullivan, ff. Tr. 6602, at 3) In fact, the Licensee takes the position that the operator's premature termination of HPI flow was the clear, dominating cause of core damage. (e.g., Keaten et al., ff. Tr. 7558 at 15)

245. TMI-1 is designed such that the operators can prevent or terminate the safety functions provided by the emergency core cooling, emergency feedwater, and containment isolation systems even if plant conditions are such that the safety functions are needed. (Pollard, ff. Tr. 6410, at 10-2, 10-3)

246. GDC-20 of Appendix A to 10 CFR 50, requires, in part that the protection system shall be designed to sense accident conditions and to initiate the operation of systems and components important to safety.

247. IEEE Std 279-1968 requires that the protection system shall be so designed that, once initiated, a protection system action shall go to completion. (UCS Ex. 16, at 5)

248. 10 CFR 50.55a(h) requires that, for construction permits issued after January 1, 1971, protection systems shall meet the requirements of editions or revisions of IEEE Std 279 in effect on the docket date of the construction permit application.

249. As is discussed below, there was considerable debate among the witnesses for UCS, Licensee, and Staff over whether the language of IEEE Std 279 and GDC-20 was intended to apply, or has been applied in the past, to equipment actuated by the protection system.

250. UCS' position, however, does not depend solely on the language or past application of IEEE Std 279. UCS' contention is that the TMI-2 accident graphically demonstrated the unacceptable consequences of permitting the operator to interfere with the functioning of safety systems and that a clear lesson of the accident is therefore that such interference ought not to be permitted. (Pollard, ff. Tr. 6410, at 10-1 to 10-4, 10-16 to 10-19)

251. UCS contends further that GDC-20 and IEEE Std 279 has been interpreted in past instances to apply to equipment which is not part of the protection system. (Pollard, ff.

Tr. 6410, at 10-6 to 10-16) and should, in the light of the TMI-2 accident, be interpreted to support UCS' contention. (Tr. 6438-6454, 6490-5, Pollard)

252. Beyond arguments over the language of the regulations, UCS' testimony was that the current design of TMI-1 is unsafe because the operator can prevent or prematurely terminate the critically important safety functions provided by emergency core cooling, emergency feedwater, and containment isolation functions. (Pollard, ff. Tr. 6410, at 10-2 to 10-4, 10-18, 10-22)

253. The issues which emerged during litigation of this contention were:

a) Considering the TMI-2 accident, does the present design of TMI-1 provide reasonable assurance that public health and safety is adequately protected or should the design be modified to provide additional protection against premature termination of a safety system by the operator?

b) Do the provisions of IEEE Std 279 require a design which precludes termination of a safety system by operator action prior to completion of its safety function? If the provisions' language does not itself require such a design, does the purpose of the standard and its past interpretation support its application

in the manner UCS proposes?

c) Is TMI-1 required to comply with the requirements of IEEE Std 279?

The three issues are addressed below in sequence.

254. The Licensee, with assistance from B&W, has analyzed all design basis accidents and developed operator procedures for those accidents (Tr. 6245, Ross)

255. The procedures are quite specific regarding when a safety system like high pressure injection may be throttled. (Tr. 6246, Ross)

256. The Licensee's witness testified that, for design basis accidents, the operator is instructed to follow the procedures strictly and not depart from them. (Tr. 6245, Ross; Tr. 6245-6251, Clark; Tr. 6299, Clark)

257. UCS' position is that, given that the Licensee, with B&W's assistance, has clearly defined the conditions constituting completion of a safety function (or the goal of the safety system), the plant can and should be designed to preclude termination of the safety system until those conditions are attained.

258. For example, TMI-1 emergency procedures state that HPI may be throttled only if the LPI flow is greater than 1000 gpm in both loops and stable for greater than 20 minutes (Lic. Ex. 48, at 8.0, 11.0) or the degree of

subcooling in the primary system is at least 50°F and throttling is necessary to prevent pressurizer level going off scale high. (Lic. Ex. 48, at 8.0) These instructions even take precedence over the normal restrictions on pressure-temperature limits for the reactor vessel. (Lic. Ex. 48, at 8.0)

259. The question thus arises whether the operators can be relied upon in all future cases to follow the appropriate emergency procedures and not prematurely terminate operation of a safety system. In this regard, it should be noted that the Licensee has instructed its operators to follow the emergency procedures unless they believe some other course of action is required. (Tr. 6248-6249, 6299-6300, Clark) The problem this raises is that not all possible combination and sequences of failures have been identified even considering only accidents within the design basis. TMI-2 had the equivalent of a small LOCA which is a design basis accident. The result was a combination of indications that led the operator to terminate HPI when the correct action was to leave it in operation.

