GPU ACCIDENT REVIEW TASK FORCE

FINAL SUMMARY REPORT

R. W. KEATEN RWKeaten

R. L. LONG R L Long

A. TSAGGARIS A Tsaggaris

T. L. VAN WITBECK TL Van Witbeck

December 15, 1980

TABLE OF CONTENTS

I. INTRODUCTION

On March 29, 1979, the day after the TMI-2 accident, H. Dieckamp established a task force to review the events associated with the accident. Members of this task force proceeded to the site, but immediately became involved in supporting the plant operation. As a result, only limited investigative results were obtained.

On July 2, 1979, R. C. Arnold, Vice President-Generation, GPU Service Corporation established a new task force to complete the investigation of key issues related to the accident. The specific issues considered by the Task Force are shown in Table I. The charter of the task force was to perform the necessary investigations and make a report to GPU management, with recommendations.

In support of this charter the task force established the following guidelines:

The task force will restrict its investigation to the key elements of the TMI-2 accident listed in Table I.

The investigation will address agencies other than the utility only in so far as they have a direct bearing on the accident.

The task force will be objective in its examination of the accident. No attempt will be made to justify events, actions or circumstances; nor will an attempt be made to place blame for the accident.

The task force will make no attempt to address any liability for non-performance of contractual obligations.

The task force will not restrict the evaluation of its findings to the standards which existed at the time of the accident. The task force approach rather will be to examine the findings in light of the new understanding which has been gained as a result of the accident.

The task force will draw conclusions based upon the examination of the accident and the related events preceding and following the accident.

Constructive recommendations will be developed by the task force. The intent of the recommendations will be to identify and provide guidance in those areas where improvement will result in improved performance and safety.

In carrying out this investigation the task force pursued several types of activities:

1. Detailed discussions were held with selected members of the plant staff covering (a) the events of March 28 and the following days and (b) previous plant and system policies and procedures which may have contributed to the accident.

2. Plant documents, including selected operating procedures, emergency procedures, and startup and test procedures, were reviewed for accuracy, thoroughness and clarity.

3. Examinations were made of selected plant systems and components to determine their overall condition and conformance to design. In addition tests were performed to determine the system and component response to certain conditions.

4. Testimony before other investigative bodies was reviewed in detail, as were the findings of those bodies, where available.

5. Selected analytical tasks were performed to support the investigations.

The task force received substantial assistance from many individuals. Some of the major participants are listed in Table 2.

This final report summarizes the results of the investigation. Details of the investigation are given in the references, which include a detailed sequence of events and narrative description of the accident. The summary of the findings in Section II is structured around the seven key elements listed in Table I. Section III gives the conclusions drawn by the task force, and Section IV presents recommendations.

TABLE 1

KEY ELEMENTS OF TMI-2 ACCIDENT
OF MARCH 28, 1979

TO BE INVESTIGATED BY THE GPU TASK FORCE

1. The factors related to the trip of the main feedwater pumps including system design features, equipment malfunctions, operating procedures and practices, awareness by operators, supervision and management of system problems prior to March 28 and significant actions by the auxiliary operators prior to and subsequent to the loss of feed conditions.

2. The rationale for the control room and staff personnel response to the plant upset conditions during the first few hours, including information availability, procedural considerations and exercise of authority by supervision. In particular, evaluate the circumstances that caused the operators to modulate high pressure injection when reactor coolant system pressure was abnormally low.

3. The Emergency Plan implementation, including timeliness of declaration of site and general emergencies, notifications, identification of off-site releases, and communication of plant status to appropriate management and public officials.

4. The pressurizer electromatic relief valve failure mode, including failure data from other installations and consideration of full scale testing of a prototypical valve.

5. The pathways by which radioactive fluids were transported from the Reactor Building to the Auxiliary Building, the chronology of transfer and the quantities associated with the transfers.

6. The factors leading to the incorrect status of EF-V12A and EF-V12B at the time of the accident, including the reasons the surveillance procedures were written so as to simultaneously isolate both trains of emergency feedwater, the practices that apparently permitted the completion of the procedure without insuring attainment of proper valve lineup, and the reasons the improper positions of the valves could apparently exist undiscovered for almost two days.

7. The adequacy of assessment by plant supervision and company management of the extent of the damage to the core, and the potential for off-site releases, including timeliness and flow of information and technical accuracy.

TABLE 2

INVESTIGATION PARTICIPANTS

GENERAL PARTICIPANTS:	T. G. Broughton, GPUSC L. Kittelson, Met-Ed E. G. Wallace, GPUSC P. S. Walsh, GPUSC R. L. Williams, GPUSC
CONTRIBUTORS TO SPECIFIC TOPICS:	
Initiating Event:	G. Lehmann, GPUSC K. Lucien, EI W. Marshall, Met-Ed
Pressurizer Relief Valve:	Q. Billingsley, GPUSC W. Bogert, GPUSC J. Correa, GPUSC
Radiation Release Pathways:	B. Center, EI J. Flaherty, EI L. Kripps, EI J. Paradiso, GPUSC
Emergency Feedwater Valves:	J. Miller, Consultant J. J. Wagner, Penelec
Sneak Circuit Analysis:	J. Gulati, GPUSC J. Lawton, Met-Ed J. Tana, Ebasco
Emergency Feedline Discoloration:	R. Greenwood, Gilbert
PLANT STAFF DISCUSSION PARTICIPANTS:	J. J. Blessing, CRO R. R. Booher, CRO K. P. Bryan, Shift Supervisor C. C. Faust, CRO J. R. Floyd, Unit II Oper. Sup. E. F. Frederick, CRO K. R. Hoyt, Shift Foreman G. Kunder, Unit II Tech. Supt. J. Logan, Unit II Supt. B. Mehler, Shift Supervisor G. Miller, Station Manager F. J. Scheimann, Shift Foreman B. G. Smith, Shift Supervisor W. H. Zewe, Shift Supervisor
General Assistance in Arranging Interviews	R. Harbin, Met-Ed

II. SUMMARY OF FINDINGS

A. FACTORS RELATED TO THE TRIP OF THE MAIN FEEDWATER PUMPS

The investigation of the feedwater pump trip was directed both towards identifying the specific cause of the trip and performing a more general evaluation of the secondary side of the plant in terms of the adequacy of design, construction, installation, checkout, operating and maintenance practices. In the course of the investigation a number of relevant features were identified.

1. Cause of the Trip

The immediate cause for the trip of the feedwater pumps was a trip of the A and B condensate booster pumps.[1] The loss of these booster pumps resulted in a trip of the main feedwater pumps. The condensate booster pumps tripped on low suction pressure, due to closure of the condensate polisher discharge valves. The auxiliary "A" operator who was in the area at the time reported that immediately after the trip he went to the polishers to make the usual post-trip alignment and found that all of the discharge valves were closed. This condition was also observed later by the shift supervisor.

Water in the instrument air system is believed to have caused the sudden closure of the condensate polisher discharge valves. An incident which occurred on July 5, 1979, demonstrated that water will cause the valves to close.[2] As the Number 8 polisher was being put into service the outlet valve oscillated and finally slammed shut. When the air supply line to the Number 8 polisher valve was opened, approximately 1/2 to 1 cup of water was obtained. After the water was removed, the polisher was again placed in service and functioned satisfactorily.

The source of the water which initiated the March 28 trip, however, is still uncertain. Two hypotheses were: (1) the water was introduced into the Instrument Air System during attempts to unblock a plugged resin transfer line between the Number 7 Condensate Polishing Demineralizer and the Resin Receiving Tank; and (2) a leak existed in the resin regeneration system which permitted water to be transferred to the Instrument Air System at the Polishing Demineralizers.

The second hypothesis was rejected after a chemical analysis of water found in the Condensate Polisher Demineralizer outlet valve actuators did not indicate the presence of regeneration chemicals. In addition, a daily check of the systems during a two week period of normal use including regeneration indicated no water had been added to the Instrument Air System.

Several formal tests were performed in an attempt to validate the first hypothesis. Water was injected into the instrument air supply at the condensate polisher control panels under various test conditions. The test results showed that all of the condensate polisher discharge valves went shut only when an inlet stream consisting entirely of water was introduced into the water trap. This caused the water trap dump valve to open and remain open until the water was passed. As a result, a loss of pressure downstream of the water trap was experienced. In one test, the dump valve was jammed open by a foreign material, tentatively identified as desiccant from the Instrument Air System air dryers.

An additional result of the tests which casts some doubt on the first hypothesis is that the pneumatically controlled stylus on the system chart recorders spewed water onto the charts. This condition was not found after the accident. In addition, other systems which are normally supplied by the Instrument Air System and are located upstream of the Condensate Polishing System did not operate in an abnormal manner during the accident as would be expected if the water had been transferred through the Instrument Air System to the Condensate Polishing demineralizer outlet valves.

Nevertheless, the state of knowledge of the system and the test results lend credence to the hypothesis that the water was introduced into the Instrument Air System while attempting to unplug a resin blockage by the use of demineralized water and fluffing air.

2. System Design Features

Investigations started prior to the TMI-2 accident have indicated that the condensate and feedwater systems operated very close to design limits when the plant was operating near full power. The systems have very limited capability to accommodate upsets or transients, in part apparently due to the lack of detailed transient analysis performed as part of the system design process. In addition, some component control systems were not normally operated in the "Auto" mode due to bad experiences with component trips in this mode. As a result of these and other problems, the spare condensate and spare booster pumps would not start automatically to maintain the plant on-line in the event of an operating pump failure.

A design feature highly relevant to the accident was the inability of the system to accommodate loss of instrument air without inadvertent valve closure. The original design provided sensors which act to lock the valves in their current (open) position upon loss of either instrument air or control power. However, physical inspection revealed that this design protection had been negated both by disconnection of wires between the sensors and the associated solenoids, and by solenoids placed in the "manual operate" position.[1] Attempts to discover when and why these changes were made were unsuccessful because they were apparently not documented.

The polisher bypass valve (CO-V12) was designed to be opened from the control room. The valve motor operator overload heaters, however, were not adequately sized for the torque required to open the valve with a high differential pressure across the valve. The valve thus had to be operated manually on March 28. Although verification of the valve operation in the presence of a differential pressure was part of the original test plan, it was deferred to hot functional testing and placed on the "incomplete work list." This item was noted by Met-Ed to be a "significant item at time of turnover." During the later hot functional testing, however, this test was apparently not performed.[1]

Another error found during the investigation was in the wiring arrangement of the condensate pump control circuit. When the auto/manual mode selector switch was in manual, this circuit caused the "A" condensate pump to trip when the "A" condensate booster pump tripped. This wiring error was in the 4160 Volt switchgear. The wiring error was identified in November 1972 and a field change was initiated. For reasons unknown, however, the alterations were not completed for the A condensate and condensate booster pump train. The test program philosophy to accept without verification the internal wiring of components furnished as packaged units permitted this wiring error to escape detection during the preoperational testing of the circuits.

