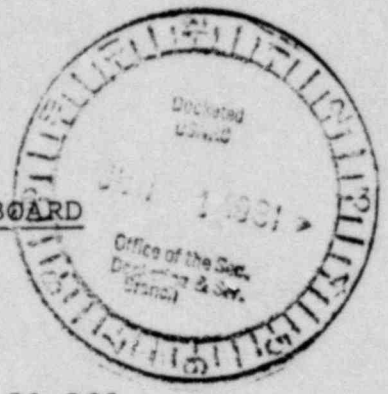
SHOLLY, 6/1/81




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) | ) | |


INTERVENOR STEVEN C. SHOLLY
PROPOSED FINDINGS OF FACT AND
CONCLUSIONS OF LAW
ON PLANT DESIGN ISSUES

1 June 1981

STEVEN C. SHOLLY
Intervenor pro se

DS03
S
0/1

8106040308

G

TABLE OF CONTENTS

INTERVENOR STEVEN C. SHOLLY PROPOSED FINDINGS OF FACT AND CONCLUSIONS OF LAW ON PLANT DESIGN ISSUES

INTERVENOR STEVEN C. SHOLLY
PROPOSED FINDINGS OF FACT AND
CONCLUSIONS OF LAW
ON PLANT DESIGN ISSUES

I. SHOLLY CONTENTION 6-a
(Integrated Control System
Failure Modes and Effects
Analysis)

1. The Integrated Control System (ICS) is a non safety-grade plant control system designed by Babcock and Wilcox Company (B&W) for use in their pressurized-water nuclear plants (Tr. 7005, Joyner). The basic function of the ICS is to match generated megawatts with the megawatt demand by coordinating the flow of steam to the turbine and controlling the rate of steam production in the once-through steam generators (OTSG's) (Thatcher, ff. Tr. 7122, at 2).

2. The ICS represents an evolution from control systesm that were used in the control of B&W-designed OTSG's in fossil-fueled power plants. The ICS utilized on B&W-designed nuclear plants is very similar to the control system utilized in fossil-fueled plants which have OTSG's designed by B&W (Tr. 7021, Joyner).

3. There are two models of the ICS installed in operating B&W nuclear plants. The Model 721 ICS is installed at the three Oconee nuclear plants and at TMI-1, whereas other operating B&W plants utilize a Model 820 ICS. The

two ICS models are similar from a functional standpoint, and share the same inputs (Tr. 6984, Joyner). The Model 820 ICS is used at the newer B&W plants, and has due to major hardware changes, demonstrated improved reliability when compared with the Model 721 ICS (Licensee Ex. 18, at 5-8 and 5-9).

4. The TMI-2 accident did not involve any ICS failures (Broughton, Sadauskas, & Joyner, ff. Tr. 6949, at 2). The TMI-2 accident did, however, involve a loss of main feedwater (Tr. 5999, Lanese) which can be caused by failure of the ICS involving, for example, failure to the "low" failure mode of Functional Module 27, Feedwater Pump Control (Licensee Ex. 18, at 4-60). The TMI-2 accident also involved a temporary loss of emergency feedwater (Capodanno, Lanese, & Torcivia, ff. Tr. 5642, at 6) which might also be caused by ICS failure (Sholly Ex. 2, at 6).

5. Shortly after the TMI-2 accident, the NRC Staff began a study of the sensitivity of the B&W reactor design to feedwater transients, and the role that this sensitivity might play as a precursor or contributor to a TMI-2 type accident. As part of this study the Staff examined the sequence of events that accompanied typical B&W feedwater transients and the role played in such transients by the plant control and safety systems (Ross & Capra, ff. Tr. 15,855, at 1-2).

6. On April 25, 1979, based on the preliminary results of the sensitivity study and in preparation for a Commission meeting on the matter, the NRC Staff prepared a report entitled, "NRR Status Report on Feedwater Transients in B&W Plants." In the report, the Staff expressed five specific concerns about the role played by the ICS in feedwater transients in B&W plants: (a) uncertainty about the reliability of the ICS, (b) the lack of a failure modes and effects analysis of the ICS, (c) operating data which indicated that the ICS might initiate 10-15% of all feedwater transients in B&W plants, (d) the possible contribution of the ICS to a total loss of feedwater through ICS control of emergency feedwater, and (e) concern that even when the ICS works well, there may be, in response to a feedwater transient, wide swings in reactor pressure, pressurizer level, and average reactor coolant temperature (Ross & Capra, ff. Tr. 15,855, at 2).

7. As a result of meetings between the Staff and B&W following the April 25, 1979 Commission meeting, B&W committed to perform a reliability analysis of the ICS, including a failure modes and effects analysis (FMEA). Formal submission of the scope of the reliability analysis and a schedule for its completion came in a letter from B&W to the NRC Staff dated April 28, 1979 (Ross & Capra, ff. Tr. 15,855, at 3).

8. According to the April 28, 1979 letter, the

reliability analysis to be performed by B&W would concentrate on ICS failure modes that could affect the main feedwater system, the emergency feedwater (EFW) system, pressurizer level, and reactor coolant system pressure (Sholly Ex. 2, at 30).

9. Subsequent to the commitment by B&W to perform the reliability analysis on the ICS, confirmatory orders issued by NRC to B&W plants other than TMI-1 incorporated the requirement to perform an FMEA on the ICS as soon as practicable. The FMEA requirement also became incorporated in the later Commission order on the restart of TMI-1 (Ross & Capra, ff. Tr. 15,855, at 3).

10. During the same time frame in which the confirmatory orders were sent to B&W licensees, the Staff released the final version of the study into the sensitivity of B&W reactors to feedwater transients (NUREG-0560, "Staff Report on the Generic Assessment of Feedwater Transients in Pressurized Water Reactors Designed by Babcock & Wilcox Company," May 1979) (Ross & Capra, ff. Tr. 15,855, at 2).

11. In NUREG-0560, the NRC Staff made recommendations for additional analyses related to plant control systems, including: (a) the role of control systems and their significance to safety, (b) the rate at which transients initiated by control systems challenge plant safety systems, (c) the rate at which transients initiated outside the control systems are not successfully mitigated by the control systems,

and (d) analyses to identify realistic plant interactions resulting from failures in non-safety systems, safety systems, and operator actions (Sholly Ex. 2, at 2).

12. On August 17, 1979 B&W submitted its reliability analysis of the ICS to the NRC Staff, BAW-1564, "Integrated Control System Reliability Analysis." (Sholly Ex. 2, at 27). The Licensee, by letter dated October 26, 1979 referenced BAW-1564 as applicable to TMI-1 and adopted BAW-1564 as its response to the Commission's August 9, 1979 Order item on the ICS (NRC Staff Ex. 1, at 1D-1).

13. The Staff undertook an evaluation of BAW-1564 and determined that, due to the nature of the Commission's confirmatory orders on B&W licensees and due to manpower limitations within the NRC Staff, it was necessary to obtain outside assistance to assist the Staff in its review of BAW-1564. The Staff had previously used Oak Ridge National Laboratory (ORNL) to review the ICS and, therefore, ORNL already had a certain amount of expertise on the system (Tr. 7257-58, Thatcher). The Staff testified that they have used ORNL extensively as consultants for a number of years, and that the Staff views ORNL as an "extension" of the NRC Staff's instrumentation and control expertise (Tr. 15,869, Ross).

14. Through an interagency agreement with the U.S. Department of Energy, the NRC Staff sponsored a review of BAW-1564 by the Instrumentation and Controls Division

of ORNL. ORNL subsequently subcontracted part of the work of reviewing BAW-1564 to Science Applications, Inc. (SAI) (Sholly Ex. 2, at cover letter and 1).

15. After a preliminary review of BAW-1564, ORNL submitted a number of questions to B&W through the NRC Staff (Sholly Ex. 2, at 20; Sholly Ex. 1, at Enclosure 1). At ORNL's suggestion, a meeting was held on October 23, 1979 at B&W's Lynchburg, Virginia, facilities to discuss ORNL's questions on the ICS and BAW-1564. The meeting included representation from ORNL, SAI, NRC, B&W, and three B&W licensees (Duke Power, Consumers Power, and Toledo Edison) (Sholly Ex. 1, at 1 and Enclosure 2).

16. In a letter to the Licensee dated November 7, 1979 the NRC Staff requested the Licensee to evaluate the recommendations made by B&W in BAW-1564 and report to the Staff on followup actions taken by Licensee in response to these recommendations (Thatcher, ff. Tr. 7122, at 6).

17. A draft of ORNL's review of BAW-1564 was submitted to the NRC Staff on December 4, 1979 (Sholly Ex. 2, at cover letter). The NRC Staff reviewed the draft and submitted comments to ORNL (Tr. 7260-61, Thatcher). The final ORNL review report was transmitted to the NRC Staff on January 21, 1980 (Sholly Ex. 2, at 2).

18. As would be noted by ORNL, the evaluation of the ICS is a principal requirement in the evaluation of potential or real abnormal events in B&W plants because of

the influence of the ICS on the course of events (Sholly Ex. 2, at 4-5). The ICS participates so directly in the coordination of the generation, transport, and removal of heat from the primary system that the ICS influences the behavior of the whole plant (Sholly Ex. 2, at 7).

19. There is a tight coupling between the secondary system of the plant (which is controlled by the ICS) and the primary system (which includes the reactor and the primary coolant system) (Sholly Ex. 2, at 16). The NRC Staff has expressed this tight coupling as a greater sensitivity to feedwater transients (Tr. 15,770, Ross). The Staff has found that among the factors which contribute to this greater sensitivity are the design of the OTSG's and the reliance on the ICS to automatically regulate feedwater flow (10 N.R.C. 141, at 142-143, 1979).

20. As a result of such factors, the Staff has concluded that the B&W design places more reliance than other pressurized-water reactor designs on the reliability and performance characteristics of the Emergency Feedwater System, the ICS, and the Emergency Core Cooling System (ECCS), and that this, in turn, places a large burden on the plant operators to respond in the event of off-normal system behavior during transient conditions (10 N.R.C. 141, at 143, 1979).

21. By virtue of its design, the ICS can participate in major plant events, including loss of main feedwater, steam generator overfill, secondary depressurization through

turbine bypass or atmospheric dump valves, and, possibly, combinations of these events due to instrument failures (Sholly Ex. 2, at 8).

22. The task of evaluating the ICS is complicated by several engineering considerations, including: (a) the complexity of the ICS due to its "feed-forward" approach to control as augmented by feedback fine-tuning, (b) the complexity of the plant response to control actions, and (c) the sensitivity of the plant to secondary system perturbations (Sholly Ex. 2, at 4-5).

23. Another factor complicating the analysis of the ICS is a lack of information. The Staff testified that unless there is an unusual event which requires detailed analysis and followup, there is not a significant amount of information upon which to base conclusions about the cause of a particular event (Tr. 15,771-72, Capra). For example, the Rancho Seco event which occurred on March 20, 1978, is believed to represent the most severe and prolonged overcooling transient experienced to date, in which the Technical Specification cooldown limits were exceeded by a factor of approximately 3. That event involved a power fault to the non-nuclear instrumentation (NNI) and the ICS which affected the response of nearly 2/3 of the NNI/ICS equipment and led to confusion on the part of the operators due to lack of information about the status of feedwater delivery to the OTSG's (UCS Ex. 35, Reference 1, at 2-4). As of October 29, 1980, the NRC Staff had been unable to

determine whether the turbine bypass and/or atmospheric dump valves were opened to the 50% open position (UCS Ex. 35, Reference 1, at 5). Such information is important since the presence of open turbine bypass or atmospheric relief valves can increase the severity of overcooling events (UCS Ex. 35, Reference 1, at 4).

24. The ICS is a non-safety grade plant control system (Tr. 7005, Joyner). B&W does not perform design basis event testing on the ICS (such as seismic qualification testing). The ICS was not designed to meet physical separation criteria nor was it designed to meet electrical isolation criteria (such as Regulatory Guide 1.75), nor does the ICS meet the single-failure criterion (Licensee Ex. 18, at 4-2).

25. B&W groups the control circuitry of the ICS into four major functional groups: (a) the Turbine Control block represents the control functions that manipulate the atmospheric dump valves, the condenser dump valves, and the turbine throttle valves; (b) the Steam Generator Control block, which represents the control functions that control the flow of feedwater to the OTSG's; (c) the Reactor Control block, which represents the control functions which control the regulating control rod drive system that causes insertion or withdrawal of control rods from the reactor core; and (d) the Integrated Master Control block which coordinates or integrates the operation of the other three blocks

(Tr. 6951, 6955, and 6957, Joyner).

26. In addition, there is the Unit Load Demand control which "interfaces" with the operator to ensure that the ICS does not allow the plant to operate outside of the desired envelope. For example, the plant operator inputs the desired megawatt electric requirements to the Unit Load Demand control and that control interacts with the Integrated Master Control to adjust plant functions to produce the desired electrical output. The Unit Load Demand control limits operation of the plant based on operating restrictions, such as operation with only three reactor coolant pumps, in which case plant power output is restricted to 75% of full power. The control also restricts power output based on other restrictions such as only one main feedwater pump and asymmetric rod position limits (Tr. 6958-59, Joyner).

27. For the purposes of the failure modes and effects analysis (FMEA), B&W defined the ICS as that equipment, excluding power supplies, contained within the ICS cabinets (Licensee Ex. 18, at 1-1). The NRC Staff concurred with B&W's definition of the ICS, but testified that ORNL (the Staff's consultants in reviewing BAW-1564) disagreed with B&W's definition of the ICS (Tr. 7126, Thatcher).

28. ORNL took the position that the ICS should be more broadly defined, stating (Sholly Ex. 2, at 6):

> "A control system, particularly one claimed as 'integrated,' should include sensing, signal conditioning, and actuating equipment and perhaps power supplies--if not primary power sources. The system being controlled includes a number of process loops that are highly interactive and which must often operate within rather narrow individual constraints."