260. Thus, in future potential accidents, the operator may again be confronted with a sequence of events causing unforeseen control room indications that could lead to premature termination of ECCS, EFW or containment isolation

during design basis accidents.

261. In this connection it should be noted that the Licensee has not committed to install core water level instrumentation (Staff Ex. 14, Item 2.1.3.b., pp.27-30), the safety-grade automatic emergency feedwater system (including instrumentation and control) will not be installed for possibly as long as two years (Staff Ex. 14, Item 2.1.7.a., pp. 36-38, Tr. 21,255-7, Jacobs), the more thermocouples will not be safety-grade (Tr. 21,364, Jacobs) and the licensee's submittal providing the analysis, emergency procedures and training to substantially improve operator performance during transients and accidents, including events that are caused or worsened by inappropriate operator actions (Item 2.1.9.c) was delayed by at least one year (Contrast Staff Ex. 1, p. C8-49 with Staff. Ex. 14, p. 46) and has not been reviewed by the staff. (See the Board's findings on Board Question 11)

262. In addition, we are heavily influenced by the fact that the post-TMI-2 training and requalification of operators is in many respects inadequate. (See Commonwealth of Pennsylvania's Proposed Findings of Fact and Conclusions of Law on Management Issues) The TMI-1 post-accident training and requalification to date does not engender confidence that the operators can be relied upon to react appropriately under a range of accident conditions. Despite

the fact that in the wake of the accident, special training has been given to the operators on post-TMI-2 subject areas, the failure rate of operators has been alarmingly high.

(Commonwealth of Pennsylvania's Proposed Findings, supra at paras. 36-45). After the period of relatively intense retraining is over, the Board cannot expect the operators to retain even this level of competence indefinitely.

263. The Staff apparently did not consider the implications of this aspect of the TMI-2 accident. The principal staff witness on this contention did not base his testimony on an evaluation of the TMI-2 accident and its implications. The testimony was the same as it would have been prior to the TMI-2 accident. (Tr. 6630, Sullivan)

264. UCS asked whether any Staff member had changed their views of the concept of a protective action going to completion as a result of the TMI-2 accident and the witness testified that he did not know. (Tr. 6666-6667, Sullivan) UCS produced a memorandum by Dr. Stephen Hanauer, Assistant Director for Plant Systems, DSS, which the witness had received. (Tr. 6667-6668, Sullivan) Dr. Hanauer's memorandum set forth the changes in his thinking as a result of the TMI-2 accident. Dr. Hanauer stated that the changes in his thinking included: 1) Core damage is credible and 2) Long-term plant operation is essential; initiation isn't enough. (UCS Ex. 18, at 1)

265. Prior to the TMI-2 accident, the NRC's position was that core damage beyond the limits specified in 10 CFR 50.46 was incredible. The Staff's testimony was that the Staff generally does not require safety systems to be designed to

prevent the operator from interrupting the safety function at any time subsequent to initiation. (Sullivan, ff. Tr. 6602, at 5)

266. While acknowledging that Dr. Hanauer's memorandum appears relevant to the question of how one defines a safety function going to completion, the Staff's witness testified he could not interpret what Dr. Hanauer meant, that he made no attempt to ascertain what Dr. Hanauer meant, and that he never responded to Dr. Hanauer's memorandum. (Tr. 6668-6669, Sullivan)

267. Another Staff witness testified that the thing that should be "sacred" in the operation of a nuclear power plant is that operators should not defeat safety systems. Without giving proper attention to the serious consequences of operator action in defeating safety systems, efforts to upgrade the design of safety systems could be thwarted. (Tr., 8625-8627, Conran)

268. While eventually conceding that modifications to the plant to preclude premature safety system termination would be effective for all foreseen events (Tr. 6345-6253, Clark, Ross), the Licensee argued nonetheless that such a design would pose a hazard because of the added circuit complexity and by limiting the flexibility of the operator in dealing with unforeseen accident sequences. (Tr. 6237, Clark)