Still another problem was the impact of turbine bypass flow on condenser level. The design resulted in direct impingement of the bypass steam onto the condenser level transducer, causing it to indicate an artificially low level. This caused full makeup flow and high condenser level, with the potential for flooding the condenser and loss of vacuum. Work was in progress prior to March 28 to solve this problem.

A final example of a poor design feature is the configuration of the resin transfer line from the condensate polishers to the regeneration tank. This is a 2-1/2-inch diameter pipe with eleven 90° elbows. The combination of resin transfer about once every two days and the torturous transfer path made resin blockage a not infrequent occurrence.

3. Equipment Malfunctions

The basic malfunction which ultimately resulted in the unit trip was the inadvertent closure of the condensate polisher discharge valves. In addition to initiating the sequence of events, the closure of these valves also made it impossible to reject condensate from the hotwell. This condition directly contributed to the high hotwell level problem which caused the shift supervisor to go to the condenser area, as discussed in Section II-B.

A water hammer in the condensate system piping, of undetermined origin, resulted in two cases of equipment malfunction. The suction pipe for condensate booster pump A was observed to move by an auxiliary operator and resulted in the severance of an instrument air line to the condensate reject inhibit valve (CO-V57). This severance caused the valve to fail closed, which had no immediate effect on system operation since the condensate flow path was already blocked by the closed polisher valve. CO-V57 was later opened manually to provide a flow path for the condensate to the storage tanks. The water hammer also caused a leak in the flange joint in the booster pump A suction piping downstream of the pump isolation valve (CO-V27A), which contributed to the confusion in the condensate area. The valve was shut approximately 15 minutes later to stop the leak.

4. Operating Procedures and Practices

Investigations[3] reveal that operation of the secondary plant was in general carried out in accordance with approved operating procedures. The procedure for transfer of resins for regeneration, given in OP-2106-2.2, was used to govern that operation as it was performed immediately prior to the trip on March 28th. The attention to that procedure is clearly indicated by the nine revisions that have been made to date. The procedure did not, however, include instructions for clearing a resin plug if one developed, even though such plugs occurred frequently. Such operations should be performed in accordance with written instructions containing at least guidelines and precautions.

The control room operators' awareness of actions being taken by auxiliary operators in the plant was also explored. The control room operators interviewed stated that they were kept informed of activities outside the control room which could influence the plant performance. This viewpoint was also expressed by the shift supervisors and shift foremen interviewed. The investigation was limited to these interviews, but the consistent responses indicate that the operators were satisfied with the level of communication.

5. Awareness of System Problems

The plant staff members interviewed[3] have generally reported they were aware of the various problems in the secondary side of the plant. It is not clear that the awareness was uniform at all levels of the organization. In addition, although the maintenance staff was attempting to correct problems, it is not clear that adequate resources were dedicated to this purpose. For example, operators found water in the instrument air system many times, and had to blow out the system in order to get it to function correctly. There is, however, no evidence that a systematic attempt was made to isolate and eliminate the source of the water in the lines.

During interviews with the operators, the task force was informed that suggestions for improvements usually vanished into the system with no feedback. Even in cases where suggestions were adopted, the suggestor was not always informed of the decision and when action might be expected. This problem may have been compounded by the fact that the operators apparently preferred informal rather than formal submittals of suggestions.

B. RATIONALE FOR THE CONTROL ROOM AND STAFF PERSONNEL RESPONSE

The accident sequence of events including operator actions is given in Ref. 4. In summary, the power-operated relief valve on the Pressurizer opened and then stuck open, creating a small-break loss of coolant accident (LOCA). This eventually led to major core damage because no one in the control room recognized that the plant was experiencing a LOCA. The task force investigation has concentrated on identifying and understanding the factors which led to this lack of perception and the subsequent errors. The investigation results clearly show that a variety of different factors rather than one single factor led to these results. The important factors are discussed in the following sections, with a view towards identifying underlying causes and developing corrective recommendations.

1. Effect of the Leak Location

A loss of coolant accident (LOCA) is one of the basic events analyzed to demonstrate that adequate reactor core cooling can be maintained under adverse conditions. The analyses cover a spectrum of break sizes and locations, to demonstrate that all are within the design capability of the plant safety systems. The results of these safety analyses also provide the data base for plant operation, operator training, and emergency procedures.

Although different leak locations were considered in the safety analyses, the objective was to identify the locations providing the most severe test for the engineered safety features. No emphasis was placed on determining whether any particular leak location might present special problems to the operators in recognizing or responding to the leak. The data base for operator training and emergency procedures thus was inadequate to prepare the operators to respond to the LOCA which occurred on March 28.

A leak from most locations in the reactor coolant system will result in two symptoms: 1) decreasing reactor coolant system pressure, and 2) decreasing water level in the pressurizer. Both the training programs and the emergency procedures for TMI-2 were based on the assumption that both these symptoms would be present if a LOCA occurred.

The TMI accident, however, was a leak from the pressurizer vapor space which resulted in a reduction of reactor coolant system pressure but an increase in the water level in the pressurizer. Because of the data base deficiency, neither the training programs nor the emergency procedures provided the operators any guidance in recognizing or responding to this type of leak. Furthermore, as discussed below, the operators did not have information on a previous similar occurrence at another facility. The operators, therefore, interpreted the rising pressurizer water level as an indication that the system water inventory was increasing rather than decreasing, and did not take the actions necessary to maintain adequate inventory.

3. Operator Training

Inadequate operator training was clearly one of the most important factors which contributed to the accident. The training program included classroom work, hands-on simulator training, and in-plant reviews and drills. The program covered both normal operations and casualty response. This training was inadequate, however, to enable the operators to handle the situation they faced on the morning of March 28.

The fundamental concept of the training program was to focus on single, separable situations. Training in casualty response required that the operator recognize the symptoms associated with predefined single casualty events, and relate these symptoms to a specific emergency procedure which would govern the response. There was no consideration of multiple failures with a potential for conflicting or distracting symptoms. The events on March 28 resulted in a unique set of symptoms which did not correspond to any single set in the training program. In addition, as discussed above, the training programs had emphasized the type of LOCA which results in loss of both reactor coolant system pressure and pressurizer level, with pressure dropping to a few hundred psi. In fact, the symptoms from the accident were that reactor coolant system pressure dropped only to the saturation pressure (about 1400 psi initially) and pressurizer level rose rather than continuing to fall.

Other aspects of the training also contributed to the problem. The B&W reactor operating philosophy is never to take the plant solid except for hydrostatic test. Although there are advantages to this approach, it resulted in lack of experience in taking the plant solid. Training included no discussion of conditions under which solid operation might be desirable or necessary. In fact, taking the plant solid would have been a violation of the technical specifications as well as several operating procedures. The situation was compounded by the incapability of the B&W simulator to simulate solid plant operations and in fact, the simulator computer program became unstable when the pressurizer went solid. The net effect was certainly to condition the operators against solid plant operation.

The training program also placed little emphasis on the transition to natural circulation. So far as the task force has found, there was no simulator training in natural circulation, and the only mention of it was in review of emergency procedures. There appears to have been no experience in operating the plant in this mode.

Finally, the operators had not been trained in how to respond to a situation which fell outside the specific casualties they had studied. In particular, there was no training which stressed the importance of focusing on preselected key plant parameters in such a case in order to determine the basic condition of the plant.

2. Operating and Emergency Procedures

A review[5] of procedures relevant to the actions taken in the early hours of the accident revealed a significant weakness in the LOCA procedure (2202-1.3). This procedure is used to govern operators' responses to a loss of reactor coolant system pressure and loss of pressurizer level. The procedure, however, does not cover the spectrum of possible leaks, but gives guidance for only two extreme cases:

(1) A small leak in which primary pressure and pressurizer level decrease and then quickly stabilize without automatic HPI initiation.

(2) A major rupture, in which pressure and pressurizer level continue to decrease and other symptoms appear such as decrease in core flood tank level and pressure.

There is no guidance for how the operators should respond to a small-break LOCA in which pressure drops to the saturation pressure and stabilizes. As discussed above, there is also no guidance for a LOCA from the pressurizer vapor space, in which pressure decreases but pressurizer level increases.

The operators referred to this procedure (2202-1.3) early on March 28, and a better procedure with more specific guidance for LOCA's falling between the two extremes might have been very helpful. Even more crucial, however, was the use of this procedure as a training document. As discussed below, operator refresher training in emergency procedures was accomplished by periodic review of the procedures. Each time an operator went through this training process, he was encouraged to believe that if a LOCA occurred, reactor pressure would drop to a very low level and pressurizer level would also drop.

During the limited procedure review which has been performed, other deficiencies have been found. The actions required to place the plant in natural circulation were found in three separate procedures. The precautions associated with the transfer to natural circulation, however, were not the same in the three procedures, even though there is no reason why they should be different. In particular, the procedure referred to on March 28 (Station Blackout 2202-2.1) did not include the caution found in other procedures against attempting natural circulation with less than 35°F subcooling in the reactor coolant system.

Finally, the general content of the procedures could be improved. The intent of some procedures was not clear and should be explicitly stated. The requirements for transfer between procedures were poorly covered. There was no cross-reference system showing under what conditions a new procedure should be referred to and used.

Given this lack of training, the absence of the symptoms the operator had been trained to recognize as indicating a LOCA, and the perception by the operators that the reactor coolant system water inventory was increasing coupled with a conscious or subconscious orientation against solid plant operation, the failure to maintain full HPI flow is understandable.

A more basic issue is that training was geared primarily to insure the operators would attain and maintain an operating license. This was based on the assumption that the licensing process reflected the knowledge required for safe operation. The basic training documents were the plant procedures, with much less emphasis on technical information such as contained in the FSAR. Classroom training in emergency procedures, for example, consisted of the instructor reading the procedure to the class and elaborating on the areas he believed important. On-the-job review likewise consisted of the operator reading an assigned set of procedures and taking a classroom examination on them. This was consistent with the emphasis on the licensing process, since examiners focused on procedural compliance and verbatim knowledge of immediate action statements. In retrospect, this approach did not ensure a thorough understanding of basic plant response under a wide variety of conditions.

The general review of the training program revealed other weaknesses. The staff in the training department had shrunk in recent years. Attendance at training classes had dropped below 50%, which triggered memos from the training department to the operations department. It also required the training department to prepare large numbers of makeup lesson packages. This resulted in the instructors spending significant amounts of time on paperwork and less time on lesson preparation. Certain aspects of training which had been utilized previously, such as progressive formal certification of auxiliary operators, had been dropped. Further investigation is needed to address the required training resources, the need to expand the program to cover more of the plant and support staffs, and special training needs for other members of the organization. This investigation was deemed to fall outside the scope of the Task Force activities, and is being pursued by others (e.g. Ref. 6).

