NUREG/CR-1270
Vol. I

Human Factors Evaluation of Control Room Design and Operator Performance at Three Mile Island-2

Final Report

Manuscript Completed: December 1979
Date Published: January 1980

Prepared by
T. B. Malone, M. Kirkpatrick, K. Mallory, D. Eike, J. H. Johnson, R. W. Walker

The Essex Corporation
333 N. Fairfax Street
Alexandria, VA 22314

Prepared for
Three Mile Island Special Inquiry Group
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
NRC Contract No. 04-79-209

1-a

NRC FORM 335
(7-77)

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

1. REPORT NUMBER *(Assigned by DDC)*
NUREG/CR-1270, Vol. 1

4. TITLE AND SUBTITLE *(Add Volume No., if appropriate)*
Human Factors Evaluation of Control Room Design and Operator Performance at Three Mile Island-2

2. *(Leave blank)*

3. RECIPIENT'S ACCESSION NO.

7. AUTHOR(S)
T.B. Malone and others

5. DATE REPORT COMPLETED

MONTH	YEAR
December	1979

9. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS *(Include Zip Code)*

The Essex Corporation
333 N. Fairfax St.
Alexandria, Va.

DATE REPORT ISSUED

MONTH	YEAR
January	1980

6. *(Leave blank)*

8. *(Leave blank)*

12. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS *(Include Zip Code)*

Three Mile Island Special Inquiry Group
U. S. Nuclear Regulatory Commission
Washington, D. C. 20555

10. PROJECT/TASK/WORK UNIT NO

11. CONTRACT NO.
04-76-293-08

13. TYPE OF REPORT
Final

PERIOD COVERED *(Inclusive dates)*

15. SUPPLEMENTARY NOTES

14. *(Leave blank)*

16. ABSTRACT *(200 words or less)*

This report describes a study of human factors engineering aspects of the Three Mile Island-2 (TMI-2) accident on 28 March 1979. The objective of the study was to evaluate the causal contributions, if any, of operator performance and effects on operator performance of:

- Control room design
- Operator training
- Emergency procedures

The topic of the current report is the degree to which operator errors were, in turn, caused by human factors engineering aspects of the control room design, operator training, and emergency procedures.

17. KEY WORDS AND DOCUMENT ANALYSIS

17a. DESCRIPTORS

17b. IDENTIFIERS/OPEN-ENDED TERMS

18. AVAILABILITY STATEMENT
Unlimited

19. SECURITY CLASS *(This report)*
Unclassified

20. SECURITY CLASS *(This page)*
Unclassified

21. NO. OF PAGES

22. PRICE
$

*U.S. GOVERNMENT PRINTING OFFICE : 19800-308-886/6765

EXECUTIVE SUMMARY

Background

Almost immediately following the events that comprised what is now known as the 28 March 1979, accident at Three Mile Island, the NRC initiated a Special Inquiry Group to investigate the causes and consequences of the accident. Since it has been widely recognized that "human error" played a role in the accident, the Special Inquiry Group was interested in the extent to which factors incorporated within the discipline of human factors engineering (e.g., man-machine interface design, procedures, manning and training) were influential in causing or contributing to the course of the accident. In August 1979, NRC contracted with the Essex Corporation of Alexandria, Virginia, to conduct an assessment of the impact of human factors engineering in the accident. This report constitutes one product of that contractual effort.

Objectives and Scope

The specific objectives of the Essex effort are as follows:

- Establish if design of the interfaces between operators on the one hand, and equipment and information on the other, had an influence on the accident
- Determine if the control room at TMI-2 was designed according to human engineering methods, principles and standards
- Compare the design of TMI-2, from a human engineering standpoint, with the design of two other plants designed in the same time frame as TMI-2
- Determine if the design of TMI-2 is in compliance with NRC and industry standards and criteria
- Establish if design and use of procedures contributed to the accident
- Determine if manning levels and selection criteria contributed to the accident
- Establish if operator training contributed to the accident.

The scope of the study was limited to the initial 150 minutes of the accident which covers the period in which the accident developed to the point of uncovering the core. The remaining time within the accident period involved actions and reactions associated with the recovery from this event. The study was also limited to an assessment of the human factors engineering aspects of the control room as compared with other workstations within the plant. The study identified activities of all personnel involved in the initial 150 minutes of the accident but focused on the actions (and inactions) of the four control room shift personnel: the two control room operators, the shift foreman, and the shift supervisor.

The study was concerned with establishing the role of human factors engineering in the accident. Human factors engineering is defined as the science of applying behavioral principles to systems. It is concerned with integrating the human element of a system with the hardware, software, environments and information which make up the system. The province of human factors engineering essentially involves the prevention of human error. This is accomplished by designing hardware components, software and information specifically for the people who will use them, and by ensuring that these people have the prerequisite skills and knowledges to effectively perform the duties associated with their designated job. The primary areas of interest for human factors engineering in the TMI-2 incident, therefore, involve hardware design (controls, displays, labels, workspace), information content and format, procedures, operator selection and training, and control room manning.

Study Approach

The study was conducted in four tasks:

TASK A Control Room Design at TMI-2
TASK B Analysis of Control Room Activity
TASK C Evaluation of Operator Performance
TASK D Evaluation of Human Factors Engineering in CR Design

TASK A, Control Room Design at TMI-2, was basically concerned with the degree to which human factors engineering considerations were addressed in the TMI-2 design development process. This process was reviewed in light of human factors engineering criteria and practices existing at the time when TMI-2 was undergoing development. The design and development process and the product of the process for TMI-2 was then compared with processes and products for two plants designed in the same time period. This latter effort was undertaken to determine to what extent were plants generally constrained by existing standards and criteria. The assessment of the role of human factors engineering in the TMI-2 design process extended to criteria applied in the process (10CFR, industry standards, reactor technical memos, safety guides, regulatory guides, and the Standard Review Plan), management of the process, control room design planning, actual design of the control room and consoles, control room test and evaluation, and operations conducted in the control room.

TASK B, Analysis of Control Room Activity, was directed at an assessment of the effect of control room layout and arrangement on operator performance. The principal products of this task were a detailed sequence of activities for the 150 minute period, and a full-scale mockup of the consoles within the TMI-2 control room. The mockup was composed of exact scale photographs (280 in all) of TMI-2 panels mounted on Foam-Core representations of the consoles. The mockup was used to assess operator movements throughout the 150 minutes, and also to validate the sequence of activities. In the validation of operator timelines the crew on duty at TMI on 28 March 1979, directed a walkthrough of their actions during the 150 minutes.

TASK C, Operator Performance, was concerned with identifying the extent to which the accident was caused or influenced by factors such as control room manning, operator selection, and training. Assessments were conducted of the adequacy of manning, selection and training procedures and methods at TMI-2. Interviews with operators and training personnel provided inputs and insights into the adequacy of the selection and training practices.

TASK D, Evaluation of the Control Room Design in Terms of Human Factors Engineering, essentially involved application of human factors engineering test and evaluation methods and measures used in military systems T&E to the assessment of TMI-2 lighting, labeling, workspace, controls, displays, information processing and procedures.

Findings

The findings of this investigation concerning the human factors engineering aspects of the TMI control room and operations include the following:

Control Room Design

- Information required by operators is too often non-existent, poorly located, ambiguous, or difficult to read.
- Annunciators are poorly organized, are not color coded, are often difficult to read, and are not arranged in priority order.
- For the RCS, Pressurizer and Secondary System sub-panels of Panel 4, a total of 91% of applicable human engineering criteria for displays were not met.

- At TMI there are 1900 displays located on the vertical panels. Of these, 503, or 26% cannot be seen by a 5th percentile operator standing at the front panels.
- Labeling of controls and displays is in many cases inadequate or ambiguous, as indicated by the 800 changes made by the operators to the labels provided.
- For the RCS, Pressurizer and Secondary System sub-panels of Panel 4, a total of 68% of applicable human engineering criteria for labels were not met.

Control Room Development

- Human engineering planning at TMI-2 was virtually nonexistent.
- NRC and the nuclear industry have virtually ignored concerns for human error.
- Where operator - oriented control panel design bases were used (Calvert Cliffs and Oconee) the result was more effective man-machine integration.

Procedures

- A detailed asssessment of EP 2202-1.3 "Loss of Reactor Coolant/Reactor Coolant System Pressure" revealed serious deficiencies in content and format.
- There is little consistency between nomenclature used in procedures and that used on panel components.
- Instructions for control actions seldom provide an indication of the correct (or incorrect) system response.
- Procedures place an excessive burden on operator short-term memory.
- Charts and graphs are not integrated with the text.
- It is not clear which procedures apply to which situations.
- There is no formal method for getting operator inputs into updates of procedures.
- Procedures were grossly deficient in assisting the operators in diagnosing the feedwater system, diagnosing the PORV failure, determining when to override HPI, and determining when to go to natural circulation.

Training

- The Met. Ed. training program was in full compliance with government imposed standards concerning training.
- TMI-2 training was deficient in that it was not directed at the skills and knowledges required of the operators to safely job requirements.

- The essential operator skill is to be able to diagnose what is happening in the plant. The most effective training method of acquiring this skill is simulation. Only 5 percent of training time is used for simulation training.
- Training in emergency procedures was deficient.
- Training at TMI-2 failed to provide for measurement of operator capabilities.
- Training at TMI-2 was deficient in its training of instructors.
- Training at TMI-2 was based on an archaic approach to learning.
- Training at TMI-2 was not closely associated with procedures.
- Training at TMI-2 generally ignored the fact that operators are dealing with a slowly responding system..
- The training program at TMI-2 did not provide for formal updating and upgrading of methods, materials, and course content.
- Training at TMI-2 failed to establish in the crew the readiness necessary for effective and efficient performance.

Conclusions

The primary conclusion reached on the basis of this investigation was that the human errors experienced during the TMI incident were not due to operator deficiencies but rather to inadequacies in equipment design, information presentation, emergency procedures and training.

This general conclusion is supported by several more specific conclusions which are:

- TMI-2 was designed and built without a central concept or philosophy for man-machine integration.
- Lack of a central man-machine concept resulted in lack of definition of the role of operators during emergency situations.
- In the absence of a detailed analysis of information requirements by operator tasks, some critical parameters were not displayed, some were not immediately available to the operator because of location, and the operators were burdened with unnecessary information.
- The control room panel design at TMI-2 violates a number of human engineering principles resulting in excessive operator motion, workload, error probability, and response time.
- The emergency procedures at TMI-2 were deficient as aids to the operators primarily due to a failure to provide a systematic method of problem diagnosis.
- Operator training .failed to provide the operators with the skills necessary to diagnose the incident and take appropriate action.

- Conflicting implications between instrument information, training, and procedures precluded timely diagnosis of and effective response to the incident.

With these conclusions the present study is in full agreement with the President's Commission on TMI, which stated in their final report:

> In conclusion, while the major factor that turned this incident into a serious accident was inappropriate operator action, many factors contributed to the action of the operators, such as deficiencies in their training, lack of clarity in their operating procedures, failure of organizations to learn the proper lessons from previous incidents, and deficiencies in the design of the control room. . . Therefore — whether or not operator error explains this particular case — given all the above deficiencies, we are convinced that an accident like Three Mile Island was eventually inevitable.

ACKNOWLEDGEMENTS

The authors wish to thank the staff of the NRC Special Inquiry Group for their support and cooperation in the conduct of this study. Special thanks are extended to Mr. Gordon Chipman, Mr. Bernard Doyle, and Mr. Charles Miller. Appreciation is also extended to Met. Ed. personnel, especially training personnel and control room operators, for their patience and cooperation. Finally recognition must be made of the effort of a number of Essex people who significantly contributed to the study itself, to the fabrication of the mockup, and to the final report. These include:

Mr. William Brann, Systems Engineering Division, Camp Hill Office
Mr. Robert McGough, Systems Engineering Division, Camp Hill Office
Mr. Doug Metcalf, Systems Engineering Division, Alexandria Office
Mr. Kenneth Moore, Systems Engineering Division, Alexandria Office
Mr. James Bathurst, Behavioral Sciences Division, Huntsville Office
Mr. Kem Robertson, Behavioral Sciences Division, Huntsville Office
Mr. Nicholas Shields, Behavioral Sciences Division, Huntsville Office
Ms. Jane Shafer, Behavioral Sciences Division, Alexandria Office
Ms. Robin Walker, Behavioral Sciences Division, Alexandria Office
Mr. John Jacoby, Behavioral Sciences Division, Alexandria Office
Ms. Jessica Haher, Behavioral Sciences Division, Alexandria Office
Mr. Mark Fall, Behavioral Sciences Division, Alexandria Office
Ms. Vanessa Weedon, Behavioral Sciences Division, Alexandria Office
Ms. Kim Sanders, Behavioral Sciences Division, Alexandria Office
Ms. Mary Malone, Behavioral Sciences Division, Alexandria Office

1.0 INTRODUCTION

This report describes a study of human factors engineering aspects of the Three Mile Island-2 (TMI-2) accident on 28 March 1979. The objective of the study was to evaluate the causal contributions, if any, of operator performance and effects on operator performance of:

- Control room design
- Operator training
- Emergency procedures

A number of independent investigations have reached the conclusion that operator error was a significant cause of the accident (33, 48). This conclusion would be difficult to question. The topic of the current report, however, is the degree to which operator errors were, in turn, caused by human factors engineering aspects of the control room design, operator training, and emergency procedures.

1.1 Human Factors Engineering, Systems Engineering and the Three-Mile Island Accident

Human factors engineering is the science of applying behavioral principles to systems. It is concerned with integrating the human element with the system hardware, software, environments and information. The province of human factors engineering in systems development lies in two general areas: human engineering design and evaluation; and human resources development. Human engineering involves the research, development, test and evaluation necessary to ensure that systems hardware, software, environments and information are designed to support and enhance human performance capability. Human engineering provides the design and evaluation methods and criteria to ensure that equipment, procedures, documentation, environments, and information are designed in terms of human operator capabilities, limitations, and requirements. Human resources development is directed at specifying the role of people in the system as well as the number of people (manning), job entry skills and knowledge (selection), and development of required skills and knowledge (training).

The overall objective of human factors engineering is to prevent human error. This is largely achieved by ensuring that systems are developed which are compatible with the capabilities and limitations of personnel who operate, control, maintain, repair, manage, or otherwise use them. The scope of human engineering involves all of the interfaces between the human operator and systems hardware, software, information procedures, environments, and other operators. The scope of human resources development involves establishment of requirements for manning the system with fully qualified personnel in sufficient numbers to ensure optimal human performance.

As stated above, human factors engineering is defined as the science of applying behavioral principles to systems. Human factors engineering is, therefore, one of the many disciplines under the umbrella. Systems engineering is concerned with the analysis of system requirements, and the development and integration of system elements which satisfy these requirements within limitations imposed by operational, technological, and fiscal constraints. Systems engineering focuses on integration of diverse and often competing requirements to ensure that the system can process its inputs and achieve its outputs. Systems engineering achieves its primary outputs, design concepts and criteria through a process of compromise and trade-off. One of the more important trade-off issues within the system development process surrounds the questions of what role should man play in the system, what does he need to accomplish this role, and how is he to be integrated with the operations, components, information and environments of the system. These questions comprise the raison d'etre of human factors engineering. The contribution of human factors engineering to system development lies in design of system elements for operability, maintainability, habitability and safety, in the evaluation of human performance and safety in the conduct of human operations, and in the development of skilled personnel to manage, operate and repair the system. Human factors engineering can only be practiced within the context of a system engineering effort. If the two are independent, then human factors engineering concepts and criteria, requirements and standards will, by definition, fail to even begin to address the integration of systems personnel with other systems elements.

The Three Mile Island accident was clearly a case of man-machine system which failed to perform one of its intended functions. Both hardware failure and human error were causative in the accident. Because of the human error involvement, complete investigation required evaluation of the system design process and the relationship of the resulting man-machine integration (or lack thereof) to the accident.

1.2 Study Objectives and Scope

The primary issue addressed was, to what extent was operator performance, or lack of performance, directly caused or influenced by equipment design features, information availability and usability, emergency procedures, selection and training, and control room manning levels. The other side of this issue is, to what extent was operator performance the result of operator error with little or no impact from human engineering design and selection, manning and training. If human engineering and/or human resources development is judged to have contributed to the cause and severity of the accident, the next question is, why? Do other nuclear power plants exhibit the same problem to a similar extent, or are the problems unique to TMI-2? How adequate are the NRC and industry standards and criteria relating to human engineering design and training program development and operation? Is the TMI-2 design and training in compliance with these standards and criteria? How does human engineering of nuclear plants compare with the human engineering provided to other complex man-machine systems, e.g., weapon systems?

Specific study objectives included the following:

- Establish if design of the interfaces between operators on the one hand, and equipment and information on the other, had an influence on the accident
- Determine if the control room at TMI-2 was designed according to human engineering methods, principles and standards
- Compare the design of TMI-2, from a human engineering standpoint, with the design of two other plants designed in the same time frame as TMI-2
- Determine if the design of TMI-2 is in compliance with NRC and industry standards and criteria
- Establish if design and use of procedures contributed to the accident
- Determine if manning levels and selection criteria contributed to the accident
- Establish if operator training contributed to the accident

The scope of the investigation was limited to the intial 150 minutes of the accident. This period covers the development of the accident as opposed to the recovery from the accident. Shortly after the 150 minute point, radiation alarms associated with uncovering the core were received. Recognition of the severity of the problem and declaration of the site emergency followed shortly thereafter.

Analysis of personnel activities in the control room was focused on the principal operating staff — the shift supervisor, shift foreman, and two control room operators.

1.3 Study Approach

The study was conducted in four tasks:

TASK A, "Control Room Design at TMI-2" was concerned with identifying the criteria which influenced the control room design, and establishing the actual design basis and operating logic which led to the as-built design of the control room (CR). An assessment was made as to whether or not the CR was designed in accordance with the design bases and criteria. Finally the human engineering design of the TMI-2 CR was compared with that of two other same-vintage plants.

TASK B, "Control Room Activity" led to the development of operator timelines identifying what each operator did and where he was located. A full scale mockup of the complete control room was constructed and used to identify operator activities and traffic patterns. Figure 1 presents a view of the TMI-2 control room while Figure 2 depicts a portion of the Essex control room mockup.

TASK C, "Operator Performance" was concerned with evaluating the adequacy of the TMI-2 training program and of selection of manning criteria.

TASK D, "Application of Human Factors Principles to CR Design" comprised an evaluation of the human engineering aspects of the CR, specifically in terms of their contribution to operator actions and inactions within the initial 150 minutes of the accident.

The task activities and methods are described in Appendix A. Results of all tasks and conclusions reached are described in Section 2 in relation to the major operator actions/inactions during the incident. General results and conclusions are described in Section 3. The role of human factors in the nuclear power industry is assessed in Section 4. Details of methods and results are presented in Appendices.