269. The Licensee's witness, however, had only a vague, general understanding of the question of circuit complexity. He was unaware of the intended interpretation of the emergency procedures and postulated an unnecessarily complex circuit to define stability. (Tr. 6277-6278, Clark) He was not familiar with the design of the saturation meter circuits. (Tr. 6280, Clark) He was not aware whether indications available in the control room were safety grade. (Tr. 6280, Clark)

270. UCS testified, however, that relatively minor modifications to the circuitry could be used to incorporate the same signals used by the operator and that this would not add major complexity to the circuits. (Tr. 6431-6432, Pollard)

271. None of the witness... who testified on this contention could identify a situation involving emergency core cooling, auxiliary feedwater or containment isolation where preventing premature termination would pose a hazard to the public.

272. The Licensee's witness purported, in direct testimony, to give several examples of situations during which termination of safety systems was necessary. (Clark, et al, ff. Tr. 6225, at 6,7) During cross-examination of the witness, it was demonstrated that none of the examples was relevant.

(Tr. 6291-6292, Clark) The witness was unable to postulate even one sequence of events where allowing the core cooling, auxiliary feedwater or containment isolation systems to complete their safety function would result in any hazard to the public.

273. The Staff's witness was not able to discuss the specifics of the TMI-1 design and instead postulated an abstract design and common mode failures. (Tr. 6641-6646, Sullivan) In the end, the Staff could give no example where any conceivable hazard to the public could result from operation of a safety system prior to completion of its safety function.

274. It is important to emphasize that a design conforming to UCS's proposed criteria would in no way restrict the operator's scope of action after the safety function is completed.

275. Failing to identify a single instance of a design basis event where UCS's proposed design would pose a hazard, the Licensee and Staff advanced the notion that for unforeseen accident sequences the proposed design would preclude correct operator action. (Tr. 6299-6300, Clark; Tr. 6646, Sullivan)

276. This proposition has initial appeal. In order to consider its merit, however, one must view the issue in

the following way. On the one hand, UCS proposes a design which permits completion of a safety function, such as core cooling, for all foreseen accident sequences, both within and outside the design basis. It prevents the operator from prematurely terminating the operation of safety systems during design basis accidents and unforeseen accidents only until the conditions defined as completion of the safety function for design basis accidents are met.

277. On the other hand, Licensee and Staff support the current design which has the disadvantage of risking safety system termination prior to completion of a safety function during design basis (or foreseeable) accidents in exchange for the advantage of allowing the operator maximum freedom for unforeseen events.

278. These two alternatives must be balanced against each other. (Tr. 6423-6 , Pollard)

279. The following questions, then, become important. First, what is the probability of the occurrence of an unforeseen event? If it is exceedingly low, then the potential advantage of freedom for operator action becomes correspondingly small at the outset.

280. Second, what is the probability that, should an unforeseen accident occur, proceeding in accordance with

current emergency procedures - that is, permitting the safety systems to operate until the safety function is completed - would be the incorrect response? Obviously, if operation of the safety systems as currently called for is the correct response (as it was during the TMI-2 accident, an unforeseen accident sequence), then inhibiting the operator's ability to prematurely terminate such systems has no disadvantage.

281. Finally, even assuming all the above, what is the probability that the operator in the midst of this unforeseen accident will divine and take the appropriate action of terminating operation of the safety system?

282. UCS's witness testified that the probability of an unforeseen event for which following the emergency procedures is incorrect and for which the operator takes correct action is so low that a design allowing operator interference with safety system operation prior to completion of its function is not worth the risk of improper operator action during a design basis accident. (Tr. 6423-6, 6563-6564, Pollard)

283. The Licensee's witness had no opinion on the probability of the foregoing combination of events, although he was unwilling to even agree that the probability of an unforeseen

accident sequence was lower than the probability of a design basis accident. (Tr. 6255, Clark) Of course, if that were true, TMI-1 could not be permitted to restart without regard to UCS' contention since there would be no basis upon which to find reasonable assurance that the plant can be safely operated.