29. The B&W analysis of the ICS (BAW-1564) considered failure modes caused by single failures of ICS inputs, ICS outputs, and functional blocks of the ICS. These failures were considered in their failed state one at a time (Licensee Ex. 18, 4-1).

30. The Board found that the framework within which ICS failures are viewed is greatly influenced by the definition of just what constitutes a failure. NRC Staff witnesses focused only on ICS-related failures that occurred within the ICS cabinets, noting that only 6 such failures out of the 162 studied led to reactor trips, and that these 6 trips were the only trips out of the 310 studied which were caused by ICS failures (Thatcher, ff. Tr. 7122, at 6; Ross & Capra, ff. Tr. 15,855, at 5-6).

31. The description of the ICS boundary appears to have greatly influenced the definition of ICS failure. The position of the Staff's consultants at ORNL on what constitutes the boundary of the ICS led these consultants to question the definition of a "failure," noting for

example that instrument drift not normally associated with a failure might be sufficient to initiate an ICS-induced transient (Sholly Ex. 2, at 5). This may be significant since 71 of the 162 instances of ICS involvement in trips were due to calibration problems (Licensee Ex. 18, Table 5-8, at 5-14).

32. A review of the tabulated data on B&W reactor tirps presenting in the operating history section of BAW-1564 (Section 5) reveals that the ICS has been involved in reactor trips in several ways. Direct failures of ICS internal components have caused five reactor trips (Tr. 7122, Thatcher). The Staff has repeatedly relied on this statistic (Tr. 7122, Thatcher; Ross & Capra, ff. Tr. 15,855, at 4). However, Licensee's witness Joyner, who co-authored BAW-1564 (Tr. 6950, Joyner), testified that although BAW-1564 lists only 6 trips out of the 310 studied as being caused by ICS failures, in reality this number could be as high as 20 (Tr. 7083-84, Joyner).

33. Power supply failures in non-nuclear instrumentation (NNI) and the ICS have been found by B&W to be vulnerable to single failures and human errors (Licensee Ex. 18, at 2-2). Power supply failures to the ICS have caused 11 reactor trips out of the 310 studied by B&W in BAW-1564. These 11 trips include only electrical failures, and do not include human actions which caused an additional 6 trips involving loss of power to the ICS (Licensee Ex. 18, Table 5-1 at 5-11, Table 5-3 at 5-12, and at 5-5).

34. Power supply failures to NNI/ICS have led not only to reactor trips, but to overcooling incidents as well (Licensee Ex. 18, at 2-2). Power supply failures can be important since such failures within the NNI can affect the performance of the ICS and other key systems simultaneously (Sholly Ex. 2, at 7). An example of such an event is the Rancho Seco transient of March 20, 1978 in which adequate control room readout of steam generator conditions and the primary system was lost for over an hour. Such a "common cause" failure like loss of power can not only initiate the transient, but "blind" the operator due to instrument failure (UCS Ex. 35, Reference 3, at 4).

35. The accident at Crystal River Unit 3 in February 1980 is also an example of the consequences of NNI/ICS power failure, in which such a power failure (lasting 21 minutes) caused the opening of the PORV, rendered information inputs to the ICS false, caused partial withdrawal of the control rods from the reactor core, caused the pressurizer spray valve to open, and caused a reduction in feedwater flow (Tr. 15,800, Ross).

36. Significantly, the FMEA as performed by B&W could not highlight NNI/ICS power failures because of B&W's definition of the ICS boundary as excluding power supplies (Sholly Ex. 1, at 3). The B&W Reactor Transient Response Task Force recommended in NUREG-0667 that there be a qualified Instrumentation and Control Technician on duty at B&W plants on all shifts as a result of NNI/ICS power problems, although

the NRC's Division of Safety Technology later concluded that while this is advantageous to the utility, the NRC should not make this a requirement, based on the installation of a safety-grade panel of vital instruments (NUREG-0737, item I.D.2) and on the revision of procedures to incorporate emergency procedures for dealing with NNI/ICS power loss (to which Licensee committed in a letter dated 5/29/80, TLL-245) (NRC Staff Ex. 9, at 1-2).

37. Failures of ICS inputs other than power supply have caused reactor trips as well. B&W found that 11 trips were caused by ICS input failures, five caused by loss of reactor coolant flow signals, three from loss of RCS temperature signals, two from loss of neutron flux signals, and one from a loss of feedwater flow signals (Licensee Ex. 18, Table 5-3 at 5-11).

38. B&W also found that the ICS has a tendency to cause or participate in feedwater oscillations, causing an additional 11 trips (Licensee Ex. 18, table 5-2 at 5-11). In addition to causing reactor trips, these feedwater oscillations have resulted in actuation of ESF and loss of main feedwater (Licensee Ex. 18, at 2-2).

39. Concern about the role of the ICS in feedwater oscillations was one of the five concerns which the NRC Staff raised in its April 25, 1979 "Status Report" on transients in B&W reactors, and was one of the reasons for requiring the FMEA to be performed (Ross & Capra, ff. Tr. 15,855, at 4). Despite this prominent concern, ORNL's review of

BAW-1564 found that B&W used analysis methodology in BAW-1564 that is incapable of evaluating the involvement of the ICS in feedwater oscillations. ORNL noted two distinct regimes of feedwater oscillations, one of which occurs during operation at up to 70% of full power in some plants. ORNL concluded that the ability of plant systems, including the ICS, to withstand such perturbations has not been determined, and that it was not clear that the effects of feedwater oscillations had been included in the "plant duty cycle" (Sholly Ex. 2, at 9).

40. The control response of the ICS has led to an additional 16 reactor trips. Twelve of these trips were caused by feedwater/power mismatches and four were caused by causes primarily related to switching modes of control of the ICS from automatic to manual or vice versa (Licensee Ex. 18, at 5-4, and Table 5-2 at 5-11).

41. Finally, operator error could have caused additional trips. The Staff testified that although they have looked at the possibility of human-error-induced trips involving switching the ICS to manual mode, they could not specify how many such instances had occurred. The 16 trips listed in Table 5-5 of BAW-1564 as involving manual control error would, however, be the bounding case for such trips (Tr. 15,885-86, Capra, Licensee Ex. 18, Table 5-5 at 5-13).

42. The Staff also testified that some of the 19 trips listed in Table 5-5 of BAW-1564 as involving operator

error in misunderstanding an instruction or procedure could have involved operator actions in controlling the ICS in manual (Tr. 15,885, Capra; Licensee Ex. 18, Table 5-5 at 5-13).

43. In evaluating operating experience involving ICS failures, the evaluation may be complicated by a lack of significant information (Tr. 15,771-72, Capra). The Board has already noted the information problems associated with the Rancho Seco transient on March 20, 1980. Licensee witness Joyner, who co-authored BAW-1564, testified that in order to compile the information for the operating history section of the reliability analysis B&W sent two engineers to each B&W plant to gather information and talk to plant personnel (Tr. 6965, Joyner). The schedule for the reliability analysis which was submitted to the NRC gave a period of 14 days to gather this information (Sholly Ex. 2, at 31), although the witness could not recall how much time was actually spent in gathering the data (Tr. 6965, Joyner).

44. According to BAW-1564, the data base for the operating history section of the reliability analysis included reactor trip writeups, control room logs, Licensee Event Reports (LER's), transient records (where available), allowable operating transient cycle (AOTC) data (where available), and records of maintenance and repair from the instrument shop records. This data base was utilized to perform analyses of plant transient events and ICS hardware failures (Licensee Ex. 18, at 5-1).

45. Licensee witness Joyner testified that failures involving the ICS are very dependent on the time in core life at which the failure occurs, the initial power level at which the failure occurs, the response of the plant operators to the failures, and other unspecified factors (Tr. 6967, Joyner).

46. Despite the extent of the dependency of failures on these factors, the B&W analysis of the ICS failure modes and effects was limited with respect to each of the specified factors. A basic assumption in the computer simulations used to evaluate the effects of ICS failures is that the reactor core was at its midpoint in core life (Licensee Ex. 18, at 4-2). This is significant since such computer simulation was used in evaluating the effects of ICS failures on the nuclear steam system in 75% of all cases (Sholly Ex. 2, at 22).

47. Secondly, all analyses of the ICS by the NRC Staff, the Licensee, and B&W dealt with normal full-power operation of the plant (Tr. 15,896, Capra). BAW-1564 discussed a number of conditions of off-normal operation which result in operation at reduced power levels, such as the loss of one or two reactor coolant pumps (resulting in power limitations of 75% and 45% of full power, respectively), loss of a feedwater pump (limits power to 55%), asymmetric rod CRD runback fault conditions (limits power to 60%), reductions in reactor coolant flow, and any hand/auto selector station of the ICS in manual mode (Licensee Ex. 18, at 4-5). ORNL's evaluation of BAW-1564 found that B&W failed

to address the consequences of single ICS failures during off-normal conditions of plant operation, despite the fact that such conditions of operation are allowable and their occurrence is not uncommon (Sholly Ex. 2, at 10-11).

48. In response to a question posed by ORNL on this matter, B&W asserted that it did not miss "any significant transients or protective system challenges" by not including off-normal initial conditions in their analysis. ORNL's review of BAW-1564 noted, however, that the operating history showed that the majority of events involved off-normal initial conditions and/or with some functions of the ICS in the manual or tracking mode, and that this tended to deny B&W's assertion. B&W noted that it had no data available for manual operating modes of the ICS (Sholly Ex. 2, at 21 and 23).

49. Regarding the third factor upon which ICS failures are dependent, Licensee witness Joyner testified that B&W did not consider the effect of operator action on the events which were covered in the B&W study (Tr. 7086, Joyner). Tabular data in BAW-1564 shows that nearly one-third of all the trips studied in BAW-1564 had causes that were attributable to operator/technician action. Half of these trips resulted from misunderstood instructions and procedures, manual control errors, and valve mispositioning (Licensee Ex. 18, at 5-11 through 5-13). Regarding trips caused by valve mispositioning, B&W has stated that the ICS is not

designed to deal with many abnormal situations such as odd alignment of equipment (Sholly Ex. 2, at 23).

50. Apart from these concerns, the Board finds that the ORNL/SAI review of BAW-1564 has identified a number of other weaknesses in the B&W reliability analysis. ORNL found that the B&W analysis in BAW-1564 utilized a technique that is not suited for analyzing multiple failure situations (Sholly Ex. 2, at 8). Since the ICS is not safety-grade (Tr. 7041, Joyner; Tr. 5711, Lanese) and it does not meet the single-failure criterion (Licensee Ex. 18, at 4-2), the Board can find no basis for assuming that multiple failures are not credible events with respect to the ICS. In fact, ORNL found that since there is insufficient evidence to the contrary, multiple-failure-induced transients may have a significant probability of occurrence (Sholly Ex. 2, at 8).

51. ORNL judged multiple failure events involving the ICS to be significant since single failures within the ICS can occur without being annunciated, and can go undetected by plant personnel until the failed component is called upon to function when a second component fails (Sholly Ex. 2, at 8). B&W notes in BAW-1564 that very few failures within the ICS are self-annunciated to plant operators (Licensee Ex. 18, at 4-2).

52. BAW-1564 points out, and Licensee witness Joyner confirmed, that the only failures considered in the FMEA were single failures of ICS inputs, ICS outputs, and ICS functional blocks, failed one at a time. No combinations

of these failures nor any other type of failure were considered in the FMEA (Licensee Ex. 18, at 4-1; Tr. 6964, Joyner).

53. Specifically, the B&W analysis failed to consider mid-scale failures, undetected failures, and multiple failures due to common causes (Sholly Ex. 2, at 8). Whereas B&W explicitly assumed that "high-scale" or "low-scale" failures represented the worst case (Tr. 6965, Joyner), the NRC Staff testified that at least in some cases, mid-scale failures might be worse than high- or low-scale failures (Tr. 15,896, Capra). ORNL could find no specific evidence to support B&W's position on mid-scale failures and, to the contrary, pointed out that operating experience confirms that mid-scale failures are highly credible events (at least for cases involving multiple input signal failures) (Sholly Ex. 2, at 21). ORNL pointed to the Rancho Seco event on March 20, 1978 (the so-called "light bulb incident") as an example of such a failure (Sholly Ex. 2, at 21). An NRC Staff review of overcooling transients in B&W plants noted in particular that the turbine bypass and atmospheric dump valves at Rancho Seco are designed to fail to the 50% position on loss of ICS power (UCS Ex. 35, Reference 1, at 5).

54. ORNL concluded that mid-scale failures of inputs to the ICS are of particular concern because there may be a simultaneous adverse impact on the ICS and other key systems, and because such failures may remain undetected and thus contribute to multiple component failure events (Sholly Ex. 2, at 8).

55. The NRC Staff confirmed that it had not analyzed even the ICS cabinets for possible multiple failures (Tr. 15, 394, Capra), with the possible exception of so-called "cascaded failures" (Tr. 7235, Thatcher). The Staff could point to no study, report, or analysis which was concerned with multiple failures in the ICS and their potential impact on the plant (Tr. 7240, Thatcher).

56. Multiple failure events involving the ICS have been identified, however. Licensee witness Joyner testified that if multiple failures are assumed, the ICS can cause emergency feedwater valves in both OTSG's to go to the full open or full close position (Tr. 7039-40, Joyner). Another Licensee witness noted that if the pressure in a steam generator drops below 600 pounds, the steam line rupture detection system will isolate that steam generator (this event is within the design basis of TMI-1). Assuming a subsequent failure after the isolation of the steam generator, a single ICS failure could cause a total loss of feedwater (Tr. 5730-31, Lanese).

57. A second weakness noted by ORNL in its review of BAW-1564 is B&W's use of the functional block approach in analyzing failures internal to the ICS cabinets. B&W expressed the view that very few observations made by B&W as a result of utilizing the functional block approach would be in error, but ORNL noted that an example of incorrect or incomplete conclusions arising from this approach is that failure considerations involving turbine bypass valve control

do not include details of whether condenser cooling is actually available, and whether the control will be transferred to the condenser dump or to the atmospheric dump. Also not included in such situations was any consideration of operator actions (Sholly Ex. 2, at 20).