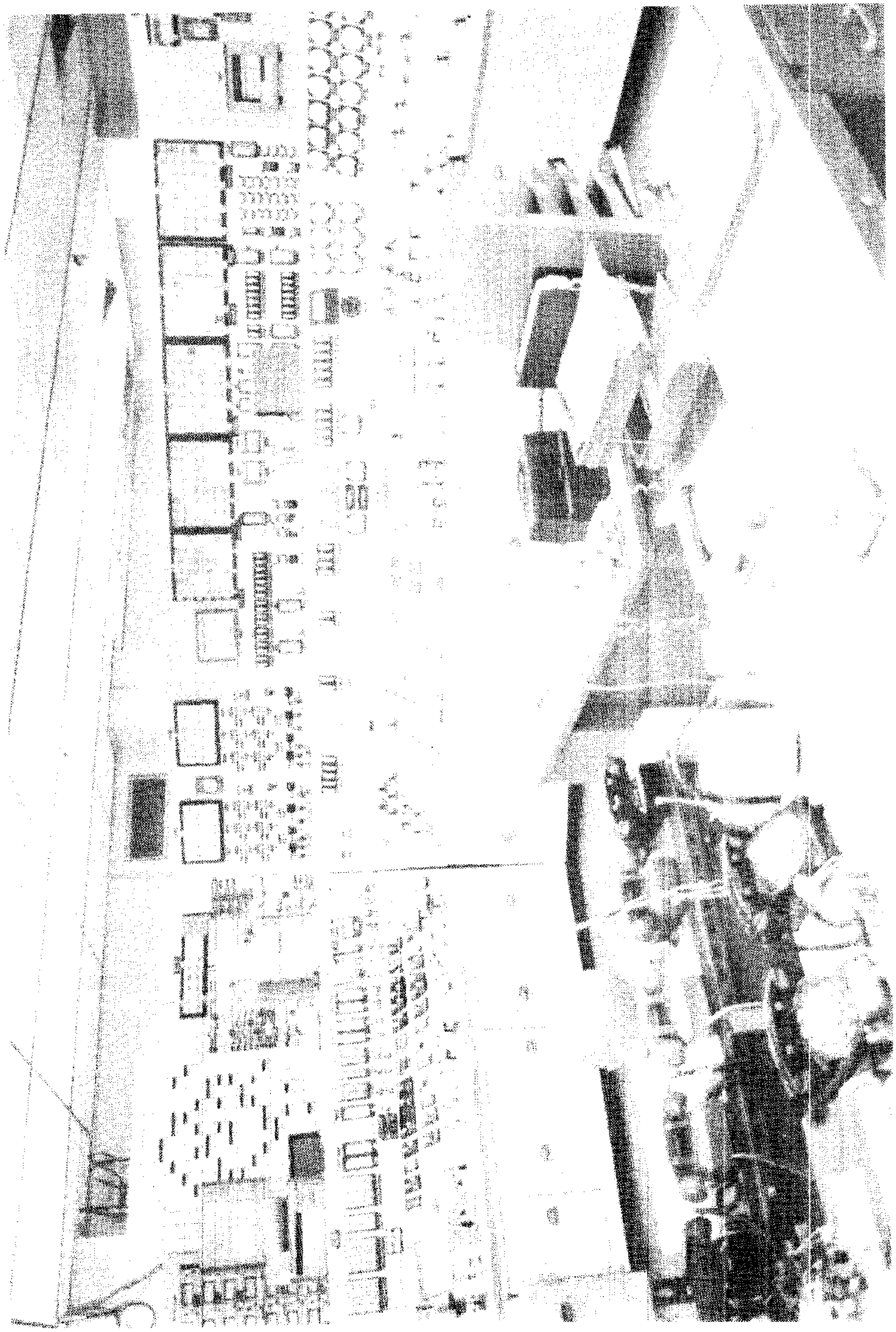


FIGURE 1
THE CONTROL ROOM AT TMI-2

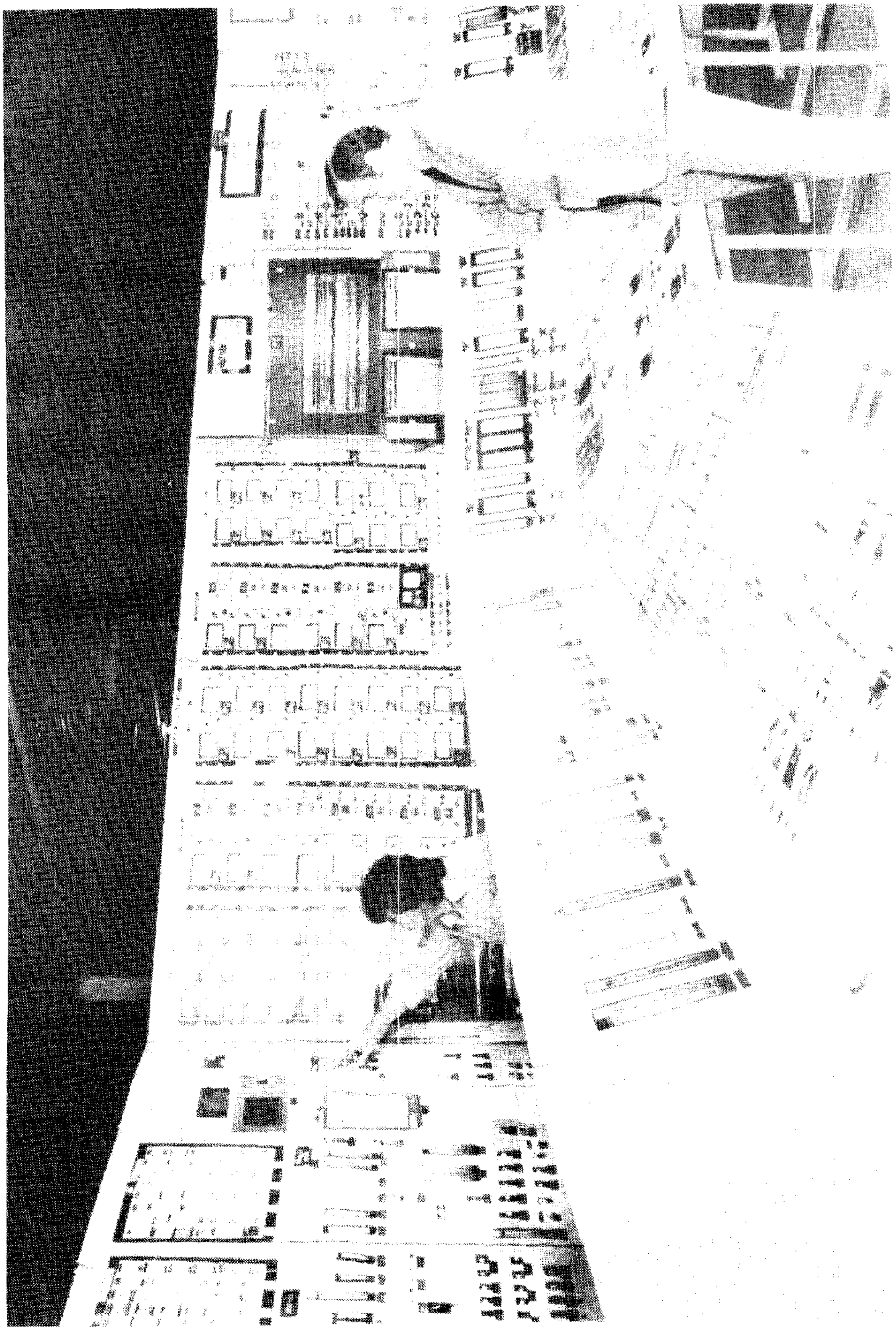


FIGURE 2
THE ESSEX TMI-2 MOCK-UP

2.0 THE ACCIDENT

2.1 TMI-2 Incident Summary

The incident at TMI-2 which began at 0400, 28 March 1979 was basically a Loss-of-Coolant Accident (LOCA). The loss of reactor coolant inventory through a Pilot Operated Relief Valve (PORV) resulted in rapid depressurization of the primary system and eventual core damage. During the incident, radioactive coolant which had been lost from the primary system was transferred to the auxiliary building and eventually to the atmosphere.

The fundamental LOCA situation was complicated by a number of unrelated plant problems which occupied a good deal of the operators' time and which considerably complicated the process of diagnosing the fundamental problem.

The current report focuses on operator activities and the relationship of significant operator actions/inactions to human engineering aspects of the control room design and to aspects of operator training and written procedures. For this reason, the chronology presented here is devoted to operator activities rather than to events in the plant itself. Detailed event and plant status chronologies have been presented elsewhere (33, 43) and this report does not attempt to duplicate such data except as they relate to displayed information available to the operators, operator decisions, and operator actions.

The scope of this report is the events transpiring in the CR during the first 150 minutes of the incident. This period of time includes the identification and blocking of the PORV but does not include the site emergency declaration. The period of 150 minutes is, therefore, a transition point between identification of the basic problem and emergency recovery operations.

The 28 March 1979 incident at TMI-2 began at approximately 0400 with closing of condensate polisher valves due to water in the instrument air lines. Lack of suction pressure led to tripping of condensate and condensate booster pumps. The main feedwater pumps tripped by plant design on loss of suction and the turbine tripped by plant design on loss of main feedwater. The emergency feedwater pumps started.

Loss of the turbine results in reduction of heat transfer from the primary system with consequent increases in volume, temperature, and pressure in the reactor coolant system. Pressure rapidly reached the PORV opening setpoint of 2255 psi and the PORV opened releasing coolant to the reactor coolant drain tank (RCDT). The PORV opening was a normal response to relieve high primary pressure. Pressure increased to the reactor trip setpoint of 2355 psi and the reactor tripped at about 8 seconds. Decreasing RCS pressure should have resulted in closing the PORV at 2205 psi, but it failed to close and remained open at this point. The open PORV was not recognized by the operators until 138 minutes during which time depressurization of the primary system led to void formation and extensive core damage.

Dropping RCS pressure reached 1640 psi at about 2 minutes when high pressure injection was initiated automatically by the engineered safety features logic. RCS pressurizer level was rising at this point as expected by the operators. Operator training and procedures stress control of level in the pressurizer to avoid a solid primary system. With pressurizer rapidly increasing, operators became concerned about going solid due to continued HPI flow. They, therefore, bypassed the ES and throttled makeup flow despite the fact that primary pressure was decreasing.

Shortly after this, the RCS hot leg temperature and RCS pressure reached saturation conditions with resulting void formation. Under these conditions, pressurizer level is not a valid indicator of total primary inventory. Based on training, however, the operators considered pressurizer level to be a positive indication of core coverage.

On the secondary side, feedwater flow to the once-through steam generators (OTSGs) was lost when the main feed pump tripped. The emergency feed pumps started automatically but flow was blocked by closed valves in the EFW system. The valves in question are required to be open during operation but had been closed at some time prior to the shift. The lack of EFW flow was detected at about 5 minutes and restored at about 8 minutes during which time the OTSGs boiled dry and all heat transfer from primary to secondary was lost.

Establishing this transfer was further complicated by several problems in the condensate system, all of which resulted in loss of capability to reject from the condensate hotwell, high hotwell level, and lack of enough suction pressure to run condensate booster pumps. Since flooding out the hotwell could result in loss of a number of pumps, the hotwell and hotwell reject line-up became an area of major concern. Restoration of steam generator levels and condensate system operation occupied the attention of the shift supervisor and one control room operator from a few minutes until one hour into the accident. Despite these efforts, hotwell rejection was not restored due to a failed reject valve. The operators were forced to go to the use of atmospheric relief valves in order to obtain secondary heat transfer without flooding the hotwell. This procedure was initiated at about one hour into the incident.

By this time, the primary system had been in saturation for approximately 54 minutes. Pressurizer level was oscillating between 375-390 inches out of an indicated 400 inches when solid. RCS pressure was at 1100 to 1200 psi. By this time, numerous clues to the LOCA situation were known to the operators including:

- Continued low RCS pressure despite running makeup and let down at normal values
- Rupture of the RCDT diaphragm and flooding of the reactor building (RB) sump
- PORV outlet temperatures in the vicinity of 280° compared with code safety outlet temperatures of 220°

Countering these indications were a continuing high pressurizer level, absence of reactor building indication alarms, and a panel status light erroneously indicating the PORV to be closed. Training and procedures both assert that the classical LOCA symptoms are low pressurizer level <u>and</u> low RCS pressure. In this event, however, pressure was low and level was high, which does not match emergency procedure symptoms.

Two problems absorbed the attention of operators during a period of time following one hour into the incident. The reactor coolant (RC) pumps had been pumping two phase mixture resulting in vibration alarms and reduced flow rate. The operators had specified criteria for shutting down the RC pumps. These criteria were exceeded. The operators were faced with a conflict between keeping the pumps running to maintain RCS circulation and reduce RCS temperature at the risk of pump failure versus shutting down the pumps as required by procedure and losing RCS circulation.

During the same time period, the symptoms of a tube leak in the B OTSG misled operators as to the reason for the water in the RB sump. Level continued to rise in the B OTSG after the control valves were shut leading operators to suspect a primary to secondary leak with loss of inventory into the reactor building. Consequently, the B OTSG was isolated resulting in a small decrease in RB pressure. This tended to confirm the hypothesis that an OTSG leak was responsible for the full RB sump and increased RB pressure when, in fact, the stuck PORV was the cause of both phenomena.

At about 74 minutes the B loop RC pumps were stopped due to the alarms and flow reduction noted above. Shortly after this, an analysis of coolant showed a boron concentration of 700 ppm despite a concentration of over 1000 ppm in the makeup water being supplied. Oscillation and an increasing trend on the source range NI's were noted. At about 90 minutes, a second coolant analysis showed 400-500 ppm boron. Continued alarms were received associated with the operating A loop RC pumps. These were secured at about 101 minutes as required by the operating procedure.

With no forced circulation in the primary system, the operators began feeding up the A OTSG in an attempt to achieve natural circulation. Due to the two phase mixture in the primary system and the low primary pressure, little heat was transferred by this method. The loop A hot and cold leg temperatures diverged widely over the next period of time.

Significant portions of the core appear to have been uncovered during this time.

At about 138 minutes, the operators finally interpreted the relative PORV and code safety temperatures as indicating a possible PORV leak. The block valve for the PORV was closed at this time. RB pressure dropped immediately and RCS pressure began to increase showing the open PORV to be the problem.

Following isolation of the PORV discussions were held concerning entry into the containment to vent the hot legs. Radiation alarms were then received showing high readings at about 150 minutes. Existence of a radiation release became increasingly clear shortly after the 150 minute period leading to the site emergency declaration at about 174 minutes (0654).

2.2 Analysis of Human Error in the Accident

Human errors may be defined as a failure, on the part of the human operator, to perform an assigned task within specified limits of tolerance; with such limits generally being couched in terms of accuracy, sequence or time. Human error is best conceived within the context of an input-mediation-output model, such as that described by McCormick (1976). This model derives from the basic sequence of psychological functioning, specifically, S (stimulus), O (organism), R (response). As McCormick points out, human error occurs when any element in this sequence is disrupted, such as ". . .failure to perceive a stimulus, inability to discriminate among various stimuli, misinterpretation of meaning of stimuli, not knowing what response to make to a particular stimulus, physical inability to make a required response, and responding out of sequence" (p. 25).

While the phrase "human error" covers a multitude of sins, it also results from a multitude of causes, not all of which imply a deficiency on the part of the operator. Human errors result from a variety of causes including: the operator himself; conditions under which he is operating; design of equipment and information required for the performance of tasks; design of procedures which support the completion of task sequences; and training. Specific factors in the incidence of human error in each of these areas are as follows:

- Operator factors in human error incidence
  - fatigue
  - disorientation
  - distraction
  - motivation
  - forgetting
  - confusion
  - expectancy or set
  - psychological stress
  - inadequate reasoning/problem solving capability
  - inadequate skill levels
  - inadequate knowledge
- Operational factors in human error incidence
  - time constraints
  - interfering activities
  - poor communications
  - excessive workloads
  - environmental stress (noise levels, lighting levels, temperature, etc.)
- Design factors in human error incidence
  - control/display location
  - control/display arrangement
  - control/display identification or coding
  - control/display operation or response
  - information availability
  - information readability
  - availability of feedback information
- Procedural factors in human error incidence
  - erroroneous instructions or directives
  - incomplete or inconsistent instructions
  - confusing directives
- Training factors in human error incidence
  - inadequate knowledge training
  - inadequate skill training

In regard to the March 28th incident at TMI, it appears that human error had a significant impact on the course and severity of the accident. Of particular consequence were operator actions/inactions during four major operational sequences: delay in isolating the failed PORV; inadequate management of the O steam generator levels; bypassing SI/throttling HPI; and, control of RC pumps/establishing conditions for natural circulation. The following sections describe the relationship between human errors occurring during these sequences and the design, training and procedures extant in the system.

2.2.1 Delay in Isolating Failed PORV

Time — 00:00:12 - 02:18:00

Plant Status — Following initial turbine trip, there was an anticipated increase in pressurizer pressure resulting in the lifting of the PORV. As pressure decreased below the setpoint value (2205 psig) following reactor trip, the electrical power to the pilot valve was automatically cutoff signaling to the PORV to close. The valve, however, remained in the full open position which resulted in the loss of the pressurizer steam bubble, and, subsequently, a signficant decrease in RCS level and pressure.

Operator Actions/Inactions — At approximately 48 seconds into the accident, the pressurizer level reached a minimum level of 158 inches and began a rapid increase. By 3 minutes 28 seconds into the accident, the level had increased beyond the nominal high level setpoint of 260 inches and was still increasing. At this point, it is assumed that the operator checked the status of the PORV indicator (Figure 3), which erroneously indicated that the valve was closed, dismissed the PORV as a possible cause of pressurizer malfunction, and proceeded to stop makeup pump 1 C (MU-P-1C) and throttle HPI isolation valves (MU-V-16A, B, C, D) to avoid allowing the pressurizer to become "water-solid" (00:04:38).

During the next 134 minutes of the accident, the operators continued to assume the accuracy of the PORV-closed indication, which resulted in the development of a number of false hypotheses concerning the loss of control over pressurizer level.

Design Problems — The following design deficiencies significantly contributed to operator performance during this sequence:

- Invalid Information. The PORV status indicator is a single red light located on Panel 4. The light is designed to come on when an electrical signal is transmitted to the PORV to open, and go out when a signal is transmitted for the valve to close. As indicated in Figure 3 the light is labeled "Light on — RC-RV2 open." This design is a violation of basic HFE principles as referenced by the following provision of MIL-STD-1472B, paragraph 5.2.2.1.4. "The absence or extinguishment of a signal or visual indication shall not be used to denote a 'go-ahead,' 'ready,' 'in-tolerance,' or completion condition... Changes in display status shall signify changes in functional status rather than results of control actuation alone."

- Nonavailability of Information. There is no displayed indication of flow through the pressurizer relief valve discharge line. As a result, the operator had to infer flow through the line by monitoring the temperature of the PORV exhaust pipe.
- Improper Display Location. The status panel for the reactor coolant drain tank (RCDT) is located on panel 8A which is outside the main operating area of the control room. Emergency Procedure 2202-1.5 "Pressurizer System Failure" (Revision 3, 9/29/78) lists RCDT pressure and temperature as primary symptoms of a failed PORV.
- Labeling. As indicated in Figure 3 the PORV indicator panel has several operator added labels, which reflects the inadequacy of the original labeling approach. Label nomenclature is not consistent with procedures which refer to RC-V2 as the electromatic relief isolation valve rather than the pressurizer .relief isolation valve (EP 2202-1.5, page 1).

Training and Procedures Problems — The following training and procedures inadequacies significantly contributed to operator performance during this sequence:

- Operators were conditioned to avoid having a solid pressurizer; therefore, they attended almost completely to pressurizer level and neglected RCS pressure. This conditioning was derived directly from TMI-2 Technical Specifications which state that the pressurizer must not be filled with water to solid water condition, 400 inches, except as required for system hydrostatic tests.
- They thought the drop in RCS pressure was due to the loss of the bubble in the pressurizer, an event that they had never experienced on the simulator.
- The emergency procedures for a LOCA state that symptoms include loss of pressure and level. Operators were trained to assume that a RCS leak must be followed by a reduction in level.
- Operators were conditioned to believe that as long as they had coolant in the pressurizer, the core was covered.
- Operators were conditioned to believe that the absence of illumination of the PORV status light must mean that the PORV is closed, rather than simply that a signal commanding the valve to open was not present.
- Operators had expected higher than normal PORV exhaust pipe temperatures since the pressurizer was known to have been leaking earlier and had opened at 3 seconds into the accident. This is an example of the phenomenon of prior experience serving to establish expectancies in the absence of adequate training. In addition, they had no real guidance concerning how high PORV outlet temperature should be, or how great a difference between PORV outlet temperature and code safety valve outlet temperature was tolerable.

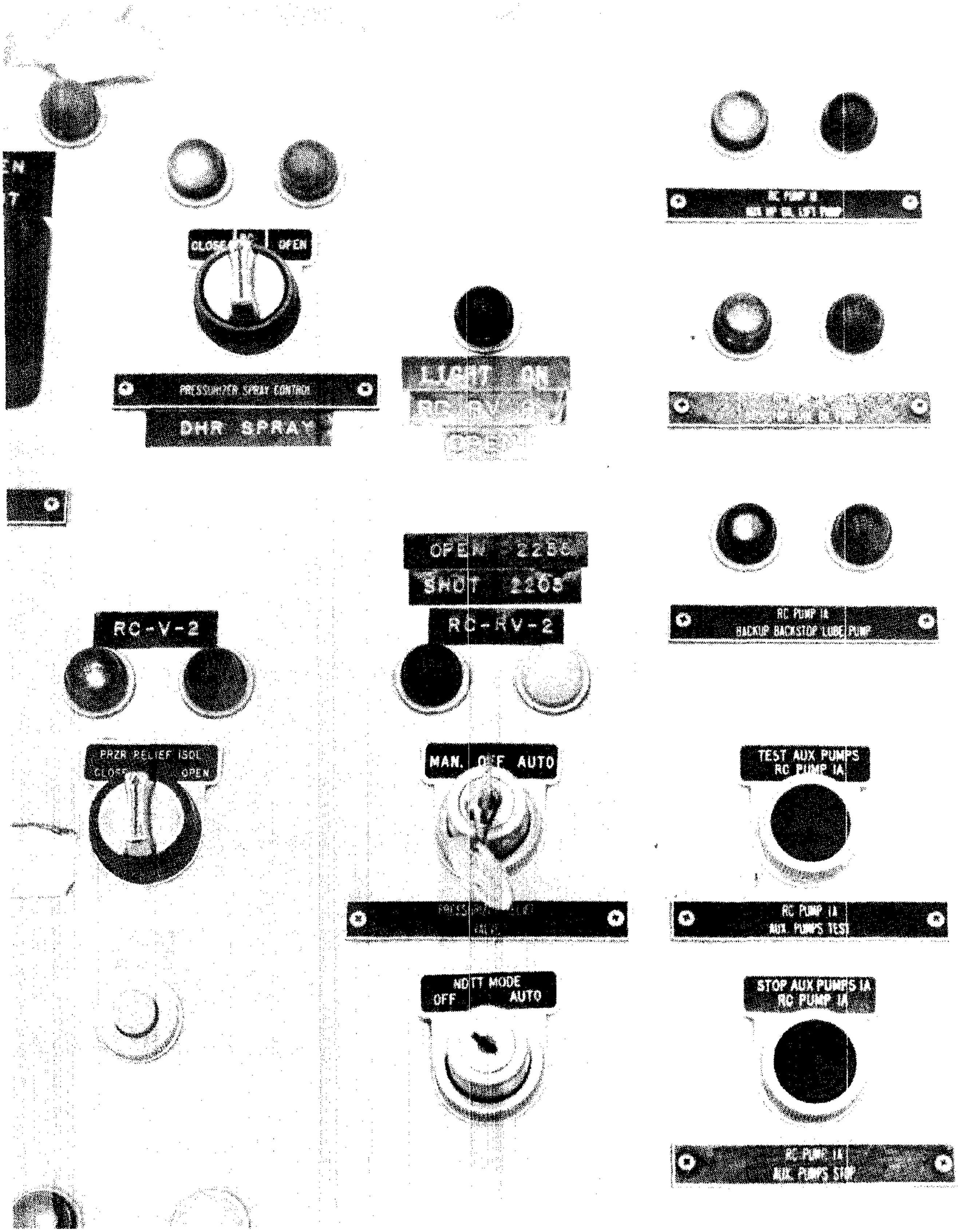


FIGURE 3
PILOT OPERATED RELIEF VALVE (PORV) PANEL

Analysis — Isolation of the failed PORV was obviously the most critical operator action which occurred during the first 150 minutes of the accident. The fact that the operators failed to recognize the PORV as the source of the primary system leak resulted in a series of operator actions/inactions which ultimately led to the uncovering of the reactor core. In retrospect, however, it is apparent that the operator performance was driven by a conception of plant status which was based on inadequate and erroneous information.

The PORV status indicator clearly misled the operators concerning the position of that valve. In the absence of a direct indication of flow through the relief valve discharge line, the operators were forced to rely on extrapolation of flow from temperature. This method was patently inadequate since the exhaust pipe temperature would be expected to increase following the lifting of the valve and no information is provided to the operators regarding the expected rate of cooling for that line. Finally, information concerning the status of the various RCDT parameters was displayed on a panel outside the main operating area of the control room. The operators would have had to leave their principal operating stations to monitor RCDT status, which was untenable, given that they were in manual control of the system. Additionally, the information displayed on the RCDT panel is not recorded on a strip chart. As a result, when the operators did go to the panel, they had no way of determining the trends of the drain tank parameters.

2.2.2 Bypassing SI/Throttling HPI/Increasing Letdown

Time — 00:04:00 - 01:40:00 (Approximate)

Plant Status — Following the reactor trip, the RCS pressure decreased below the safety injection system low level setpoint of 1640 psig, resulting in initiation of safety injection (approximately 2 minutes into accident).

Operator Actions/Inactions — At approximately 4 minutes into the accident, the operator bypassed safety injection, throttled the HPI, increased letdown and removed makeup pump 1C from operation in an attempt to arrest pressurizer level increase. The HPI was maintained in a throttled condition until approximately 100 minutes into the accident, resulting in an average net input of 70 gpm during this period. Emergency Procedure 2202-1.3 "Loss of Reactor Coolant System Pressure" cites a minimum design injection flow to the reactor core of 250 gpm per HPI flow leg.

Design Problems — The following design deficiencies significantly contributed to operator performance during this sequence:

- Invalid Information. As previously described, the erroneous closed indication for the PORV, in combination with high pressurizer level, delayed recognition of a primary system leak.
- Nonavailability of Information. There is no direct indication of coolant level within the reactor core. RCS inventory must be inferred from pressurizer level, which presumes an intact pressurizer.