4. Knowledge of Relevant Previous Events

The nuclear industry has placed inadequate emphasis on insuring that information from significant safety occurrences at a particular nuclear station are understood and widely disseminated to improve the operation at all nuclear stations. The prior event most relevant to the TMI transient was a similar transient which occurred at Davis-Besse, in which a stuck open PORV resulted in similar symptoms to those observed at TMI and went unrecognized by the operator as indication of a small break LOCA for over 20 minutes. According to published testimony (Ref. 7) the technical staff of the NSSS vendor reviewed this transient and recognized its significance, but this information was not disseminated to other users. Had this information been effectively communicated to the TMI operators both through an updated training program and a revised small-break LOCA procedure, the TMI-2 accident might have been avoided.

There is evidence that previous events even at TMI were not used effectively to upgrade the training and procedures. The March 1978 transient, for example, in which the PORV first stuck open, received inadequate attention. Although an indicating light was installed in the control room to permit recognition of the particular type of failure which had occurred, the task force found no evidence of a more general review of PORV failure modes and means of detection. No attention was given to use of the temperature monitors as a means of detecting an open valve, since the monitors were not installed for this purpose. Had this transient been more fully analyzed, the need for improved means for identifying a stuck open PORV might have been recognized.

5. Safety Analysis Philosophy

An underlying reason for the operator's lack of knowledge of how to respond to the TMI small-break LOCA lies in the philosophy used in defining the design basis accidents for the plant and performing the associated safety analyses. The approach, as set forth by NRC regulatory practice, has been to attempt to identify bounding accidents, and then to perform very conservative and bounding analyses of the possible consequences. The results of these analyses are not reflective of actual plant response but rather of bounding responses used for licensing purposes.

A direct consequence of this approach is that little attention was given to predicting the actual plant response to real events. Training programs and operating procedures, therefore, did not have the data base needed to provide the operator with guidance on the anticipated plant response. A further difficulty is that accidents which are theoretically smaller than the bounding accidents, but which because of their special nature present a unique set of symptoms to the reactor operators, were not recognized as a special problem. This was critical to the TMI accident. Even though some analysis was made of a leak from the pressurizer, there is no evidence of any emphasis on the peculiar perception problems such a leak would present to the operators.

Still a further difficulty in the general approach to safety analysis has been concentration on the initial plant response, with no quantitative analysis of the potential problems that might arise later in the transient. This deficiency was also reflected in the simulator training programs, which were limited to the immediate responses to casualty conditions.

6. Previous Experience

TMI-2 had undergone several previous transients in which high pressure injection (HPI) had occurred. The operators were, in fact, convinced that HPI might occur on any reactor trip.[3] The basic reason for this relatively frequent occurrence of HPI was the small size of the pressurizer, which resulted in initiation of HPI for reactor trips if off-normal conditions were present. The procedural requirements to manually secure letdown and start an additional makeup pump following reactor trip are a reflection of the small pressurizer size; these actions were correctly performed on March 28.

Because of these previous experiences, coupled with information in training programs and procedures, HPI following a reactor trip was not necessarily regarded as an indicator of a loss-of-coolant accident. Furthermore, in the previous occurrences of HPI, the proper action had been to throttle the HPI flow to control pressurizer level. Thus when HPI occurred on March 28, and was followed by the pressurizer level stabilizing and then increasing, operators repeated their previous actions. While the previous experiences probably would not in themselves have blocked the recognition of a LOCA, they certainly contributed significantly to the operator response to HPI.

Operators may in fact have become "desensitized" to abnormal conditions, due to previous experiences combined with some plant design features and conditions which existed just prior to the event. At TMI-2, leaking pressurizer safety valves produced elevated discharge pipe temperatures before the event. Reactor building sump pump operation had become routine due to leakage. Some radiation alarms were expected after a reactor trip. Following a loss of feedwater, steam generator levels normally decreased below the 23 inch alarm setpoint and remained there for several minutes.

Such conditions make it more difficult to recognize valid deviations from expected performance. For example, alarms which are "expected" may not receive the proper level of attention. Such an alarm is no longer a valid indication of abnormal conditions. To determine if the condition is actually abnormal, the operator must consider the length of time the alarm condition exists, how much the parameter exceeds the alarm setpoint and other conditions which could be affecting the alarming parameter. It may not be possible to apply this judgment to many alarms simultaneously.

7. Use of Procedures

Some deficiencies were found in the use of procedures.[5] Specific examples are lack of attention to the low reactor coolant system pressure, the actions associated with operating the reactor coolant pumps under abnormal system conditions, and the attempt to transfer to natural circulation.

The LOCA procedure (2202-1.3) which was referred to by the operators states that "continued operation" depends upon the capability to maintain the reactor coolant system pressure above the HPI setpoint (1640 psig). While this procedure did not specifically mention the conditions which existed during the TMI accident, the operators should have recognized that the continued inability to restore reactor coolant system pressure to the normal value was an indication that additional remedial action was necessary. They instead concentrated on trying to control pressurizer level, as required by other procedures and the technical specification.

The Nuclear Plant Limits and Precautions procedure (2101-1.1) defines a specific operating envelope for the reactor coolant pumps in terms of reactor coolant system temperature and pressure. The actual reactor coolant system conditions moved outside this allowable envelope very early in the accident and remained there for over an hour prior to the time the pumps were actually turned off. This is not to suggest that the pumps should have been turned off earlier. An early recognition, however, that the pumps were exposed to conditions outside their normal operating envelope might have facilitated a correct diagnosis of the reactor coolant system conditions.

Procedure 2101-1.1 also gives a limiting curve for the use of natural circulation. More specific prerequisites are given in 2102-2.3 "Decay Heat Removal via OTSG" and 2202-2.5 "Station Blackout with Loss of Diesel Generators." One prerequisite is that the system be 35°F subcooled prior to attempting natural circulation. The operators attempted to transfer to natural circulation without meeting the requirement for subcooling and did not recognize that the hot leg was at saturation condition. They felt that they had to use natural circulation to avoid destroying the pump seals and thus causing a LOCA. As discussed above, the operators referred to a different procedure which did not include the requirement for subcooling, but which did reference the curve in 2101-1.1.

8. Man-Machine Interfaces

Several aspects of the man-machine interface in the TMI-2 control room contributed to the lack of recognition of the LOCA. The most clear was the lack of positive position indication on the pilot-operated relief valve (PORV) and/or flow measurement in the PORV line.

As originally designed the PORV had no position indication. This situation was changed, however, after the March 29, 1978, incident in which the PORV stuck open due to a faulty control signal. Because of this event a light was installed in the control room to indicate the state of the control demand signal to the PORV. In the case of the March 28 accident, however, the control signal correctly indicated that the valve should be closed.

Temperature indicators downstream of the PORV could be used to provide indication of continuing flow in the line, and the operators did in fact attempt to use them for this purpose. The temperature readings, however, were not permanently displayed to the console operator, and had to be called up through the computer, which was not particularly conveniently located as discussed below. When the shift supervisor instructed an operator to call up and read the temperature, the information was apparently[3] miscommunicated back to the shift supervisor as 232°F rather than the actual reading of 285°F. In addition to this confusion over the actual reading, no firm guidance had been given to the operators as to what temperature readings to expect if the valve did stick open. The shift supervisor believed that the March 1978 incident resulted in a downstream temperature of about 320°F. The net result was that the temperature readings were interpreted as being caused by the earlier leakage followed by the momentary opening of the PORV.

Another problem was the location and type of instrumentation on the reactor coolant drain tank (RCDT) which accepts fluid released by the PORV. The indication of this instrumentation is on a back panel which is not visible from the control console. It furthermore consists of only meters rather than recorders. RCDT pressure was recorded by the reactimeter and thus was available subsequently for post-transient analysis. About 40 minutes into the transient, the operators checked the readings on the drain tank as a test of whether there was a continuing leak through the PORV. At about 15 minutes into the transient, however, the rupture disc on the drain tank had burst, reducing both temperature and pressure. Since there was no recorder, the operators simply saw normal pressure in the tank.

In addition to these specific deficiencies, the general presentation of information in the control room, particularly alarms, does not facilitate diagnosis of an abnormal plant condition which affects many systems. Following reactor trip it was normal for the operators to be presented with over 100 alarms occurring in a relatively short span of time. Many of these alarms were irrelevant following reactor trip, and only made it more difficult to sort out the important information. The system did not assign any priority to the various alarms, and there was little or no segregation of alarms by function to facilitate effective scanning. The operator had only one acknowledge button to cover the entire set of alarms in the control room. It was therefore common practice not to acknowledge alarms when they were occurring rapidly, so that flashing indications would continue. The net result of this design was to force the operators to respond to plant transients in an environment of constant alarm buzzing, many flashing lights, and little help in sorting it all out.

The plant computer, which in principle could be of great assistance in this type of complicated situation, was not designed for this purpose. It was small and performed only limited data logging and display functions. The Cathode Ray Tube (CRT) display unit was small, located outside the normal range of vision of the control panel operator, and required an operator to move within a few feet of the display to read it. The typewriter printers used for alarm and utility printouts were very slow and incapable of keeping up with the mass of information normally generated following reactor trip. The alarm printer ran up to 1-1/2 hours late on March 28th. Furthermore, there was no prioritization or selection of alarms. It is reported[3] that approximately 90% of the alarms following a reactor trip originated in the heater drain system and were irrelevant for the current plant conditions. The net result was that the operators had come to expect no assistance from the computer during transients and used it only during steady-state plant operation.

9. Secondary Side of Plant

The conditions existing in the secondary side (see Ref. 4) appear to have contributed to the lack of recognition of the LOCA by diverting the attention of the shift supervisor and at least one control room operator away from the reactor coolant system. The closed emergency feedwater valves, problems in the condensate system, and the water hammer effects all contributed.

The erroneously closed emergency feedwater block valves (EF-V12's) exerted a significant influence on the plant behavior for the first few minutes. Following the initial transient, the primary system average temperature began to rise because no heat sink was present. As reactor coolant system pressure decreased and reached the saturation pressure in the system it became controlled by the RCS hot leg temperature (rather than by the pressurizer) and therefore also started to increase. Since pressurizer level was rising and RCS pressure had (apparently) stabilized, the operators felt that modulation of HPI was appropriate. After the emergency feedwater block valves were opened, RCS temperature decreased, and pressure dropped down along the saturation curve. Both temperature and pressure finally leveled out at the values they would have reached sooner had the EFW valves been open initially. It appears likely,[3] however, that the operators ascribed the unusual RCS behavior to the initial feedwater starvation followed by overfeed. Thus, a certain bias against consideration of a LOCA may have been established by the initial system behavior.