58. Although ORNL agreed with B&W that functions can fail because of equipment failures, ORNL pointed out that it is not clear that in using the functional block approach (as opposed to the equipment block approach) that there are no undisclosed couplings or interactions of blocks. An example of common elements that may involve multiple functional blocks is the arrangement of power supplies and their protective features (such as fuses and breakers) within the ICS (Sholly Ex. 2, at 6).

59. The third weakness in the B&W analysis relates to the computer model used by B&W to simulate plant response to ICS failures. The hybrid computer model upon which the computer simulations of ICS failures were run is based on the ICS at the Rancho Seco nuclear plant (Sacramento Municipal Utility District, or SMUD) (Licensee Ex. 18, at 4-1). It should be noted that Ranch Seco has a Model 820 ICS, whereas TMI-1 has a Model 721 ICS (Tr. 6986, Joyner; Sholly Ex. 2, at 23).

60. The computer model used by B&W, POWER TRAIN IV (PT-IV) models the ICS (which is an analog system) as a digital system based on functional blocks. As a result, the same weakness in general approach cited by ORNL (using the

functional block approach rather than the equipment block approach) was carried through into the B&W computer simulation model as well. The computer model was used to determine the effect on the plant of ICS failures (Sholly Ex. 2, at 12 and 22).

61. There are other problems with the computer simulation as well. There are limitations inherent in the PT-IV programming, including limitations on primary system pressure (limited to 1500-3000 psi), secondary system pressure (500-1500 psi), primary and secondary system temperatures (400-700 degrees F.), and limits on feedwater temperature (350-700 degrees F.) (Sholly Ex. 1, at 4).

62. Further, a single feedwater valve is used to represent all feedwater valves. In general, there is not much detail of the feedwater system. A more complete model of the feedwater system would include pump drains, flash tank levels and condensate pumps as well as main feed pumps. The condensate pumps have suction pressure trips that sometimes actuate when the interceptor valves close; this is not modelled in the PT-IV simulation either (Sholly Ex. 1, at 5).

63. The Board also notes B&W's admission that the PT-IV computer model is not valid at low power (Sholly Ex. 2, at 22). The lack of detail in the feedwater system in B&W's computer model, which B&W used to determine the effects on the plant of ICS failures, is very disturbing to the Board since the response of B&W reactors to feedwater transients is the main reason why the ICS was studied in the first

place (10 N.R.C 141, at 142, 1979).

64. Another weakness in the B&W study of the ICS which was identified by ORNL is the failure of B&W to consider control systems interaction. ORNL concluded that interactions among control systems (including human operators) and controlled equipment may result in a transient even though no specific equipment failure has occurred. In fact, ORNL found that it would not be impossible for peculiar operating conditions or equipment interactions to place the ICS at such a disadvantage that it would respond, although as designed, in an undesirable manner. According to B&W, the ICS is not designed to deal with many abnormal situations such as odd alignment of equipment (Sholly Ex. 2, at 7 and 23).

65. The issue of control systems interaction with controlled equipment is important, having been recently classified by the NRC Staff as an "unresolved safety issue" (Tr. 15,765, Ross).

66. ORNL also found that BAW-1564 failed to respond in a meaningful way to concerns about the ICS and the rate at which protective features are called upon to respond to transients. ORNL found that BAW-1564 failed to address whether the ICS can cause the plant to malfunction in a credible way so that the protective systems cannot handle the problem. B&W seldom carried consideration of a particular event beyond reactor trip, if the trip occurred. ORNL concluded that neither of these two concerns can be answered meaningfully

by consideration of only a relatively small portion of the entire control structure, such as the ICS was defined in BAW-1564 (Sholly, Ex. 2, at 6-7).

67. BAW-1564 also failed in many cases to pursue the effect of operator posttrip actions, and failed to pursue the posttrip operation of the ICS, even though the ICS controls equipment that is important in posttrip situations. For example, ORNL suspects that some failure modes of the ICS could initiate a loss of feedwater event and then inhibit emergency feedwater flow via the flow control valves, but the limitations placed by B&W on consideration of posttrip actions of operators and posttrip actions by the ICS eliminated consideration of such sequences (Sholly Ex. 2, at 6).

68. Operator posttrip action may be a significant factor in determining the severity of feedwater transients. The Rancho Seco event of March 20, 1978 was classified as the most severe and prolonged overcooling transient experienced to date and was initiated by a loss of NNI/ICS power (UCS Ex. 35, Reference 1, at 4-5). That event could have been made worse through human inaction, such as failure to partly secure emergency feedwater or prolonged inattention to OTSG heat removal (UCS Ex. 35, Reference 1, at 6). Human error probabilities in such situations may be high; a preliminary assessment of overcooling transients in B&W reactors performed by the Acting Chief of the Reliability and Risk Assessment Branch of the NRC's Division of Safety Technology postulates a human error probability, assuming that the operator is

already trained to stay within pressure-temperature limits and maintain adequate primary system subcooling, of 0.6 for a situation in which inadequate instrumentation to monitor transients is unavailable due to NNI/ICS power failure and there is over 30 minutes to respond to the event (UCS Ex. 35, Reference 3, at 6-7). The assessment noted that there may be an uncertainty in the estimated human error probability of a factor of 2 to 10 (UCS Ex. 35, Reference 3, at 7).

69. Another possible weakness in BAW-1564 is the description of the effects of failures provided by B&W. ORNL apparently did not delve deeply into this problem, but they did cite an important example. According to B&W, they used a combination of computer simulation on POWER TRAIN IV and engineering evaluation of the ICS and the primary system response to determine "the worst credible NSS effect" of ICS failures (Licensee Ex. 18, at 4-21). The example cited by ORNL relates to the effects of steam generator overfill occasioned by an ICS failure. B&W described the consequences of the event as ". . . overcooling of the primary, and possible loss of pressurizer inventory and/or level indication." (Licensee Ex. 18, at 4-33 as cited in Sholly Ex. 2, at 11). ORNL cited another description of the same event which appeared in an NRC meeting summary prepared by Staff witness Capra (Sholly Ex. 2, at 12):

> "The resultant carry-over of liquid into the main steam lines could lead to equipment damage to both the main turbine and any auxiliary turbines (i.e., AFW pump turbines) being supplied steam from the main steam system. In addition, the carry-over could lead to excessive waterhammer. It is also possible that the weight of the water in the steam lines could cause excessive stresses on the piping system and pipe supports."

While taking no position on the appropriateness of either description, ORNL notes that the latter description places "a greater emphasis on the potential need for remedial action" (Sholly Ex. 2, at 12).

70. Overcooling transients are of particular concern to this Board since the Licensee has testified that TMI-1 is sensitive to overcooling transients and that the ICS is usually a contributor to such events (Tr. 5881, 5888, Lanese). In this regard, the Board notes the recent Board Notification on the subject of pressurized thermal shock to PWR reactor vessels (BN-81-06, UCS Ex. 35, cover letter at 1). The Staff presented a witness near the end of the proceedings to address this issue, but the witness's ability to respond to cross-examination on the matter was limited, and the Board noted its displeasure with the quality of the record which was created on this issue. Despite this, neither the Staff nor the Licensee proposed any remedy for clarifying the record on a matter of some significant importance.

71. In summary, the issue is as follows. Severe

overcooling events can be followed by repressurization, resulting in a relatively high primary system pressure (1500-2100 psig) while primary system temperature decreases significantly (down to the 280 degrees F. range). Such events can be caused by instrumentation and control system malfunctions (such as loss of power to ICS/NNI), and postulated accidents such as small-break LOCA's, main steamline breaks, and feedwater pipe breaks. Rapid cooling of the reactor vessel internal surface causes a temperature distribution acorss the RV wall, resulting in a thermal stress. This thermal stress combines with the "hoop stress" caused by the internal pressure in the RV. As long as the fracture resistance of the RV remains high, such events will not cause failure of the reactor vessel. Neutron irradiation during plant operation reduces the fracture toughness of the vessel. Once reduced sufficiently, severe thermal transients can cause fairly small cracks near the inner surface. If these cracks propogate, reactor vessel failure can occur. The reactor vessels which are of concern are those with a history of high radiation exposure and which are made of material that has a high sensitivity to radiation damage (such as those made with high copper content welds). For failure to occur, a number of contributing factors must be present: (a) a reactor vessel flaw of sufficient size to propogate, (b) high copper content welds, (c) relatively high level of irradiation, (d) a severe overcooling transient with repressurization, and (e) a resulting crack of such

size and location that the ability of the RV to maintain core cooling is affected (UCS Ex. 35, Attachment to 4/28/81 memo from Eisenhut to Denton and Case, at 1-2).

72. The Staff has concluded, based on a preliminary evaluation, that the probability of an overcooling transient similar to or greater in magnitude than the March 20, 1978 Rancho Seco event is about $10^{-3}$ per reactor year for B&W-designed plants (the Rancho Seco transient represents the most severe overcooling transient experienced by any PWR in the U.S.). The safety concern associated with such an overcooling transient (i.e., the probability of vessel failure following pressurized thermal shock) increases with neutron irradiation time (UCS Ex. 35, cover memo, BN-81-06, at 2).

73. The Staff concludes that even if another Rancho Seco-type event occurs at a B&W facility over the next "few years" that RV failure would be "unlikely." Nontheless, the Staff could not rule out the possibility that vessel failure could occur as a result of an overcooling transient (UCS Ex. 35, 4/28/81 memo from Eisenhut to Denton and Case, at 2). Regarding the Rancho Seco transient, the Staff has concluded, based on an evaluation by ORNL, that if the Rancho Seco event had occurred after ten effective full power years (EFPY's) of neutron irradiation (more than twice its current level), "the probability of failure of the Rancho Seco vessel would have been very high" (UCS Ex. 36, at 2).

74. One of the factors which governs the probability of vessel failure following pressurized thermal shock is the

copper content of the welds on the reactor vessel (UCS Ex. 35, BN-81-06, cover letter, at 1). The Board notes the testimony of Staff witness Klecker that Rancho Seco's RV has welds with a copper content of 0.23%, while TMI-1's welds have an even higher copper content of 0.31% (Tr. 21,445, Klecker). Staff witness Klecker characterized the TMI-1 weld copper content as being "in the high range" (Tr. 21,427, Klecker).

75. Another factor which governs the probability of vessel failure following a pressurized thermal shock is the degree fo neutron irradiation of the vessel. Witness Klecker testified that in general for B&W reactors this concern becomes effective at about 10 EFPY's. TMI-1 has accumulated 3.45 EFPY's of neutron irradiation (Tr. 21,447, Klecker). There is disagreement within the Staff, however, on when the concern becomes effective. One reactor safety engineer on the NRC has stated, in a letter to Congressman Morris K. Udall (dated 4/10/81), that in his view the level of neutron irradiation which represents a "dangerous level" with regards to possible vessel fracture following a pressurized thermal transient is "probably as low as 4 EFPY of opertion with vessels with high copper alloy wells or welds" (UCS Ex. 35, Reference 5, at 1). This same engineer (Demetrios L. Basdekas) also states in the same letter that the Rancho Seco transient of March 20, 1978 is not as severe as can be expected on a "reasonable worst case basis", and that there has been discovered a discrepancy between the estimated versus the measured values of neutron fluence for the Maine

Yankee reactor vessel which, in his view, indicates a generic problem that "makes things worse." Mr. Basdekas proposed that all PWR's with high copper content welds which have operated for 4 EFPY be shut down until the issue is resolved (UCS Ex. 35, Reference 5, at 1-2).

76. Regarding another factor which determines the probability of reactor vessel failure following pressurized thermal shock, the presence of a reactor vessel flaw of sufficient size to propogate, Staff witness testified that the Staff does not have sufficient statistics to tell what the probability is for a small crack existing in the reactor vessel (Tr. 21,447, Klecker).

77. The Staff witness could not specify at what level of neutron irradiation between TMI-1's current level of 3.45 EFPY and the generic level of concern at 10 EFPY the level of concern about reactor vessel failure following pressurized thermal shock increases, other than to state that the effect is highly nonlinear and that it would take vessel specific calculations to determine the precise number for TMI-1 (Tr. 21,453-54, Klecker).

78. The Board is not at all satisfied with the state of the record on this matter. Reactor vessel failure is an extremely serious matter. It is widely known, and the Board herein takes official notice of the fact, that reactor vessel failure is beyond the design basis of any currently licensed commercial nuclear reactor. The Board notes that severe overcooling transients (as defined by the Staff,

an overcooling transient which causes the cooldown rate of 100 degrees F./hour to be exceeded) are not limited to high power operation. Indeed, there are several events described by the Staff which have occurred at relatively low power levels: (a) the Rancho Seco event reported on 10/8/79 which was initiated at about 15% power, (b) the Oconee-3 event reported on 6/27/75 which was initiated at about 15% power, (c) the TMI-2 event on 12/2/78 which was initiated at 22% power, and (d) the Davis Besse event of 4/29/78 which was initated at about 20% power (UCS Ex. 35, Enclosure 1 to Reference 1, at 2, 3, and 4).

79. The Staff presented the only witness and then only by oral testimony in response to cross-examination, Neither the Staff nor the Licensee cross-examined the Staff witness on substantive matters related to the reactor vessel fracture issue.

80. The Staff witness, Mr. Klecker, by his own admission had no formal education in materials science or materials engineering, but had rather learned about the matter by experience (Tr. 21,419, Klecker). The witness could not answer questions which appear to the Board to be critical to the issue. For example: (a) the witness could not quantify the probability of vessel failure other than, indirectly, to indicate that the probability falls between $10^{-4}$ and 1, and that it probably would not be that low or that high (Tr. 21,447-451, Klecker); (b) the witness could not quantify, even roughly, the probability of the failure of the TMI-1 vessel if at 10 EFPY of neutron irradiation

the TMI-1 vessel underwent a Rancho Seco-type pressurized thermal shock (Tr. 21,448, Klecker); (c) the witness could not specify when the neutron irradiation level for TMI-1 would become of concern for such an event other than to reference the generic level of 10 EFPY, despite the fact that the TMI-1 copper content in the reactor vessel welds is about 35% greater than the copper content at Rancho Seco upon which the generic figure is apparently based (Tr. 21,448, Klecker).