Training and Procedures Problems — The following training and procedures inadequacies significantly affected operator performance during this sequence:

- Operators were conditioned to bypass the ES since, following a turbine trip, the pressure has on occasion dropped below the 1640 psig SI initiation point.
- Operators were conditioned to avoid going solid; therefore, they concluded that, with a high pressurizer level, keeping HPI full on would only further increase the pressurizer level, increasing the likelihood of achieving a solid water condition.
- Operators were trained to reset the ES as soon as possible to prevent injection of sodium hydroxide into the reactor.
- In the deposition of Mr. M. L. Beers of the Met. Ed. Training Division before the President's commission on the accident at TMI, Mr. Beers was asked "... trying to track through if an operator in that situation on the 28th of March had the question of whether he should throttle HPI, it is your reading of the procedures that under the circumstances that prevailed, there was no direct guidance as to what criteria should be used to throttle HPI in this procedure itself?" Answer: "That is true." Question: "What you are saying is that in the absence of some specific guidance in an emergency procedure, the operator fell back on his general training and that related to the control of the pressurizer level?" Answer: "Yes."

Analysis — Operator performance during this sequence was consistent with their training in regard to the equivalence of pressurizer level to RCS inventory. Operating under the assumption that the PORV was closed, and in the absence of a verifiable indication of RCS inventory, the operators attempted to reestablish pressurizer level by throtting the HPI and increasing letdown.

2.2.3 Management of Steam Generator Level

2.2.3.1 Delay in Opening Closed Feedwater Header Isolation Valves

Time — 00:00:00 - 00:08:00 (Approximate)

Plant Status — Prior to the onset of the accident, steam generator feedwater pumps 1A and 1B, condensate booster pumps 2A and 2B, and condensate pumps 1A and 1B were in service. Operators were attempting to transfer spent resins from a condensate system polisher to the regeneration receiving tank. At this point, water was inadvertantly forced into the instrument air system causing the polisher isolation valves to close. Subsequently, the condensate booster pumps tripped which resulted in the tripping of the main feedwater pumps, and an almost simultaneous tripping of the turbine. Following the tripping of both feedwater pumps, three emergency feedwater pumps started, and both emergency feedwater valves 11A and 11B (EF-V11A & 11B) began travelling open. Feedwater head isolation valves 12A and 12B were closed.

Operator Actions/Inactions — At approximately 45 seconds into the accident, the operator noted that both feedwater pumps had tripped, and steam generator level was approximately 30 inches and decreasing; however, all three emergency feedwater pumps were running and emergency feedwater valves 11A and 11B were travelling open. The operator did not notice that EF-V12A and 12B were closed; however, he would not have been expected to check these valves since they are normally open.

The operator then proceeded to the turbine station (panel 5) to monitor turbine status. When he returned to the feedwater station, at approximately 2 minutes into the accident, he noticed that the steam generator level had decreased to 10 inches, which is equivalent to dry. At this point, the operator assumed manual control of EF-V11A and 11B and increased demand for opening. It was not until approximately 8 minutes into the accident that the operator noted the EF-V12A and 12B were closed. Upon recognition of this fact, the operator opened both valves allowing feedwater to be introduced into the dry steam generator. One problem noted in identifying the status of the normally open 12 valves was that the status lights for EF-V12B were covered by a tag as depicted in Figure 4.

Design Problems — The following design deficiencies significantly contributed to operator performance during this sequence:

- Nonavailability of Information. There is no displayed indication of emergency feedwater flow to the steam generator. The operator must infer flow to the steam generator by monitoring changes in steam generator level and/or RCS temperature.

  There is no displayed indication or alarm to indicate that the emergency feedwater system is in a misaligned or inoperative condition. The operator must visually inspect pump status and valve alignment to confirm that the system is functioning properly.

- Workstation Design/Panel Layout. The feedwater panel is not laid out in a sequential or otherwise logical fashion (i.e., mimic). Control and display placement on the panel is inconsistent: as indicated in Figure 5, "A" loop components are placed above "B" loop components

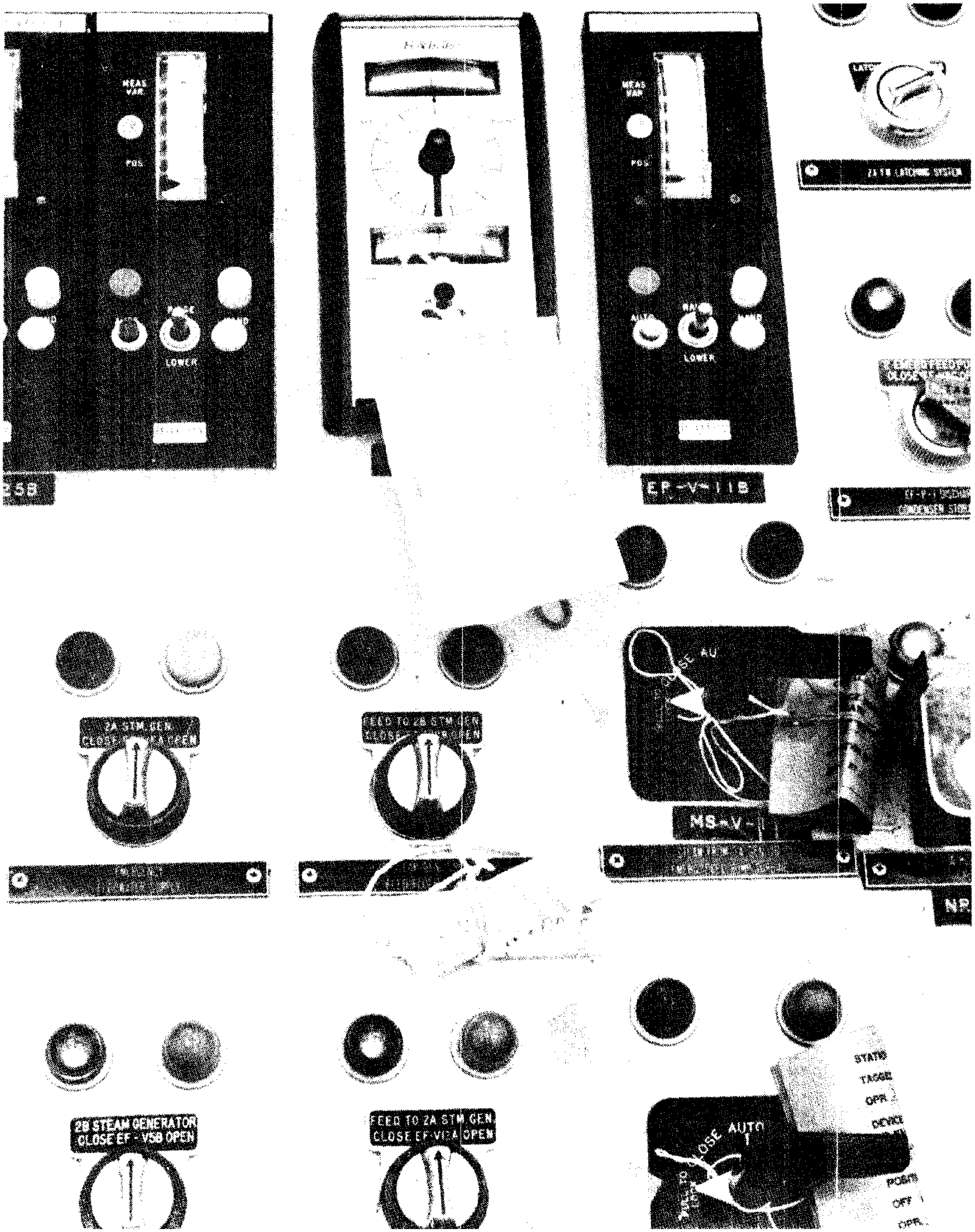


FIGURE 4
EMERGENCY FEEDWATER CONTROLS AND DISPLAYS

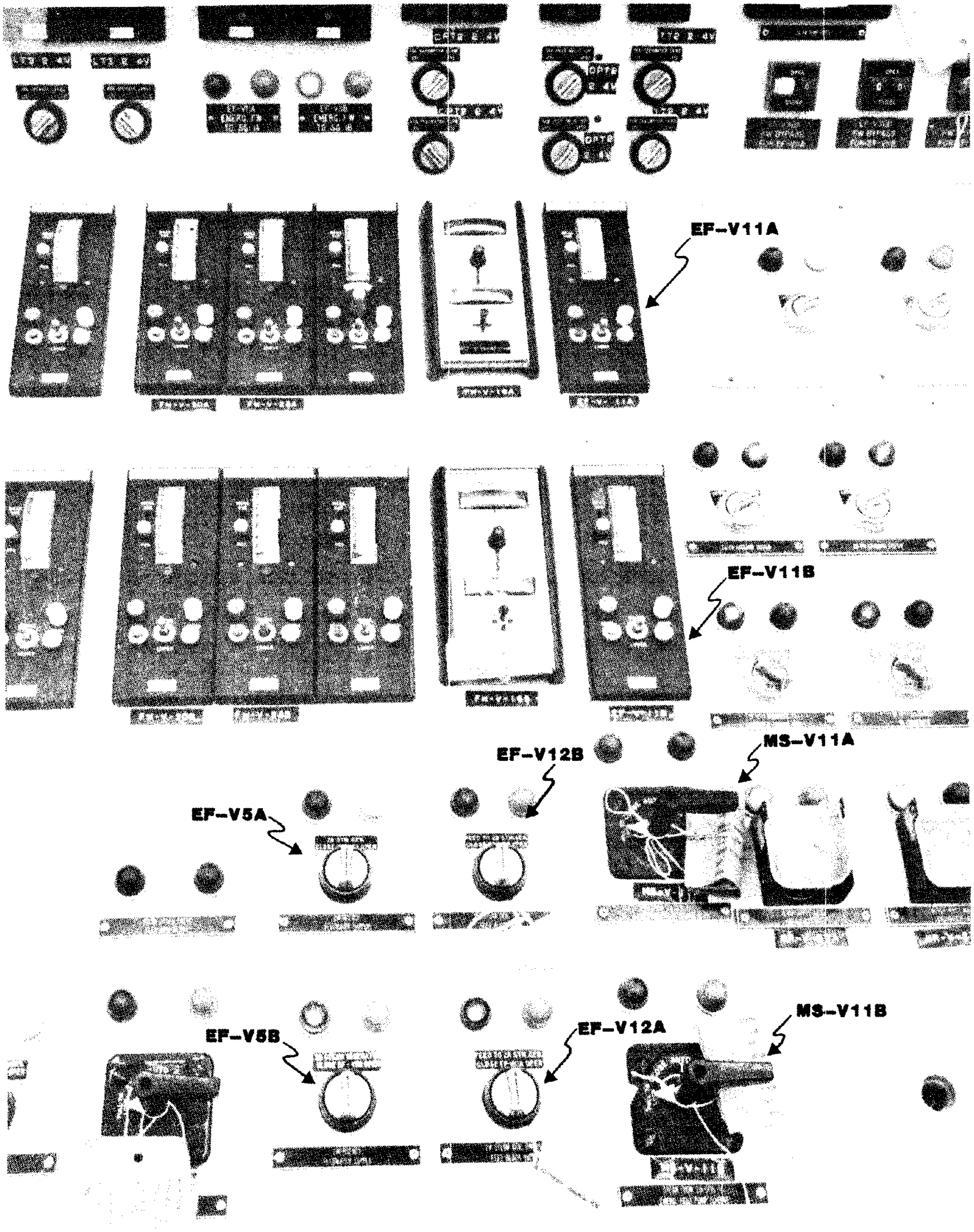


FIGURE 5
ARRANGEMENT OF EMERGENCY FEEDWATER CONTROLS AND DISPLAYS

(e.g., emergency feedwater control valves 11A and 11B), in other cases "A" loop components are placed below "B" loop components (e.g., feed water header isolation valves 12A and 12B). In still other cases, "A" loop and "B" loop components are placed side-by-side (e.g., feedwater latching system). There are two pairs of controls labeled 11A&B (EF-V11A&B and MS-V11A&B) located one on top of the other. The arrangement of system A and B controls is haphazard with EF-V5A, EF-V12B, and MS-V11A all side by side. Control-display relationships are not obvious or consistent. For example, indicator lights for the emergency feedwater control valves are placed on the vertical panel of the console several inches to the left of their associated controls.

Training Problems — The major training requirement during this sequence involves the development of effective visual search strategies. There is no indication that the operators received such training.

Analysis — In the absence of an alarm or indicator to annunciate inoperative emergency feedwater system, the operator was forced to rely on his visual search skills to determine the correct alignment of the system. The visual scan requirements necessitated by the feedwater panel layout are excessive and unorganized, and, therefore, not conducive to effective operator performance. Had the panel been laid out in a sequential or mimic fashion, moving consistently from left to right and top to bottom, the operator would most likely have observed the closed feedwater header isolation valves.

2.2.3.2 Allowing Steam Generator "A" to Boil Dry

Time — 00:94:00 (Approximate)

Plant Status — At approximately 74 minutes into the accident, the operators stopped reactor coolant pumps 1B and 2B in response to decreasing RCS pressure. Steam generator "B" level was increasing and pressure decreasing inexplicably, and steam generator "A" level was steady at approximately 30 inches (± 10 inches).

Operator Actions/Inactions — At approximately 87 minutes into the accident, the "B" steam generator was isolated. This action was based on the hypothesis that the increase in reactor building pressure may have been due to a leak in the "B" steam generator secondary side. At aproximately 91 minutes into the accident, there was a significant increase in steam flow from the "A" generator, followed by a rapid decrease. Subsequent to this point, the operator increased feedwater flow to the "B" steam generator which was isolated, allowing the "A" steam generator to boil dry.

Design Problems — As previously described, the panel layout of the feedwater station necessitates excessive and unorganized visual scan requirements, inhibiting efficient operator performance.

Training Problems — Again, formal training in visual search might have prevented this error.

Analysis — There is no apparent logic in the fact that the operator increased that the A-B sequencing of the "12" emergency feedwater header isolation valves is reversed to that of the "11" valves, it may be convincingly argued that the operator actually manipulated the wrong control; that is, he thought he was increasing feedwater flow to the "A" steam generator, when he was in fact increasing flow to the isolated "B" generator. This position is supported by the fact that there is no direct indication of emergency feedwater flow.

2.2.4 Reactor Coolant Pump Operation/Establishing Natural Circulation

Time — 00:00:00 - 01:41:00

Plant Status — Prior to the accident, the plant was operating at full power (97%), and all four reactor coolant pumps (RC-P1A, P2A, P1B, P2B) were operating. At approximately 6 minutes into the accident, RCS temperature and pressure reached saturation conditions (585°F and 1050 psig, respectively). There was an increase in RCS pressure to approximately 1275 psig by 15 minutes into the accident, at which time pressure began to decrease. From approximately 20 to 60 minutes into the accident, system parameters were generally stable, with RCS pressure at 1015 psig, RC average temperature at 550°F, and pressurizer level between 380-395 inches. From approximately 22 minutes into the accident until the RC pumps were tripped, RCP full speed and vibration alarms were occurring.

Operator Actions/Inactions — During this sequence, one of the operator's major concerns was the reduction of RCS temperature. To achieve this, it appeared necessary to continue RC pump operation, despite RCS pressure and pump vibration indications outside of established operating limits. At this writing, the impact of this action remains to be determined; however, it is clear that when the pumps were stopped, conditions for natural circulation had not been established.

Design Problems — The following design deficiencies may have contributed to operator performance during this sequence:

- Improper Display Location — Displays for RC pump vibration and eccentricity are located 7 feet off the floor on back panel 10, approximately 20 feet from the main RC pump station on panel 4. At such a distance, it would have been impossible to read the displays accurately from the main operating position. Additionally, the location of control with respect to the operator's normal line of sight, results in extreme parallax problems, and greatly increases the probability of reading error.
- Display Design — Alarms for high vibration are located above the vibration indicators on panel 10, approximately 7 feet 4 inches off the floor. The size and luminance of these alarms are inadequate for the expected viewing distance, making them difficult to perceive.

Training and Procedures Problems — The following training and procedures inadequacies contributed to operator performance during this sequence:

Failure to Trip RC Pumps

- Procedure 2202-1.3A, "Loss of Reactor Coolant/Reactor Coolant System Pressure" step 3.2.7 states that RC pumps should be tripped before RC presssure decreases below pump (NPSH (net positive suction head). The same procedure, Section B, 2.2.4 directs the operator to trip the RC pumps before reaching 1200 psig. RC pressure decreased to 1200 psig 15 minutes into the accident and was at about 1020 when the last two pumps were finally tripped at 101 minutes. While the operators did have a procedure indicating what action they should take with respect to RC pumps, they did not know at the time that the procedure was in effect. The draft EPRI report on the TMI accident, Appendix OPS "Operator Action," indicates that while procedure 2202-1.3 was a "procedure of significance" from 13 seconds on, it was not in effect until 138 minutes, when the PORV block valve was closed. Without any formal guidance the crew must have been making decisions based on best available data, and displays of RC temperature presented to them at that time probably led them to decide to keep the pumps on.

Attempts to Establish Natural Circulation

- Procedure 2102-3.3, "Decay Heat Removal via OTSG" states that RC temperature, pressure and cooldown rates must be maintained within the limits specified in a contained figure. The RC pressure and temperature existing at the time that the crew decided to go to natural circulation were well outside these limits (pressure low and temperature high). The crew had not received any specific training in natural circulation either in classroom training or on the simulator. The report of the NRC Office of Inspection and Enforcement on the accident at TMI concludes that the lack of training contributed to the attempt of the operators to place the plant in natural circulation mode of decay heat removal when parameters were outside the procedural requirements.

2.2.5 Causes of Human Error in the TMI Accident

As indicated in the above sections the operators did make several errors which had serious consequences in terms of plant safety. An analysis was conducted to determine the extent to which these errors were due to operator factors and were in the true sense of the phrase "human errors." The influence of each of the operator factors identified in Section 2.2 was assessed. In reviewing the transcripts of the several interviews conducted with the control room operators there is no evidence that, at the time of the accident, the actions and inactions of the operators were significantly influenced by fatigue, disorientation, or distractions. They obviously had not forgotten immediate actions prescribed by emergency procedures. Confusion did play a part in that operators stated on several occasions that they did not understand what was happening at the plant. The cause for this confusion, however, was inadequate information presentation rather than any inherent limitation on the part of the operators. It is apparent that several operator errors were caused or influenced by expectancy or set. Set is a psychological construct defined as a temporary but often recurrent condition of a person that: (a) orients him toward certain stimuli and events rather than others, selectively sensitizing him for those stimuli and events; and (b) facilitates certain activities or responses rather than others (English and English, 1958). The influence of expectancy or set in the TMI incident is evident in the tendency to evaluate indications of present plant status in terms of events or conditions occurring in the recent past. Thus the high exhaust pipe temperature of the PORV was not considered excessive due to the fact that the valve had been leaking for some time prior to time that the valve failed to open. Operators also seemed conditioned to expect problems in the secondary system and not in the primary system due to their prior experience with both systems. Such expectancies, combined with the slow response of the system, had the effect of delaying recognition of the real problems. Development of these errorenous expectancies, however, does not reflect on the operators themselves but rather on their training. In the absence of adequate training, operators will use whatever information is at their disposal, including their knowledge of what has been happening in the plant in the recent past, and over the period of their involvement with the system. It is the function of training to provide a capability of integrating displayed information to arrive at an understanding of what is happening in the plant and what action is required, independently of what has been happening in the recent past. The training provided the TMI operators was obviously deficient in this regard. It might also be noted that the importance of operator expectancy or set in the TMI incident is evident from the fact that several decisions, including the determination that the PORV was open, were reached by personnel who were fresh to the problem, who did not have the recent experience with the plant and who were able to assess available information on its own merits without reference to prior influences.

The influence of psychological stress as a determinent in the TMI accident is difficult to determine given available data. It is apparent that the operators were increasingly under stress over the course of the accident; however, there is no indication that inappropriate actions or inactions were due directly to the stress condition.

Another operator function in human error incidence is inadequate reasoning or problem solving capability on the part of the operators. No evidence has been obtained in this investigation to indicate any problems whatsoever in the reasoning or problem solving capabilities of any of the operators or duty at the time of the accident. To the contrary, when scores of the requalification examination for 1978-79 were reviewed it was determined that the shift supervisor on duty at TMI-2 on 28 March scored highest of all TMI operators. The two control room operators for whom scores are available both scored in the upper fifty percent of the population of operators. There is then no evidence that human errors were due to intellectual deficiencies on the part of the operators.

The remaining operator factors in human error incidence are inadequate skills and knowledges. It must be conceded that the operators were not skilled, nor were they sufficiently knowledgeable, to diagnose what was happening in the plant and to determine what were the actions appropriate for restoring the plant to a safe condition. They were apparently unable to account for a situation wherein pressurizer level is increasing while RCS pressure is decreasing. They seemed to be ill prepared to deal with a condition of saturation. They obviously did not understand the prerequisite conditions for going to natural circulation. The next questions is, why? Why was a crew of qualified, experienced and evidently intelligent operators unable to solve the problem of a failed open PORV Could a different group of operators have done better? Do the obvious inadequacies in skills and knowedges of the March 28 TMI-2 crew reflect a problem in operator selection, or in operator training and support? An ancillary question is, to what degree were the operators prepared for the stress imposed on them by the events of the accident? How well were they trained in diagnosis of failure conditions? How effective were abnormal and emergency procedures in supporting them to determine a course of action which returned the plant to a safe condition? How effective was control room design in providing them with information on what was happening and what they had to do, and when, and how? Consider the support given the operators in the accident. They were presented with:

- A supposedly direct display of PORV status, which was wrong!
- No training or procedures telling them how to diagnose high PORV exhaust temperatures or how to determine the meaning of the difference in temperature between the PORV and the code safety valves.
- No training or procedures instructing them what to do in the situation of a high pressurizer level with decreasing RCS temperature.
- No display of emergency feedwater flow, requiring the operator to infer flow by monitoring steam generator levels and RCS temperature.
- No display of flow through the PORV
- No display that the system has reached saturation.
- Display of RC pump vibration and eccentricity several feet above the control room floor.
- No display of coolant at the core.
- RCDT displays on the back of control room panels, out of sight of operators at normal operating stations.
- Strip charts of critical parameters, such as pressurizer level, which are difficult to read.
- Annunciators (750 total) which are not functionally grouped nor prioritized and which were of no real use to the operators during the 150 minutes.
- Arrangement of ESF indicators such that only half of the indication can be seen by a 6 foot tall operator.
- Inconsistency between the labeling of controls and displays on the panel, and the designations identified in emergency procedures.
- Emphasis during training on avoiding a solid pressurizer, without regard to the implications of throttling HPI, such as uncovering the core.
- Poorly arranged panels wherein controls and displays are not grouped by function or sequence of operation.
- Absence of specific training on natural circulation conditions or conditions of saturation.

It can therefore be concluded that the human errors experienced during the TMI incident were <u>not</u> due to operator deficiencies but rather to inadequacies in design, training and procedures. One question that remains is, why were the EF-12V controls closed? It had to be a human error that caused these normally open valves to be closed. The reason for their closure has not even been determined. If there was a human error which resulted from operator factors, it was the closure of these valves and the failure to make it known that they were closed.