284. The Staff's witness simply espoused the philosophy that because one might not be able to think of unforeseen events is no excuse not to protect against them. He did not elaborate whatever on how to accomplish that protection. (Tr. 6642, Sullivan)

285. We find that the modifications to TMI-1 are not sufficient to protect the health and safety of the public in light of the TMI-2 accident where premature termination of a safety system by the operator was a principal contributor to the accident.

286. We now address the question of whether the language or interpretation of IEEE Std 279 supports a design proposed by UCS.

287. The scope section of IEEE Std 279 defines the protection system as extending from the sensors to the actuation

device input terminals (UCS Ex. 16, at 3) Thus, a literal reading of the standard means that none of its requirements apply to equipment or systems actuated by the protection system.

288. The literal language of the standard could be met by a design which permits the operator to terminate an automatically initiated safety system as soon as an actuation signal has been transmitted to the input terminals and before the safety system has even begun to operate.

289. UCS testified that such an interpretation of the standard ignores the purpose of the standard and would permit trivial differences unrelated to the safety of the design to determine the acceptability or unacceptability of safety system designs. (Pollard, ff. Tr. 6410, at 10-4 to 10-6)

290. The example given by UCS compared a design where the operator can interrupt the initiation signal into the actuation device input terminals and a design where the operator can interrupt the initiation signal on the other side of the actuation device input terminals. According to the staff's view of the standard, the former design would violate IEEE Std 279 and the latter would not, but in either case the safety function would not go to completion. (Pollard, ff. Tr. 6410, at 10-5 to 10-6) It is thus apparent that the narrow interpretation of the requirement renders it nearly valueless to assuring plant safety.

291. Testimony presented by UCS argued that such a narrow application of the requirements ignored the purpose of IEEE Std 279, the history of its development, continuing work on new standards, the Commission's past policy and practice in applying IEEE Std 279, and the lessons to be learned from the accident. (Pollard, ff. Tr. 6410, at 10-4)
292. UCS gave several examples of instances where the Staff has applied the requirements of IEEE Std 279 to equipment in safety systems that is not part of the protection system. (Pollard, ff. Tr. 6410, 10-12 to 10-16; Tr. 6470-6471, Pollard)
293. The Staff agreed that the requirements or "principles" of IEEE Std 279 have been applied beyond the strict definition of protection system in the scope section of that standard. (Tr. 6626-6627, Sullivan)
294. The Staff gave a specific example of how the provisions of IEEE Std 279 concerning completion of a protective action had been applied to equipment not part of protection system. (Tr. 6639-6640, Sullivan)
295. The example was the application of the requirement to reactor scram systems. Circuit modifications were required to prevent the operator from stopping the insertion of control rods when the protection system initiated a scram.

This example is entirely consistent with current NRC Staff practice set forth in the Standard Review Plan (SRP) which states that "Termination by deliberate actions of the operator should never inhibit the protective action." (SRP, at 7.2-16; SRP, Rev. 1, at 7.2-18) This section of the SRP implements the requirements of IEEE Std 279 as they are used in the review of the reactor trip (scram) system.

296. The Staff testified that since an operator had stopped the control rods from being fully inserted after automatic initiation of a scram signal, common sense dictated that the design be modified to prevent such operator action. However, in the Staff's review, such a design change pursuant to common sense was not "required" by IEEE Std 279. (Tr. 6677-6678, Sullivan)

297. The inconsistency between the Staff's testimony and the application of IEEE Std 279 requirements in the Standard Review Plan can be explained by the witness' lack of involvement in the development of the SRP and lack of experience in using the SRP to conduct license application reviews. (Tr. 6686-6687, Sullivan)

298. UCS testified that continued work by the Staff and industry standards committees to expand the application

of IEEE Std 279 requirements to the entire safety system supported its view of the proper interpretation of IEEE Std 279 requirements. (Pollard, ff. Tr. 6410, at 10-8 to 10-12 and 10-17 to 10-18)

299. IEEE Std 603 is being developed to apply the requirements of IEEE Std 279 to the systems actuated by the protection system. (Pollard, ff. Tr. 6410, at 10-8; UCS Ex. 15, at unnumbered second page of Foreword)

300. IEEE Std 603 requires that the design basis for a safety system set forth the plant conditions after which operator intervention may prevent completion of a protective action and the point in time, or plant conditions, which define completion of a protective action. (UCS Ex. 15, at 13)