The condensate system also contributed significantly to the confusion.[3,8] The high hotwell level which resulted from closure of the condensate polisher discharge valves caused the shift supervisor to leave the control room at about 0415 and go to the condensate system area of the turbine building basement in an attempt to prevent loss of condenser vacuum. He made this decision based on his personal knowledge of earlier similar problems, and the availability of another shift supervisor to remain in the control room. The subsequent inability to open the polisher bypass valve with the motor operator and the lack of a hand wheel for manual operation prolonged his absence from the control room until about 0500. The air line rupture and water leak which resulted from the water hammer probably also contributed. It is impossible to gauge the real effect of the shift supervisor's 45 minute absence from the control room, but his presence in the control room might have been helpful.

Another contributor was the water hammer noise on the Loose Parts Monitor for the "A" steam generator. This noise caught the attention of the control room operator controlling the feed system and caused him to throttle the EF-V11 valves to reduce the thermal shock to the steam generators. This may have further contributed to a focus on the secondary side of the plant as the source of problems.

C. EMERGENCY PLAN IMPLEMENTATION

Review of the emergency plan implementation concentrated on five issues:

1. Timeliness of the emergency declaration.
2. Adequacy of information flow to state agencies.
3. Special conditions associated with the events of March 30.
4. Identification of off-site radioactivity releases.
5. Overall adequacy of the emergency plan.

The findings[9] in these areas are summarized in the following sections:

1. Timeliness of Emergency Declaration

Radiation emergencies were classified into three levels by the emergency plan: local emergency, site emergency and general emergency. The emergency plan requires that a local emergency be declared whenever two radiation monitors in the same building reach alarm levels. On March 28, although two "process" radiation monitors in the same building reached alarm levels, a local emergency was never declared because previous plant practice indicated that this criterion referred only to "area" monitors.

The timeliness of the site emergency declaration is subject to controversy. Most criteria for a site emergency involve radiation levels, and when radiation monitors indicated that these criteria were satisfied, the shift supervisor did in fact declare a site emergency. One criterion for a site emergency, however, is not related to radiation levels. This criterion requires that a site emergency be declared whenever there is "loss of reactor coolant system pressure coincident with a high reactor building pressure and/or high reactor building sump level." This is generally referred to by the senior operators as the "LOCA criteria." The criterion does not specify exactly what constitutes loss of reactor coolant system pressure or high building pressure. On the morning of March 28, the shift supervisor did evaluate plant conditions against the criterion but, as discussed in a previous section, he did not recognize that a small-break LOCA was occurring and, therefore, did not declare a site emergency at that time. The only clear conclusion is that the criterion as written was far too vague, and more specific criteria are required. Whether in fact the shift supervisor should have responded to this criterion by declaring a site emergency much earlier in the accident depends on the interpretation of the criterion.

The criteria for declaration of a general emergency include the requirement that it be declared when the dome monitor in the reactor containment building reaches 8 R/hr. When this occurred at approximately 0724, a general emergency was declared by the Emergency Director (station superintendent).

2. Information Flow

A review of various Pennsylvania Emergency Management Agency (PEMA) log books and discussions with representatives of relevant agencies along with the testimony of state Bureau of Radiation Protection (BRP) personnel, indicate that once the emergencies were declared, prompt notification of all individuals required by the emergency plan was accomplished.[9] The site emergency was declared at 0655 and by 0715 all the notifications had been completed. Similarly the general emergency was declared at 0724 and by 0740 the notifications were complete. By 0815 on-site assembly and accountability was completed with all personnel accounted for.

After emergencies are declared the emergency plan specifies that a line of communication be maintained with the Pennsylvania BRP. The log books maintained by this agency and the testimony of agency officials indicate that the information flow regarding radiation releases was generally satisfactory for the needs of this agency. The Unit 1 control room was established as the area from which radiological dose projections and monitoring on- and off-site were directed. Open telephone lines were maintained with both the NRC and BRP. The communications appear to have continued throughout the period when there were measurable releases of radioactivity.

Up-to-date information on plant status was not communicated as fully as desirable to the senior utility management and the NRC. It should be noted, however, that NRC personnel were in both control rooms by about 1000 hours, and they maintained continuous communication with their regional office.

3. Events of March 30

At 0710 on Friday, March 30 Unit 2 began an approximate two hour venting of the makeup tank to the vent header. This process was required to relieve the pressure buildup in the makeup tank in order to reseat the relief valve on the makeup pump suction. The vented gases normally flow to the vent header and are then transferred by compression into waste gas decay tanks. Manual venting of the makeup tank for short intervals had been initiated on March 29 and was periodically repeated throughout March 30. Releases to the environment occurred during each venting process due to leakage in the vent header system (see Section II E).

When venting started on Friday morning, radiation monitoring teams surveyed levels in the down-wind direction and a helicopter monitored the airspace over Unit 2. The staff in the Unit I control room promptly reported the releases to the BRP, and continued to keep them informed regarding the current activity levels being released and the anticipated duration of the release. During the morning, however, some of the operating crew in the Unit 2 control room were unaware that this line of communication existed. To make sure that state agencies were aware of the events in progress, a supervisor in the Unit 2 control room notified the PEMA that a release was in progress. There was apparently some confusion in the communication and PEMA personnel interpreted one statement as indicating that an evacuation of surrounding personnel might become necessary.

The situation was further complicated by an NRC misunderstanding. The readings taken March 30 at 0800 by the helicopter monitoring the plume directly above Unit 2 were approximately 1200 mR/hr. Since this coincidentally corresponded to an NRC prediction of the expected ground level doses in the event of a waste gas tank rupture, officials in the NRC Bethesda office apparently interpreted the measured values as ground level readings. An NRC official then called the PEMA and recommended a local evacuation out to 10 miles. Eventually the confusion was untangled, but a precautionary evacuation of pregnant women and small children was agreed upon by Pennsylvania and NRC officials (see Ref. 7).

4. Identification of Off-Site Releases

Radiation monitoring teams were dispatched and began reporting on- and off-site doses as of 0746 on March 28. Initial radiation survey results on site in the downwind direction and off-site on the east shore of the river indicated radiation levels less than 1 mR/hr beta-gamma. The initial wind direction was toward the west shore. Realizing that it would take a monitoring team a significant amount of time to drive to the west shore, the Emergency Director requested the State Police helicopter. The helicopter arrived on site at 0835 and picked up a monitoring team. The helicopter team reported radiation levels of less than 1 mR/hr beta-gamma in Goldsboro at 0842. The TMI Emergency Director concurrently dispatched a monitoring team by vehicle to the west shore.

As field monitoring readings were received in the Unit 1 control room, they were transmitted to the BRP over the established phone line. This method of information flow to the state began at 0725 on March 28 and continued for the next several weeks. During the first several weeks following the accident at least four teams were used for monitoring, one team on the west shore, one on the east shore, one on-site and one in the helicopter. Once it was realized that a leak existed in the vent header system, it became standard procedure to position the monitoring teams in the down wind direction and place the helicopter over the vent stack during a makeup tank venting evolution.

5. <u>Emergency Plan Adequacy</u>

The emergency plan as written was effectively implemented. In retrospect, however, it is clear that the emergency plan which existed at the time of the accident underestimated the organizational and communication difficulties which would arise. The plan, training, and drills were designed to cope with rapidly developing scenarios which could be handled by an augmented on-site emergency organization and a simplified communications network between the licensee and state agencies. This type of scenario was not the one experienced at TMI.

The protracted series of events which actually occurred revealed inadequacies in the organizational support, in the communication system and in the predefined information flow network required for accident management. The TMI experience showed that a large off-site support organization is needed to assist the in-plant organization and this organization grew out of necessity. The TMI-2 scenario permitted many organizations, both inside and outside GPU, to become involved in accident management and information release to the media and public. The events which occurred the morning of March 30 vividly point out the communication deficiencies in the plan.

There were also problem areas with communication equipment. Although adequate for initial notification, the phone capability in each control room was inadequate to cope with the subsequent communication load. The walkie-talkies used by the off-site monitoring teams did not possess sufficient signal strength to provide reliable communication capability at the longer distances traversed by the teams. Until additional phone lines were added, communications with off-site support personnel were very restricted. There was no predefined communication mechanism to provide adequate management awareness, utilize B&W, GPU and NRC technical support, and provide for unified releases of information to the media from a single source.

Off-site monitoring teams encountered two other problems. First, the DC/AC inverter units used to power the air samplers were used so heavily that a significant number of them burned out. Secondly, the SAM-2 analyzers were unable to accurately determine iodine concentrations because the air sample charcoal cartridges became saturated with xenon. Analyzing iodine concentrations in a significant xenon cloud may in the future require sending the samples to an offsite counting lab.

D. PRESSURIZER RELIEF VALVE FAILURE MODE

The TMI-II power-operated relief valve (PORV), also called a pilot-operated relief valve, is an electromatic relief valve manufactured by Dresser Industries. This same valve is used on all but one of the B&W series 177 nuclear plants, and is also used on at least one Combustion Engineering plant (Palisades).

The most complete list of instances in which a power operated relief valve failed open is contained in a supporting staff report to reference 5. The 12 known instances in which the valve failed open are summarized in Table 3. The failures at Beznau and Davis Besse occurred on valves supplied by other manufacturers. Of the 8 failures of Dresser valves with known causes, 3 were electrical failures, 4 were mechanical failures, and 1 (Rancho Seco) was a leaking valve rather than a real failure. It is significant that 5 of the 8 failures occurred prior to commercial operation of the plant.[10]

A review of the observed failure modes does not provide any clear indication of why the valve failed to close at TMI-2.[11] Most of the problems are not of a generic nature but rather random causes. The one generic failure mode associated with the Oconee-3 and Crystal River events was binding of parts which prevented closure of the pilot valve. Dresser subsequently initiated a design modification to prevent future failures of this type. The PORVs on both TMI Units were modified in 1977 per Dresser and B&W instructions.

The history of the TMI-2 PORV also does not reveal the cause of failure.[11] The Unit 2 valve was originally installed in 1974 on Unit 1 as replacement for Unit 1 valve while it underwent modifications. The valve was returned to Unit 2 in September 1975. Minor modifications were subsequently made to the valve in 1977 and 1978 but none of these are suspected to have led to its failure in 1979.

An earlier investigation[12] concluded that the PORV had been leaking prior to the accident. This conclusion was based on the elevated tail pipe temperatures downstream of the PORV. A more thorough investigation[13] however, has shown that one of the code safeties had been leaking, and a repair request had been generated by the plant operating staff to repair it. Since the PORV and safety valves discharge to a common header, the leaking safety valve was the cause of the elevated tail pipe temperatures.