An ancillary implication of the above discussion of human error is that the NRC must establish a clear discrimination between human error attributable to operator factors, which is real human error, and error on the part of the human operator which is a direct result of poorly designed control room components and information, inadequate procedures, or ineffective training. The NRC Office of Nuclear Reactor Regulation, in its report on TMI Lessons Learned (NUREG-0578, 1979) attempts to differentiate human error from design error. The report states that "design errors that lead to a loss of a safety function are generally not correctable without plant shutdown and redesign under current limiting conditions for operations. . . Human errors that result in a loss of safety function are usually amenable to prompt and specific correction" (page A-62, emphasis added). It is apparent that the Lessons Learned report does not acknowedge the fact that many situations typified as cases of human error are caused by design deficiencies, and, as such, will not be corrected promptly. A memo written by M.I. Cotton on 6 November 1979 concerning the NRC Report NUREG 0600 "Investigation into the March 28, 1979, Three Mile Island Accident by Office of Inspection and Enforcement" is eloquent on this point. Mr. Cotton states correctly that if an operator action is incorrect as a result of how information is supplied to him during an emergency, then the operator should not be at fault. To call the incorrect action operator error without determining whether or not the operator was led into the action by poor control room engineering is improper and without it the (NUREG 0600) report is incomplete. Mr. Cotton goes on to state that an operator who is considered poorly trained is not at fault for an action he takes as a result of his training. He states that NUREG 0600 implies that operators were at fault for not following plant procedures. If one keeps the operator training in mind while reading procedures for mitigating a LOCA, according to Mr. Cotton, one cannot conclude that the operators were at fault.

2.3 Conclusions

It can be concluded that operator error played a significant role in the TMI accident. Investigation of operator responses and support provided to operators in selecting these responses led to the conclusions that:

- Failure to isolate the failed PORV resulted from:
  1. An inadequate display of PORV status
  2. Absence of a display of flow through the PORV 3.Location of the RCDT on the back of the control panel
  4. Procedures which failed to indicate the implications of a high PORV exhaust temperature, how high was too high, and what

    was the maximum tolerable difference between the PORV temperature and the temperature of the code safety valves
    5. Complete absence of guidance concerning what procedure was applicable
    6. No guidance, in any procedure, which enabled the operator to diagnose the problem as a leak at the top of the pressurizer, which would result in increased level and decreased pressure

- The inappropriate bypassing of safety injection and throttling of HPI by the operators resulted from:
    1. Absence of a direct indication of coolant level in the core
    2. Training and procedures which stressed bypassing ES after a turbine trip
    3. Training which emphasized avoiding a solid pressurizer
    4. Absence of procedures containing guidance on criteria for throttling HPI
    5. Training which conditioned them to believe that a high coolant level in the pressurizer meant that the core must be covered
    6. Procedures which failed to indicate what should be done in the situation of high pressurizer level and low RCS pressure

- The errors in controlling steam generator levels resulted from:
    1. Absence of a direct display of emergency feedwater flow to the steam generators
    2. Absence of an alarm indicating that the emergency feedwater system is inoperative
    3. The confusing arrangement of controls and displays on the feedwater panel which initially inhibited the detections that the 12 valves were closed and which also probably caused the operator to increase feedwater flow to the B generator rather than to the A OTSG, allowing the A generator to boil dry

- Failure to trip RC pumps and failure to establish natural circulation was caused by:
    1. Absence of guidance concerning what procedure was in effect at what time
    2. Improper location of RC pump vibration/eccentricity displays, 7 feet high and on the back panel, 20 feet from the main RC pump panel
    3. Absence of training concerning conditions for natural circulation.

The overall conclusions are: (1) operators did commit a number of errors which certainly had a contributory if not causal influence in the events of the accident; and (2) these errors resulted from grossly inadequate control room design, procedures, and training rather than from inherent deficiencies on the part of the operators.

3.0 TMI-2 CONTROL ROOM DESIGN AND OPERATIONS

The likelihood of operator errors, such as those involved in the March 28th accident, can be significantly reduced by the systematic integration of human factors engineering into system planning design and operations (41). To determine the extent to which TMI-2 was designed and operated to prevent operator errors, an effort was undertaken to determine:

(a) The quality of human factors engineering exhibited in the as-built control room, procedures, and training

(b) The steps taken by the TMI-2 A-E, utility and NSSS vendor in integrating human engineering into the CR development and operations cycle

(c) The relative importance of human factors engineering in the TMI-2 control room as compared with other same-vintage control rooms.

3.1 Control Room Design

The object of human factors engineering is to integrate the human component into the system. This integration has the effect of preventing human error. One means to reduce the likelihood of error is to design the operator's workspace to fit his capabilities, limitations and requirements in performing the required tasks. For instance, visual acuity must be considered in determining the size of displays to be read at a distance, and short term memory should be considered when a determination is made of the amount of information to be contained in a written instruction.

In the late '60's human factors had advanced to the point where the vast majority of control room design characteristics (e.g., distances between controls and displays, colors, display sizes, labeling, lighting, etc.) had been thoroughly researched and widely reported (see Appendix T). Furthermore, the academic, research, and engineering aims of human factors engineering were incorporated into the Human Factors Society which published a journal dealing specifically with human factors engineering issues, and the IEEE had a special committee on human factors engineering in electronics. Finally, the designers of nuclear power plants had access to many firms specializing in human factors engineering services.

Against this backdrop of extensive information on human engineering, the question can be asked, how well was the control room at TMI-2 designed to prevent human error? Were the proven principles and data applied in the TMI-2 design? Were other control rooms of the same vintage of design similar to TMI-2?

Two concurrent approaches were used to answer these questions: (1) a formal Human Factors Engineering Test and Evaluation (HFE T&E) which involved examining the human engineering of selected control panels and; (2) a general human engineering comparison of the TMI-2 control room to two other control rooms.

(a) Human Factors Engineering Test and Evaluation

Human factors engineering test and evaluation (HFE T&E) encompasses the techniques, methods, principles and data used to assess the adequacy of a system's design. In general, effective system performance is dependent on the extent to which the system's design incorporates the requirements of its constituent elements. For the human factors engineer, this tenet is expressed in terms of the capabilities and limitations of the human operator as they relate to the operator's functions within the system. By corollary, the crux of effective design, from an HFE perspective, is the translation of operator functions into specific tasks and, subsequently, into quantifiable information and performance requirements. These requirements are then used as standards against which the adequacy of the design of the man-system interface is measured. For the nuclear power plant, the keystone of this interface is the control room. As it relates to the incident at TMI-2, HFE T&E provided the tools for estimating the degree to which the control room's design and established operating procedures precipitated and/or compounded the sequence of events and associated operator actions which led to the accident. The specific objectives of this effort are listed below:

1. Identify systems, components and procedures in the control room which played a critical role during the first 150 minutes of the accident
2. Identify relevant human factors considerations for each system, component and procedure which had a critical relationship to the accident
3. Evaluate degree of compliance of critical systems, components and procedures to applicable human factors principles and standards
4. Assess the impact on operator performance of specific systems, component and procedural features which fail to comply with human factors principles and standards.

The core of this task involved the development of a timeline/decision-action sequence describing plant status and operator activities during the first 150 minutes of the accident. This sequence was developed through a comprehensive review of the available documentation, including transcripts of operator interviews and various chronologies, and interviews with TMI-2 control room operators. The sequence was validated and revised during a walk-through of the accident, using a mockup of the control room, at which time inputs were made by four of the operators who participated in the incident. (A complete description of the sequence is depicted in Appendix C while a description of its development is contained in Appendix A of this report.)

In the course of developing the sequence, principal operator tasks were analyzed to identify critical systems, components and operator actions/inactions. Criticality was defined in terms of the subject item's relationship to the course and outcome of the accident.

Each of the critical systems and components was analyzed to determine HFE considerations relevant to its design. This analysis focused on the following characteristics:

- Control/display integration
    - position relationships
    - movement relationships
    - control/display ratio
- Visual displays
    - information
    - location and arrangement
    - coding
- Audio displays/warnings
    - signal characteristics in relation to operational conditions and objectives
    - clarity of meaning
- Controls
    - selection (appropriateness)
    - direction of movement
    - arrangement of grouping
    - coding
    - prevention of accidental activation
- Labeling
    - orientation and location
    - content
    - design of characters

- Workspace
    - visual envelope
    - reach envelope

Operator actions/inactions were analyzed to identify the information and control requirements of the operator.

Based on the above analyses, applicable HFE design checklists were selected from the Army Test and Evaluation Command document TOP-1-2-610, Human Factors Engineering Test Procedures (26). Checklists selected included:

- Labels, Markings
- Controls
- Displays and measures
- Workspace.

(Copies of the above checklists are contained in Appendix D.)

During the course of the evaluation, four separate visits were made to TMI to collect data. The focus of these visits were as follows:

- Visit 1: initial familiarization with control room layout, systems and components
- Visit 2: application of HFE design checklists
- Visit 3: interviews with TMI-2 control room operators
- Visit 4: analysis of control room design in relation to critical operator tasks.

In addition, a full scale mockup was used to evaluate control-display design and workspace.

The test and evaluation reported below leaves little room to doubt that the TMI-2 control room was not designed to minimize human error — even in highly critical systems.

(b) Comparison of TMI-2 Control Room Design to Same Vintage Plants

In order to determine if other nuclear power plant designers arrived at the same solutions to human engineering problems as did the designers of TMI-2, two same-vintage plants were selected for comparison. Aside from date-of-design, other criteria used for selection included: Pressurized Water Reactor Plant; different Architect-Engineer and Utility; and approximately the same plant output.

Two plants were chosen:

- Calvert Cliffs - Unit 1
- Oconee - Unit 3.

Human Engineering personnel visited each of these plants and collected the following information:

a) Procedures

b) Number of Switches/Displays in Primary Areas

c) Particular Control/Display Solutions to Specific Control Problems (Appendix D)

d) Photos of Specific Control/Display Components

e) Description of Annunciator Procedures & Designs

f) Role of Automation

g) Description of Auditory Alarms

h) Description of Communications Network

i) Actual Color Coding Practice

j) Photos of CR and Panel Arrangements

k) Panel/Room Dimensions.

These data were synthesized into the following results:

a) Control Room Descriptions

b) Procedures Comparison (Reported in Section 3)

c) Control Panel Human Engineering Comparisons (Notable Human Engineering Features of Panels)

d) Reach and Visibility Surveys.

The major issue addressed by this section is whether the human engineering design solutions used in the TMI-2 control room were a function of the state-of-the-art in the nuclear power plant industry in the late 1960's. The approach used was to compare the human engineering features of TMI-2 to the features of two other plants (Calvert Cliffs-1 and Oconee-3) designed around the same time. It is shown below that in some aspects TMI-2 represents the state-of-the-art (i.e., color coding, procedures and, perhaps, labeling), but in other aspects (i.e., reach and visibility, and man-system integration) TMI-2 design was not bounded by the state-of-the-art. While other research (39, 45, 46) shows that the human engineering (or lack thereof) in TMI-2 is not unusual for its generation of power plant, the data collected on Calvert Cliffs-1 and Oconee-3 clearly show that better human engineering was being practiced in at least two other plants.

3.1.1 Control Room Descriptions

All three of the control rooms surveyed are designed for single operator monitoring during normal operations; all have a centrally located reactor panel with critical or frequently-used systems located nearby; and all have near-horizontal consoles for mounting most controls. Most of the meters and digital displays are mounted on vertical panels in all plants.

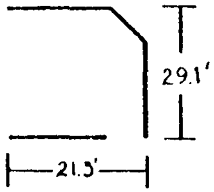
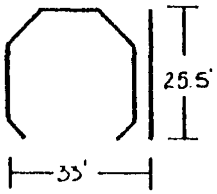
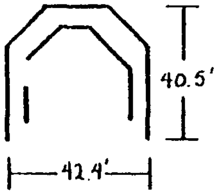
As shown in Figure 6 TMI-2 is larger than the other two control rooms and has more panel space, controls, displays, integrated controls/displays and annunciators than the other two plants. While TMI-2 provides one video monitor, it is not larger or as easily-readable, and operators have no means to view critical parts of the plant from the control room.

Calvert Cliffs-1 occupies one side of a U-shaped control panel housing the controls and displays for Units 1 and 2. Unit 2 layout is a mirror image of Unit 1. When both Units are staffed by the same operators, this arrangement increases the likelihood of operator error through negative transfer of training.

Oconee-3 appears to be very simple. This is a combination of actual design economy and the lack of a Power Distribution Panel, which is included in both the Calvert Cliffs-1 and Three Mile Island-2 panels.

The difference between the three plants in terms of numbers of components may not be as large as it seems. The TMI-2 philosophy was to maximize the information available to the operator, whereas Calvert Cliffs-1 and Oconee-3 attempted to optimize the information by assigning some data to computer printouts and, in the case of Calvert Cliffs, dispatching a large number of controls/displays to satellite control room areas.

The operator's visual burden appears to be substantially less in Calvert Cliffs and Oconee than in TMI-2. By making alarm information available over video displays and by using summary (system level) annunciators for systems located in satellite areas, this improvement in operator information load did not sacrifice or even compromise safety or reliability. In fact, it is probably the case that reducing the number of annunciators in the control room enhances the operator's ability to detect and recognize patterns in events, thus improving diagnosis of root causes of transients or accidents.

PLANT \ PARAMETER	PRIMARY CONTROL ROOM SHAPE & DIMENSIONS	PANEL SPACE	NO. OF COMPONENTS				MAX. VIEWING DISTANCE	MAX. WALKING DISTANCE	NO. OF CRT's	PLANT TV MONITOR
			CONTROLS	DISPLAYS	INTEGRATED CONTROLS/DISPLAYS	ANNUNCIATORS				
CALVERT CLIFFS - 1		~ 400 sq. ft.	500	1700	400	400	32 ft.	32 ft.	1	YES
OCONEE - 3		~ 500 sq. ft.	800	2000	900	600	31 ft.	52 ft.	2	YES
THREE MILE ISLAND - 2		~ 900 sq. ft.	1200	2400	1500	800	48 ft.	50 ft.	1	NO

NOTES: ★ ALL ENTRIES ARE APPROXIMATE.

FIGURE 6 COMPARISON OF BASIC CONTROL ROOM FEATURES*

3.1.2 Workstation Design

One of the fundamental tenets of human factors engineering is that workstation design must facilitate operator performance and reduce the probability of operator error. This is accomplished by thorough analysis of the tasks to be performed at the workstation in conjunction with consideration of the perceptual, cognitive, anthropometric and biomechanical characteristics and limitations of the human operator (28). A well-designed workstation provides the operator with the controls and displays necessary for him to perform his tasks in an expedient, error-free manner. Controls and displays are organized according to function, sequence, or relation to the larger system (i.e., mimic) in order to minimize the operator's visual and reach envelopes and his time to locate specific controls or displays. In all cases, control/display relationships are obvious and consistent, thereby reducing the operator's time to respond.

It is evident from the design of the TMI-2 control room that little attention was paid directly to the tasks which must be performed at the various workstations, or the capabilities and limitations of the operators performing such tasks. The following deficiencies identified in the HFE T&E effort, are indicative of this shortcoming:

- In many cases, workstation design appears to maximize rather than minimize visual scan, reach and walking requirements.
  - RC pump seal pressure is on panel 10, seal temperature on panel 8, while the pump controls are on panel 4.
  - Feedwater pump auxiliary oil pump control is on panel 17, whereas main pump control is on panel 4.
  - Main turbine supervisory instruments are on panel 16, while primary turbine controls are on panel 5.
  - Borated water storage tank controls, which are necessary to emergency makeup, are on panel 8, whereas other makeup controls are on panel 3.
  - Uncompensated pressurizer level indicators are on panel 5, while all other pressurizer indicators are on panel 4.
  - Decay heat indicators are on panel 8, while decay heat pump controls are on panel 3.
  - ECCS actuation control is on panel 3, while ECCS status is displayed on panel 13.
  - Some feedwater controls and displays are on panel 5, while others are on panel 17.
  - Some electrical panel breakers are on panel 6, while their associated displays are on panel 18.
  - Controls for the intermediate closed cooling pumps are on back panel 8, despite the fact that control of these pumps is required during letdown, which is controlled from panel 3.
  - There is no indication of RCS pressure adjacent to feedwater controls, despite the fact that feedwater dramatically affects RCS pressure.

  - Turbine oil temperature indicators are not adjacent to turbine oil pressure indicators.
  - Controls placed at the back of the operating consoles results in excessive reach envelopes (e.g., 42 inches to MU-V-376).

- Controls and displays are not logically or consistently sequenced.
  - Makeup valve controls: A, C, B, D
  - RC pump start switches: AB AB
  - Header pressure indicators: B, A
  - Pressurizer heater controls: 3, 2, 1
5, 4
  - Pressurizer narrow range indicators: B, A
  - Main steam bypass valve control locations are opposite to those of the main steam bypass block valve controls:

AB	AA
AB	BB
Bypass	Bypass block

  - RC auxiliary pump controls for loops A and B are not grouped according to loop.

- Indicator lights are inconsistently placed above, beside, or below their associated controls.

- Nonessential displays are located in primary panel space.
  - Sodium Thiosulfate T/C temperature indicator on panel 3 is not used.
  - Feedwater pump speed indicator on panel 5 is not used.

- In some cases, necessary controls and displays are remote from the control room.
  - There are various block valves for the inlet and discharge headers for the makeup pumps. These are not indicated or controlled in the control room.
  - There are no controls provided within the control room for main instrument or service air compressors.

- Controls on several panels were evaluated against standard human engineering control criteria (details are contained in Appendix D).
  - 14 of 29 (48%) applicable criteria were not met by controls on Reactor Control System — Panel 4.
  - 35 of 43 (81%) applicable criteria were not met by controls on Pressurizer System — Panel 4.
  - 29 of 38 (76%) applicable criteria were not met by controls on Secondary System — Panel 4.
  - 20 of 39 (50%) applicable criteria were not met by controls on Makeup System — Panel 3.

Reaching over benchboards to actuate switches or to manipulate recorders not only obscures the displays under the reaching operator, but it increases the risk that the operator will unintentionally actuate some switch. Frequently it prevents the operator from monitoring important displays during switch operation.

To assess reach envelopes, the benchboards and attached vertical panels in TMI-2, Oconee-3 and Calvert Cliffs-1 were examined with respect to the reach required to manipulate controls and recorders. The levels of excessive reach requirements were defined using the stature of the fifth percentile male (street clothes) as a basis.[1] Components falling in the first section required a reach of 10"-14" greater than the fifth percentile male standing erect could provide without bending over the panel. Components in Section 2 required 14"-18" greater reach, and components in Section 3, a reach extension of greater than 18".

- Calvert Cliffs — Section 1 (10"-14")
  - 3 Rotary switches
  - 1 TV control
  - 1 Key sort switch
- Oconee — Section 1 (10"-14")
  - 22 Recorders
  - 2 Contról units (24 switches each)
  - 1 Test panel (18 switches)
  - 1 Reset unit (8 switches)
  - 1 Flow unit (3 controls)
  - 3 Counter reset (1 control each)
  - 1 Typewriter control panel (4 controls)
  - 5 Switches (very infrequent use)
- Oconee — Section 2 (14"-18")
  - 4 Video monitor control units (approximately 4 controls each)
- Oconee — Section 3 (greater than 18")
  - Remote video switching unit (8 controls)
- TMI-2 — Section 1
  - 18 Chart recorders
  - 10 Control stations (10 switches)
  - 31 Switches (most with frequent use)
- TMI-2 — Section 2
  - None
- TMI-2 — Section 3
  - None

3.1.3 Control and Display Design

The design of individual controls and displays will, to a large extent, determine the utility of their associated workspace. Obviously, the size of the workspace will vary

[1] Ninty-five percent of all males are taller than the fifth percentile male. U.S.A.F. surveys conducted in the early 1950's were used as a basis (23).

according to the size of controls and displays contained within it; therefore, care must be taken to select appropriate controls and displays to minimize the operator's visual and reach envelopes. Of greater concern, however, is the selection of controls and displays which will facilitate the performance of tasks assigned to a particular workstation. This can only be accomplished through thorough identification and analysis of the information and performance requirements of the tasks to be performed at the workstation, within the context of the capabilities and limitations of the human operator.

During the evaluation of the TMI-2 control room, the following control and display design inadequacies were noted:

- Controls have been selected without regard for the relationship between size and performance. As a consequence, many controls (e.g., "J-handle" switches) are unnecessarily large requiring extensive panel space to contain them.
- Displays have been selected without concern for the information processing requirements of the operator. As a result, rarely used or noncritical displays (e.g., electrical displays on panel 6) are unnecessarily large and prominent in the workspace, whereas critical displays (e.g., pressurizer level) are smaller and less easily seen.
- Critical controls are not well guarded.
  - Reactor trip pushbutton
  - Turbine trip pushbutton
- Vertical displays used throughout the control room have both parallax and glare problems.
- Meters do not have integral emergency backlighting (CRO stated that emergency overhead lighting is inadequate).
- Bulbs are difficult to change in pushbutton/legend light control-indicators — in some cases resulting in shorting out of the switch. (Note: CROs stated that the process is so unmanageable that they generally wait until the plant is shutdown before attempting to replace burned out bulbs).
- Auditory displays associated with annunciators lack directional properties which would assist the operator in locating alarming annunciators.
- Auditory displays associated with annunciators are not prioritized to assist the operator in discriminating critical alarms.
- Controls having common operating modes (i.e., automatic and manual) are not designed so that mode selection is constant between controls. In some cases control is turned clockwise to place system [illegible] manual, in other cases, counterclockwise.

  - There is no displayed indication of direction of valve travel or percent open, making it impossible for operators to "fine tune" valve positioning.
  - RC pump amp meters are marked in 30 amp increments with 150 amp major graduations.
  - Reactor power is displayed in increments of 2.5%.
  - Strip charts are overloaded, in some cases displaying up to 72 separate channels on the same chart, making output difficult or impossible to decipher.
  - Critical controls have no obvious indication of being in manual (e.g., when the pressurizer spray valve is set to manual, the handle is "up" (out), but the pointer is at "AUTO").
  - ICS has no obvious indication of being in the "Track" mode (i.e., turbine response driving system response). This shortcoming is particularly critical since the system may automatically place itself in the track mode.

- The annunciator system, which includes over 750 annunciator lights (some of which are outside the main operating area, e.g., RCDT panel), is poorly organized, both in terms of grouping and relationship of alarms to associated subsystems. In addition, critical alarms have not been color coded or otherwise prioritized to permit immediate identification. In many cases, legends are excessively wordy or contain inconsistent abbreviations, increasing the time required to ascertain their meaning (see Figure 7).

- There is no annunciator for reactor trip.

- Extinguished lights are used as positive indication of system status (e.g., PORV seated). This situation is compounded by the fact that, in most cases, indicators contain single incandescent bulbs with no provision for lamp testing.