81. Of additional significance, and perhaps most to the point, the Staff has been aware of the potential seriousness of this matter for some time. This issue is the subject of a NUREG-0737 requirement for B&W reactors (Item II.K.2.13, page 3-129); NUREG-0737 was issued in draft form as a clarification letter to the Licensee on September 5, 1980, and the final version was issued in November 1980. The requirement in this regard was that by 1/1/81 the Licensee shall submit the results of their thermal-mechanical report. According to the Staff's SER on NUREG-0737 items outside the Commission's August 9, 1979 Order (dated 4/22/81), the Licensee did not comply with this requirement until 2/23/81, over seven weeks late. The Staff has had information on the frequency of severe overcooling transients since October 29, 1980. Despite this, the Staff made no apparent effort to inform this Board about the serious issue of possible reactor vessel failure following a pressurized thermal shock until the Board

Notification (BN-81-06) was issued on May 8, 1981, nearly seven months after the start of the evidentiary hearing and only days of hearing time prior to the anticipated close of the record.

82. The Board finds a distinct void in the record on this matter. The Board cannot understand the failure of the Staff (or the Licensee for that matter, who cannot be presumed to have been totally uninformed on this issue) to bring this matter to the Board's attention promptly. Failing this, the Staff put on a witness who could obviously not respond substantively to cross-examination on the issue, and both the Staff and the Licensee utterly failed to cross-examine the witness on substantive matters. After hearing the Board's displeasure with the quality of the record on the issue, the Licensee nor the Staff made any suggestions or made any effort whatsoever to suggest how the record might have been completed.

83. The burden of proof in this proceeding is clearly on the Licensee (10 C.F.R. §2.732). This very point was brought forward by the Commonwealth of Pennsylvania well before the start of the evidentiary hearing (See, Commonwealth of Pennsylvania's Report on Positions Formulated Based on Information Available as of July 25, 1980), and no party controverted this basic legal point. The Board finds nothing to persuade it that the situation is other than as stated above. On the issue of possible reactor vessel fracture following a pressurized thermal shock,

the Licensee has clearly not met the burden of proof. Based on the record on this issue, the Board most emphatically disagrees with the Staff's evaluation that there is no reason to delay the restart of TMI-1 pending further resolution of this issue (NRC Staff, Safety Evaluation Report on NUREG-0737 items outside the Commission's Order, 4/21/81, at II.K.2.13-1). This issue is of such concern that there is no basis for a finding of reasonable assurance that TMI-1 can be operated without endangering the public health and safety.

84. The Board wishes to make it clear that the burden does not fall entirely on the Licensee, however, since it is the Staff's obligation to inform Licensing Boards of significant developments. This obligation does not arise when the Staff has completed its own evaluation, but rather arises immediately upon the Staff's discovery of the information. Virginia Electric & Power Co. (North Anna Power Station, Units 1 & 2), CLI-76-22, 4 N.R.C 480, 491 (1976); Consolidated Edison Company of New York (Indian Point Station, Units 1, 2, & 3), CLI-77-2, 5 N.R.C. 13 (1977). In this case, the Staff has failed in discharging its obligation.

85. Returning to the reliability analysis, the Board now addresses the conclusions of the Licensee and the NRC Staff regarding the ICS and the adequacy of the reliability analysis. Licensee's conclusions are fourfold: (a) the reactor core remains protected for any ICS failure which was studied, (b) for postulated ICS failures which

cause reactor trip, safety systems operate independently of the ICS malfunction, (c) ICS hardware performance has not led to a significant number of reactor trips, and (d) the ICS has prevented more trips than it has caused, thereby resulting in a decrease in the number of challenges to the reactor protection system (Broughton, Sadauskas, & Joyner, ff. Tr. 6949, at 3).

86. Regarding Licensee's first conclusion, the Board notes that BAW-1564 does not consider any type of multiple failure (Tr. 6964, Joyner; Licensee Ex. 18, at 4-1), despite the fact that the ICS is not a safety-grade system and does not meet the single-failure criterion (Tr. 7041, Joyner; Tr. 5711, Lanese; Licensee Ex. 18, at 4-2). The Board also notes that the FMEA did not consider even single failures of ICS components, inputs or outputs during off-normal conditions of plant operation, even though such conditions are allowed conditions of operation and their occurrence is not uncommon (Sholly Ex. 2, at 10-11). The Board further notes that the Licensee has not analyzed the impact on the plant of a total power failure to the ICS (Tr. 6991, Sadauskas). This may be significant since both the NNI and ICS receive power from the same power sources (Tr. 5716, Capodanno), and, in instances where NNI/ICS power is lost, such events can both initiate a transient and "blind" the operator due to lack of information caused by the power failure (UCS Ex. 35, Reference 3, at 4).

87. The Board also notes that B&W's analysis did not consider the effects of operator actions (or inaction) in its analyses (Tr. 7086, Joyner). At best, therefore, assuming, arguendo, that all safety systems work as designed and that B&W's analysis is complete in all other respects (which the Board does not believe is the case), the Licensee has demonstrated that for single failures of ICS inputs (except power supplies), ICS outputs, and ICS internal functional blocks as defined by B&W, the reactor core remains protected. The Board would regard this is a very minimal demonstration with somewhat less than a great deal of safety significance. The Board agrees with ORNL on this point--the B&W analysis simply did not go far enough, therefore the results of the analysis are of limited value (Sholly Ex. 2, at 4).

88. Regarding Licensee's second conclusion, the Board notes ORNL's finding that the B&W analysis presented in BAW-1564 does not answer in a meaningful way the question of whether the ICS can cause the plant to malfunction in a credible way so that the protective systems cannot handle the problem (Sholly Ex. 2, at 7). Further, the Board notes that B&W failed to address the effect of operator posttrip actions, nor did B&W address the posttrip operation of the ICS despite the fact that ICS controls equipment that is important in posttrip situations (Sholly Ex. 2, at 6). The Board also notes that B&W did not postulate any multiple failures, thus greatly decreasing the

significance of Licensee's second conclusion.

89. Regarding Licensee's third conclusion, the Board notes that this conclusion is highly dependent on the definition of the ICS (Sholly Ex. 2, at 6). The Board finds that if ICS internal failures, ICS control response, and ICS input failures are considered (the latter is reasonable since it is the control response of the ICS to the failure that leads to the reactor trip; Tr. 15,874-74, Capra), the ICS may be found to have caused 56 reactor trips out of the 310 studied by B&W (Licensee Ex. 18, Table 5-1, at 5-11). This total of 56 trips does not include any trips which may have resulted from operator error in taking over manual control of the ICS, nor does it include any trips which may have resulted from operator error in misunderstanding an instruction or procedure, even though in both of these cases the NRC Staff has conceded that such trips may have occurred (Tr. 15,885-86, Capra).

90. Reactor trips are not the only result of ICS failures which are of concern to this Board. NUREG-0667 reveals that there were 29 failures of NNI/ICS power supplies through the spring of 1980. Twenty of these failures resulted in reactor trips, and nearly all of these were accompanied by feedwater transients. Six of these events resulted in overcooling transients in excess of permissible cooldown limits. In addition, four actuations of high-pressure injection (HPI) were experienced during these NNI/ICS failures (UCS Ex. 35, Reference 1, at 5).

91. The Board also notes the unresolved concern about the participation of ICS in feedwater oscillations (Sholly Ex. 2, at 9).

92. Regarding Licensee's fourth and final conclusion, the Board finds ORNL's finding that while this may be true, it is not substantiated by historical data nor by the FMEA to be particularly significant (Sholly Ex. 2, at 11). The Licensee is also relying, in making this conclusion, on data from the Rancho Seco plant, which utilizes a Model 820 ICS, whereas TMI-1 utilizes a Model 721 ICS (Tr. 7082-84, Joyner). Although the Staff disagreed, both ORNL and B&W found the Model 820 ICS to be more reliable than the Model 721 ICS (Sholly Ex. 2, at 13; Licensee Ex. 18, at 5-10). The Staff's position is that there is an inadequate statistical base upon which to make a comparison, and ORNL agrees to a limited extent (Tr. 7142, Thatcher; Sholly Ex. 2, at 13). B&W concludes that the 820 Model ICS had improved reliability when compared with the Model 721 ICS due to a number of major hardware changes, including (Licensee Ex. 18, at 5-8, 5-9): (a) extensive use of integrated circuits, (b) use of a single printed circuit board as opposed to the mother board/daughter board concept, (c) elimination of module level power supplies, (d) greatly decreased use of aluminum electrolytic capacitors, (e) elimination of most internal wiring, (f) a change in the type of relays used, and (g) in general, a system which generates less heat in operation.

93. B&W found significant differences in the mean time between failure (MTBF) for the two ICS models. The MTBF for the Model 721 ICS is between 2754 and 3660 hours, whereas the MTBF for the Model 820 ICS is between 33,000 and 49,000 hours, a difference of an order of magnitude in MTBF's for the two ICS models. It is B&W's view that the hardware design changes made in going from the Model 721 ICS design to the Model 820 ICS design account for the difference in MTBF's (Licensee Ex. 18, at 5-9).

94. The Staff's conclusions are different from the Licensee's conclusions. Staff witness Thatcher concluded that the present ICS has a low failure rate and does not initiate a significant number of plant upsets. The Board disagrees. The Board finds that ICS failures are responsible for between 1/5th and 1/6th of all reactor trips on B&W reactors. Twenty trips, nearly as many feedwater transients, six severe overcooling transients, and four automatic HPI acutations have resulted from the failure of a single input to the ICS (power supply) (UCS Ex. 35, Reference 5, at 5), and this input was ignored in the FMEA and considered only in the historical operation data (this results from B&W's definition of the ICS boundary as excluding power supplies as an ICS input; Licensee Ex. 18, at 1-1).

95. The Staff also concludes that anticipated failures of and within the ICS are adequately mitigated by plant safety systems and that many potential failures would

mitigated by cross-checking features of the ICS. The Board's findings regarding the superficial nature of the "anticipated failures" of the ICS are as applicable to the Staff's findings as they are to the Licensee's similar findings. The B&W analysis was simply too limited to be very useful in this regard. The only "anticipated failures" the Staff seems to be concerned with are those single failures analyzed by B&W. As the Board observed earlier, it is not reasonable to assume that only single failures will occur, since the ICS is not safety-grade and does not meet the single-failure criterion. Regarding the Staff's reliance on "cross-checking" features of the ICS to mitigate many ICS failures, the Board agrees that to an extent this is correct. However, the Board also notes ORNL's admonition that cross limits, though useful, are not infallible (Sholly Ex. 2, at 14). Indeed, since there is no evidence which suggests that the cross-limiting features of the ICS are of higher reliability than other ICS components, the Board finds no basis for assuming that such devices cannot also fail, especially since such devices can fail without being annunciated, thereby "announcing" their failure when they are called upon to function and do not.

96. The Staff also places a great deal of reliance on procedures and design changes that will be in place at the time of restart regarding feedwater control independent of ICS. While the Board agrees that this will provide some benefit, the degree of improvement is not clear and remains

unquantified. Further, the Board sensitive to the fact that many ICS failures are not annunciated to the plant operators, and the plant operators need to promptly recognize failures in order to implement the proper emergency procedures for dealing with the failure.

97. The Staff testified that its conclusions that the ICS has a low failure rate and does not initiate a significant number of upsets are based "mostly" on operating experience as presented in BAW-1564, and that the FMEA did not have any impact on these conclusions (Tr. 7270-72, Thatcher). The Board is aware of the Staff's own expressed concerns about the adequacy of the operating history data base with regards to the ICS (Tr. 15,771-72, Capra). The Board also finds a conclusion by ORNL particularly significant in this regard (Sholly Ex. 2, at 7):

> "The supplementary operating statistics indicate that the control system is of reasonable reliability, but they also give a somewhat hazy image of a system that has some performance deficiencies. It does not appear to be an unworkable system, but it falls short of being a strong influence for safety." (Board's emphasis)

ORNL further stated that the operating statistics should not be regarded as a source of insight into the sensitivity of the plant to the ICS (Sholly Ex. 2, at 13).

98. The Staff later stated during the proceeding

that during the time period since the B&W analysis (BAW-1564), the Staff had not identified any additional concerns regarding the role of the ICS in feedwater transients (Ross & Capra, ff. Tr. 15,855, at 7-8). The Board has been presented with no evidence which even suggests that additional studies of the ICS have been undertaken in this time frame, therefore the Staff's statement is hardly a surprise. More importantly, however, the Board finds that the five original concerns that the Staff expressed about the ICS at the April 25, 1979 Commission meeting have still not been fully resolved, Staff representations in testimony notwithstanding. The Board will address these five concerns individually.

99. The first concern expressed by the Staff was concerned with the reliability of the ICS (Ross & Capra, ff. Tr. 15,855, at 2). The Staff relies on their interpreration of the operating history of the ICS which leads them to conclude that only 6 trips have been caused by ICS failures and that the Staff has found no evidence which suggests that the ICS provides more frequent or more severe challenges to the plant protection systems than other control systems of similar scope (Ross & Capra, ff. Tr. 15,855, at 4). This conclusion is apparently based on the ORNL review of BAW-1564 (Sholly Ex. 2, at 14). The Board has already stated its disagreement with the Staff view on the number of trips caused by ICS failures and will not reiterate that matter here. On the latter point, the Board finds no evidence in the record

which addresses whether the revised PORV and reactor trip setpoints have increased the frequency of challenges to the reactor protection system, only the Staff's naked conclusion that the answer to the question is in the negative. The Board has found information to the contrary. The Board was requested very late in the proceeding to take official notice of certain portions of NUREG-0667. One of the matters brought to the Board's attention in this request was the conclusion, at least by the Task Force which prepared NUREG-0667, that since the inversion of the PORV and reactor trip setpoints following the TMI-2 accident, the responsiveness of the B&W design to undercooling events reflects a high challenge rate to the plant protection system. The Board is compelled to take official notice of this fact in the context that it presents a contradictory conclusion to a Staff position taken in the proceeding which was not addressed by the Staff's witnesses (NUREG-0667, at 5-20). The fact that this different conclusion was not raised by the Staff is especially puzzling to the Board since the Staff's conclusion that there has been no increase in protective system challenges as a result of the ICS operation was sponsored in part by Staff witness Capra, who also served as the Editor for NUREG-0667 (Capra, Statement of Professional Qualifications, ff. Tr. 15,855, at 3).