In summary the cause for the PORV failure in the open position cannot be determined from information currently available. The failure mode may be determined once the valve can be inspected.

TABLE 3 - STUCK OPEN PORVs in PWRs

REACTOR	DATE	ASSIGNED CAUSE
Palisades **	9/71	Loss of power
Oconee-2 **	8/73	Wiring error
Oconee-2 **	11/73	Pilot leakage
Beznau	8/74	Fractured housing
ANO-1 #**	8/74	Pilot vent line
Oconee-3 #**	6/75	Corroding leakage
Crystal River **	11/75	Stuck solenoid
Davis-Besse #	9/77	Missing relay
Davis-Besse	10/77	Pilot stem clearance
TMI-2 #**	3/78	Loss of power
Rancho Seco #**	6/78	Leakage
TMI-2 **	3/79	Unknown

** Dresser supplied PORV

Reported in NUREG-0560

Note: The Rancho Seco event of 6/78 was included in the open PORV listing of NUREG-0560, but was apparently of leakage variety.

E. PATHWAYS BY WHICH RADIOACTIVE FLUIDS WERE TRANSPORTED

The principal releases of radioactivity resulting from the TMI-2 accident were gaseous releases which occurred on March 28, 29 and 30. Several investigations have been carried out to determine the pathways by which these releases occurred.[7,12,14,15] GPU has sponsored an independent evaluation of the pathways[16] and this is believed to be the most thorough and definitive of the investigations.

It is now believed that the principal pathway for releases of gaseous activity (see Figure 1) was via leaks in the radwaste gas system into the auxiliary building and out the stack. On March 28 the radioactive gas was transported to the radwaste system from vents on the reactor coolant drain tank and bleed tanks. The drain tank received the discharge from the PORV. The bleed tanks contained large amounts of radioactive gases probably due to lifting of relief valves in the letdown and makeup system. On March 29 and 30 the radioactive gas in the radwaste gas system resulted from deliberate venting of the makeup tank which was required to support safe operation of the plant.

These release paths as well as others which were smaller contributors to the total releases are discussed in the following sections.

1. Gaseous Releases from the Radwaste Gas System

Helium leak tests performed after the accident identified seven leaks in the RWGS. Six of these were on the discharge from the waste gas compressors: five flange leaks and one valve body to bonnet leak. The other leak was on a pipe common to the inlet of both compressors, on the outlet flange from a liquid drainer. The existence of leaks in the system is supported by observations prior to the accident that, the waste gas decay tanks would lose a couple of psi over the several day period after pressurization. Since the tanks were kept constantly at a pressure of greater than 80 psig for the day following the accident, leakage was likely. It is believed that radioactive gases released through these leaks and thence through the station vent to the environment constituted a principal source of offsite doses.

There were several known releases from the radwaste gas system (RWGS) associated with the construction and testing of a discharge bypass line from the waste gas decay tanks to the reactor building on March 30 and April 1. These releases combined with those associated with venting the makeup tank (discussed below) are believed to have accounted for essentially all of the releases on March 29 and 30.

2. Reactor Coolant Bleed Holdup Tanks

The reactor coolant bleed holdup tanks are known (from shift logs) to have received increases in inventory on the 28th. In addition, extremely high levels of radiation (1000 R/Hr) existed in the area

PRINCIPAL PATHWAYS FOR RELEASE OF GASEOUS RADIOACTIVITY

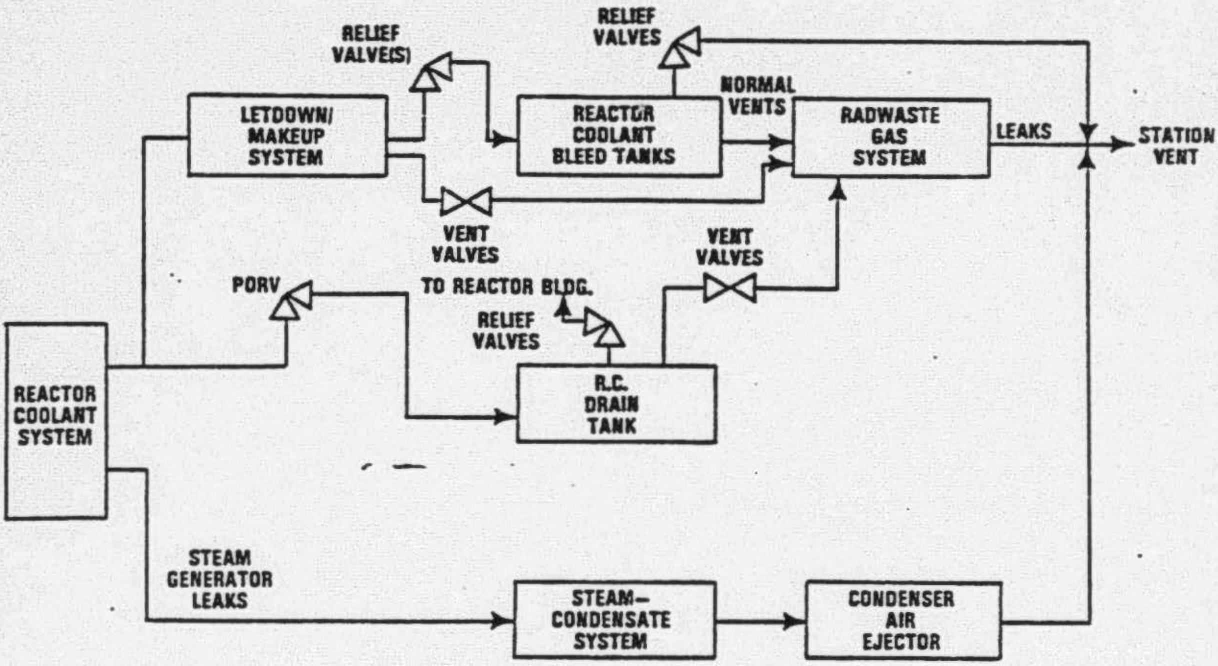

FIGURE I

of the tanks after the accident. The bleed tanks are normally vented to the vent gas system, which utilizes two parallel compressors to transfer waste gas to the waste gas decay tanks. Since leaks were subsequently found in this system, this appears to be a part of the major release pathway on March 28.

In addition, the releases from the makeup and purification system (discussed below) probably caused a significant pressure buildup in the bleed tanks. Two relief valves on each tank (setpoint 20 psig) discharge directly to the station vent via the waste gas system relief header, bypassing the waste gas filters. Pressure relief may thus have contributed to the releases.

3. Reactor Coolant Drain Tank Vents

The reactor coolant drain tank (RCDT) vent also discharges to the RWGS vent header. This vent line is normally open and discharges to the RWGS via the reactor building vent header. Therefore, it is probable that during periods of high pressure, prior to the rupture disc bursting, water was discharged to the RWGS. Considering the pressures involved it is possible that the pressure relief valve on the reactor building vent header lifted, discharging water to the reactor building sump. Following the bursting of the rupture disc, opening of the PORV block valve caused sufficient pressure buildup in the RCDT to transport high activity vapor to the radwaste gas vent header. This was a viable pathway for release of radiation on March 28 until 0756 when the containment was isolated.

4. Relief Paths from the Makeup & Purification System

Pressures greater than normal were experienced in parts of the letdown portion of the Makeup-Purification system on March 28. This resulted from flow restrictions caused by physical blockage of the purification filters and demineralizers by "crud" or boron percipitated from the reactor coolant system, and/or the accumulation of reactor coolant system gas in the makeup tank. The increased pressure almost certainly resulted in the lifting of one or more of the relief valves in the letdown system. This is confirmed by observed makeup tank level and letdown flow oscillations, which indicate relief valves opening and closing.

The letdown and makeup system contains various relief valves. Of these, MU-R3 is considered likely to have been a pressure relief path. It is set at 130 psig and is upstream of the demineralizer filters (MU-F5A & B). Blockage by solid matter filtered from the reactor coolant system would cause flow restrictions and higher than normal pressures in the section of the letdown line where MU-R3 is located. As a result, reactor coolant (with higher than normal activity levels following the loss of cladding integrity) would be transported to the reactor coolant (RC) bleed holdup tanks and vented to the waste gas system.

Relief valve MU-R1 is located downstream of the makeup tank. Off gassing in the makeup tank probably caused a pressure buildup sufficient to lift MU-R1 (set point 80 psig) which also discharges to the RC bleed holdup tanks.

The lifting of relief valves MU-R5A & B is unlikely by either of the above mentioned mechanisms. Pressure drops across both the filters and demineralizers would prevent MU-R5A & B (located downstream of the demineralizers) from seeing high pressures. The higher setpoint of 150 psig for MU-5A & B also supports the conclusion that it was MU-R3 which provided the primary relief path. High pressure in the makeup tank would be relieved by MU-R1, and check valves MU-V133 and MU-V107A & B (all located downstream of MU-R5A & B) would prevent backflow through the letdown line and out MU-R5A & B.

Starting 0435 on March 29th the makeup tank was periodically vented to the radwaste gas system vent header by opening MU-V13. Examination of strip chart recorders shows a strong, repetitive correlation between this venting and the increase in radiation levels on several area gamma monitors in the auxiliary building and fuel handling building. It has been concluded by all investigations that releases associated with venting the makeup tank represent a large fraction of the total releases on March 29 and 30. There is no evidence of similar venting activities on March 28th.

5. Steam Generator Leak

Based on the behavior of steam generator "B", the operators suspected on March 28 that a primary to secondary leak had occurred, and this was confirmed by subsequent water samples. Steam generator "B", after being isolated at 0527, was reactivated at 0645. Strip chart recorders (HP-UR-3236-CH 7) indicate a gaseous release from the condenser vacuum pump exhaust beginning at approximately 0700 with a rapid increase in activity. The discharge of the vacuum pumps bypasses the Auxiliary Building filters and is routed directly to the station vent. Steam generator "B" was reisolated at 0704, and remained isolated. The count rate on the exhaust monitor peaked at 0715, then decreased and stabilized by about 0830.

Attempts to quantify the releases from this pathway were not totally successful. Based on the available information, however, the total releases from the secondary system were believed to be substantially less than those via other pathways.

6. Liquid Releases

The large quantity of water which was released to the Auxiliary Building during the accident resulted primarily from leaks in the river water pump. These were known to be leaking prior to the accident. The relatively small quantity of radioactive water which led to contamination of the river water is believed to have been released through normal operation of the liquid drainers in the radwaste gas system, since some of the conditions discussed above undoubtedly led to significant quantities of radioactive water in the radwaste gas system.