- Displays on several panels were evaluated against standard human engineering criteria.
  - 32 of 40 (80%) applicable criteria were not met by displays of Reactor Control System — Panel 4.
  - 48 of 50 (96%) applicable criteria were not met by displays on Pressurizer System — Panel 4.
  - 57 of 60 (95%) applicable criteria were not met by displays on Secondary System — Panel 4.
  - 54 of 60 (90%) applicable criteria were not met by displays on Makeup Systems — Panel 3.

Parallax — All three plants reviewed make extensive use of moving-pointer, arc-scale vertical indicators. Unless these indicators are viewed on a line passing through the pointer and perpendicular to the scale plate, parallax will occur. Parallax, which produces a difference between the actual and the seen indicator reading, becomes increasingly harmful as the importance of small pointer movements increases.

With vertical indicators, parallax will occur when the pointer is high on the scale if the indicator is placed so high on the panel that the operator cannot "look down" on it. Parallax increases as the indicator is placed higher on the panel.

Aside from placing the vertical indicator on the panel so it can be read easily, parallax can be minimized by 'selecting an indicator where the pointer is mounted very near the scale, and where the scale plate is mirrored. By using the mirrored scale, the operator can line up the pointer with its image and be confident that his reading is accurate.

Another means to improve the operational reliability of a vertical indicator is to select indicators with limit alarms (upper and/or lower). This removes the identification of critical or degrading situations from the operator who would usually examine the indicator at intervals or when the situation necessitates.

The parallax survey of the three plants focused on vertical meters in the primary area above the eye level of the fifth percentile male (street clothing), based on U.S. Air Force surveys during the early 1950's (23).

- Oconee had only one indicator above the limit.
- Calvert Cliffs had 75 indicators above the level.
  - All had mirrored scales
  - 25 had limit switches
- TMI-2 had 115 vertical indicators above the eye level of the fifth percentile male. None had mirrored scales or limit switches.

3.1.4 Displays

The single most critical design requirement for the nuclear power plant control room is the effective display of information to the operator. This requirement is most pronounced during emergency conditions, where prompt, accurate diagnosis of a problem by the operator may be critical to plant survival. To perform this task effectively, the operator must have immediate access to information regarding all system parameters reflective of plant status; the information must be easily seen and read, well organized, and unambiguous in its content and meaning.

The design of the TMI-2 control room evidences a patent disregard for the information processing requirements of the operator. The following examples serve to underscore the magnitude of this problem:

- In some cases, the status of critical parameters must be inferred from changes in associated parameters.
  - There is no displayed indication of emergency feedwater flow. The operator must infer flow through the system by monitoring changes in steam generator level and/or RCS temperature.
  - There is no displayed indication of flow through the pressurizer relief valve discharge line. The operator must infer flow from temperature at the relief valve sensor point.

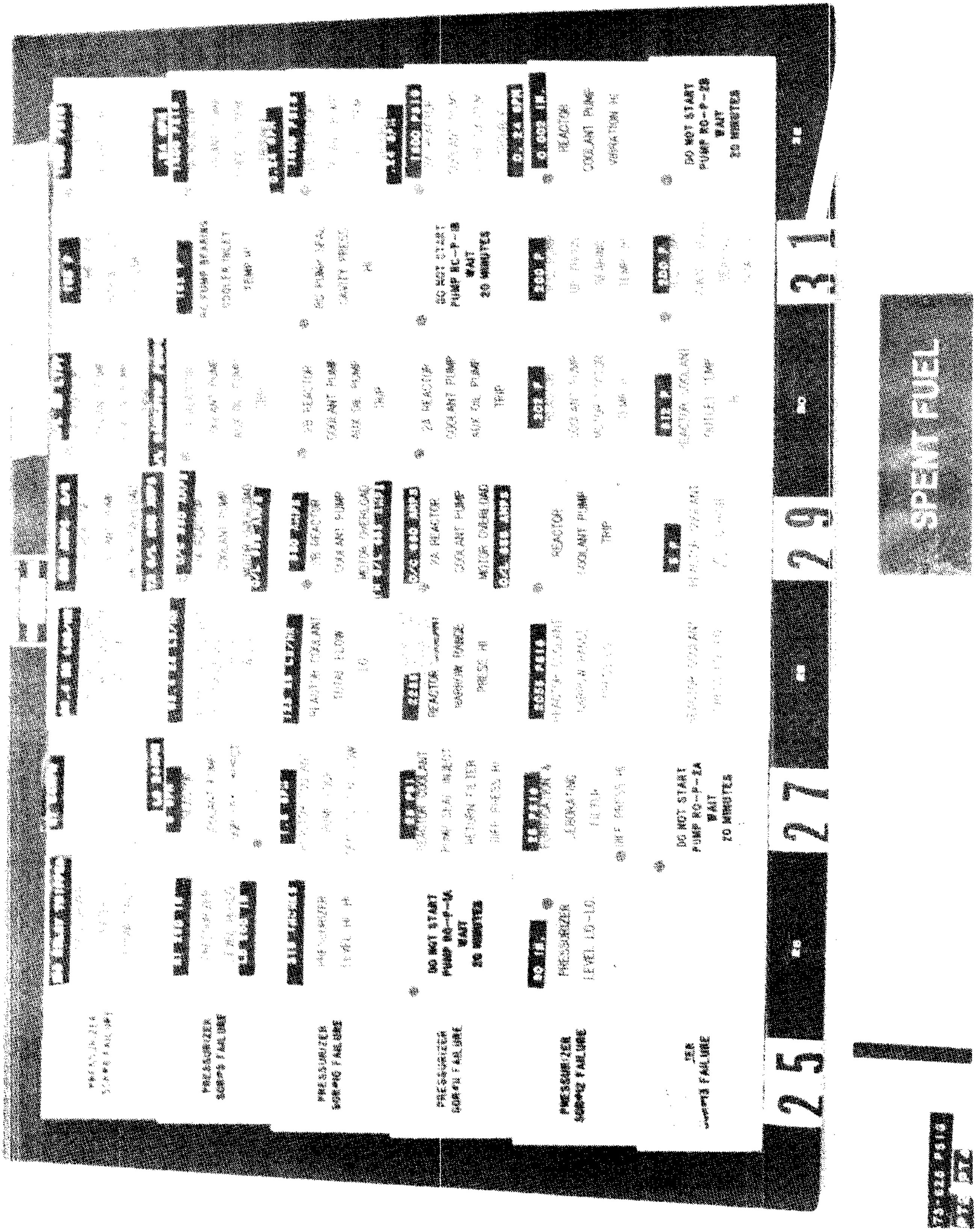

SPENT FUEL
25
27
29
31
DO NOT START PUMP RC-P-1A WAIT 20 MINUTES
DO NOT START PUMP RC-P-2A WAIT 20 MINUTES
DO NOT START PUMP RC-P-1B WAIT 20 MINUTES
DO NOT START PUMP RC-P-2B WAIT 20 MINUTES
PRESSURIZER LEVEL LO-LO
REACTOR COOLANT PUMP VIBRATION HI
2A REACTOR COOLANT PUMP
1B REACTOR COOLANT PUMP

FIGURE 7
EXAMPLE TMI-2 ANNUNCIATOR PANEL

  - There is no displayed indication that the system has reached saturation condition. Saturation must be inferred by comparing RCS temperature and pressure to saturation curves contained in control room procedures.

- Displays are incorrectly located, both with respect to their associated controls as well as the operator's optimal field of view.
  - RC pump vibration-eccentricity indicators and alarms are located approximately 7 feet off the control room floor, resulting in excessive parallax and increased probability of reading errors. In addition, these displays are on back panel 10, approximately 20 feet from the RC pump controls on panel 4.
  - Emergency makeup flow indicators are on back panel 8, approximately 12 feet from HPI valve controls (MU-V-16) on panel 3.
  - ESF indicator board on panel 13 consists of 16 rows of indicator lights. Due to placement and organization of this panel, a 6 foot operator can see only 8 rows of lights from his normal operating position.
  - RCDT instrumentation is located on panel 8A which is completely outside the main operating area.
  - In general, indicators on back panels are difficult to read from primary operating position.

- Information is inadequate and/or ambiguous, making precise determination of plant status difficult or impossible.

Obscured Displays — To different degrees TMI-2 and Oconee both use vertical panels behind the benchboard to support primary operations. Oconee's vertical panels contain some 500 displays whereas TMI-2's contains some 1900 displays. (Note: Displays include indicator lights.) Depending on their mounting height, displays on the vertical panels could be obscured, by the vertical portion of the benchboard, from viewing by an operator standing at the benchboard.

To determine the degree to which displays are obscured, those displays below the line of sight of a fifth percentile male standing at the benchboard and looking directly at the vertical panel were counted.

- Calvert Cliffs — no obscured displays in primary area (no vertical panels behind benchboards)
- Oconee — 2 Indicator lights
- Three Mile Island
  - 470 Indicator Lights
  - 24 Legend Switches
  - 3 C/D Units
  - 3 Vertical Indicators
  - 1 Stripchart

- 1 Dial
- 1 Counter.

Viewing Distance — Because of the time required, a thorough analysis of display viewing distance (visual acuity requirements) during control panel operations was not performed. However, there are some strong indications that the TMI-2 control panel presents many more opportunities for misreading displays at a distance than do Calvert Cliffs-1 or Oconee-3.

- First, the Calvert Cliffs-1 single-panel design keeps all displays within easy viewing range. No problems should occur unless a design principle (see Appendix O) is violated and the displays for one system are mounted on a panel at some distance from the controls for that system. This seems highly unlikely. Therefore, the viewing distance problems for Calvert Cliffs should be minimal.
- Oconee-3, on the other hand, has some 17 vertical meters located on a back panel (3VB3) that could pose some viewing distance problems from within the primary panel area. Minimum reading distance is about 11 feet.
- Three Mile Island-2 presents at least 250 meters located on vertical panels and visible from the primary benchboard. Minimum reading distance is about 10½ feet.

Operators indicate that some TMI-2 meters must be read while operating controls on panels that are not directly facing the display. For instance:

- Starting up the primary feedwater system and observing primary system pressure
- Using the turbine bypass valves and observing the header pressure stripchart to maintain header pressure.

While a more thorough analysis must be made before firm conclusions can be drawn, every indication is that the placement of numerous relatively small vertical indicators on the TMI-2 vertical panels will either promote reading errors, and/or necessitate two-operator actions, and/or encourage the operator to leave the primary panel areas to view the indicator up close.

3.1.5 Labeling

Labeling, although actually a subset of information display, has unique characteristics and requirements which significantly impact operator performance. To ensure efficient, accurate operator performance, labeling must be consistent in location with respect to associated controls and displays; characters must be of adequate size to be easily read from the operator's normal operating position (for normal 28" viewing distance, 1/8-inch characters should be used);[1] coding and abbreviations must be consistent throughout the system; and, labels should be graduated in size, increasing approximately 25% from smallest to largest in the following order: (a) control position, (b) control/display designation, (c) functional group, (d) panel, (e) equipment console or rack (28).

Labeling used in the TMI-2 control room was judged inadequate in the following areas:

- Labeling on back panels is difficult or impossible to read from main operating positions (identification labels on radiation monitors subtend only three arc minutes at the eye of an operator at Panel 4).
- Due to inadequate and/or incorrect labeling, many controls and displays have "label-tape" labels applied by CROs.
- Labels are inconsistently placed in relation to their associated controls and displays — sometimes above C/D, sometimes below.
- Labels are often obscured by their respective controls and displays — this is particularly true for C/Ds on lower part of back panels.
- Labels do not always correspond to their associated indicator lights (e.g., diesel fire pump labeling is contradictive of its indicator lights).
- Labeling is sometimes inadequate or ambiguous as indicated by the prevalence of hand-written operator adjuncts to existing labels — this is a particular problem with concern to inclusion of accepted operating ranges.
- Labels and markings on several panels were evaluated against standard human engineering criteria.
  - 14 of 21 (67%) applicable criteria were not met by labels on Reactor Control System — Panel 4.
  - 23 of 27 (85%) applicable criteria were not met by labels on Pressurizer System — Panel 4.
  - 25 of 27 (93%) applicable criteria were not met by labels on Secondary System — Panel 4.
  - 14 of 25 (56%) applicable criteria were not met by labels on Makeup System — Panel 3.

Labeling on the TMI-2 panels was apparently considered as an adjunct to control panel design, rather than an important communications link necessary for the efficient and reliable operation of the plant. Labels should serve several purposes: 1) they should help the operator to learn and remember the location and function of components and systems; 2) they should provide the basis for a common language among operators within a

[1] Tables on the vertical panels should have letters of 1/3-inch in height to be read from the benchboards, according to the Peters and Adams formula (27).

plant; 3) with color coding or other symbology, they should caution the operator of potential hazards; 4) they should enable the operator to absolutely verify the identity of the component he is addressing, thereby reducing the chance for error; and 5) they can provide special instructions.

Labels from TMI-2, Calvert Ciffs-1, and Oconee-3 were compared with respect to:

1. Frequency of operator backfit (additions or modifications to original-equipment labels)
2. Consistency of label location with respect to the referenced component
3. Frequency of components without original-equipment labels
4. Provisions for adding labels
5. Use of summary labeling (e.g., component-subsystem-system levels)
6. Use of functional/system demarcation lines
7. Special instruction and caution labels
8. Annunciator labeling.

The following paragraphs summarize the findings of this survey. Data in Section numbers 1, 2, and 3 below are based on a review of a random sample of 100 components per plant.

1) Frequency of Operator Backfit Labels

- Oconee-3: 34% of component sample with backfits
- TMI-2: 43% of component sample with backfits
- Calvert Cliffs-1: 65% of component sample with backfits.

2) Consistency of Label Location (Original Labels)

	Label Above Component	Label Below Component
Oconee-3	61%	31%
Calvert Cliffs-1	61%	26%
Three Mile Island-2	34%	55%

3) Frequency of Components Without Original-Equipment Labels

Oconee-3	6%
Calvert Cliffs-1	8%
Three Mile Island-2	6%

4) Provisions for Adding Labels

Calvert Cliffs-1: label embossing and engraving machines
Three Mile Island-2: label embossing and engraving machines
Oconee-3: label embossing and engraving machines

5) Use of Summary Labels

None of the plants made any significant use of summary labels.

6) Use of Demarcation Lines

None of the plants made any significant use of demarcation lines.

7) Special Instruction and Caution Labels

Calvert Cliffs used red original-equipment labels for caution notices. None of the plants made significant use of special instruction labels.

8) Annunciator Labeling

Within plants, annunciator labels are usually of uniform font. In all plants, annunciator windows virtually always give the system or component in trouble, and frequently give the nature of the trouble. Oconee has backfitted some windows with colored acetate to indicate priority.

3.1.6 Color Coding

All three control rooms make extensive use of color coding. Indicator lights give value position in red or green; pilot lights indicate if a piece of equipment is operating; and, at Calvert Cliffs, annunciators report system status in red, green, white or dull orange.

Human engineering, growing out of the military and aerospace tradition, is somewhat at odds with the color coding practices of the nuclear power industry which grew out of experience with fossil fuel power plants. Therefore, the usual color coding conventions and criteria used for Human Engineering Test and Evaluation are not particularly relevant to power plant control room designs.

To assess color coding in the three plants, several design guidelines, which transcend the military vs. fossil fuel arguments, were derived from the basic intents for color coding, viz., to call attention to some condition or to provide specific information to the operator. These guidelines were:

1. Colors should be unambiguous. The fewer meanings the better (one meaning per color is best).
2. Colors should never have contradictory meaning (if red equals valve open, it should never equal valve closed).
3. Colors intended to draw attention should not be used in the general surround.
4. Colors should not be used where a written legend is appropriate.

The color coding practices used in each as-built control room were examined against these guidelines.

- All three plants attached several meanings to each color used (Appendix E). In fact, the operator in many cases would have to know the specific component being observed to know how to interpret the color.

TABLE 1
NUMBER OF DIFFERENT MEANINGS GIVEN
TO EACH COLOR

	RED	GREEN	AMBER
Calvert Cliffs-1	6	4	5
Oconee-3	4	3	4
Three Mile Island-2	14	11	11

- None of the plants color coded meter faces to any significant extent. Such coding aids the operator in determining if a reading is safe, marginal or out-of-tolerance.
- Because of electrical and valve coding conventions the color for "open" and "closed" is often reversed for circuit breakers and valves.

  green = valve closed
  green = circuit breaker open.

  While the logic for these color assignments is clear, the chance for misinterpretation, particularly when the operator is under pressure, is very real. "Manual" and "Auto" modes are frequently associated with the same color on the same panel.
- Annunciators, when alarming, intend to draw attention to the window of interest. Oconee and TMI-2 use flashing white on a white background. Contrast is particularly bad if several lights are on around the alarming window. Calvert Cliffs has a better scheme: the alarming window shows bright white against a dull orange background. Acknowledged alarms show red and cleared alarms, green. This very high contrast and color shift will assist the operator in maintaining cognizance over incoming alarms.
- Deciding where to use colored lights seems to be a matter of tradition rather than reason. The SBM switch with two overhead indicator lights is a standard in all three plants. The "Christmas Tree" effect in the CR is overwhelming to the observer and must be distracting, and at times confusing, to the operator. The number of lights makes it virtually impossible to determine, with confidence, the status of any switch or system from across the control room, particularly if the component is benchboard-mounted.

In summary, current practices observed in all three plants sharply reduce the value of color coding to the operator. The number of meanings given to each color and the number of colored lights used combine to produce considerable ambiguity in the man-machine communication link. In practice, it is up to the operator to resolve this ambiguity before undertaking any meaningful task.

3.1.7 Operator Performance

In order to demonstrate the relationship of control room design deficiencies to operator performance, a basic sequence of operator tasks was developed from the general operator activities which occurred during the first 150 minutes of the accident. This sequence, presented in Appendix C, in intended only to familiarize the reader with the relationship between control room design and operator performance and is in no way intended to be an exhaustive enumeration of design deficiencies or operator activities. A summary of control room design problems identified in the sequence is presented below.

1. Recognition of Incident Onset

   Nonavailability of Information — There is no annunciator for reactor trip; operators must monitor a number of system parameters to determine if trip has actually occurred.

   Improperly Displayed Information — Annunciator for turbine trip is left of center on the bottom row of panel 17. This annunciator was not originally color-coded or otherwise prioritized; however, the operators have since colored the annunciator red.

2. Monitoring ESF Response

   Improper Display Location — The ESF indicator panel consists of 16 rows of indicator lights on the back of panel 13. Due to the placement and organization of this panel, a 6 foot operator can see only 8 of the 16 rows from his normal operating position. As a result, if the operator is to ensure the adequacy of the ESF response, he must leave his station, walk around the inner console to the back panel, and inspect the indicator lights, or request assistance. This process is time consuming and unnecessarily distracts the operator from performance of his other tasks.

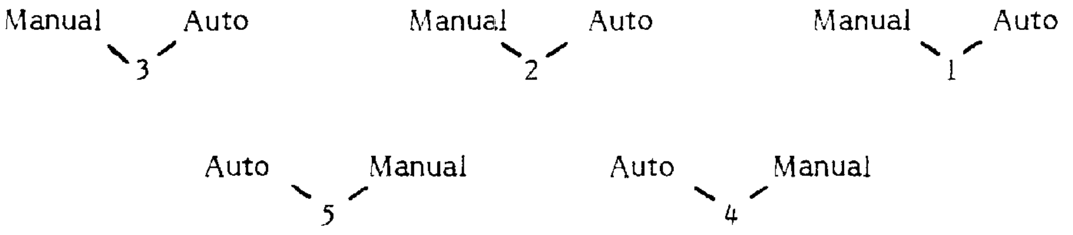
3. Monitoring PORV Status

   Inadequate Information— The PORV status indicator is a single red light which initiates when an electrical signal is transmitted for the pilot valve to open, and extinguishes when a signal is transmitted for the valve to close. There is no indication to the operator of actual flow through the discharge line or percent that the relief valve is open.

Improper Display Design — As previously described, the indicator extinguishes when a signal is transmitted for the valve to close. This design is inherently ambiguous, since a failure of the bulb or circuit would be perceived as an indication that the valve had closed. This condition is compounded by the fact that there is no provision for lamp testing provided to the operator. Additionally, the fact that the indicator represents transmission of an electrical signal, and not actual valve position, is decisively inadequate from a human engineering standpoint. As occurred during the March 28th accident, a signal can be transmitted to the valve without the valve responding. Such a condition would not be reflected by the indicator. This type of ambiguity in displayed information can only increase operator uncertainty and attendant stress during emergency conditions.

4. Control of Pressurizer Heaters and Spray

Workstation Design/Panel Layout — There are 5 "J-handle" switches provided for control of the 5 groups of pressurizer heaters. The arrangement of pressurizer heater controls is depicted below and in Figure 8.



Notice that the heater groups are not only organized contrary to convention (i.e., left-to-right, top-to-bottom), but the control positions for auto and manual modes are reversed, as well. Additionally, the control for the pressurizer spray has the auto mode in the center position. Such inconsistent and illogical panel layout increases both the operator's time to respond and the probability that he will commit an error.