100. The fact that inverting the PORV and reactor trip set points would result the reactor trip circuit being challenged "far more often" was acknowledged by Staff witness Ross (Tr. 15,882, Ross).

101. The third concern raised by the Staff is that the ICS may initiate 10-15% of all feedwater transients (Ross & Capra, ff. Tr. 15,855, at 5). The Board notes that the witnesses' response to this concern was to discuss the number of reactor trips caused by ICS failures. This, in the Board's view, totally misses the point. Again, in response to a motion to take official notice of certain facts in NUREG-0667, the Board's attention was drawn to the conclusion of the B&W Transient Response Task Force that NNI/ICS power failures alone caused 18% of all observed feedwater transients in B&W plants through the period of that study (spring of 1980) (NUREG-0667, at 4-8). Again, the Board is compelled by a void in the record to take official notice of this fact. Neither the Staff nor the Licensee has addressed how much improvement will result in power supply reliability from improvements in power supplies undertaken by the Licensee, nor has either the Staff or the Licensee addressed the degree of improvement to be expected from improved ICS/balance of plant tuning, both of which were cited by the Staff as "proof" that this concern had been resolved (Ross & Capra, ff. Tr. 15,855, at 6). The Board cannot, as a result, find that this matter has been completely resolved.

102. The fourth concern expressed by the Staff, regarding ICS control of emergency feedwater, has been resolved for the long term in the Board's view by provision for EFW control completely independent of the ICS. For the interim period during which procedures will be available for accomplishing EFW control independent of ICS, the Board is concerned about the likelihood that the operators may not be able to promptly detect ICS failures involving EFW control due to lack of annunciation of many ICS failures and the problems involved with mid-scale failures. Neither the Staff nor the Licensee addressed this problem.

103. The fifth and final concern expressed by the Staff regarding the ICS relates to the sensitivity of the B&W design and feedwater oscillations. The Board agrees with the Staff that some of the recommendations in BAW-1564 are aimed at reducing this sensitivity, but the Board can find in the record no qualitative or quantitative information as to the degree of reduction in this sensitivity. Furthermore, the Board reiterates its conclusion (as noted by ORNL) that B&W used methodology in BAW-1564 that was incapable of evaluating the involvement of the ICS in feedwater oscillation.

104. The Board, as a result of these facts, must disagree with the Staff and conclude that the B&W reliability analysis as performed and documented in BAW-1564 did not resolve the concerns which occasioned the study. As observed by ORNL, ". . . the B&W analysis is more notable for what it does not include than for what it does include." (Sholly Ex. 2,

at 3). In the Board's view, BAW-1564 and the ORNL review of BAW-1564 raised far more questions than they answered. It it the Board's view that the Staff looked at the ORNL conclusions which supported the Staff's position on the adequacy of the reliability analysis, and conveniently ignored other findings and recommendations.

105. The Board found recommendations made by ORNL which were ignored by the Staff and the Licensee (and, apparently, by B&W as well) which appear to the Board to address some of the outstanding concerns raised by the B&W reliability analysis. In summary form, these recommendations are:

a. Despite apparent agreement among the Staff, B&W, ORNL, and several B&W licensees that additional work was needed, no additional work appears to have been initiated on the subject of the detection and annunciation of ICS failures. There was apparent agreement at a group meeting that such additional study was needed because of the fact that many ICS failures are not self-annunciated and may remain as undetected failures for long periods of time, thereby leading to multiple failure incidents (Sholly Ex. 1, at 6).

b. Power supplies for ICS input instrumentation were not addressed in the FMEA, and although B&W agreed that more work in this area needed to be done, no such work has been brought to the attention of this Board (Sholly Ex. 1, at 6).

c. ORNL recommended that a fault tree analysis be performed for the loss of feedwater event using an equipment block diagram. The results should be used to

judge whether it would be appropriate to develop additional fault trees for other major events involving the ICS (Sholly Ex. 2, at 8). The Staff referenced the development of fault trees in the ATOG program (Ross & Capra, ff. Tr. 15,855, at 5), but the Board was not presented with sufficient information to determine whether the specific event of loss of feedwater was being evaluated in a fault tree evaluation, nor was the Board able to conclude whether the ATOG work met ORNL's concern.

d. ORNL recommended that a dynamic analysis be performed on the ICS to answer the following questions:

(1) Since the dynamic response of the feedwater pump control is generally slower than that of the feedwater valves, will transition from valve to pump control of feedwater cause stability problems?

(2) Do the pressurizer controls mitigate or amplify pressure oscillations and how are the pressurizer and the ICS interdependent with regard to stability?

(3) Are feedwater oscillations caused or mitigated by the ICS?

(4) What conditions involving the ICS could lead to plant instability? (Sholly Ex. 2, at 11).

e. A full-plant simulator should be developed to evaluate the interaction of the primary, secondary, and control systems (Sholly Ex. 2, at 15).

f. Additional investigations should be performed of ICS failures (component failures) under off-normal conditions of operation, and postscram heat removal should be followed in order to demonstrate the medium-term consequences of the event and the adequacy of the computer predictions made by B&W in BAW-1564 using POWER TRAIN IV (Sholly Ex. 2, at 11).

106. The recommendations for additional study or additional actions are especially significant in the Board's view due to ORNL's conclusion that is was difficult for ORNL to assess the need for further evaluations or for potential design modifications to the ICS because B&W's analysis of the ICS in BAW-1564 was so limited (Sholly Ex. 2, at 11).

## II. SHOLLY CONTENTION 1 (Containment Isolation)

107. Both Licensee witness Lanese (Tr. 7352, Lanese) and NRC Staff witness Hearn (Tr. 7379, Hearn) comfirmed that one of the recommendations arising from NUREG-0667 was for a safety-grade high radiation containment isolation signal for the reactor building vent and purge system. Neither witness, however, could explain why the recommendation was not approved for implementation.

108. The TMI-2 accident demonstrated that significant fuel damage can occur in the absence of a high reactor building pressure signal, thus resulting in delayed containment isolation (Lanese, ff. Tr. 7349, at 3).

109. A non-safety grade high radiation containment isolation signal has always been in place at TMI-1 for the containment purge system. Licensee's witness asserted that the diverse containment isolation signals now used at TMI-1

are "superior" to a high radiation signal, and that the non-safety grade high radiation signal is acceptable because of the additional presence of the anticipatory reactor trip containment isolation signal (Lanese, ff. Tr. 7349, at 1, 4).

110. Upon cross-examination, however, it was revealed that this assessment is based on the assumption that no spurious PORV opening occurs (Tr. 7354, Lanese). Even under this case, the witness still preferred the anticipatory reactor trip signal, but provided no justification for this preference.

111. Furthermore, NRC Staff witness Hearn testified that is is possible to have the purge line open on an operating or maintenance bypass and have it fail to close on the reactor trip signal (Tr. 7384, Hearn).

112. The only radiation monitors in the reactor building at TMI-1 which are safety-grade are the containment dome monitors (Tr. 7362, Lanese). There are two nuclear plants in the U.S. with safety-grade high radiation monitors (Tr. 7350-51, Lanese), demonstrating that such instruments are available.

113. The Board concludes that a safety-grade high radiation signal isolation for the containment purge system is clearly preferable to a non-safety grade signal. The Board therefore requires the Licensee to obtain and

install a safety-grade high radiation containment isolation signal on the containment purge system as soon as practicable. In the interim, the Licensee is ordered to prepare and submit for NRC Staff review and approval, procedures which will assure that the containment purge line will be promptly isolated upon detection of a high radiation signal from the existing equipment. The Licensee shall submit these procedures to the NRC Staff and secure their approval for the implementation of these procedures prior to restart of TMI-1, and shall report an estimated date for the completion of the installation of the safety-grade high radiation isolation equipment to the NRC Staff as soon as practicable. Licensee must demonstrate reasonable progress toward completion of the safety-grade installation as a condition of restart.

## III. SHOLLY CONTENTION 13 (Plant computer)

114. Both the Staff and the Licensee agreed that the plant computer at TMI-1 is not relied upon in order to demonstrate Licensee's compliance with General Design Criterion 13 (GDC 13), but rather that compliance is achieved by the provision of hard-wired safety-grade instruments in the plant control room (Joyce, ff. Tr. 7467, at 3-5; Hamilton

& Keaton, ff. Tr. 7397, at 3).

115. Since the compliance (or lack thereof) with GDC 13 was largely the thrust of the contention, this conclusion would seem to end the Board's inquiry into the matter. This is not the case, however. The testimony on the plant computer raised, perhaps for the first time, novel issues regarding the reliance of plant operators on non-safety grade plant computers for information, which is then used to make decisions about operational maneuvers, particularly under accident conditions.

116. From this standpoint, the Board is mainly concerned about the Staff's role in reviewing plant computer systems and possible operator reliance on computers as an operational aid. The Staff witness who testified on the plant computer, Mr. Joyce, was a member of the human factors review team which examined the TMI-1 control room (Joyce, ff. Tr. 7467, at 1). The witness testified that the TMI-2 accident was an example of why the plant computer is not needed to assist operators with responding to feedwater transients or small-break LOCA's (Joyce, ff. Tr. 7467, at 4). Yet, under cross-examination, the witness revealed that he had not reviewed the TMI-2 accident sequence of events and related documentation with regard to how the plant operators may have used the plant computer (Tr. 7472, Joyce). Since the possible use of the plant computer during the TMI-2 accident appears to have been the genesis of the

contention, the Board is puzzled as to the reason the Staff put on a witness who had not at the very least assured himself by reviewing the TMI-2 accident records that the operators did not rely unduly on the plant computer. In fact, the Board wonders if any member of the Staff has examined this issue, although the general subject of the role of the computer has apparently been the subject of some work by the Staff (Tr. 7472-73, Joyce).

117. Staff witness Joyce testified that in a number of control room reviews (from a human factors standpoint), operators were observed in walk-throughs on emergency procedures, both in the plant control rooms and at simulators, and that he had never seen operators use the computer, and he had never seen emergency operating procedures reference the use of the computer (Tr. 7474-74, Joyce).

118. The witness testified, however, that he did not routinely or even periodically observe operators at the controls of the power plant while the reactor is at power. Moreover, the witness testifed that such observations would be a function of the Inspection and Enforcement Office of NRC, rather than a function of the Office of Nuclear Reactor Regulation, suggesting that no one from the human factors branch (or any branch of NRR) observes operators at the controls during actual operating situations (Tr. 7476, Joyce).

119. The witness also testified that the Staff does not review plant computers in any way (Tr. 7483, Joyce).

The Staff does not review the computer to determine its reliability, nor its adequacy for whatever use is being made ofthe computer by plant operators (Tr. 7485-86, Joyce).

120. Even though emergency operating procedures do not reference the use of the computer, neither do such procedures specifically prohibit the use of the computer (Tr. 7485-86, Joyce). The Staff's human factors consultant, Mr. Price, testified that even if operators were instructed specifically not to rely exclusively on information from the computer in the performance of their emergency functions, this would not stop the operators from using the computer in such situations (Tr. 10,587-88, Price). Licensee's witness Keaten acknowledged that Licensee has no such policy of prohibiting operators from utilizing the computer during upset conditions (Tr. 10,595, Keaten). The Staff's computer witness agreed that there is nothing to prevent the operators from using the plant computer whenever they see fit to do so (Tr. 7485-86, Joyce).

121. Licensee's witness testified that he would normally expect the operators not to rely on the computer during the first portion of a transient when conditions are changing rapidly (Tr. 10,595, Keaten). This is mostly because of the training which the operators have received and also a result of the design of the control room which would result in the operator being forced to leave his instrument panel station and go behind the main panel to

access the computer. Operators would not be expected to do this until the first portion of the transient is over and the plant has stabilized (Tr. 10,595, Keaten).

122. During this period of time, however, it would not be unusual for the Shift Supervisor or Shift Foreman to use the computer to obtain additional or backup information (Tr. 10,595-96, Keaten). During the TMI-2 accident, the Shift Supervisor and/or Shift Foreman did use the computer in this manner (Tr. 10,592-96, Keaten). The first time the operators themselves (the operators actually manipulating the controls) accessed the computer during the TMI-2 accident was at approximately 27 minutes, when the operators called up information from the computer to try to assist with their determination of whether or not the pressurizer relief valve (PORV) or safety valves were stuck open (Tr. 10,597, Keaten). In fact, temperatures from the PORV and the safety relief valves are normally accessed through the plant computer (Tr. 10,597, Keaten).

123. During the TMI-2 accident, operators also used the computer to call up "raw input" data from the computers to use to determine if control room instrumentation was operating properly (Tr. 10,598, Walsh). In general, during the TMI-2 accident, operators used the computer as a matter of convenience (Tr. 10,603, Keaten).

124. The Board finds it clear that not only did operators, including senior shift personnel such as the

Shift Foreman and Shift Supervisor, use the plant computer at TMI-2 during the TMI-2 accident, there is no reason to suspect that the operators at TMI-1 will not utilize the computer in all kinds of situations in the future. Staff witnesses in particular addressed this issue during cross examination in the proceeding, and it became abundantly clear that this is expected behavior from plant operators. Staff witness Ramirez testified that most operators at most plants have a tendency to use the process computer because it is easy to get to (Tr. 10,515, Ramirez). Staff human factors consultant Price agreed, stating that if there is a process computer present, the operators will use it because it is convenient. The witness further testified that if the computer is there, it becomes an operational aid which the operators do and will depend upon, and will attempt to use it under all conditions (Tr. 10,515, 10,541, Price).