301. IEEE Std 603 then requires that the safety system be designed so that the protective action shall continue until completion except that this requirement does not preclude those operator interventions identified in the design basis. (UCS Ex. 15, at 13)

302. UCS testified that the Licensee should be required to define those conditions where operator intervention is permissible and then design the plant so that operator intervention is precluded unless those conditions are met. (Pollard, ff. Tr. 6410, at 10-17 to 10-19)

303. The Staff testified that these provisions of IEEE Std 603 are not exclusive - i.e., they do not preclude operator intervention during any unspecified conditions. (Tr. 6623-6624, Sullivan)

304. We reject the Staff's views of the intent of these provisions of IEEE Std 603. If the Staff were correct, the requirement to specify the design basis conditions under which operator intervention in safety system operation is acceptable would be a nullity. Furthermore, the requirement for a protective action to continue until completion could simply have been worded to allow operator intervention at any time rather than allowing operator intervention during those plant conditions specified in the safety system design basis.

305. We find that past Staff interpretations of IEEE Std 279 have applied those requirements to equipment beyond the defined scope of the protection system. We also find that the continuing development of IEEE Std 603 to apply the requirements of IEEE Std 279 to the entire safety system supports UCS' argument that, as a matter of sound engineering judgment, IEEE 279 should be applied beyond the narrow limits urged here by the Licensee and Staff. Operator intervention should only be permissible under the conditions identified in the design basis.

306. The Staff testified that TMI-1 was not required to meet IEEE Std 279 because its construction permit was issued, and therefore docketed, prior to January 1, 1971. (Sullivan, ff. Tr. 6602, at 2-3) The Licensee attempted to establish the same point by cross-examination. (Tr. 6474-6476, Pollard)

307. However, the testimony established that staff practice has been to apply the requirements of IEEE Std 279 at the operating license stage to plants which received construction permits prior to January 1, 1971. (Tr. 6474-75, Pollard)

308. Moreover, the reactor protection system for TMI-1 was designed by B&W and reviewed by the Staff on the basis of IEEE Std 279 requirements. (Tr. 6271, Patterson; Tr. 6632, Sullivan)

309. It is a common situation for the provisions of NRC regulations and industry standards to lag behind the actual practice in interpretation and application of design requirements. Regulations are frequently applied before their formal adoption. (Tr. 6491-6492, Pollard; Tr. 6633, Sullivan; UCS Ex. 14, at 2)

310. We find that the requirements of IEEE Std 279 apply to TMI-1.

311. Based upon the foregoing, we find that TMI-1 should be designed so that the operators cannot terminate automatically-

initiated core cooling and containment isolation systems until the plant has reached stable conditions as defined by the licensee. We base this on the principles of Section 4.16 IEEE Std. 279, incorporated in 10 CFR 90.55 (a) (h) as they have been historically developed and applied, up to and including the development of draft IEEE Std. 603.

312 While we are fully cognizant that the requirements of IEEE Std. 279 have not previously been applied in this manner, we do not find that dispositive. Our finding is based on the TMI-2 accident and the safety lessons which flow therefrom. Operators can (and did) defeat the critical engineered safety systems provided for protection of the public health and safety. This record offers no assurance that a recurrence is incredible or even remotely unlikely. Considering the absolutely crucial role which such systems play in protecting the public, and the exceedingly close attention which is devoted to their design, fabrication, testing, etc., the potential for rendering all such redundant and diverse systems useless by inappropriate operator action is intolerable.

313. Therefore, we find that the short-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.

UNITED STATES OF AMERICA
NUCLEAR REGULATORY 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))

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

Ms. 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 & Trow-
bridge
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

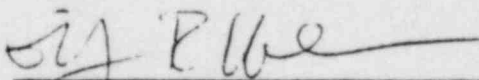
Robert Q. Pollard
609 Montpelier Street
Baltimore, Maryland 21218

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

Marvin I. Lewis
6504 Bradford Terrace
Philadelphia - Pennsylvania 16801

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

I hereby certify that copies of "Union of Concerned Scientists Proposed Findings of Fact and Conclusions of Law on UCS Contentions Nos. 1, 2, 3, 4, 5, and 10 have been mailed postage pre-paid this 1st day of June, 1981 to the above listed parties.



Elyn R. Weiss