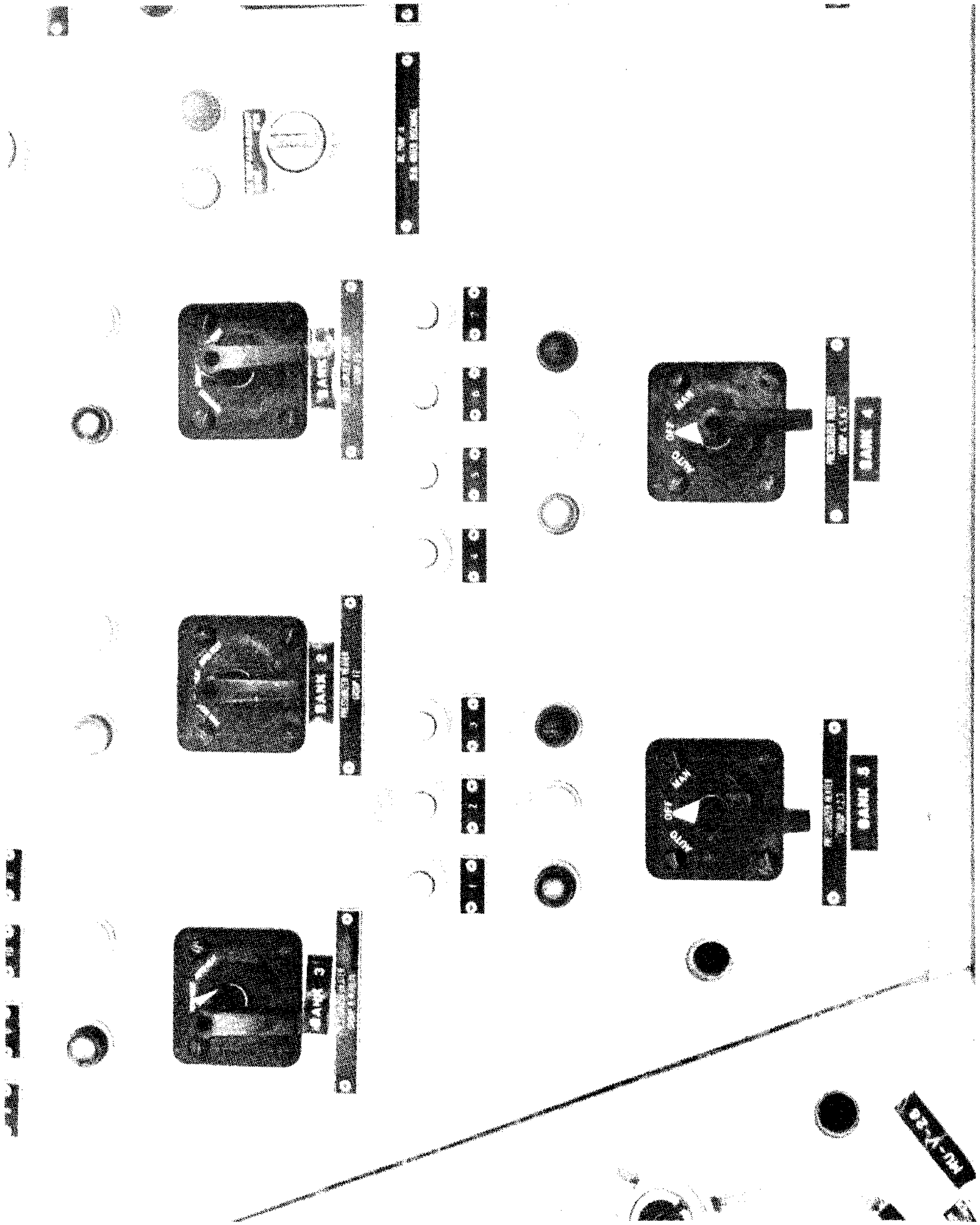


FIGURE 8
PRESSURIZER HEATER CONTROL AND DISPLAY ARRANGEMENT

5. Operating Letdown Valve 376 (MU-V376)

Inadequate Labeling — The label for this control reads "Letdown Isolation." There is no indication that this is MU-V376, despite the fact that such nomenclature is used throughout the emergency procedures (e.g., EP 2202-1.5, Pressurizer System Failure, Section D, paragraph D.2, B2). In addition, the placement of the control 31 inches from the front edge of the panel results in a 42 inch reach envelope and causes the label to be obscured by the control. The inconsistency between labeling and emergency procedures increases both the time required for the operator to perform his assigned tasks, and the probability that he will commit an error.

6. Control of Makeup Pumps

Control Design — A three-position "J-handle" switch is provided for control of the makeup pumps. To start a pump, the operator must place the control in the start position and hold it there until the pump starts. This design inhibits the flow of operator activities, particularly during emergency conditions.

7. Verification of Emergency Feedwater Flow to Steam Generators

Nonavailability of Information — There is no direct indication displayed of emergency feedwater flow to the steam generators. During the accident, the operators were forced to verify the status of a number of pumps and valves, and monitor changes in various system parameters (e.g., steam generator level) to confirm the flow of emergency feedwater. This condition greatly increased the operator's workload and resulted in an inaccurate appraisal of system status.

Workstation Design/Panel Layout — The panel layout of the feedwater station lacks any apparent logic in its design. The components contained in this panel are not organized according to operational sequence or relation to the larger system (i.e., mimic). In addition, physical relationships between "A" loop and "B" loop components are not consistently maintained (e.g., "A" loop components are sometimes located above "B" components, sometimes below, and sometimes beside). In the absence of consistently logical panel layout, the operator is forced to rely on memory or random search to locate a particular component. This condition significantly increases both the operator's workload and the probability that he will commit an error.

8. Controlling HPI Flow

Control/Display Integration — Control of the HPI is accomplished through "jog" controls on panel 3, while makeup flow indication is displayed on panel 8, approximately 12 feet from the makeup control station. At this distance, it is impossible for the operator to read the display accurately. As a result, the operator must either leave his station to determine flow, request assistance from another operator, or estimate the makeup flow rate. In any case, the process is unnecessarily complicated and error-prone.

Display Design — In addition to being 12 feet from the operating station, the display is not color-coded to indicate normal, marginal and out-of-tolerance operating ranges. This increases the time required for the operator to extract the necessary information from the display.

Control Design — The use of a 2-position rotary switch to perform continuous adjustment of a valve is inadequate, since it requires the operator to perform a number of trial-and-error adjustments to achieve the desired valve setting. Such a design significantly increases the time required to perform the task, with an attendant increase in operator workload.

Inadequate Labeling — Controls are labelled "Emerg. Inject. Flow A (B, C, D)." There is no indication that the controls are associated with MU-V16A (B, C, D), despite the use of this nomenclature throughout the emergency procedures (e.g., EP 2202-1.1, Reactor Trip, section 2.2, paragraph e). This inconsistency between labeling and emergency procedures increases both the time required for the operator to locate the control and the probability that he will commit an error.

9. Aligning the Borated Water Storage Tank with the Makeup Tank

Workstation Design/Panel Layout — For any plant condition which requires a significant input of makeup, the BWST must be aligned with the makeup tank to ensure an adequate supply of borated water. The controls associated with makeup (HPI) are located on panel 3, while the controls required to align the BWST (DH-V5) are on vertical panel 8, requiring the operator to relinquish control of the HPI or call for assistance to align the systems. This situation is particularly undesirable given the criticality of makeup during many emergency conditions.

10. Monitoring Pressurizer Level

Display Design — Pressurizer level is displayed on a strip chart on panel 4. The display indicates from 0 to 400 inches, with increments of 4 inches and major graduations of 40 inches. Due to difficulties in reading the chart through the display "window" (a combination of window size and glare), the operators must operate with the window open, and, if they require information concerning longitudinal trends, the chart must be pulled out.

11. Monitoring Status of Emergency Feedwater Valves 11A and 11B

Inadequate Information — Valve status (open-closed) is indicated by the onset of one of two indicator lights located above and to the left of the valve controls on panel 4. The valve traveling is indicated by both lights being on. There is no indication of rate-of-travel or percent open for the valve; additionally, there is no indication of the valve failing while traveling. During the accident, there was a disruption of the instrument air which may have delayed the opening of the valves. Since the operator had no indication of rate-of-travel or percent open, he had to repeatedly return to the feedwater station to monitor valve status. This requirement distracted the operator from his other tasks and may have contributed to the delay in recognizing the closed emergency feedwater header isolation valves.

12. Monitoring Hotwell Status

Display Design — This display indicates from 10 to 50 inches, which is inadequate for the actual volume of the hotwell. During the accident, this indicator was off-scale, contributing to the uncertainty experienced by the operators concerning plant status.

13. Control of Turbine Bypass Valves

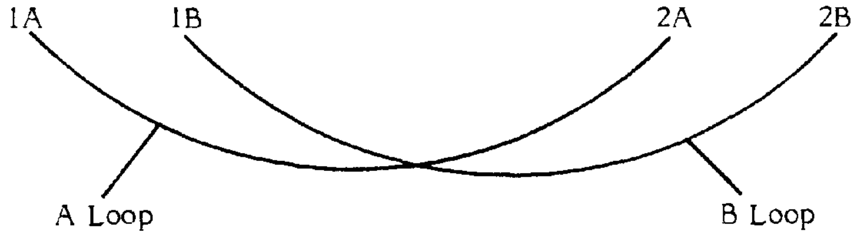
Control/Display Integration — Control of the turbine bypass valves is accomplished through two Bailey controls on panel 5. The effect of turbine bypass is reflected in changes in the turbine header pressure on panel 4, approximately 9 feet away. When the operator is adjusting the setpoint for the bypass valves, he must monitor turbine header pressure closely, requiring him to move back and forth between the two panels. This process is unnecessarily complicated and error-prone.

14. Control of Reactor Coolant Pumps

Control/Display Integration — Displays for RC pump vibration and eccentricity are located on panel 10, approximately 20 feet from the main RC pump station on panel 4. At this distance, it is impossible for the operator to read the displays accurately without leaving his primary operating position.

Display Design/Location — The indicators for RC pump vibration and eccentricity are vertical displays located approximately 7 feet off the control room floor on panel 10. This results in extreme parallax problems when trying to read the upper 50% of the display. Such a design increases both the time required to extract information from the display and the probability that a reading error will be committed.

Workstation Design/Panel Layout — Controls for the auxiliary pumps for the RC pumps are not organized in a logical fashion according to loop, as depicted below:



This layout increases the time required to locate the control and the probability that an error will be committed.

3.2 Control Room Development

To the extent that control room design caused or contributed to the events of 28 March 1979, the processes used to develop the control room are implicated as possible root causes for the accident.

In the following section the Human Engineering development process used for TMI-2 is compared to the processes used for two plants of the same vintage to determine if major differences existed in the use of human engineering system development processes or data.

Several questions are answered in this section, including:

(a) What were the human engineering regulations and standards imposed on TMI-2?

(b) .Did TMI-2 meet these standards?

(c) What were the bases for human engineering decisions on TMI-2 and how do they compare to other plants?

(d) What role did human engineering considerations play in TMI-2 planning, design, testing, and operations? How did this compare to other plants?

In the following analysis, development of the control room at TMI-Unit 2 is viewed as an evolution from early planning concepts to the operational control room used during the accident on 28 March 1979. TMI-2 underwent a rather unusual series of events during this evolution, which undoubtedly left their marks on the final as-built control room design.

During the early phases (Figure 9) of CR development (1967-1968) the Unit-2 plant was not being designed for Three Mile Island and Metropolitan Edison Co. (Met. Ed.), but for construction at Jersey Central Power and Light Co.'s (JCPL) facility at Oyster Creek, N.J. JCPL provided project management and, at the time of the transition from Oyster Creek-2 to TMI-2, JCPL managers were involved with B&R in making fundamental CR planning decisions (1). Many of these decisions were carried forward, in fact or in principle, into the TMI-2 design.

The transition from Oyster Creek to Three Mile Island, started late in 1968, was accompanied by a period of management instability where B&R personnel report difficulties in obtaining directions from their client (GPU/Met. Ed.) (1).

At this point the control room concepts and designs were being developed almost exclusively by B&R, including both NSSS and Balance-of-Plant (B-O-P) panels. With the

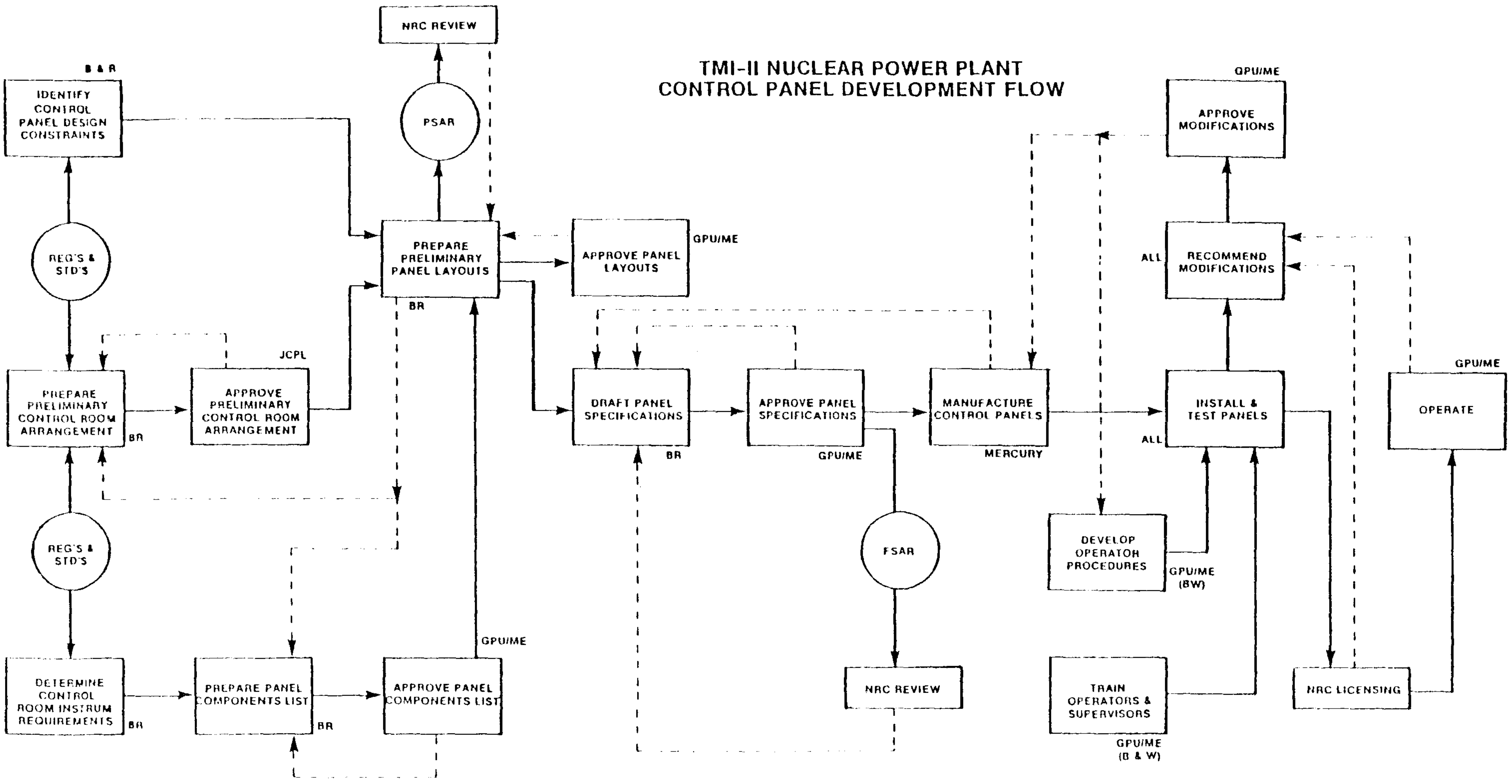

TMI-II NUCLEAR POWER PLANT
CONTROL PANEL DEVELOPMENT FLOW
B & R
IDENTIFY CONTROL PANEL DESIGN CONSTRAINTS
REG'S & STD'S
PREPARE PRELIMINARY CONTROL ROOM ARRANGEMENT
BR
REG'S & STD'S
DETERMINE CONTROL ROOM INSTRUM REQUIREMENTS
BR
JCPL
APPROVE PRELIMINARY CONTROL ROOM ARRANGEMENT
PREPARE PANEL COMPONENTS LIST
BR
APPROVE PANEL COMPONENTS LIST
GPU/ME
NRC REVIEW
PSAR
PREPARE PRELIMINARY PANEL LAYOUTS
BR
APPROVE PANEL LAYOUTS
GPU/ME
DRAFT PANEL SPECIFICATIONS
BR
APPROVE PANEL SPECIFICATIONS
GPU/ME
FSAR
NRC REVIEW
MANUFACTURE CONTROL PANELS
MERCURY
QPU/ME
APPROVE MODIFICATIONS
ALL
RECOMMEND MODIFICATIONS
ALL
INSTALL & TEST PANELS
DEVELOP OPERATOR PROCEDURES
GPU/ME (BW)
TRAIN OPERATORS & SUPERVISORS
GPU/ME (B & W)
NRC LICENSING
GPU/ME
OPERATE

FIGURE 9 TMI-2 CONTROL PANEL DEVELOPMENT

exceptions of an aborted attempt to redesign the TMI-2 CR along the line of TMI-1, and some rearranging of panels (1, 2, 7), GPU/Met. Ed., while retaining its approval function, had minimum input into design. Earlier, the NSSS vendor, Babcock and Wilcox (B&W) attempted to convince B&R that the NSSS panels should match their simulator (2), but B&R refused the suggestion and B&W's role was reduced to specifying the controls and displays for the NSSS sections of the control boards (1, 2).

By the early '70's the CR at TMI-2 was designed. This design survived until the accident on 28 March.

The decisions shaping the TMI-2 control room were made, without formal human engineering guidance, in a series of phases beginning in 1967 and continuing through planning, design development, testing and operation.

About the same time as TMI-2 two other nuclear power plants, Oconee-3 and Calvert Cliffs-1, were going through the development process but with different results.

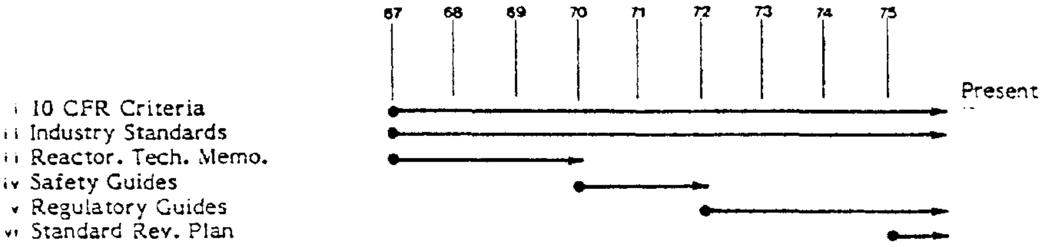
Using data from interviews, the following paragraphs explore the role of human engineering in the CR decisions made for each plant. The first examines the human engineering constraints placed on the power plants by Government regulations and industry standards; the second examines management factors; and the remaining examine planning, design development, testing and operations.

3.2.1 Criteria Identification

In designing a nuclear power plant during the late 1960's, engineers were obliged to follow certain criteria, and advised to follow others. Federal Government criteria were imposed or recommended by the AEC using Title 10 Code of Federal Regulations, Reactor Technology Memoranda,[1] Safety Guides, Regulatory Guides, and industry standards. Voluntary criteria were industry standards or recommended practices issued primarily by the American Nuclear Society (ANS), the Institute of Electrical and Electronics Engineers (IEEE), and the American National Standards Institute (ANSI). In 1975, the NRC consolidated its criteria in a Standard Review Plan aimed at providing a comprehensive approach to the examination and approval of Power Plant Safety Analysis Reports submitted by the utility constructing a nuclear power plant.

[1] AEC memoranda aimed primarily at reactor safety, and preceeding Safety Guides and Regulatory Guides.

In order to obtain an accurate picture of the human engineering criteria imposed on CR design as well as the human engineering data widely publicized to the nuclear power engineering community, the criterion documentation available from 1967 to the present was identified and reviewed. In addition, engineers and managers participating in the development of TMI-2, Oconee-3, and Calvert Cliffs-1 were asked, during interviews, to identify standards or other criteria important to control room design.



(i) 10 CFR Criteria — As noted in the chart above, 10 CFR Criteria were available from 1967 to the present. The entire 10 CFR, Chapter 1 — Nuclear Regulatory Commission was reviewed for human engineering criteria. Then each of the criteria was traced to its genesis. Design criteria published during the period 1967-1973 were considered to be operative for TMI-2 (the TMI-2 FSAR was published in 1974).

(ii) Industry Standards — To identify currently applicable standards, the 765 documents named by the Nuclear Standards Management Board (NSMB) of the American National Standards Institute were subjected to a title review by a Nuclear Engineer and a Human Engineer who sorted out documents that might contain criteria impacting the control room. Then 75 documents were reviewed and those containing criteria within the domain of human engineering were set aside for further analysis. Each criterion was classified and recorded according to its subject matter:

- Operator/System Integration
- Instrumentation and Control
- Control Room Environment
- Operator Procedures
- Operator Support Equipment
- Human Factors Test and Evaluation
- Policy, Planning and Management

Documents containing criteria within the human engineering domain were then traced back to "trial use" standards, or to other predecessor documents which in turn were traced back. This process was facilitated by ANSI-NTAB[1] Project Status Reports dating back to 1972 and listing standards and standards development projects for the Nuclear Industry. Standards available during the 1967-1973 time frame were selected for closer analysis. Each of the 1967-1973 criteria within the domain of human engineering was examined to determine if its language imposed or suggested design features or principles that would improve Operator Performance. If so, it was identified as a human engineering criterion.

It should be noted that the completion of this review would not have been possible without the continuing and patient cooperation of the American Nuclear Society, the Institute of Electrical and Electronics Engineers, and the American National Standards Institute.

(iii) Reactor Technology Memoranda (RTM) — RTM were the predecessors to Safety Guides and Regulatory Guides, and were rather informal in nature. As such, all of the RTMs could not be located for review. Those reviewed include:

- Recording Seismographs in Nuclear Facilities, RTM
- Combustible Gas Control System, RTM 8
- Control Room Design Considerations, RTM 6
- Emergency Core Cooling System Evaluation Guidelines, RTM 4
- Seismic Design Criteria, RTM 3

During the review, five criteria were noted within the human engineering domain. None of these imposed or suggested features or principles that would improve operator performance.

(iv & v) Safety Guides and Regulatory Guides — Safety Guides are the predecessors of Regulatory Guides, which are issued to describe and make available to the public methods acceptable to the NRC staff of implementing specific parts of the Commission's regulations. The titles to 324 Regulatory and Safety Guides were reviewed by a Control Room Operator, a Nuclear Engineer and a Human Engineer with instructions to identify those guides that will or might impact any aspect of Control Room design. Sixty (60) guides were identified and reviewed to determine which, if any, contained

[1] Nuclear Technical Advisory Board.

criteria within the human engineering domain. Twenty (20) guides had human engineering criteria which were classified using the same titles as in Industry Standards (ii-above).

Guides were then traced to their origins. If their origin was 1973 or earlier (eight Guides), each criterion was examined to determine if its language imposed or suggested design features or principles that would improve operator performance.

(vi) Standard Review Plan (SRP) — The entire 1,800 page SRP was reviewed by a Nuclear Engineer and a Human Engineer to identify all criteria that impact Control Room design. One hundred forty-two (142) criteria were located and each criterion was classified according to the scheme outlined in Industry Standards (ii-above).

Since the SRP was published in 1975, no additional analyses of SRP criteria were performed.

(vii) Results — In order to determine the criteria (mandatory and voluntary) imposed on Nuclear Power Plant development during the period of TMI-2, the 10 CFR, industry standards, Regulatory and Safety Guides, Reactor Technology Memoranda, and Standard Review Plans from 1967 to the present were reviewed for Human Engineering Criteria (Appendices I, J, K, L, N).

Since the TMI-2 FSAR was submitted in 1974, the 1973 and earlier standards and Regulatory/Safety Guides pertaining directly to human engineering were selected for evaluation of TMI-2 (Appendix M).

Even though TMI-2 had serious human engineering shortcomings, it met the mandatory and voluntary human engineering standards and regulations extant in 1967 through 1973. These include (see Appendix M for a complete list):

- "Indication of Bypasses. If the protective action of some part of the system has been bypassed or deliberately rendered inoperative for any purpose, this fact shall be continuously indicated in the control room." (IEEE 279, 1968)[1]
- "Manual Actuation. Means shall be provided for manual initiation of protection system action. Failure in an automatic protection circuit shall not prevent the manual actuation of protective functions. Manual actuation shall require the operation of a minimum of equipment." (IEEE 279, 1968)

[1] At the time that TMI-2 received its CP and during its construction, this criterion was interpreted by the nuclear industry and the AEC as applying only to the reactor protection system and not to engineered safety features.