125. Staff witness Price also testified that from a human factors viewpoint, he would be surprised if the operators did not use the computer during an upset condition, and that he would be upset if operators were told not to use the computer during upset conditions because the computer is a source of very fast information (Tr. 10,544-45, Price). Licensee witness Keaten agreed that if the computer is present, operators will attempt to use it under all conditions (Tr. 10,547, Keaten).

126. Both Staff witness Ramirez and Staff consultant Price agreed that if the computer is available, the operators will put some reliance upon it, and Price testified that in his view the operators will use the comuter as much as possible if it is present (Tr. 10,556-57, Ramirez & Price).

127. Operator utilization of the process computer raises some concerns in the Board's view. The Board is especially concerned with Staff witness Price's observation that if real system status and the process computer get out of synchronization, there could be problems if operators are trying to use computer information, and the witness thought it likely that operators would try to use the computer even in these situations (Tr. 10,545, Price).

128. The Board agrees with the general observation by the Staff that although computers are not required, it they are present as operational aids, the Staff should be concerned that the data presented is accurate and reliable (Tr. 10,514, Ramirez). Staff human factors consultant Price agreed with this viewpoint, noting that if the computer is going to be present in the control room, it should be adequate from both an engineering and a human factors point of view (Tr. 10,516, Price).

129. There have been concerns about the existing process computer at TMI-1. The Board notes that the Licensee is in the process of upgrading the computer facilities at TMI-1, including new CRT's, new printers, and new software,

but the modifications will not be completed prior to restart (Hamilton & Keaten, ff. Tr. 7397, at 7-8). Licensee witness Keaten agreed that the existing CRT system is "totally unsatisfactory" from a human factors standpoint, and noted his preference for a faster computer system at TMI-1 than is present now, asserting that a faster computer system would have distinct advantages associated with it (Tr. 10,537, 10,543, Keaten).

130. Licensee's witness could not, however, state with certainty exactly what new computer functions would be present at the time of restart, and he expressly left open the option of modifying the existing Bailly 855 computer system, even though he acknowledged that this modification would be difficult to accomplish due to the vintage of the system and the lack of replacement parts (Tr. 10,538-40, Keaten). The witness testified that the existing computer was not designed to be used under plant upset conditions, but that operators have used it under such conditions to call up specialized data points from the computer (Tr. 10,543, Keaten).

131. The Staff's control room design review report (NRC Staff Ex. 2, at 7) raised problems with the existing computer system, noting that the vintage of the system raised concerns about the reliability of information coming from the computer. Elaborating under cross-examination, Staff witness Ramirez testified that this general concern

arose from conversations with TMI-1 plant operators and with one individual who works with the computers at TMI-1 (Tr. 10,510-12, Ramirez). Witness Ramirez testified that operators had informed the human factors review team that the computer has failed in the past and is not always available, specifying that it was his understanding that availability referred both to the physical availability of the information and the accuracy of the information (Tr. 10,471, Ramirez). When asked to specify the conditions under which accuracy of information from the computer became a concern, witness Ramirez expressed the concern that it is not always immediately recognizable when the computer begins to have problems unless the computer absolutely quits operating, and it is during the period from the start of computer-related problems until the problem is discovered that there is concern about the accuracy of the information presented by the computer. The witness also testified that the operators at TMI-1 had noticed this problem as well (Tr. 10,471-72, Ramirez).

132. Staff witness Ramirez also expressed concern with the computer being slow, referring both to the printout capability and the processor capability (Tr. 10,511, Ramirez). Staff witness Price also noted problems with readability of computer displays and the response time of the computer (Tr. 10,544, Price).

133. Although expressing the view that no computer would be better than one that is too slow (Tr. 10,516),

Staff human factors consultant Price testified that if the computer is present, it will be used by the operators along with other indications, and that it is essential that the computer be at least as accurate as other indications would be (Tr. 10,516, Price). Both Staff witnesses testified that the computer is a positive influence on the operator and that it should be regarded as a tool to be used as appropriate (Tr. 10,566, Ramirez & Price).

134. Although noting his preference for the improved computer capability as proposed by the Licensee, Staff witness Ramirez agreed that the existing computer would be better than no computer, provided that the Licensee establishes a verification program to assure that computer data output is accurate and reliable, and that operator training highlight how the computer is to be utilized (Tr. 10,560-61, Ramirez).

135. The Board expressed three major concerns about the computer: (a) the timeliness of the data presented, (b) the accuracy of the data presented, and (c) the down time of the computer system and components (Tr. 10,475, Administrative Judge Little). The Board's concerns will be handled in the following manner. The Licensee is directed to establish a schedule for completing its computer upgrade and submit this schedule to the NRC Staff for approval. The schedule shall identify the components which remain to be obtained and installed, shall specify a schedule for implementing each of these items, and shall provide details of operator training to be provided on each of these components. The Staff shall

monitor Licensee's adherence to this schedule through the Office of Inspection and Enforcement, and the Staff shall assure that the Human Factors Branch of NRR is involved in evaluating the human factors adequacy of the new installation as it proceeds.

136. The Licensee is also directed, though negotiations with the Staff, to design and implement prior to restart a monitoring program to assess the reliability (both in terms of availability and accuracy) of the computer system. The monitoring program shall continue with the installation of new computer hardware and software until there is a sufficient data base upon which to make a determination as to the sufficiency and accuracy of the new computer system. The Licensee is also directed to propose appropriate modifications to the Technical Specifications to TMI-1 to incorporate this requirement along with periodic reporting requirements for the information generated by the reliability monitoring program for the process computer. The Staff is directed to monitor Licensee's reports through the Inspection and Enforcement staff.

137. The Staff, through the Office of Inspection and Enforcement (with appropriate consultation and cooperation with the Human Factors Branch of NRR), is directed to undertake periodic routine observations of TMI-1 plant operators during normal (and emergency operations to the extent feasible) operations to ascertain

the degree to which plant operators rely on the process computer, for which functions the operators rely upon the plant computer, and to what purposes the information from the plant computer is utilized. Such information, in addition to being necessary to evaluate the human factors and operational appropriateness of utilizing the process computer, will assist the Staff in reaching a determination as to what standards, if any, should be applied to process computers to ensure that they are properly designed and qualified for the purposes for which they are being utilized. This program shall also be utilized, to the extent feasible, to verify the conclusions of Staff and Licensee witnesses that operators do not rely solely on computer information as a basis for making operational decisions, especially in upset conditions.

138. Further, it is the Board's view, after examining the record on this issue, that the process computer is an important operator aid, and that the operators will rely on the computer in the performance of their duties during normal as well as emergency situations. As a result, the Board finds that it is essential that the computer be available to the maximum extent feasible, comparable with the availability desired, for example, of the Integrated Control System. The Board is therefore directing that the Licensee investigate the feasibility of powering the plant computer from Class 1E power sources, and further directs

that this feasibility study be completed promptly, before restart if possible. In the interim, the Licensee is directed to ensure that the power supply for the computer is of reliability comparable to the power supply for the ICS, at the very least assuring that the computer has redundant power sources and that there is reasonable assurance that the computer will be available in the event of a station blackout. The Staff is directed to monitor Licensee's compliance with this requirement through the Office of Inspection and Enforcement.

## IV. SHOLLY CONTENTION 15 (Human factors engineering review of control room design)

139. Both the Licensee and the NRC Staff completed reviews of the TMI-1 control room from a human factors engineering perspective. Reports on both reviews were received into evidence (Licensee Ex. 23; NRC Staff Ex. 2, with Supplement No. 1 dated April 1981). The Licensee's review was undertaken prior to the publication of any NRC guidance on how to conduct such a review, and was in response to generic criticisms of control room design which arose from the TMI-2 accident (Licensee Ex. 23, at I-1). The Staff's review was undertaken in response to

to the requirements of NUREG-0694, "TMI-Related Requirements for New Operating Licenses," generally referred to as NTOL requirements (Near-Term Operating License) (NRC Staff Ex. 2, at 1).

140. The Staff review took place during the week of July 21 through July 25, 2980. A draft control room design review report was submitted to the Licensee for comments, and the Licensee and the Staff met on October 10, 1980 to discuss the Staff's draft report. Licensee submitted a draft response to the Staff's draft control room design report on October 27, 1980, and submitted its final response on November 7, 1980. Additional discussions with the Licensee were held through early December 1980; the final Staff control room design review report (NUREG-0752) was published in December 1980 (NRC Staff Ex. 2, at 1-2).

141. The Staff conducted its review using an intensive week of observation and discussion with plant operators. An 8-9 man Staff team performed the review at TMI-1. One of the Staff team members was a human factors consultant, Mr. Harold E. Price. As guidance for the review, the Staff relied upon NUREG/CR-1580, draft control room design human factors criteria developed by Essex Corporation for the NRC (Tr. 10,486-87, Ramirez).

142. Licensee's review was conducted by an eight man team, including two human factors consultants, three members of Licensee's engineering staff, and three members

of MPR Associations, Inc. Using "Human Engineering Design Criteria for Military Systems, Equipment and Facilities (MIL-STD-1472B) as a guide, and incorporating other human factors guides as appropriate, the review team formulated a set of human factors guidelines against which the TMI-1 control room design was evaluated. The final study was published in December 1980 (Licensee Ex. 23).

143. As a result of the two human factors reviews of the TMI-1 control room design, numerous changes were recommended. Additional studies were committed to by the Licensee, and alterations to the control room were begun to correct certain deficiencies.

144. The Staff will bear a heavy responsibility for determining that the alterations to the control room which were committed to by the Licensee are carried out and that the Licensee's operations staff has been fully trained on these changes. The Staff Division of Human Factors Safety has made specific arrangements with the Office of Inspection and Enforcement to followup on the implementation of the changes to the TMI-1 control room (Tr. 10,502, Ramirez). However, a further review by the Staff human factors specialists will be necessary prior to restart because some of the changes involve inspection of changes which are simply not within I&E's capabilities (Tr. 10,503, Ramirez). An example of such an item is the implementation of color-coding of alarms to prioritize important alarms: the implementation evaluation of such an item requires a trained human

factors specialist (Tr. 10,503, Price).

145. The link drawn by the Board between the implementation of human factors improvements to the TMI-1 control room design and the training of operators in those improvements (Finding 144) is particularly important in the Board's view because of the intimate interaction between human factors engineering and operator training (Christensen, ff. Tr. 12,409, at 8). Licensee's human factors and training witness Christensen noted in particular that training can be used to compensate for control room design shortcomings (Christensen, ff. Tr. 12,409, at 6; Licensee Ex. 23, at III-13). This is especially important due to the impracticality (for the short term, at least) of a complete redesign of the control room (considering the lead time for design, installation, testing, and training of operators in the new control room design).

146. A key element in training as it is related to human factors is simulator training. Simulator training is an essential element of both initial operator training and requalification training (Long, et al., ff. Tr. 12,140, at 29). Licensee has relied upon and continues to rely upon the B&W simulator facility at B&W's Nuclear Training Center at Lynchburg, Virginia for simulator training. The B&W simulator is similar to, but not a replica of, the TMI-1 control room (Long, et al., ff. Tr. 12,140, at 29). The B&W simulator is useful for functional or conceptual training, but, because of the differences in design, it is not useful

for "reflexive" or stimulus-response type training (Tr. 12,476, Christensen), training the Board regards as proficiency training.

147. Licensee is committed in the long term to purchase a full replica simulator for use in its onsite operator training. Licensee's witness on training estimated that there would be a four-year lead time to obtain a replica simulator for TMI-1 (Tr. 12,145, Long). Purchase of such a "full-mission" simulator was recommended by the OARP Committee (Licensee Ex. 27, at 110) to improve overall operator training and permit more use of simulation (Licensee Ex. 27, at 109, 144).

148. Simulators offer unique training as compared to classroom instruction. It is impossible, for example, to evaluate shift crew interaction in written examination, but such evaluation is accomplished in simulator training, and is a very important part of simulator training (Tr. 12,264-65, Long). The simulator is utilized to develop skills which cannot be developed in the classroom (Tr. 12,201, Knief). Simulator training is used to eliminate operator candidates with low stress tolerance, and is also useful to training to reduce the stressfulness of transients and promote effective response during transients (Gardner, ff. Tr. 12,409, at 7-8).

149. Purchase and installation of an onsite replica simulator for TMI-1 would have numerous advantages. The availability of the onsite simulator would result in increased

utilization of the simulator in training programs (Licensee Ex. 27, at 109, 144; Tr. 12,257, Long). The simulator would also be used to train new operators and the engineering staff. The use of the simulator to train other personnel is also being evaluated (Tr. 12,258, Long). The simulator will also be used to examine the control room design (Tr. 12,149, Long). The Board observes that the presence of an onsite simulator will facilitate operator training regarding control room and procedural modifications, and would permit testing, under controlled conditions, of alternative control room modifications in order to find the most effective arrangement.

150. Staff human factors witneeses also agreed that simulator training is useful. Witness Ramirez testified that the use of video/audio taping in simulator conditions would reduce the objections of operations personnel to the constant observation of on-shift performance (Tr. 10,501, Ramirez). Staff witness Price noted that much more valuable experience can be gained by the use of simulators. For example, detailed analyses of operator performance can be performed, rather than simply a "right" or "wrong" evaluation (Tr. 10,501, Price). Video-taping of training on the simulator would be useful for proficiency exercises to facilitate evaluation of operator performance (Tr. 10,499, Price).

151. Licensee has implemented a new practice of reviewing all modifications to the TMI-1 control room from a human factors standpoint prior to implementation (Tr. 10,252, Walsh). Such evaluations would, in the Board's view, be greatly

enhanced by the use of an onsite simulator. Although revisions to operating and emergency procedures do not receive a similar human factors review (Tr. 10,304-305, Walsh & Estrada), the board recommends on the basis of the record developed in this proceeding, that a human factors review of procedural changes also be implemented by the Licensee. Such reviews would also be enhanced by a replica simulator which could be used to evaluate procedures to be certain that the procedures are compatible with the existing control room design at the time the procedures are revised.