F. FACTORS LEADING TO THE INCORRECT STATUS OF EFV-12A AND B

Investigations by several different bodies[1,7,12,15,17,18] have failed to identify the reason why the emergency feedwater block valves EF-V12A and B were found closed on the morning of March 28. The valves are known to have been closed on March 26 as part of performance of Surveillance procedure 2303-M27A/B. Existing documentation and operator testimony indicate that the valves were reopened at the completion of the procedure. The signed checkoff list, however, was considered only an operating tool and was not kept, so the only documentation is an entry that the entire procedure was completed. There is no evidence as to whether or not the valves were subsequently closed either deliberately or inadvertently. In particular, no evidence of sabotage was found.

The task force did not reinterview the operators involved in the surveillance procedure, because the thoroughness of the previous investigations made it unlikely that new information would be obtained. The investigation was rather centered on other aspects of the valve closure, including whether the surveillance procedures violated technical specifications, the practices which should guarantee proper line up of safety systems, the reasons why apparently incorrect positions could go undetected for a period of time, and such subsidiary factors as the possibility of a sneak circuit and the reason for the discoloration in one of the emergency feedwater train piping systems. These are discussed in the following sections.

1. Surveillance Procedure

Surveillance Procedure 2303-M27A/B is performed to ensure compliance with technical specification 4.0.5.a.2, which references section 11 of the ASME boiler and pressure vessel code for inservice testing of class 1, 2 and 3 pumps and valves. The valve operability portion of the surveillance procedure includes the checking of the non-return check valves to ensure they do not leak. It is the inclusion of this requirement in the procedure that led to having all feedwater paths to the steam generators simultaneously under pressure during the surveillance test. This was initially accomplished with valves EF-V11A & B, which are normally closed.

The simultaneous closure of the 12A and B header isolation valves during the surveillance test was the direct result of a procedure change request (PCR) dated August 10, 1978. This change, which called for the 12A and B valves to be in the closed position for the duration of the test, was requested because of leakage through the 11A and B valves, which resulted in relatively cold water being introduced into the steam generator and thermally cycling the emergency feedwater nozzles. The procedure change request was initiated by the Mechanical Maintenance Department, prepared by the Engineering Department, and reviewed and approved by the PORC and GRC groups. Procedure change requests have a nuclear safety evaluation section that must be filled out; section 2C questions "Does the attached procedure change or reduce the margin of safety as defined in the basis for any technical specification." The answer given was "No".

The applicable technical specification, 3.7.1.2.a & b, defines the emergency feedwater system as three independent steam generator emergency feedwater pumps and associated flow paths, and requires that it shall be operable as a limiting condition for operation. One "system" may be inoperable for 72 hours but must subsequently be returned to service or the plant be placed in hot shutdown within the next 12 hours.[12] The specification makes no statement regarding flow paths and/or components out of service, and is unclear as to the real requirement. While the surveillance procedure may not have violated the literal requirements, the Task Force believes that it was contrary to the intent of the specifications. In contrast the TMI-1 surveillance procedure indicates that at no time may two emergency feed trains simultaneously be out of service.

It should be noted that Surveillance Procedure 2303-M14A/B/C, Rev. 8 (Emergency Feedwater System Valve Lineup Verification and Operability Test and Turbine Driven Emergency Feed Pump Operability Test) (Rev. 7) also calls for simultaneous closure of feedwater header block valves 12A and 12B during the test.

2. <u>Alternate Procedure for Surveillance Tests on Emergency Feedwater Systems</u>

The procedure change that required closing the EF-V12 valves was initiated because of concern that the EF-V11 valves leaked. An obvious alternative is reduce the leakage past these valves so that the EF-V12 valves can remain open. If leakage cannot be stopped, the effect of the leakage should be evaluated to determine if the leakage and the thermal shock problem are in fact significant. Another approach would be provision for the EF-V12 valves to open automatically on emergency feed demand. They could then be closed during testing.

If none of the above approaches are practical, the ASME Power Test Code, Section XI Subsection IWV 3521 allows check valve testing to be deferred to plant shutdown as follows: "check valves shall be exercised to the position required to fulfill their function unless such operation is not practical during plant operation. Valves that cannot be exercised during plant operations shall be specifically identified and shall be full stroke exercised during cold shutdown. Full stroke exercising during cold shutdowns for all valves not full stroked exercised during plant operation shall be on a frequency determined by the intervals between shutdowns as follows: for intervals of 3 months or longer, exercise during each shutdown; for intervals of less than 3 months, full stroke exercise is not required unless 3 months have passed since the last shutdown exercise."

This postponement of testing would have to be justified by showing that testing during plant operation is not practical. If so, the Technical Specifications allow isolation of the emergency feedwater system when in Mode 3 with the steam generator pressure below 800 psig, so testing could be performed with the EF-V12 valves shut in this hot shutdown condition.

3. Why Improper Valve Alignment Went Undiscovered

The procedures and practices of the control room operators did not require written documentation of the status of valve positions. The operators were expected to routinely monitor the bench board parameters and indicators available. The actual watch-standing practices, however, apparently did not include a systematic check of safety system status as part of the routine duties. Control room operators interviewed by the task force reported[3] that they believe improperly aligned systems could have gone undetected for an extended period of time.

Shift turnover procedures also did not guarantee that incorrect alignment would be identified. Status lists or check lists were not used as part of the routine turnover. The shift change routine would reveal a particular system misalignment only if the system were known to be in an abnormal condition or if a test was in progress at the time of turnover. Since the test on March 26 was initiated and completed during the regular shift hours, the oncoming shift would only have been informed that the test had been successfully completed.

Finally, the color convention used for indicating lights at TMI-2 does not facilitate recognition of an improper system alignment, since red (or green) lights may be correct for some components and improper for others.

4. Surveillance Completion Practices

The general practice for completing a surveillance procedure was that the operator carrying out the test would complete it and sign off on a checklist. This checklist would then be taken to the shift foreman who was expected to verify that all steps had been signed off, and to make and maintain a record that the procedure had been satisfactorily completed. There was no provision for double checking either by the control room operators or by a second operator making an inspection in the plant, that the system was left in the correct alignment. There was thus no verification of the completion of the procedure.

5. Sneak Circuit Investigation

A separate investigation[18] was carried out to determine if a sneak circuit or other unknown circuit anomaly could have caused an inadvertent closure of the EFV-12 valves. The investigation consisted of a careful review of the design documentation followed by a detailed in-plant hardware check. The latter included physical inspection of components and cabling, and trial operation of the valves from the various control stations. It also included insulation resistance measurements for all cables and conductor resistance measurements, compared to the calculated resistance of the known length of the conductor.

No sneak circuits or other anomalies were found which could have resulted in accidental valve closure. The local control station buttons have rubber caps which make inadvertent operations extremely unlikely. Other components in the circuit were found to be in a normal condition.

Three discrepancies, however, were found between the installed circuitry and the design requirements:

1. In one case three conductors were terminated to a single terminal point in direct violation of the design requirement that no more than two conductors be terminated at any one point. This did not, however, affect the operation of the circuit.

2. A spare limit switch which, in the design documentation, was shown unconnected to any circuit, was, in fact, wired into the circuit in series with the limit switch which should have terminated valve closure on reaching the desired torque. The superfluous limit switch was actuated by the position of the valve actuator, and, due to the incorrect wiring, actually functioned to stop the valve closure prior to the time the desired torque had been achieved.

3. The overload heaters in the circuit which opened the valve were found to be undersized by a factor of three compared to the design requirements. The net result was that if the valve had temporarily stuck while being opened, the undersized overload heaters might have prevented the necessary torque from being exerted to complete the valve opening.

6. Feedwater Pipe Discoloration

Physical examination of the plant indicated that the feedwater piping between EFV-11B and the containment penetration was substantially discolored. The discoloration was greatest at the point of entry of the piping into the containment and in fact, the paint was actually blistered at this location. The discoloration diminished upstream from the containment entry.

Investigation has revealed that the discoloration was probably caused by hot water from steam generator "B" flowing backwards in the discolored line. Such discoloration would occur if the crossover check valve leaked or failed open, since there were many hours on March 28 when the pressure in steam generator "B" was significantly higher than that in steam generator "A". A test performed by heating a section of pipe support painted with the same paint used in the emergency feedwater line achieved the level of discoloration observed in the emergency feedwater line at temperatures ranging from 265°F for minimum discoloration to 420°F for the maximum discoloration and blistering observed. The actual water temperature in steam generator "B" was above 420°F concurrently with the required pressure differential for at least 4 hours on March 28.

G. ADEQUACY OF ASSESSMENT OF THE EXTENT OF DAMAGE TO THE CORE

Based on interviews with operators and other station personnel present in the control room early in the accident, it appears that early perception of the core condition differed greatly from the current understanding. The general opinion seems to have been that some fuel damage had occurred, but this was limited to cracking of some percentage of the fuel cladding. Some quotations referred to approximately 1% of the fuel having ruptured cladding.

The high incore thermocouple readings taken at about 8:00 a.m. on March 28 might have triggered recognition of the true core condition, but these readings were not widely known and were apparently not recognized as valid by the senior station management who did hear of them.

The task force found no indication that anyone made a substantial effort during the day of the accident to rigorously assess the likely state of the core. The personnel who might have made such an assessment were concentrating on reestablishing a stable core cooling mode, carrying out the emergency plan, and communicating with the many agencies and individuals who needed information. Realization of the presence of large quantities of hydrogen in the primary system appears to have first led to the realization that core damage was major. This assessment occurred late Thursday night, March 29 and early Friday morning, March 30. (Ref 19).

III. CONCLUSIONS

This investigation of the TMI accident has concentrated on identifying and evaluating the basic factors which contributed to the accident or related events. The approach has been to evaluate the significant factors using the perspective which has arisen as a result of the accident rather than previous standards. The intent of the evaluation has been to identify those areas where performance improvements are desirable and achieveable.

The overall conclusion of this investigation is that the TMI-2 accident was the result of a complex combination of factors. Problems arose from equipment design and/or operation, software (e.g., training and procedures), and human performance. No single factor would have been sufficient to cause the accident.

Equipment problems were found to result from deficiencies in design, installation, startup and test, operation and maintenance. Operation and maintenance problems in the condensate system, coupled with the limited capability of the system design to accommodate transients, resulted in the unit trip. Failure of the pilot operated relief valve (PORV) to reclose initiated the accident, and the plant operators had no direct indication of this failure. The plant design was such that previous non-LOCA transients had led to occurrences of high pressure injection (HPI), so initiation of HPI was not taken as a signal that an accident was in progress. Problems with the secondary plant systems distracted the operators. Finally the limited application of human engineering in the design of man/machine interfaces left the control room operators without ready access to some useful information, while besieging them with irrelevant alarms.