Documentation (FSARs) on the two comparison plants indicates that they also met the mandatory requirements, and design reviews show no departure from mandatory or voluntary standards.

Comparisons of nuclear and military standards (e.g., 1472) shows that AEC and industry human engineering regulations and standards were patently insufficient in the time of TMI-2 development.

3.2.2 Management

Much like the disciplines of system safety and reliability, human factors engineering is most effectively implemented when management is sensitive to the operator and his capabilities and limitations under all operational circumstances.

In the Nuclear Industry, NSSS, A-E, and utility requirements for the control room must be integrated and an overall design philosophy acceptable to each must be developed and implemented with each participating in the design.

The role of each member of this team in CR development was assessed during Essex and NRC interviews with cognizant engineers and managers from the various firms (Appendix S):

TMI-2	Oconee-3	Calvert Cliffs-1
• Metropolitan Edison (Utility)	• Duke Power (A-E & Utility)	• Balt. Gas & Elec. (Utility)
• Babcock & Wilcox (NSSS)*		• Bechtel (A-E)
• Burns & Roe (A-E)	• Babcock & Wilcox (NSSS)*	• Combustion Eng. (NSSS)

*Not interviewed — NSSS vendor specified equipment, but did not actively participate in layout.

Questions dealt with the following management issues:

- Coordination in CR Design
- Procedure for Design Changes
- Selection Criteria for the A-E (Human Engineering considerations?)
- Meetings/Reviews on Control Panel
- Documentation Requirements
- Personnel Experience.

Notes, memoranda, meeting reports and letters pertaining to TMI-2, were used, in addition to interviews, to evaluate management factors.

From a human factors engineering point-of-view the management at Oconee-3 and Calvert Cliffs-1 used a "systems engineering type" approach to CR development, where TMI-2 used a "discipline type" approach. In the systems engineering type approach, all man-machine interfaces (controls and displays, etc.) are controlled by management personnel affected by the interface. No change is made to panel design without the review and critique of everyone involved.

> The systems method provides a means for the orderly, integrated, and timely development of systems. Where people are involved, careful consideration must be given to human capabilities and limitations. When these guidelines are not followed, penalties must be paid in terms of increased costs, decreased performance, slipped schedules, accidents, and loss of life.

In discipline type management, one individual, usually a Lead Engineer, has primary responsibility for panel changes. Disciplines requiring changes to the panel make requests to the Lead Engineer, who approves or disapproves. Consultation with other involved disciplines is not mandatory.

Military and Aerospace experience has shown that human engineering aspects of the system get more reasonable attention when management is conducted on a systems basis (41). The likelihood of human engineering impacting system design in a discipline type management scheme depends on the sensitivity of the Lead Engineer to operator requirements, and human engineering criteria.

The opinion that the CRs for Oconee-3 and Calvert Cliffs-1 were developed using a systems engineering type management rests on several factors.

(1) Both Calvert Cliffs-1 and Oconee-3 control panels were mocked-up during the development process (3, 4, 5, 6). These mockups were used to examine the effects of adding/moving components on operator performance factors. At Calvert Cliffs-1 a mockup was used as a focus for 15-18 months of management meetings concerning the complement of components and layout of the panel. (6)(5)

(2) Calvert Cliffs-1 had a strong technical lead from the Utility which, when compared to the NSSS vendor and the A-E, has most concern for the operational aspects of the CR. (4) (5)

(3) Oconee-3's CR was designed by Duke Power Co., the utility. This placed A-E and Operations under one management team. (3)

(4) All three lead personnel in the Calvert Cliffs CR development had been previously employed in the Nuclear Navy and at least one had participated in systems acquisition for submarines. This provides a basis for using the "Systems Approach" and systems engineering management. (4) (5) (6)

TMI-2's discipline type management is shown in:

(1) The prominent position given to the A-E in overall CR design (1, 2). Since the A-E has little responsibility for operational concerns, use of the "Systems Approach" would have been almost impossible.

(2) The lack of design inputs from the NSSS vendor. B&W, the NSSS vendor, made early suggestions for the NSSS panel design. These suggestions were generally rejected by B&R on the grounds that the CR should reflect one design philosophy. B&W then supplied B&R with their requirements (control/displays) which were integrated into the overall design. No attempt was made to consolidate by mutual agreement the A-E and NSSS vendor design concepts. (1)

Based on interviews with A-E, utility, and NSSS vendors personnel, the following management facts were obtained.

(1) None had trained human engineering personnel. Calvert Cliffs had one engineer who had human engineering as a secondary interest. (1) (2) (3) (4) (5)

(2) Neither JCPL nor BG&E used past experience/record in CR design as a basis for selecting their A-E firms. (2) (6) Duke Power provided its own A-E services.

(3) None of the utilities levied extraordinary human engineering documentation requirements on the A-E or NSSS vendor. (1) (2) (3) (4) (5) (6) (7)

(4) While TMI-2's A-E management had meetings with the Utility's management, notes and records show that panel design from the operational standpoint was not often discussed. In contrast, management for Calvert Cliffs-1 and Oconee-3 held extensive meetings and reviews before deciding on control panel design. (3) (4) (5)

(5) None of the plants had lead personnel with extensive experience in developing large, complex control rooms. (1) (2) (3) (4) (5) (6)

Probably the most important differences between TMI-2 management and management for the other two plants was in management approach. While the TMI-2 CR was managed on a discipline basis, the others were managed on a systems basis. This difference in management approach can account for the ultimate differences in human engineering quality of their CR designs. While Calvert Cliffs and Oconee utilized a systems engineering approach they did not, however, implement a formal human factors engineering program in support of control room design. As a result there were significant deficiencies in the design of both CRs.

3.2.3 Planning

Decisions such as Control Room sizing, basic control board arrangement, specification of design bases, and determination of baseline control room crew complement are made during planning. Each of these has an important impact on the Operator's performance using the resulting control panel.

The degree to which human engineering was taken into account in CR planning was assessed by Essex/NRC interviews with engineers from the several firms named in 3.2.2 above. Interview questions addressed (Appendix S):

- Utility-imposed criteria or other constraints
- Evaluation of alternate panel configurations
- Role of precedent in selecting CR arrangement
- Number of Operators in crew and role of each
- Design Basis for:
  - anthropometrics
  - color coding conventions
  - control room lighting
  - labeling conventions or rules
  - control/display grouping
  - annunciator grouping
  - switch orientation conventions or rules
  - acoustics
  - display readout vs. computer printout assignment of variables
  - control selection
  - display selection
  - use of mimicking
  - video displays
  - separation of functions between primary and peripheral areas.

Following are the findings.

(1) While JCPL imposed virtually no criteria/constraints on B&R or B&W (1, 2), BG&E levied a whole host of requirements on CE and Bechtel, including color coding, types of switches, panel color, and annuciator system (4, 5, 6).

(2) Both B&R and BG&E personnel visited other plants prior to design. B&R visited Oyster Creek-1 for discussions with operators on desirable/undesirable features (1). BG&E visited Detroit Edison which was, at that time, doing some human engineering research into CR design (6).

(3) All three examined more than one general panel configuration before selecting the final concept (2, 3, 6).

(4) Design personnel for Calvert Cliffs-1 and Oconee-3 defined the number of operators at the panel very early in the design (3, 5). While the interviews were conflicting, it appears that TMI-2 staffing was not defined until some time well into the design phase (1, 2).

(5) During the interviews, questions surveying the CR design bases were asked (Appendix S). Table 2 lists the more important bases for each plant, while Appendix Q contains details of the design bases.

Human engineering planning in TMI-2 was virtually nonexistent. While human engineering during the planning of the other two plants was far less than optimal, the use of more powerful design bases, a full-scale mockup and, once again, systems type management, probably carried their CRs into the design phase with better human engineering design.

During early design, the responsibility for TMI-2 (then Oyster Creek-2) switched from JCPL to GPU/Met. Ed. Before this switch, the Utility (JCPL) seemed to be taking an active role in the details of CR design (1). After the switch, GPU/Met. Ed., probably because of staffing problems, did not become too involved in the operator interface on the panel (7). Without adequate regulations and with an uninvolved utility the human engineering design for TMI-2 was left up to the A-E. As was evident from the comparison of plant designs (Section 3.1), this lack of effective management oversight resulted in the CR posing unnecessary operational difficulties.

3.2.4 Design

The role of human engineering in the development of TMI-2, Calvert Cliffs-1, and Oconee-3 was determined by Essex/NRC interviews with engineers and managers of the firms listed in Section 3.2.2. Topics covered in the interviews were:

TABLE 2

PRINCIPLE D.B.s

Calvert Cliffs-1	Three Mile Island-2	Oconee-3
Fossil Experience	Fossil Experience	Fossil Experience
Operator Input	Operator Input	Operator Input
Mockups/Walk-throughs		Mockups/Walk-throughs
Prior to Manufacture Management Input		Prior to Manufacture Management Input
One Operator Control During Normal Operations		One Operator Control During Normal Operations
Industry Standards	Industry Standards	Industry Standards
Review of Other Existing Nuclear Power Plants	Review of Other Existing Nuclear Power Plants	Review of Other Existing Nuclear Power Plants

- Review of panel design with respect to operation
- Use of operator opinion during design
- Determination of personnel training and selection requirements
- Attempts to minimize the likelihood of human error
- Selection of alarm & annunciator strategies
- Enforcement of design convention
- Assessment of readability (displays & labels)
- Control/display grouping
- Design for operator wearing breathing apparatus and/or protective garments
- Operator recall/information processing requirements
- Maintainability
- Operator response times (considered in panel design?)
- Design for separation and redundancy
- Use of mockups, walk-throughs and simulators
- Noise level (taken into account?)
- Participation in developing procedures
- Task analyses (were they performed?)
- Design to protect expensive equipment.

There are several factors of considerable importance in human factors design:

- Design Criteria — As mentioned above, the regulations and standards had no real effect on the human engineering design of any of the CRs under review.
- Design Management — The dedication of management to produce a panel acceptable from all aspects is of extreme importance. TMI-2 management gave little consideration to human engineering factors. (1) (2)
- Design Bases — Reasonable bases must be used for making design decisions. Experience and opinion, and not human engineering fact, played an extremely important role in TMI-2 design. (1) (2)
- Design Philosophy — The designer must have an overall philosophy which is based on the capabilities, characteristics and limitations of the operator, on the basic functions that must be performed, and on the operational conditions under which the functions must be performed.

Design criteria, management, and bases have already been discussed. To examine the differences in design philosophies among the three plants, a set of general design philosophies and principles for TMI-2 was developed from documentation, interviews and the as-built design (Appendix R). Calvert Cliffs-1 (as-built) was then compared to the TMI-2 philosophies/principles to determine differences.

Calvert Cliffs/TMI-2

- Calvert Cliffs and TMI-2 differ in information presentation philosophy. Calvert Cliffs attempts to optimize the information in the CR, not maximize it.
- In addition to indicator lights, Calvert Cliffs also color codes annunciator lights.
- In contrast to the TMI-2 display principle (1e), Calvert Cliffs, as a general principle, uses limit switches with out-of-tolerance indicator lights.
- Where TMI-2 uses the computer printout only when panel space is exhausted (1f), Calvert Cliffs selects parameters for computer output based on operator use and importance.
- In minimizing time to respond to alarms (Philosophy 3), Calvert Cliffs locates most important control/displays in center of panel.

TMI-2 CR design was influenced by the regulatory philosophy of the AEC and NRC, and the management philosophy of GPU/Met. Ed., as well as the design philosophy of Burns & Roe.

NRC Philosophy — At the time of TMI-2 development, the AEC (NRC) regulatory philosophy focused on assuring that the complement of controls and displays was adequate to enable safe[1] operation (Appendix M). Little attention was given to regulating aspects of CR design that increase the risk of human error. Thus, with respect to human engineering, the AEC and NRC philosophies during the early 1970's was "leave it up to the utilities." This approach was in keeping with regulations.

GPU/Met. Ed. Philosophy — In the winter of 1968 when OC-2 was transferred from JCPL to GPU/Met. Ed. to become TMI-2, GPU/Met. Ed. had a very small staff to perform a very complex task — change the design of a nuclear power plant from one site to another (7). Along with staffing problems came the utility's CR design philosophy of "leave it up to Burns & Roe."

With the exception of one minor attempt to redesign the CR to match TMI-1 and one review by TMI-1 operators (both produced some design changes in TMI-2),

[1] Safe operation in this context involves those systems needed to control and cool the reactor and to limit the consequences of accidents. A major fraction of the plant systems are not considered of significance from a safety perspective.

GPU/Met. Ed. seems to have exercised no particular influence over the human engineering aspects of the CR.

3.2.5 Testing

Since the Operator is a critical "component" in the power plant system, evaluating the likelihood that he will be unable to perform properly under some conditions is a critical part of any comprehensive test program. Finding "error prone" procedures or control panels during testing can lead to corrective backfits before the plant is operational.

Personnel from the A-E, NSSS and utilities involved in testing TMI-2, Calvert Cliffs-1, and Oconee-3 were asked, during interviews, to describe any Human Engineering Test and Evaluation performed during the testing phase of their plants.

While all three plants had programs to record and process operator comments on design and procedures, none reported any effort to assess operator performance during testing. Based on a review of the nuclear criteria and standards currently imposed or available, the plants were not required to conduct human engineering tests and evaluations during plant testing.

Controlled human engineering testing in the actual CR can be best carried out before the plant is operational, when human error can occur without creating potentially dangerous situations. Furthermore, human engineering testing should occur when the CR design and relevant procedures have reached maturity, yielding a high fidelity test and more confidence in the results. Both of these conditions can be met only during CR and plant testing.

Operators will make mistakes. However, the likelihood of serious mistakes can be reduced by "fine tuning" designs, procedures and training during Control Room testing (27). While operator comments help in this fine tuning, they are no substitute for hard facts concerning the occurrence and causes of actual human error. In other words, the operator/CR systems should be tested in much the same way as other systems — try them; if they do not work, fix them; then try them again.

3.2.6 Operations

As in testing, the primary role of human engineering in Operations is to identify backfits which, if applied, would reduce the likelihood of human error. Two means to do this are apparent. First, backfit suggestions could be solicited (or accepted) from the operators who know many of the weaknesses in panel design and procedures. Second, a human performance surveillance program could be used to identify design, procedural and training problems.

To determine the role of human engineering in the Operations Phase, personnel from the three utilities were asked to describe programs aimed at improving panel designs or procedures.

None of the three plants surveyed had any program to systematically observe operator performance during operation of the plant. However, operator comments could lead to backfits of procedures and, depending on costs, in hardware. (Neither NRC nor industry criteria require human engineering observation during plant operation.)

3.2.7 Conclusions

In summarizing the findings of this review of the TMI-2 development process, two critical limitations should be noted. First, there were only two plants to which TMI-2 was compared; therefore generalizations to the whole nuclear power community are statistically unsound and potentially misleading. Second, the control room at TMI-2 was designed in the late 1960's and early 1970's, as were Calvert Cliffs-1 and Oconee-3; therefore much of the detailed information on development is lost forever, and some that was recorded in interviews is undoubtedly incorrect.

Within the confines of these limitations, however, there are sound conclusions that can be drawn.

1. During the period of TMI-2 development, the AEC (NRC) was seriously deficient in regulating control room design and operations. No serious AEC or NRC attempts at preventing operator error could be found, although a vast amount of relevant military and aerospace human engineering information existed in readily-available forms.

2. In similar fashion, the nuclear industry virtually ignored human error in its self-regulation process.

3. Human engineering was not systematically applied in the development of any of the plants reviewed herein.

4. GPU/Met. Ed. played a very passive role in control room design. In contrast, BG&E and Duke Power led the development of their control rooms. It is probably not coincidence that these two utilities produced control rooms that

better meet the needs of the operator, since the utility represents the operator in control panel design issues.

5. The constructive use of mockups and walk-throughs by BG&E and Duke Power probably improved the quality of their resulting designs. No such procedures were used by Burns and Roe or GPU/Met. Ed. on TMI-2.

6. Where operator-oriented control panel design bases were used, the result was more effective man-machine integration.

7. The TMI-2 design philosophy assumed unrealistic capabilities in the control room operators.

8. None of the plants examined had tests, evaluations, or observational programs to identify human errors and eliminate their causes.

9. Much of the human engineering in all three control rooms was derived from operator comments during design.

3.3 Evaluation Of Procedures

The ANSI standard N18.7 "Administrative Controls and Quality Assurance for the Operational Phase of Nuclear Power Plants" (1976) defines requirements for preparation of instructions and procedures. In describing the use of the procedures, the standard states that the procedures shall include appropriate quantitative or qualitative acceptance criteria for determining that activities have been satisfactorily accomplished. Furthermore, procedures shall include the following:

- Statement of applicability — The purpose for which the procedure is intended should be clearly stated
- References—Including technical specifications
- Prerequisites — The independent actions or procedures which shall be completed and plant conditions which shall exist prior to its use
- Precautions — To alert the user to those important measures which should be used to protect equipment and personnel, and to avoid an abnormal or emergency situation
- Limitations and actions — Limitations or parameters being controlled and appropriate corrective measures to return the parameter to the normal control band should be specified. Where appropriate, quantitative control guides should be provided.
- Main body — Step-by-step instructions in degree of detail necessary for performing a required function or task

- Acceptance criteria — Procedures should contain acceptance criteria against which success or failure of test-type activity would be judged.
- Checkoff lists — Complex procedures should have check off lists.

In addition to the above, emergency procedures shall include:

- Symptoms — Including alarms, operating conditions, and magnitudes of parameters
- Automatic actions
- Immediate operator actions — Examples include:
  - verification of automatic actions
  - assurance that reactor is in a safe condition
  - notification to plant personnel of the nature of the emergency
  - determination that reactor coolant system pressure boundary is intact
  - confirmation of the availability of adequate power sources
- Subsequent operator actions — Follow-up actions.

3.3.1 Evaluation of TMI Emergency Procedures — A human factors engineering evaluation of procedures is directed toward an assessent that the procedure is:

- Complete — covers all failure modes, plant conditions, and operator actions
- Comprehensive — level of detail is sufficient to ensure identification of faults and restoration of plant status to normal
- Current — addresses the current plant configuration and recognizes changes in equipment, labeling, etc.
- Clear and Concise — readable and indexed; terse statements
- Consistent — with skills of users, with other procedures, and within separate sections of the procedure
- Correct — technically accurate
- In Compliance — complies with ANSI N18.7

An evaluation of the emergency procedure 2202-1.3 "Loss of Reactor Coolant/Reactor Coolant System Pressure" revealed the following:

- The procedure was not complete in several regards
  - It failed to define a leak or rupture which is within the capability of system operation.
  - It lists symptoms but does not address diagnostic procedures and tests.
  - It omits steps which were critical in the 28 March accident, such as when to throttle automatically initiated HPI. It does address operator actions if HPI has not been initiated and if it has been initiated manually, but does not address what the operator should do when HPI has been initiated automatically.

  - Routinely fails to identify what feedback information is required to verify that a step has been accomplished and that the plant is responding as it should.
  - Indicates that the CRO should monitor liquid levels, reactor building parameters, and safety feature flow rates, but does not indicate acceptable and non-acceptable values.

- The procedure has several content coverage problems, notably
  - Step 2.2.2 under A, "close MU-V376 letdown isolation valve and start the backup MU pump if required" — does not discuss how to determine if required.
  - Step 3.2.1 under A, "verify that the makeup pumps and Decay Heat Removal Pumps start satisfactorily" — no discussion of what is satisfactory.
  - Step 3.2.1.1 "close MU-V12 and MU-V18" — no discussion of why; allows no flexibility on the part of the operator to determine if and when he should close MU-V12 and MU-V18.
  - No tolerances are given on readings — step 3.2.2 states maintain 220" pressurizer level. No statement of the tolerance allowed ± 220".
  - Section 3.2.5 (A) states that continued operation depends on the capability to maintain pressurizer level and RCS pressure above the 1640 psig safety injection actuation setpoint. The procedure completely ignores the situation where level is maintained well above its low level alarm point while pressure is below 1640 psig, the situation that was present from 2 minutes after the accident initiation through the 150 minute point.
  - Section 3.2.7 (A) states in a note that RC pumps should be tripped before the RC pressure decreases below the NPSH point — and then refers the operator to a different procedure for the curve (2101-3.1). The curve could easily be reproduced in 2202-1.3.

- Problems with procedure clarity and conciseness
  - The procedure lists symptoms for a leak or rupture which is 1) within capability of system operation and 2) of significant size to initiate ESF. In some cases the symptom states that the appearance of the symptom is a possibility, e.g., "possible makeup line high flow alarm." In fact, three of the six symptoms for the leak or rupture within system capability are "possibles." It is not clear what is intended by "possible symptoms."
  - Too many subjective statements are used in symptoms, such as "... becoming stable after short period of time."
  - It is not clear if all symptoms must be present, or only some subset, or only one of the symptoms, in order to diagnose the problem.
  - The sequencing of steps is not at all logical or consistent.
  - Steps tend to be too wordy.
  - Section 2.2.2.1 of Section B states that the CRO dedicated to recognizing a LOCA must accomplish the following steps within 2 minutes. Four steps are given. Step four states that

MUP discharge cross connnect valves must be opened within 5 minutes of the LOCA. It is not clear how a step taking 5 minutes must be accomplished within 2 minutes.
    - Section A, 3.2.8.1 states, "If not already done, throttle HPI string(s). . ." How is the operator to determine what the "if not already done" means?

- Problems with procedures consistency include
    - Nomenclature used in the procedure is consistently different from panel nomenclature, control and display labels and annunciator designators.
    - The procedure itself is not internally consistent in at times identifying valves to be monitored and at other times omitting such valves.
    - The procedure does not consistently address fault diagnostics and steps to be taken to isolate a failure condition to an item of equipment.

- Problems with correctness of procedure
    - Section B symptoms are not correct. Symptoms for leak or rupture include "rapid continuing decrease of pressurizer level."

- Problems with compliance with ANSI N18.7
    - The procedure includes the reactions designated for emergency procedures but totally ignores the sections required for procedures in general, such as:
        - statement of applicability
        - prerequisites
        - precautions
        - limitations and actions
        - acceptance criteria.

A general problem observed with all TMI-2 emergency procedures is the failure of the procedure to identify in clear and concise terms what the operator decisions are, what information he needs to make the decision, what information he needs to verify that the decision was correct, and what actions he must employ to implement the decision. This deficiency is most apparent in the area of fault diagnosis and isolation. Emergency procedures are only applicable in a fault condition. As such, they should be comprehensive and complete in terms of how the operator must diagnose the fault, isolate the equipment component affected, and act to restore the plant to safe conditions. The essential features of emergency procedures are that they must:

- Be user oriented — sensitive to his or her requirements for information and decision rules

- Be oriented to the decisions required on the part of the operator

- Be complete in terms of the steps to be followed

- Be logical and consistent in terms of the branch points, and the sequences branching off from these points

- Be readable and understandable
- Use pictorial or graphic representations to assist the operator's understanding
- Convey to the operator what he needs to know in order to understand what is going on in the plant.