152. The basis for evaluation of the TMI-1 control room was not firmly established in the Commission's regulations at the time the reviews of TMI-1 were conducted in that formal requirements had not been promulgated, nor had a final version of a regulatory guide on human factors engineering standards been published. Although the Staff disagreed (Ramirez & Price, ff. Tr. 10,452, at 6), Licensee witness Meek testified that in his view, General Design Criterion 13 (GDC 13) not only requires that adequate instrumentation be provided to monitor accidents, but implies that the arrangement of such instrumentation be logical and proper (Tr. 10,274, Meek). The Board agrees, although GDC 13 does not provide any specificity in terms of what is acceptable and what is not.

153. The Board notes that there is an ongoing process to define control room design guidelines, and recommends that the Staff complete this work and implement the guidelines as soon as practicable.

154. Before addressing the various commitments made by the Licensee regarding the upgrade of the control room design, the Board addresses itself to several areas of apparent disagreement between the Staff and the Licensee on requirements to be met before restart. A principal item of disagreement, which apparently has not yet been resolved judging from an exchange of correspondence and the Staff's Supplement No. 1 to NUREG-0752, is the provision of a backup display capability for the in-core thermocouples. Licensee's proposal is to utilize computer readout as the primary display capability, while relying upon an operator utilizing portable test equipment as the backup capability (Licensee Ex. 33, at 1; NRC Staff Ex. 15, at 11). The Staff found the backup capability to be unacceptable for four reasons: (a) in-core thermocouple information is relied upon in Licensee's inadequate core cooling procedures, (b) a similar system was shown to be inadequate during the TMI-2 accident, (c) the vintage of the present computer raises questions about the reliability of the information displays, and (d) the proposed backup system represents a poor human factors interface during stressful situations (NRC Staff Ex. 15, at 11-12).

155. To correct this problem, the Staff proposed requiring data logging or recording equipment displays capable of displaying temperature information from a minimum of 16 operable thermocouples (4 from each core quadrant) on demand in the control room. The power source for this system should

be independent of the CRT power supplies to assure redundance and reliability of displays, according to the Staff. The Staff would also require that this backup system be operational before escalation beyond 5% power (NRC Staff Ex. 15, at 11-12). The Board agrees with the Staff, and will require such a system to be operational before the Licensee is permitted to exceed 5% of rated power. The alternative offered by the Licensee is not sufficiently reliable to perform this important function, especially when it will be required under circumstances when time may be of the essence in halting or mitigating inadequate core cooling.

156. There are other areas of disagreement between the Staff and the Licensee which relate to the performance of the so-called "detailed control room design review" (DCRDR) by the Licensee. It is apparently the Licensee's position that Licensee Exhibit 23 represents its DCRDR; the Staff's position on this is not clear, but it is clear, in any event, that the Staff has not reviewed Licensee's report and does not intend to do so prior to restart (NRC Staff Ex. 15, at 5). Regardless of the outcome of this matter, the Board requires that the Licensee review and resolve the following matters which were identified in the Staff's control room design review: (a) the Licensee shall investigate systems and techniques for effective communication of indicator and display lamp status information to operators where "push-to-test" capability does not already exist (this investigation shall be completed no later than by the end of the first

refueling outage following restart) (NRC Staff Ex. 15, at 2); and (b) Licensee will premanently mark final operating ranges on all applicable vertical meters by the end of the first refueling outage following restart (NRC Staff Ex. 15, at 5-6).

157. The Board is concerned in particular with several areas related to the design of the TMI-1 control room and will require that these issues be resolved as indicated. The first such concern relates to the alarm and annunciator system at TMI-1. The Board's concern in this matter relates to the fact that once an alarm is acknowledged, it is indistinguishable from previously acknowledged alarms (Tr. 10,496, Ramirez). The Licensee is committed to an investigation of an alarm suppression system which would suppress alarms under conditions in which the alarms are meaningless (Tr. 10,254-55, Estrada). In the interim, Licensee will accomplish the goal of ensuring that operators understand alarms prior to acknowledging them by procedural changes (Tr. 10,465, Price). Although the Staff approved this approach, neither NRC Staff witness Ramirez or Price had seen the new procedure, and witness Ramirez indicated that this would be left to I&E to verify implementation of the new procedure (Tr. 10,465-66, Ramirez & Price). NRC Staff witness Price testified that the procedural change should take the form of a caution to the operations to clearly identify which annunciators are flashing and understand what these alarms mean before acknowledgement of the alarms. Price and Ramirez testified that for the short term, operator awareness of the problem, combined with the new procedure and some level

prioritization of alarms by level of importance, will be sufficient (Tr. 10,466-68, Price & Ramirez). Prioritization of alarms will be in place at restart (Tr. 10,468, Ramirez). The Board is concerned, however, about what would happen in the event of a large number of alarms coming in in a short time period. The Board recognizes that there are much fewer alarms at TMI-1 as compared with TMI-2 and other plants (350 alarms as opposed to 700-1,000 alarms) (Licensee Ex. 23, at III-11), but remains concerned because neither Staff witness evaluated the numbers and types of alarms that annunciated during the TMI-2 accident to determine whether it would have been possible under such circumstances to understand the signficance of the alarms before acknowledging the alarms (Tr. 10,469, Ramirez). The Board therefore requires that the Licensee complete its evaluation of alarm acknowledgement alternatives before the end of the first refueling outage following restart. It is the Board's view that this requirement gives Licensee sufficient flexibility to address the problem, while at the same time recognizing the importance of resolving this issue as expeditiously as possible. The Staff is directed to satisfy itself that the Licensee is making reasonable progress toward satisfying this requirement as a condition of restart. In this context, reasonable progress would be initiation of the study, together with a full description of the study and a projected date for completion and recommendations from the review.

158. A second area of concern relates to communications problems at the facility. Inoperable plant page system phones was noted in the Staff's Control Room Design Review Report as a problem at TMI-1; the Staff further noted that some areas in the plant are not reachable by telephone (NRC Staff Ex. 2, at 19-20). Licensee's control room design report acknowledges this problem, and also concludes that messages of importance to the plant might be lost in the noise of general administrative traffic (Licensee Ex. 23, at D, 1-2). The Licensee is investigating a new page system designed to keep general administrative traffic out of the control room, restricting control room communications to operational traffic only (Tr. 10,265-66, Walsh). One of the Licensee's human factors consultants (Estrada) recommended that the Licensee establish a closed 2-way communications circuit between the control room and auxiliary operators (Tr. 10,268, Estrada). A similar recommendation is made in the Licensee's control room design report (Licensee Ex. 2', at D, 2).

159. The Board is not convinced that the Licensee is giving a sufficiently high priority to this problem. A Staff human factors witness testified that communications between the control room and remote areas are important to the safety of the plant (Tr. 10,478-79, Ramirez). The Staff witness knew of no specific program of the Licensee to deal with inoperable page phones, although he testified that such a program should be implemented (Tr. 10,477, Ramirez). The Board itself noted problems with the page phone system during

a site visit held prior to the start of the evidentiary phase of this proceeding, mostly relating to nuisance usage of the paging system. The Board concludes that this is a serious problem which must be alleviated expeditiously. The Board requires that the Licensee promptly initiate its communications study (if not already initiated) and complete this study as soon as practicable, before restart if at all possible. If this is not possible, the Licensee is directed to inform the Staff at the earliest possible time, following which the Staff will undertake a review to determine if and under what conditions any operations involving safety-related equipment require the establishment of communications between the control room and a remote location. If the Staff determines that there are circumstances under which such communication with the control room is necessary, the Staff shall so inform the Licensee and the Licensee shall make such improvements as are necessary to create a highly reliable communications system for use in plant operations. Such improvements must be made, if required, prior to restart.

160. A third area of concern relates to the possible use of video and audio taping in the control room. Licensee is investigating the use of a video recorder and/or audio recorder in the control room. Licensee acknowledged that the use of audio/video taping in the control room, perhaps keyed to reactor/turbine trip annunciation, would be "an extremely valuable tool" in analyzing operator response to accidents and transients, and would also be useful in evaluating

human factors considerations associated with accidents and transients (Tr. 10,271, Walsh). The Board recognizes the implications that video/audio taping in the control room would have for the operations personnel, and is sympathetic to considerations of a "big brother" atmosphere in the control room. The Board, however, considers the manifest public interest in the safe operation of the plant to take clear precedence in this case, and finds that the benefits in terms of protecting the public health and safety exceed the risks of such a program. The Board considers the use of video-taping in the control room to be analogous to the use of flight recorders and the so-called "black box" recorder on commercial aircraft. The responsibility for safe operation of a nuclear power plant is a heavy burden to bear, and the public is entitled to know, in the event of an accident, precisely what occurred to the extent that this is possible to know. The Board is convinced that had there been a video-taping system present in the TMI-2 control room during the TMI-2 accident, our knowledge of what happened during the first hours of the accident would have been greatly enhanced. For example, it would be abundantly clear who utilized the plant computer, and when it was utilized. The Board is also certain that replay of such video tapes would have facilitated operator recall of information and events of that morning. As a result of these considerations, the Board is requiring that, prior to restart, the Licensee install a video-taping system in the TMI-1 control room. The vid o-taping system

should be activated under appropriate conditions automatically, for instance, upon receipt of a reactor or turbine trip signal and/or containment isolation or ESFAS initiation. These details, as well as the number and location of cameras shall be worked out jointly by the NRC's human factors staff and the Licensee's staff. The Staff should discuss with the Licensee the necessity for entering into any agreements concerning the use of the video tapes, especially to ensure that they are not misused; the Staff must, however, be assured of rapid access to the tapes following an accident or transient where the analysis of such tapes would assist in the evaluation of the accident or transient.

161. In its human factors review report for TMI-1, the Licensee's review team made many recommendations for changes in physical equipment and procedures related to the control room. Some of the recommendations relate to additional studies which might require on the order of years to complete and implement recommendations which may result from such studies. Other recommendations are for changes which can be effectively implemented in a short period of time, many before restart. The Staff, through a combination of the Office of Inspection and Enforcement and the Division of Human Factors Safety, is directed to closely monitor Licensee's progress in this area. A final pre-restart report on the status of Licensee's implementation of modifications to the TMI-1 control room should be prepared by the Staff and published to document which changes have been completed, which changes

might be delayed (along with explanations for the delay and a projected implementation schedule), and changes which require further evaluation on the part of the Licensee and/or the Staff. The Licensee is directed to provide whatever information is required by the Staff in preparing this report.

162. As a result of the modifications which are underway and which will be occurring for some time into the future as a result of ongoing studies, the Licensee is required to periodically document the status of his control room upgrading program. The Licensee shall propose modifications to his Technical Specifications to incorporate a reporting requirement on this matter, with the first report from the Licensee to the Staff due no later than six months after reaching full power following restart. The reports shall follow at six month intervals until the modifications contemplated in the Licensee's control room design review report are completed.

163. The Staff, through the Office of Inspection and Enforcement and the Division of Human Factors Safety, shall inspect Licensee's facility prior to restart to ascertain Licensee's progress in meeting the following commitments which were made during these proceedings:

a. New labelling will be added to panels to avoid interchanging legend switch covers (NRC Staff Ex. 15, at 3).

b. Additional training regarding Bailey controllers for licensed operators (NRC Staff Ex. 15, at 3-4).

c. Normal operating ranges on vertical meters will be temporarily marked (NRC Staff Ex. 15, at 5-6).

d. Alarm system audible tones will be adjusted so that each such tone is clearly audible and distinguishable above normal control room background noise, and so that operators can communicate with one another while the tone is sounding (NRC Staff Ex. 15, at 6-7).

e. Communications at the remote shutdown panel shall be improved to be independent of both the main control room and the relay room (NRC Staff Ex. 15, at 9).

f. Lighting deficiencies will be corrected (NRC Staff Ex. 15, at 10).

g. Important alarms will be color coded and ESFAS alarm tiles will be improved (NRC Staff Ex. 2, at 6).

h. Annunciator tile legends will be improved (NRC Staff Ex. 2, at 7).

i. A new CRT display system will be installed and operational in the control room (NRC Staff Ex. 2, at 7).

j. A new printer will be installed to improve the speed of computer printout (NRC Staff Ex. 2, at 7).

k. A guard rail or alternative means will be

provided to prevent inadvertent actuation of "J" handle controls (NRC Staff Ex. 2, at 7).

l. Improved labelling for multiple position rotary controls will be implemented to compensate for violation of convention with respect to other such controls (NRC Staff Ex. 2, at 8).

m. A formal surveillance program will be initiated to detect and replace burned out indicator lamps promptly (NRC Staff Ex. 2, at 8).

n. Improved labelling will be installed on illuminated legend switches which will lessen operator dependence on information contained on illuminated legends (NRC Staff Ex. 2, at 9).

o. Emergency feedwater flowmeters will be installed near the Bailey controllers and backup controllers (NRC Staff Ex. 2, at 9).

p. Panel legend lights will be adjusted and replaced to provide consistent illumination and improve the contrast with the panel background (NRC Staff Ex. 2, at 10).

q. Glare will be reduced by installation of light baffles (or alternatives) and by installation of glare-resistant label plates (NRC Staff Ex. 2, at 10).

r. A system of annunciators and indicators to signal upsets in power supplies to the ICS and NNI control systems will be installed, and a distinctive mark will be placed on instruments to identify the mid-scale point to assist operators in identifying instrument failures (NRC Staff Ex. 2, at 10).

s. For certain motor driven valves, a second independently powered position indicator will be installed to show valve position after the circuit breaker for the valve is tripped (NRC Staff Ex. 2, at 11).

t. Color coding will be reviewed to assure consistency (NRC Staff Ex. 2, at 11).