A basic software problem arose from lack of appreciation of the unique symptoms which would result from this event. The data base used for operator training and preparation of emergency procedures was limited to a LOCA which reduces both system pressure and pressurizer level. The limited attention which had been given to the consequences of a leak from the pressurizer did not focus on the difficulty in recognizing the leak, due to the rising pressurizer level. The operators also did not have access to information on the occurrence of a similar event at another plant. Furthermore, the simulator used for operator training did not have the capability for simulating a LOCA from the pressurizer vapor space. The operators thus expected loss of both pressure and pressurizer level if a LOCA occurred, and were not equipped to recognize a LOCA from the pressurizer vapor space in which pressurizer level did not reflect the system inventory.

A related problem arising from training and procedures was the attitude towards taking the plant solid. Although this was an appropriate response to the conditions which existed on March 28, neither the training program nor the emergency procedures gave any guidance regarding conditions under which solid operation might be desirable or necessary. In fact, taking the plant solid would have been a violation of technical specifications as well as several operating procedures. Solid operation was used only for hydrostatic testing, and never during normal operations, including refueling shutdowns. Simulator training also did not include solid plant operation. The net effect was to condition the operators against solid plant operation.

Other software and human factors played a role in the accident. Operator training in general had placed emphasis on attaining and maintaining an NRC operating license; in retrospect this approach did not guarantee a thorough understanding of the plant performance under all foreseeable situations. Casualty training, including simulator training, stressed planned response to predefined single failures, and did not deal with simultaneous multiple failures which present unique sets of symptoms to the operators, such as actually occurred at TMI. No training had been given in response to events which were not predefined. Emergency and operating procedures were found to provide unclear and in some cases contradictory guidance. Errors in operator judgement delayed isolation of the leak and resulted in prolonged operation at low reactor coolant system pressure. Precautions and limitations in some emergency procedures were overlooked or not recognized as applicable.

Finally, the nuclear design and regulatory process had emphasized conservative bounding analyses of unlikely plant accidents, which were intended to confirm that the overall design criteria had been met. For both unlikely accidents and expected plant transients, inadequate attention was given to predicting the most probable plant response. Training programs and operating procedures thus did not have a sufficient data base to provide the operator with all the needed information.

Review of the responses to the accident showed that the organizations involved had not perceived the magnitude nor duration of requirements in the post-trip period. The protracted series of events which actually occurred pointed out inadequacies in the organizational support, in the communication system, and in the predefined information flow network required for effective accident management. The TMI experience showed that a large off-site support organization is needed to assist the in-plant organization. While information flow to the cognizant state agency regarding releases of radioactivity was generally adequate, there was at least one case of contradictory information being released. Communication systems proved inadequate to properly inform utility management and the NRC of plant status and problems.

The task force investigations of other factors relevant to the accident led to the following conclusions:

(1) The root cause of the reactor trip was water in the instrument air lines to the solenoids on the condensate polisher discharge block valves;

(2) The reason why the PORV stuck open cannot be determined until the valve can be inspected, if then;

(3) The principal pathway for release of radioactive material to the environment was gaseous releases from the Radwaste Gas system;

(4) The reason for the incorrect status of the emergency feedwater block valves is not known.

(5) Plant staff and company management concentrated on plant cooldown, emergency response and communications on March 28 rather than assessment of total core damages. Realization of the extent of core damage resulted from discovery of the hydrogen bubble.

These investigations also revealed problems which, although not direct causes of the accident, should be corrected. Attempts to determine the exact nature of the initiating event led to the discovery of (1) undocumented and in some cases apparently erroneous modifications to secondary system components, (2) system and component operating problems which should have been detected and corrected during initial plant startup, and (3) substandard practices in modifications to electrical circuitry. Investigation of the emergency feedwater valve closure revealed that watch standing procedures and practices were inadequate to detect incorrect alignment of safety system components.

The task force did not perform a thorough review of the role played by TMI management relative to the identified problems, primarily because the management structure was significantly changed from that which existed at the time of the accident. The task force did, however, develop some recommendations for future management actions, as discussed in the next section.

On a broader perspective the fact that the identified problems span the scope of responsibility of nuclear vendor, architect/engineer, constructor, owner/operator and regulators suggests that the types of problems identified in this investigation are not unique to TMI. The task force investigation was specifically confined to TMI-2, and therefore reflects the performance of organizations other than GPU/Met-Ed only to the extent that those organizations directly participated in the TMI-2 project. The measures of performance available prior to the accident, however, indicated that in areas such as total resources available, performance of operators on exams, etc., TMI was at least as good as the average nuclear plant. It seems a permissible inference that the entire nuclear industry had become somewhat complacent regarding the possibility of a transient leading to major core damage. This attitude probably stemmed from the outstanding safety record of the nuclear industry, coupled with a belief that current regulatory practices provided adequate protection. In any event, it appears likely that the industry in general would profit from a careful and critical review of its current levels of performance and an upgrading of performance standards where appropriate.

IV. RECOMMENDATIONS

A. General Recommendations

The overall recommendation is for an upgraded standard of performance for all aspects of the nuclear related operation. This requires two significant changes.

1. Increased resources are required at the working level to support specific changes discussed below. This may be accomplished at least in part by improving the efficiency of the total operation, but may also require added resources. This change in resource requirements and allocation should be regarded as a continuing need.

2. New standards of personnel performance are required at all levels in the plant organization. This requires that fair and realistic but strict standards be set, communicated and enforced on a continuing basis.

The responsibilities for the safe and reliable operation of the unit must be communicated to and understood by each individual associated with the unit. Everyone must understand that management will do its part in making sure that adequate resources are available at the working level, and that each member of the organization is expected to do his or her part in ensuring that these resources are effectively and efficiently utilized.

B. Specific Recommendations

1. A comprehensive study of training needs should be conducted covering all areas of the organization including operations, maintenance, health physics, quality assurance, and plant staff, and all levels of personnel including technicians, engineers, supervisors and management. The result of this study should be used to modify the training program.

   The revised program should be structured to the groups that it will train. Operators should be trained to recognize abnormal plant response, to identify accident causes from the diverse data sources available to them, and then to apply their plant knowledge and use procedures effectively to correct the condition. Supervisors should be trained to evaluate information and to make the decisions that result in proper action during casualty situations. They must also be trained in methods of administering the plant to insure that operators are always aware of system and equipment status and are prepared to respond to abnormal situations. The plant engineering staff must be trained in plant operations so that they are better equipped to apply their knowledge to support the operations staff in areas of (a) procedure writing, review and implementation; (b) operations review; and (c) evaluating and advising during abnormal plant conditions.

The operator training program should be carefully reviewed to ensure that all operations which might be required under emergency conditions are covered in the program, both in classroom training and at the simulator. Specific operations which must be added to those previously covered in the training program include conditions under which the plant should be taken solid, methods for operating the plant when solid, transition to natural circulation and operation under natural circulation. In addition, the training program should specifically instruct the operator in how to respond to a plant condition which does not appear to be covered by the predefined events emphasized in the training program. It should include: techniques for diagnosing the problem or problems; which plant parameters to focus on to insure basic safety; methods to be used to bring additional technical resources to bear on the problem; and the authority and responsibility of the operating staff to deviate from previous directions when required to respond to unforeseen situations.

A general review of the upgraded training program should be performed by an independent group to ensure that the entire spectrum of training needs is being addressed. Reviews of the upgraded training program which are completed include (1) the Ad-Hoc Advisory Committees on Personnel Selection & Training and Man-Machine Interface & Communications, (2) the Penn State Pedagogical Review Committee and (3) the TMI-1 Operator Training Review Committee. In addition, plant management should require independent periodic assessments to evaluate training effectiveness in satisfying the established needs of the program.

2. Watch standing and shift turnover practices should be upgraded. Watch station responsibilities should be clearly defined. Formal procedures to assure operator awareness of the plant status should be critically reviewed and revised to provide an efficient integrated and manageable method for obtaining and controlling plant status. Evaluation of operator awareness by such techniques at random, unannounced checks (alertness drills) would also be useful. Watch standing communications should be formalized and utilized uniformly.

3. The emergency operating procedures should be completely revised. The basic approach should be hierarchial response to all casualty conditions, to ensure that the basic nuclear safety needs are satisfied before addressing equipment protection and recovery activities. A general diagnostic procedure should be developed to facilitate identification of applicable emergency procedures and to assist in dealing with multiple casualties. Specific procedures covering particular accident conditions would then be used for longer term recovery.

The intent of the actions required by a procedure should be clearly understandable to the user and the technical basis should be thoroughly emphasized in the training program. A procedure should establish time guidelines for completion of immediate and follow-up actions to help the operator establish priorities. Symptoms should be described in a manner that allows the operator to interpret the degree and probability of accident causes. Conditions which must exist prior to overriding safety systems must be clearly defined. Technical deficiencies in these and other procedures should be identified and corrected. The interfaces between and among procedures should be clearly explained.

In order to improve the quality of procedures, an integrated procedure development and review system needs to be implemented. The specification for the system should clearly delineate responsibilities for initial development, technical reviews, safety reviews and final product physical quality (e.g., legibility). The technical review system should provide for a multiple level of review and revision by the using group, on-site engineering, and off-site engineering and design groups. The final review by PORC or its successor should concentrate on the safety issue addressed. The group responsible for the physical quality of the final procedure should ensure the procedure is clearly written and understandable for the specific using group, and that the print, figures and tables are of good quality and legible, and understandable in the using environment (e.g., control room during a transient or maintenance location as appropriate).

4. Steps should be taken to ensure compliance with procedures. Suggested methods include classroom training in use of procedures, emphasis on use of procedures during simulator training, and in-plant audits to reveal the extent to which procedures are used and complied with. The inviolate nature of procedures in use during normal operations must be emphasized. Where procedures for normal operations are found to be inadequate or in error, changes must be made immediately using formal temporary and permanent change processes. Continuation of normal operations without these approved changes should not be allowed. For rapid transients or accidents, guidelines for making deviations should be preestablished and emphasized as part of the training program. Situations in which deviations from procedures may be required should be discussed with operators and incorporated into compliance guidelines.

   Positive steps should be taken to insure that all modifications to plant equipment are reviewed and approved in advance, and are thoroughly documented.

   Improved administrative controls for ensuring completion of operating, maintenance, and surveillance procedures should be implemented. These might involve, for example, independent check-offs by an independent party.

5. A periodic review of the watchstanding organization should be performed to ensure that the following guidelines are met on a continuing basis.

   a. The shift supervisor and shift foremen must be kept sufficiently free of other responsibilities that they can adequately perform their basic management function of assuring safe and efficient plant operation. This requires, for example, that they have sufficient time to maintain current and detailed knowledge of the plant condition and status.

   b. Adequate analytical capability must be immediately available at all times to ensure a technically correct and timely response to any unusual plant conditions.

   c. The number of control room and auxiliary operators must be sufficient to carry out all required operations, but should not be so large as to impair the efficiency of the operations.

   d. The support required by the watchstanding operation such as personnel, administrative, purchasing, etc., should be completely satisfactory in quantity, quality and timeliness.

   e. The relationship between the watchstanding organizations at Unit 1 and Unit 2 should be appropriate for the then current condition of the two plants. At present this should imply two completely separate watchstanding organizations but for future different conditions it may be desirable to explore other alternatives.