u. A hierarchial scheme of labelling will be instituted to improve labelling, at the group, function, system or panel level rather than just at the component level (NRC Staff Ex. 2, at 11).

v. Makeshift "dymo" tape labels will be replaced with permanent label plates with consistent color coding and letter size (NRC Staff Ex. 2, at 12).

w. All labels will be permanently attached (NRC Staff Ex. 2, at 12)

x. Demarcation will be added to panels to separate controls/displays by system,

subsystem and functional grouping (NRC Staff Ex. 2, at 12).

y. Related controls and displays will be reviewed to assure that consistent nomenclature and component designation are used (NRC Staff Ex. 2, at 13).

z. Labelling and demarcation of the makeup and purification system will be implemented to clearly distinguish the two control/display segments (NRC Staff Ex. 2, at 13).

aa. Operators will be trained to observe flow transients when makeup pumps are started (NRC Staff Ex. 2, at 13).

bb. The Engineered Safeguards actuation annunciator window will be clearly labelled (NRC Staff Ex. 2, at 14).

cc. Meter scales for the decay heat removal system will be changed to make them consistent with one another (NRC Staff Ex. 2, at 15).

dd. The decay heat removal system will be mimicked and the connection between the DHRS and makeup systems will be clearly indicated (NRC Staff Ex. 2, at 15).

ee. Control room ventilation controls and displays will be functionally grouped by demarcation and new labels (NRC Staff

Ex. 2, at 15).

ff. Labels for the fan start controls will be improved by adding "time to depress and hold" information (NRC Staff Ex. 2, at 16).

gg. Diesel generator control and indication displays will be improved with new labels and white indicator lights (NRC Staff Ex. 2, at 17).

hh. A flow meter for the emergency feedwater system will be installed (NRC Staff Ex. 2, at 17).

ii. Improve labelling, color coding, and demarking of the ICS controls and displays will be implemented (NRC Staff Ex. 2, at 18).

jj. Emergency lighting will be provided at the emergency shutdown panel (NRC Staff Ex. 2, at 18).

kk. Sub-cooling margin instrumentation and displays will be installed and operating (NRC Staff Ex. 2, at 22).

ll. All control room modifications will be reviewed by an in-house human factors engineering staff; procedures will be implemented (Tr. 10,252, Walsh).

mm. The following items listed in Licensee Ex. 33, at 3, will be implemented: 1-5, 7-9, 11-13, 17-22, 29-31, and 34 (these

items are identified in Licensee's Ex. 23, Table III-1, page III-25).

The above items are those to which Licensee has committed to implement prior to restart. There are many other items which have a later implementation date. The Staff and Licensee are required to identify these in the reports required by this decision and the Staff is required to monitor Licensee's progress toward achieving these additional improvements.

## V. CONCLUSIONS OF LAW

164. The general rule established by 10 C.F.R. §2.732 is equally applicable in this case. The Licensee, in proposing to restart TMI-1, clearly has the burden of proof in this proceeding for issues specified in the Commission's Order and Notice of Hearing. Metropolitan Edison Company (Three Mile Island Nuclear Station, Unit No. 1), CLI-79-8, 10 N.R.C 141 (1979).

165. The Commission's Order and Notice of Hearing (10 N.R.C. 141, 148, (1979)) mandated that the Board consider the necessity and sufficiency of the short-term and long-term requirements set forth in the Commission's Order. Where intervenors have raised issues which were not specifically identified in the Commission's Order and Notice of Hearing, a burden to establish a threshold case rests with the proponent of an issue. Once, however, this threshold is established, the

burden of proof lies clea.ly with the Licensee.

166. Absent some special statutory standard of proof, factual issues decided by the Commission are determined by a preponderance of the evidence. Tennessee Valley Authority (Hartsville Nuclear Plant, Units 1A, 2A, 1B, and 2B), ALAB-463, 7 N.R.C. 341, 343, 360 (1978); Charlton v. FTC, 543 F.2d 903, 907 (D.C. Cir. 1976); Duke Power Company (Catawba Nuclear Station, Units 1 and 2), ALAB-355, 4 N.R.C. 397, 405, n. 19 (1976); Consclidated Edison Company (Indian Point Station, Unit No. 2), ALAB-188, 7 A.E.C. 323, 356-57 (1974).

167. In accordance with Commission Order CLI-79-8, and based on the evidence of record in this proceeding and the foregoing findings of fact related to plant design issues, the Board concludes:

a. That the "short-term actions" recommended by the Director of Nuclear Reactor Regulation are insufficient to provide reasonable assurance that TMI-1 can be operated without endangering the public health and safety; and

b. That the "long-term actions" recommended by the Director of Nuclear Reactor Regulation are insufficient to provide reasonable assurance that TMI-1 can be operated for the long term without endangering the public health and safety.

168. The Board concludes that additional short-term actions and long-term actions are necessary to provide reasonable

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

169. The Board concludes that the following additional short-term actions are necessary to provide reasonable assurance that TMI-1 can be operated without endangering the public health and safety:

a. An acceptable failure modes and effects analysis must be completed on the Integrated Control System. The Board finds, however, than an FMEA is an inappropriate analytical tool for the purposes proposed, and therefore concludes that fault tree analysis should be utilized in combination with the FMEA. The analysis of the ICS shall include random multiple failures, single and multiple failures at any power level from zero power through and including the high power level trip setpoint, propogation of single and multiple failures through the ICS to other systems (both safety and nonsafety systems), operator error (both singly and in combination with other single and multiple failures, especially in situations where operator error probabilities are increased due to short response time, stressful conditions, and/or lack of normal instrumentation), and failures (both single and multiple) occurring under

abnormal initial conditions (such as odd valve alignment) and under conditions of permitted but not normal full-power operation (such as with ICS controllers in manual, operation with 3 RCP's, or operation with only one main feedwater pump). Specifically, this analysis must include a fault tree for the loss of feedwater event, including both main and emergency feedwater. If this fault tree discloses inacceptable consequences, other fault trees should be completed to analyze a range of failures in which the ICS is capable of participating.

b. The Licensee must either replace the Model 721 ICS with a Model 820 ICS or modify its existing Model 721 ICS to increase its reliability (in terms of failure rates) into a range comparable with the failure rates for the Model 820 ICS. If Licensee elects to modify the Model 721 ICS, the analysis required above at "a" must reflect the modified system.

c. Licensee must satisfactorily and completely respond to IE Bulletin 79-27 by submitting procedures which specifically address NNI/ICS power failures and operator actions following such power failures to assure that there is sufficient instrumentation presenting reliable

information with which to make control decisions. These procedures must carry through to safe shutdown.

d. Licensee shall submit detailed report on ICS/NNI power supplies. In particular, the report should address the probability of failure, the reliability of the power supply compared to Class 1E standards, the extent to which the power supply system has been "channelized", and the effects of power failures to ICS/NNI on instrument and data availability.

e. Licensee shall either staff the plant at all times with at least one qualified Instrumentation and Control Technician (I&C Technician) or demonstrate specifically why such staffing is not needed. If Licensee elects to do the latter, Licensee shall address the I&C capabilities of existing onsite staff on all shifts, the extent to which procedures and/or training compensate for the lack of an onshift I&C Technician, and shall demonstrate that extended loss of NNI/ICS power does not lead to unacceptable consequences.

f. Licensee shall submit a report addressing its capability to effect immediate repairs of NNI/ICS, including power failure problems,

and shall address, among other items which may be necessary, the availability of replacement parts and components onsite.

g. Licensee shall install and make operational a safety-grade high radiation signal on the reactor building purge system, to provide for automatic isolation of this line upon receipt of a high radiation signal from this system.

h. The Licensee shall establish a schedule for completing the upgrading of its computer facilities as set forth in Finding No. 135.

i. The Licensee shall establish a reliability monitoring program for the computer as set forth in Finding No. 136.

j. The Licensee shall assure a reliable power supply for the process computer as set forth in Finding No. 138.

k. Licensee shall implement a backup display capability for data from the in-core thermocouples as set forth in Finding No. 155.

l. Licensee shall complete its evaluation of in-plant communications as set forth in Finding No. 159.

m. Licensee shall install a video-taping system in the plant control room as set forth in Finding No. 160.

n. The Licensee shall complete the short-term upgrade of its control room as set forth in Finding No. 163.

o. Licensee shall perform such analyses as are necessary to assure that the pressurized thermal shock problem as set forth in Findings Nos. 70-84 is resolved.

1. Licensee shall propose for Staff approval (approval required before restart) certain modifications to the license Technical Specifications, including:

(1) Reporting requirements on ICS and NNI/ICS power supply failures.

(2) Reporting requirements on feedwater oscillations.

(3) Reporting requirements on feedwater transients which result in EFW, ECCS, or safety valve actuations.

(4) Testing and surveillance requirements for the ICS and associated annunciators.

(5) Reporting requirements related to the plant computer as set forth in Findings Nos. 135-138.

170. The Board concludes that the following additional long-term actions are necessary to provide reasonable assurance that TMI-1 can be operated for the long term without endangering the public health and safety, and should be required of the

Licensee as soon as practicable (or under the specific schedule as indicated):

a. Licensee shall complete the upgrading of the TMI-1 control room.

b. Licensee shall complete the upgrading of the process computer.

c. Licensee shall install a replica control room simulator as soon as possible (Licensee indicates that this should be possible by 1985).

171. The Board concludes that the long-term item on the Integrated Control System (long-term item No. 1, 10 N.R.C. 141, at 145 (1978)) shall be incorporated as a short-term item and shall be removed as a long-term item.

172. In accordance with Commission Order CLI-79-8 and based on the evidence of record in this proceeding and the foregoing findings of fact and conclusions of law, the Board concludes that the record does not support a finding of reasonable assurance that TMI-1 can be operated, either for the short-term or the long-term, without endangering the public health and safety. Unless and until the short-term and long-term actions required of the Licensee by this decision are complied with fully, Licensee is hereby ordered to maintain TMI-1 in a cold shutdown condition.

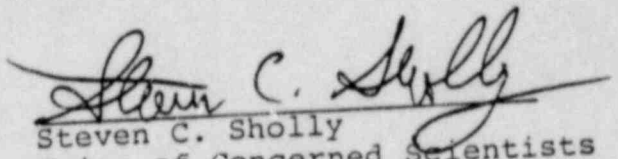
173. Upon motion by the Licensee, this Board will consider a further request by the Licensee for permission to restart TMI-1 upon a showing that the requirements imposed

in this decision have been met.

174. The Board recommends to the Commission that if the Licensee cannot provide a projected date by which it will achieve compliance with these requirements which is earlier than July 1, 1982, that a show cause order be issued requiring Licensee to show cause why TMI-1 should not be defueled and decontaminated to eliminate any risk to the public health and safety from the continued status of the plant in a refueled but cold shutdown condition.

DATED: June 1, 1981

RESPECTFULLY SUBMITTED,



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

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) | ) | |

CERTIFICATE OF SERVICE

I hereby certify that single copies of INTERVENOR STEVEN C. SHOLLY PROPOSED FINDINGS OF FACT AND CONCLUSIONS OF LAW ON PLANT DESIGN ISSUES, dated June 1, 1981, were served upon those persons on the attached service list by deposit in the United States Mail, postage prepaid, first class, this 1st day of June 1981.

Steven C. Sholly

Steven C. Sholly

## SERVICE LIST

## TMI-1 Restart, Docket No. 50-289

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

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

Dr. Linda W. Little
Administrative Judge
Atomic Safety and Licensing
Board Panel
5000 Hermitage Drive
Raleigh, NC 27612

James R. Tourtellotte, Esquire
Counsel for the NRC Staff
Office of the Executive Legal
Director
U.S. Nuclear Regulatory
Commission
Washington, D.C. 20555

George F. Trowbridge, Esquire
Counsel for Metropolitan Edison
Company
Shaw Pittman Potts & Trowbridge
1800 M Street, N.W.
Washington, D.C. 20036

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

Robert W. Adler, Esquire
Attorney for the Commonwealth
of Pennsylvania
505 Executive House
P.O. Box 2357
Harrisburg, PA 17120

John A. Levin, Esquire
Assistant Counsel
Pennsylvania Public Utility
Commission
P.O. Box 3265
Harrisburg, PA 17120

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

Thomas J. Germine, Esquire
Deputy Attorney General for
the State of New Jersey
Division of Law - Room 316
1100 Raymond Boulevard
Newark, NJ 07102

Daniel J. Cosgrove, Esquire
Counsel for the Federal Emergency
Management Agency
Office of the General Counsel
1725 I Street, N.W.
Washington, D.C. 20472

John E. Minnich
Chairman
Dauphin County Board of
Commissioners
Dauphin County Courthouse
Front and Market Streets
Harrisburg, PA 17101

Jordan D. Cunningham, Esquire
Counsel for Newberry Township
TMI Steering Committee
Fox Farr & Cunningham
2320 North Second Street
Harrisburg, PA 17110

Ms. Louise Bradford
Legal Representative for
Three Mile Island Alert, Inc.
315 Peffer Street
Harrisburg, PA 17102

Ellyn R. Weiss, Esquire
Counsel for the Union of
Concerned Scientists
Harmon & Weiss
1725 I Street, N.W.
Suite 506
Washington, D.C. 20006

Ms. Gail Bradford
Legal Representative for
Anti-Nuclear Group
Representing York
245 West Philadelphia Street
York, PA 17404

Robert Q. Pollard
Legal Representative for
Chesapeake Energy Alliance
609 Montpelier Street
Baltimore, MD 21218

Marvin I. Lewis
Intervenor pro se
6504 Bradford Terrace
Philadelphia, PA 19149

Marjorie M. Aamodt
Intervenor pro se
R.D. #5
Coatesville, PA 19320

Dr. Judith H. Johnsrud
Legal Representative for
Environmental Coalition
on Nuclear Power
433 Orlando Avenue
State College, PA 16801

William S. Jordan, III, Esquire
Counsel for People Against
Nuclear Energy
Harmon & Weiss
1725 I Street, N.W.
Suite 506
Washington, D.C. 20006

* Indicates hand delivery.