6. The approach to emergency planning should be improved. This should include the development of a predefined off-site support organization staffed by in-plant and technical support personnel. Communications concepts must be substantially upgraded and the equipment to achieve the concepts designed, purchased and installed. In-plant communications should be based on systems used only by operators, and capable of use with respirators. They should be compatible with off-site systems through plug-in phones or radios. Both on-site and off-site support centers should have real-time computer terminals with access to the plant data base. The communications of information from the company to the media must be organized and the mechanisms defined. An emergency classification system which provides for a better graded level of response must be developed. The criteria which initiate emergencies must cover a broader range of plant problems and must be clearly and unambiguously worded so that a minimum of discretionary judgment is required to determine whether one has been exceeded.

7. For all management level and operating positions in the new TMI organization and for other selected non-management positions, the accountabilities of the position and the authorities delegated to

it should be clearly delineated. This should include entry qualifications and standards used to measure the performance of individuals holding these positions. The interfaces between the plant operational staff and the supporting engineering and other technical groups should be clearly and formally defined. Considerable emphasis should be placed on insuring that all individuals involved understand how these interfaces are to work and under what conditions they should be used. The offsite groups should be assigned specific accountabilities to support the plant operation both on request and on a continuing basis. The above information should be documented in an organization manual.

8. As soon as the new nuclear organization is finalized and fully staffed, an independent team should conduct a thorough review to ensure that the organizational structure will achieve the desired performance in an effective and efficient manner. The review should also verify that each member within the organization understands how it will work and how his particular responsibilities relate to the total organization. The review team should also investigate whether resources are maximized at the point of work rather than in administrative overhead.

9. The effectiveness of the plant operational review committee (PORC) or its equivalent should be substantially improved. This may require improved committee organization and staff support, greater time commitment on the part of the senior members of the committee, and more complete reviews prior to PORC review.

10. The plant staff should be exposed to more technical data that would help them understand plant response. A formal method must be set up to insure this information flow on a continuing basis, and the involved portions of the organizations must be assigned specific accountabilities. To support this function a central technical group should be charged with providing information drawn from incident reports from other plants, transient analyses performed in support of safety evaluations, and other evaluations. In addition, this central group should review each TMI transient to determine the cause and to recommend measures to prevent or avoid reoccurrence of undesirable events. Where appropriate, specific analytical tasks should be performed by support organizations to provide the operating staff with desired data.

11. The overall information flow to the control room operator should be improved. An upgraded computer system, including modern input/output devices with data format matched to operator needs should be provided. Trending capabilities should be improved and should include capability for multi-parameter plots. The Unit 2 annunciator system should be changed to provide a better method of locating and identifying alarms. Multiple acknowledge levels should be provided, and the location and grouping of important alarms should be reviewed. Consideration should be given to the incorporation of a critical system status board or equivalent, which would make it

easy for the operator to rapidly determine whether all safety systems are in their operational state. This might be accomplished by a hard-wired panel in the control room or alternately might be accomplished through the expanded computer system.

The human engineering of the TMI 1 and 2 control rooms should be reviewed to identify the potential for human error. A comprehensive review should be conducted which considers the interaction of operators with plant systems, procedures and other operator aids during normal and off-normal conditions. Changes recommended by the review should be implemented on a schedule consistent with plant operational considerations. The TMI-1 control room study currently in progress will satisfy this recommendation. The report of the Ad Hoc Committee on Man-Machine Interface[6] contains additional detailed recommendations for TMI-1 and 2.

12. The general condition of the as-built secondary side of the plant should be verified by a careful review of design requirements and a detailed comparison of the entire BOP to these requirements. As-built drawings and associated documents should be verified and procedures and practices for control of all future changes should assure that these drawings/documents are kept current. Specific problems identified in this report (e.g. in section A.2, A.3, C.5, & F.2) and others identified by the BOP review should be corrected prior to the restart of Unit 2.

13. A formal suggestion system should be used which facilitates employees making suggestions for improved plant operation, which ensures that these suggestions receive appropriate consideration, and which guarantees that the employees will receive timely feedback on the disposition of their suggestion. The system should be simple to use and should avoid generating a proliferation of paperwork which interferes with its operation. For example, the system might utilize a printed form for making suggestions and responding to suggestions which consists of the original and two copies. The suggestor would fill out the top portion of the form by hand, describing his suggestion and the reason why it should be adopted. All three copies would be forwarded to a clerk who would log the suggestion and schedule it for review by a management team with authority to make immediate decisions. This review should occur perhaps once a month for suggestions submitted during the previous month. As a result of the review, the secretary would fill in the bottom of the form giving the disposition of the suggestion, the reasons and the anticipated schedule of any action. The original would then be forwarded to whichever department was assigned the action. One copy would be maintained in the master suggestion file and the third copy returned to the original suggestor.

14. A formal system should be implemented which documents degraded conditions of plant equipment and ensures corrective action is taken. The sytem should have as a primary objective an effective method of keeping operators on shift appraised of all critical

equipment that is out of service or operating in a degraded mode. The system should also facilitate documenting of minor deficiencies without burdensome paperwork on the part of the operations or maintenance staff.

15. Steps should be taken to ensure that desirable small improvements in the plant are not hindered by the difficulty in obtaining authorization to proceed with the improvements. This might be accomplished, for example, by making an annual resource fund available to the Manager of Plant Operations who would be authorized to spend this money for desirable improvements in the plant operation or maintenance without further approval.

16. A systematic evaluation of the response of the secondary plant to anticipated transients should be performed. This should utilize a mathematical model of appropriate portions of the condensate feedwater and steam systems. The results should be used to identify desirable improvements in control methods, setpoints, etc., in order to enhance the capability of the plant to withstand such transients with minimum interference with normal plant operation and minimum reliance on safety systems to protect the plant.

    Additional analysis of plant performance is required to increase understanding of events which are likely to occur during operation. Analysis methods such as failure modes and effects analyses, safety sequence diagrams and fault and event trees can be used to identify event sequences which may differ from those assumed in the design and licensing processes. Additional analyses are also required for each event to ensure recognition of the symptoms and response for the full spectrum of severity of that event. The results of this work should be input to design reviews, procedures and training.

    Recognizing that no attempt to predefine all possible failure methods and event scenarios can be complete, analysis is also required to aid in diagnosis of plant conditions and development of guidelines for action which do not depend on knowledge of the specific events which led to the existing condition.

17. The plant has been designed to be tolerant of some degree of degraded component and system performance. Operation with degraded conditions should be carefully evaluated to ensure that anomalies, individually or collectively, do not obscure abnormal performance directly or by reducing the sensitivity of the operator to symptoms of abnormal performance. Such evaluations might include a review of the operating and emergency procedures to determine which ones would be affected by the abnormal condition(s) and what the effect would be. Analysis, including simulation, might be required to enable a thorough evaluation. Based on this review, modifications to procedures, alterations of operating limits, alarm setpoints or monitoring requirements could be considered along with training of operators to support changes.

The final judgement as to whether to continue operations should be based on the collective impact of the existing anomalies. This judgement should be made by senior plant management.

Because of the difficulties of conducting such a objective evaluation, the goal should be to keep the number and degree of anomalies minimal.

18. Finally, Senior Management must ensure that the improvements resulting from this accident continue in effect on a long term basis. Unless this point is effectively implemented, the improved performance may gradually degrade.

V. REFERENCES

1. "TMI Unit 2 Loss of Feedwater Flow Leading to the Accident of March 28, 1979," K. P. Lucien Sept. 1, 1979. Rev. 1 July 1980.

2. Met-Ed Memo dated July 13, 1979 to J. R. Floyd from Donald A Berry, "Condensate Polisher Valve Malfunction."

3. Task Force Interviews with:

   a. W. Zewe & Crew - August 24 & 25, 1979
   b. W. Zewe & Crew - September 19, 1979
   c. C. Faust - September 19, 1979
   d. F. Scheimann, September 19, 1979
   e. E. Frederick, September 19, 1979
   f. J. Logan, September 19, 1979
   g. Bernie Smith & Crew, September 20, 1979
   h. George Kunder, September 20, 1979

4. "Preliminary Annotated Sequence of Events, March 28, 1979," Rev. 1, dated July 16, 1979.

5. TDR-054 (was TDR TMI-111), "Analysis of TMI-2 Operator Response," P. S. Walsh and T. G. Broughton, issued October 29, 1979.

6. "Report of Ad-Hoc Advisory Committee on Personnel Selection Training, Man-Machine Interface and Communications," Louis H. Roddis, Chairman, January 1980.

7. "Report of the President's Commission on the Accident at Three Mile Island," October 1979

8. "TMI Staff Interviews Concerning the March 28, 1979 Incident," Compiled by E. F. O'Connor, JCP&L, May 9, 1979.

9. TDR-TMI-114, A. Tsaggaris, "Emergency Plan Implementation," June 1979

10. TDR-080 "PORV Reliability and Change Modifications," J. H. Corea, April 24, 1980.

11. Q. Billingsley "PORV Failure Mode," TDR to be issued

12. NUREG 0600 "Investigation into the March 28, 1979 TMI Accident by Office of Inspection and Enforcement," USNRC dated August 1979.

13. TDR-126 "Investigation of TMI-2 Pressurizer PORV Discharge Pipe Temperatures," issued 2/28/80, Q. Billingsley, P. Maheshwari, et.al.

14. "Analysis of TMI-2 Accident," Nuclear Safety Analysis Center Report NSAC-1, Appendix Routes.

15. "Three Mile Island - A Report to the (NRC) Commissioner and to the Public," M. Rogovin and G. T. Frampton, Jr., January 24, 1980.

16. "Pathways for Transport of Radioactive Material Following the TMI-2 Accident," J. Paradiso (GPU), J. E. Flaherty (EI), July 1980.

17. Memo J. Miller to R. C. Arnold, "Preliminary Report on Emergency Feedwater System," dated April 18, 1979.

18. TDR 104, "Analysis of Testing of Emergency Feedwater Isolation Valves EF-V12A and EF-V12B," Ebasco and J. Gulati, dated August 24, 1979.

19. "Three Mile Island Accident Technical Support" by R. L. Long, GPUSC, T. M. Crimmins, JCP&L, and W. W. Lowe, Pickard, Lowe & Garrick, Inc., Submitted for publication in Nuclear Technology March 24, 1980.