The President's Commission on the accident at TMI published a report on a technical assessment of procedures. This assessment, authored by R.M. Eytchison (48) concluded that of the 70 procedures in use at TMI, 15 were judged to be significant to the accident. The assessment determined that 7 of the 15 procedures were adequate for their intended purposes. These seven were all operating procedures. A total of four procedures (one operating procedure, one abnormal procedure, and two emergency procedures) were judged to be usable although they contained significant deficiencies that could cause confusing or incorrect response. The four final procedures (again, one operating procedure, one abnormal procedure, and two emergency procedures) were evaluated as inadequate. These included:

- OP2103-1.3 Pressurizer Operations — which emphasized that operators are not permitted by the technical specifications to exceed a pressurizer level of 385 inches in mode 3 (the applicable mode) regardless of emergency conditions.
- AP 2203-2.6 Post-Accident Hydrogen Control
- EP 2202-1.5 Pressurizer System Failure — symptoms are incomplete, misleading, or erroneous. Two sections concerning a stuck-open PORV or code safety valve should have been in the loss-of-coolant procedure.
- EP 2202-1.3 Loss of Reactor Coolant/Reactor Coolant System Pressure — Procedure is confusing since it is not apparent which section is applicable. It is confusing and difficult to follow. It requires the operator to bypass safeguards actuation and throttle HPI regardless of the severity of the accident.

3.3.2 Survey of Procedures in Three Plants

Procedures from each of the three plants were examined against each of five factors: fidelity; accessibility; legibility; readability; and usability. All three procedures were strikingly similar in content, format and typography.

1. Fidelity

A comprehensive review of procedures fidelity was beyond the scope of this study. However, all three sets of procedures have been in use for some time and, therefore it seems reasonable to assume that, to some level, they accurately reflect the systems involved.

There were, however, some discrepancies.

- Nomenclature in the procedures sometimes disagreed with panel labeling.
- In some cases instructions for control actions provided no indication of the correct (or incorrect) system response.
- Procedures placed a tremendous burden on operator memory, and operator memory more frequently fails under high stress emergency situations. This emergency procedure should leave less to memory and thereby increase performance.

2. Accessibility

All three plants took somewhat different approaches to making procedures accessible.

- Oconee used a back projector to present slides of emergency procedures on a large screen in the middle of the control panel. Oconee also uses a trolley for hard bound procedures as well as master files.
- Calvert Cliffs provided a small trolley to convey procedures notebooks from panel to panel. This trolley was also used to rest notebooks while in use.
- TMI-2 has bound procedures on a shelf in the control room.
- Charts and graphs were not integrated into the text (TMI-2 & Oconee; no charts were reviewed for Calvert Cliffs). Like cross referencing, this practice requires flipping pages, which encourages error and increases time to operate.
- All of the procedures used the same spacing between lines within a procedure as lines between procedures. The homogeneous appearance of the text should increase the likelihood of missing a step during a procedure.
- TMI-2 procedures exacerbate the spacing problem by failing to use sufficient indentation to separate sections/subsections, etc.
- None of the plants make much use of special notation or special devices to aid the operator in keeping his place on the page.

3. Legibility

All three sets of procedures use standard typewriter font (10 and 12 pitch) with conventional separation and symbology. This practice is probably acceptable except where the operator reads the manual at a distance of greater than three or four feet.

4. Readability

Since all three plants use operational personnel to prepare and revise procedures, readability from a language standpoint should not be a serious problem. However, it would be helpful if standard terminology was used between procedures and labels.

5. Usability

All three plants represent about the same level of usability.

a) All employ one level of detail. This discourages the more experienced operators from operating from memory, and inhibits memorization.

b) Procedures are sometimes written in sentences of 50 words or more. This makes a "read and so do" strategy almost impossible since the operator is likely to forget some part of the instructions. In all three plants, procedures should be simplified to promote use of previously-memorized procedures and to recognize the limitations of short term memory.

c) With the exception of Oconee's slide projector, the plants rely on large notebooks of procedures. These books are heavy, large, cumbersome, difficult to access, prone to torn pages, and difficult to use while operating.

In summary, the procedures used at TMI-2 appear to be state-of-the-art as compared with other plants. For all three usability of procedures is poor.

3.3.3 Evaluation of the Use of Procedures at TMI-2

The evaluation of TMI-2 procedures extends beyond the assessment of the design of the procedure to include factors associated with the use of procedures. These factors include:

- Identification of which procedures are in effect
- Management of the update of procedures
- Use of procedures as job performance aids.

Identification of Procedure — The primary problem in terms of procedures access is knowing which procedures apply to what situations. A decision aid is needed which is separate from the procedures themselves and which identifies for the operators the procedures which should be in effect. The procedures should specify the conditions which cause them to cease to be in effect. No such aid is presently available to the operators and access to the procedures is based on their familiarity with what is in each procedure.

While this approach may be acceptable in a single fault situation, it fails miserably in a multiple failure condition, as witnessed by the use and non-use of applicable procedures during the accident.

Management of the Update of Procedures — The primary source of impact for procedures update should be the operators. No one can know more about the limitations and problems associated with procedures than the people who have to use them. Presently at TMI there is no formal method for getting operator inputs to procedures updates, or even for having the users identify the problems in using procedures. Procedures should exist for the sole purpose of assisting the operator in his normal or emergency activities. To the extent that operators have problems in using procedures, a mechanism is needed to 1) identify the fact that changes are required; 2) enable operator inputs to be made to the organizational element responsible for updating procedures; 3) complete the change of procedures as required; and 4) obtain further operator inputs concerning the adequacy of the change. The fact that operators are not formally in the loop to update procedures reflects the general attitude of Met. Ed. toward control room operators and senior reactor operators.

Use of Procedures as Job Performance Aids — When faced with a transient such as that which occurred on 28 March 1979, the operators have at their disposal emergency procedures, their training in similar situations, and their overall understanding of plant operation and status. Once the plant is operational, the primary task of the operator is to monitor plant status and to detect and isolate problems. The detection and isolation of problems is essentially a diagnostic operation which simply cannot rely on memory, or intuitive understanding of the plant, or even training, since a significant time period can elapse between the training for a fault situation and the actual occurrance of a fault. For the type of diagnostic task which comprises the control room operators' primary task, training is not enough to ensure effective performance. All that is left is the use of emergency procedures.

In his testimony before the President's Commission on Three Mile Island, Mr. M. Beers of the Met. Ed. Training Division made the statement that the emergency procedures are written as guidelines only, and that operators should primarily rely on their training. Even if the training was outstanding, which it certainly was not, operators could not be expected to rely solely on their training. The training of operators to respond accurately and quickly to infrequently occurring situations, which initially require a diagnosis of the situation to determine and establish plant status and which involve failure modes not even included in available procedures, is an impossible task if all the operator has to rely on is his memory and loosely written "guidelines." If in fact the emergency procedures serve only as general guidelines, then the operator does not need them. What he needs is, first of all, better training in how to diagnose what is going on in the plant, secondly, more and better simulation training allowing him to practice responding to and diagnosing different plant failures, and thirdly, accurate and readily accessible job performance aids. A job performance aid should supplement operator training and should provide him with decision criteria and steps to be taken to formulate hypotheses concerning what is happening in the plant, and to test the hypotheses employing displayed data and test sequences.

3.3.4 The Role of Procedures in the Three Mile Island Accident

Emergency procedures had a significant impact on the Three Mile Island accident. Procedures were grossly deficient in assisting the operators in diagnosing the feedwater system, especially the emergency feedwater system, to determine why the OTSG levels were not responding when emergency feedwater was introduced to the system. The procedures were of no help in diagnosing the PORV failure. They provided no guidance in situations where pressurizer level increased while RC pressure decreased. Furthermore, they presented no clear criteria for what constituted a high PORV exhaust temperature readings with a condition of prior failure.

Procedures did not provide clear guidance on when to override the automatically initiated HPI and to what degree HPI flow should be throttled. No guidance was provided in procedures concerning when to trip RC pumps while temperature and pressurizer level are high and RC pressure is low. Finally, no guidance was presented in emergency procedures concerning when and how to establish natural circulation.

Procedures are deficient because they are not user oriented. They generally are not attentive to the requirements of the operator, and specifically provide the operator with little or no guidance in the most important task, that of diagnosing what is happening in the plant.

The primary requirement of procedures, as evidenced by the 28 March accident, is to support the diagnostic decision-making of the operators. In this regard, available procedures were grossly deficient. Much of what took place in the initial 150 minutes of the 28 March accident was not even addressed by available procedures. The essential task of the control room operator is to diagnose and respond to situations which are infrequent in occurrence and highly variable in effects on the systems. Given this requirement, a comprehensive, logical and consistent set of emergency procedures is essential to plant operation. The procedures available to the operator on 28 March are far short of this standard. Those procedures did not tell the operator what he needed to know, did not assist him in his efforts to determine what was happening in the plant, and were not readily accessible.

3.4 Evaluation of Manning and Training

This section presents the findings of the evaluation of control room manning and operator training. In the area of manning, evaluations were conducted of selection criteria, licensing requirements and the adequacy of control room manning levels. The assessment of training extended to an evaluation of training methods, materials, measures, management, course content, and overall effectiveness of training in terms of the operator performance requirements inherent in the initial 150 minutes of the Three Mile Island accident.

3.4.1 Evaluation of Manning

3.4.1.1 Adequacy of Manning Levels — At 0400 on 28 March 1979 the crew on duty at TMI-2 exceeded the minimum shift crew composition requirements for their Operational Mode, (Mode 1, Power Operation). One person with a Senior Operator license, two holding Reactor Operator licenses and two non-licensed personnel were required as per TMI Technical Specifications. On duty at the time were two Senior Reactor Operators, two Control Room Operators and seven auxiliary operators. This number has proven to be adequate for most normal operations; fewer are required for modes of cold shutdown or for refueling with reactor vessel head unbolted or removed and fuel in the vessel.

For emergency situations, crew composition requirements are not as straightforward. It is clear that the number of required personnel goes up during emergencies, although the optimal number is unknown. Higgins, appearing before the Weaver Oversight Hearing (72), 15 May 1979, stated that the number of people in the control room later in the morning did not hamper or hinder the situation; rather, that the missing element was the right people with proper knowledge; however, Creswell states that 30 people are not required to operate the plant.

In order to determine the number of personnel needed on duty or on call to handle various emergencies, an analysis similar to that described by Anderson, Back and Wirstad

(29) would be required. That report describes a job analysis method used to determine competency requirements and to evaluate the training provided for three jobs, those of shift supervisor, reactor operator and turbine operator.

3.4.1.2. Adequacy of Licensing Requirements — Title 10 Code of Federal Regulations (13) stipulates the requirements for operator licensing. It requires that no person may function as an operator or senior operator except as authorized by a license issued by the NRC. Along with personal background information, the applicant must submit evidence of ability to operate controls in a safe and competent manner, and a medical examination report.

The qualified applicant must pass written examinations and operating tests. The written exam for the operator covers 12 areas intended to reveal knowledge of fundamental theory, systems, subsystems and components and their interactions, procedures, and safety items. The senior operator must pass a written exam requiring an in-depth knowledge of all of the afore-mentioned as well as nine additional technical and procedural areas that are deemed necessary for a supervisor to know.

Requalification program requirements are also stated for a continuing program comprised of lectures and on-the-job training. The required lectures cover nine areas that are primarily devoted to plant knowledge, theory, procedures and safety. On-the-job training requires operator manipulation of the plant controls, including at least 10 reactivity control manipulations. A simulator can be used for this if it reproduces the general operating characteristics of the plant and the arrangement of instrumentation and controls are similar to those of the plant.

Procedures and facility design updates are also emphasized. Requalification training effectiveness is evaluated by annual written exams, systematic observation by supervisors and training staff, and by simulation. Records are required of each licensed individual's classroom and simulation experience.

The problem that arises with licensing is that it encourages the licensee to train to pass the exam rather than ensuring safe, effective operation of the system. B&W, which provides Met. Ed.'s simulator training, has formally denied that they train students to pass the NRC exam; rather, they insist that they attempt to provide the student with skills and knowledge enabling responsible management of a nuclear plant (72). In any event, the oral portion of the NRC exam does provide the opportunity for observation of control room operators' familiarity with plant systems and components, aside from simply a knowledge of nuclear safety factors.

3.4.1.3 Selection Procedures — The selection process for nuclear power plant operators seems to be less sophisticated than that used for the selection of operators in other complex man-machine systems. Basically, the requirements are a high school education, or equivalent, with ability in math and physics. ANSI/ANS 3.1 (1978) stipulates that operators should possess a high degree of manual dexterity and mature judgement and also that maintenance personnel should possess the capability of learning and applying basic skills in maintenance operations. These requirements are basically the same as ANSI/N 18.1 (1971) under which most TMI operator personnel were selected. Most utilities rely heavily on the personal interview; however, Duke Power Company also administers validated entry level tests to identify applicants with the aptitudes necessary to deal successfully with a technology that is strongly dependent on a knowledge of mathematics and the physical sciences. Met. Ed. states in their position descriptions a requirement for passing an aptitude or comprehensive test for assignment as an Auxiliary Operator-C. There is evidence that passing this test is not used as a prime acceptance criterion (per conversation with R. Zechman of Met. Ed.'s training department), although such aptitudes may be proven essential at this level given that personnel hired for the Auxiliary Operator C positions are expected to progress to the position of Control Room Operator. Further screening does occur in that comprehensive exams are given at progress points from AO-C to AO-B and from AO-B to AO-A.

In evaluating Met. Ed.'s selection procedure, one must consider the impact of operating in a union environment. Through negotiations with the union, Met. Ed. developed a policy of promoting to the position of CRO the most senior qualified Auxiliary Operator-A, rather than the most qualified. In theory, the most senior, given the most experience, should also be the most qualified, though it is obvious that that will not always be the case.

An assessment was conducted to determine the degree to which Met. Ed.'s selection procedures and criteria were in compliance with NRC and industry criteria, guides, requirements and recommended practices. The result of this assessment is contained in Appendix F. As seen in this Appendix, Met. Ed.'s selection procedures and criteria were in compliance on 9 of 12 issues. Met. Ed. was not in agreement on STD-5.3 (health requirements), STD-5.4 (medical certification and monitoring), and RG-5.5 (medical evaluation of job candidates). While the basic requirements were addressed by Met. Ed. in selection or training descriptions or the FSAR (i.e., basic educational requirement of high school diploma or equivalency, "normal health," etc.) specific health concerns were addressed only tacitly as "normal health" and "passing a physical examination."

3.4.2 Evaluation of Training

3.4.2.1 Evaluation of the compliance of the Met. Ed. Three Mile Island Operations Training Program to Standards — An assessment was made of the degree to which the Met. Ed. training program agrees with standard training criteria, guides, requirements and recommended practices. The results of this assessment are indicated in Appendix G. The table contained in Appendix G identifies items from 10CFR, regulatory guides, ANSI standards, and the Standard Review Plan which establish requirements, directives, or guidelines for the training program. The table also identifies whether or not the cited requirements, criteria, guides or recommended practices were met by Met. Ed. in the establishment of the TMI-2 training program. It is apparent from this table that Met. Ed. unequivocally met 56 of the 58 items listed, failing to comply with RG-T.3 (recommended practice on training operators to distinguish the odor of hazardous chemicals), and possibly failing to comply with SRP-T.5 (criterion 5, refresher training for non-licensed personnel). It is therefore concluded that little or no problems existed in terms of the degree to which the Met. Ed. training program complied with NRC and industry standards and criteria. If problems are identified in a training program which is virtually in full compliance with the existing standards, the conclusion must be that the problem is in the standards themselves.

3.4.2.2 Evaluation of the Elements of the Training Program — The evaluation of training effectiveness begins with a determination of training requirements. Appendix H contains the results of a training task analysis for the emergency procedures appropriate for the initial 150 minutes of the accident. These procedures include:

- Turbine Trip 2203 - 2.2
- Reactor Trip 3303 - 1.1
- Inoperative PORV 2202 - 1.5
- Loss of Reactor Coolant 2203 - 1.3A within system capability
- Loss of Reactor Coolant 2203 - 1.3B ESF Systems initiated
- Loss of RC Flow/RC Pump Trip 2202 - 1.4.

The task analysis identifies, for each task from each procedure, information requirements, decision requirements and performance requirements associated with the task, the necessary skills and knowledges, and training objectives. The skills and knowledges include the specific skills and knowledges required by the operator to perform the task. Skills include:

- Diagnostic skills
  - formulation of hypotheses
  - detection of faults
  - isolation of faults
  - verification of system response
  - integration of information to reach a decision
  - understanding of plant status
- Procedural skills
  - identify and access procedures
  - determine what to do next
  - sequence of tasks
  - understanding of the rationale for a sequence
- Control skill
  - perceptual-motor, manipulation of a control
  - anticipating system response
  - adjusting system parameters
- Perceptual skill
  - identifying a display or control
  - reading a display
  - understanding a display.

Types of knowlege include:

- Facts
  - system structure
  - setpoints
  - expected values
- Principles
  - of system operation
  - system interrelationships
  - cause-effect relationships
  - system rate of response
- Procedures
  - steps
  - sequences
- Decision rules.

The training objectives developed from this training task analysis are summarized in Table 3. Training objectives comprise statements of the capabilities that must be possessed by the trainee at the termination of training. The essential elements of a training objective are: a statement of what the trainee must be capable of doing; a description of the conditions under which this performance capability is required; and a determination of the standards of performance which enable a judgement that performance is adequate. The essential characteristics of a training objective are that it must be: relevent, complete, and measurable. It must be relevant in that associated skill and knowledge requirements are indeed adequate for job performance. It must be complete in

TABLE 3 TRAINING OBJECTIVES

Operator should, with 100% accuracy, be able to:

- Detect a leak or rupture in the RCS
- Verify a LOCA within 2 minutes of occurrence
  - access MUP cross - connects within 3.5 minutes of LOCA
  - access MU-V16 valves within 4.5 minutes of LOCA
- Access and actuate valves to control discharge line cross-connect within 5 minutes of LOCA
- Establish a makeup flow of 125 GPM per leg within 10 minutes of LOCA
- Isolate a RCS leak to RB, OTSG tubes, or steam line
- Verify automatic response to RCS leak immediately without reference to procedures
  - Respond manually to a leak or rupture immediately without reference to procedures
- Determine that makeup tank and PZR levels cannot be maintained, and respond correctly
  - Respond with follow-up actions to leak detection, leading to shutdown
- Determine that pressurizer level and RC pressure are within limits
- Control makeup
- Bring RC system under control
- Identify a reactor trip
- Respond immediately to a reactor trip without reference to procedures
- Diagnose a failed open PORV
- Verify the response of the automatic system to failed PORV
- Respond to an inoperative PORV
- Bring pressure and temperature back to normal
- Recognize a turbine trip
- Diagnose a turbine trip and identify cause of the trip
- Determine that the automatic response to turbine trip is correct
- Respond with immediate actions in response to a turbine trip
- Reduce feedwater to produce a 15% neutron power level
- Control rods to produce a 15% neutron power level
- Determine if critical parameters are in tolerance
- Control Tave, RC pressure and steam header pressure
- Control pressurizer level to 240"
- Control OTSGs to 30"

- Determine if vacuum is lost
- Verify header pressure at 885 Psi
- Control reactor power to zero
- Determine turbine trip due to loss of FW pumps
- Verify response of FW pumps
- Control OTSG levels using EFW system
- Control heater drain pumps
- Maintain the vacuum
- Keep drain tanks open until turbine parts are cool
- Verify engagement of turning gear
- Maintain seal oil temperature
- Determine if notification of HP/Chemistry is needed
- Recognize loss of main feedwater flow to both OTSGs
- Determine the cause of loss of main FW & both OTSGs
- Respond with immediate action to loss of main FW to both OTSG's without reference to procedures
- Respond to loss of feedwater due to valves closing
- Follow-up loss of feedwater flow actions
- Recognize loss of main feedwater flow to one OTSG
- Verify system automatic response to loss of FW to one OTSG
- Respond with immediate action to loss of FW to one OTSG
- Respond with appropriate follow-up action to loss of FW to one OTSG
- Determine that an RCP has tripped automatically
- Determine that an RCP trip is necessary and trip the RCP.

accounting for all performance outputs. It must be measurable in that the capability statements are made in a way which permits determination of the achievement of the objective.

Training objectives make up the basis for the content of a training course. They define and describe the knowledge and skills which must be possessed by trainees at their point of exit from the course. From a training evaluation perspective, development of the set of training objectives associated with a set of job requirements (in this case, the conduct of tasks described in relevant standard emergency procedures) provides a basis for evaluating the adequacy of the course content. A training course is relevant to job requirements to the extent that it addresses the training objectives derived from those requirements. A classification of these training objectives was made which resulted in five categories of training objective. These are:

- Detect and isolate a fault or off-normal condition
- Detect and isolate causes for changes in system status
- Verify that the response of the system is correct
- Control the system status/response/configuration
- Respond to faults and system status changes.

Table 4 indicates training objectives assigned to each training objective category. Table 5 lists the primary skills and knowledge associated with each training objective category. As indicated in this table, diagnostic skills apply to three of the five training objective categories, while procedural skills apply to two categories and control skills to one training objective category. This indicates the importance of diagnostic skills for the tasks associated with selected procedures.

3.4.2.3 Evaluation of Training Methods — Training methods can be classified by their contribution to the acquisition of skills or knowledge. The classification is:

- Skills Acquisition methods
  - simulation
  - on-the-job training
  - research reactor training (off-site)
- Knowledge Acquisition methods
  - lecture
  - self-study
  - examination and review

TABLE 4 TRAINING OBJECTIVES BY TRAINING OBJECTIVE CATEGORIES

- Detect and isolate a fault or off normal condition
  - leak or rupture in RCS
  - LOCA
  - RCS leak in reactor building
  - leak in OTSG tubes
  - leak in steam lines
  - loss of vacuum
  - loss of main feedwater in one OTSG
  - loss of main feedwater in both OTSGs
  - RCP fault requiring a trip
  - determine that makeup tank and pressurizer levels cannot be maintained
- Detect and isolate causes to change in system status
  - Reactor trip (10 causes)
  - turbine trip (11 causes)
  - RCP trip (7 causes)
- Verify that system response is correct
  - automatic response to RCS leak
  - pressurizer level and RC pressure are within limits
  - automatic response to failed PORV
  - automatic response to turbine trip
  - critical parameters in tolerance
  - header pressure at 885 psig
  - response of FW pumps
  - engagement of turning gear
  - automatic response to loss of FW to one OTSG
- Control system status/response/configuration
  - activate valves to control discharge cross-connect
  - establish MU flow of 125 GPM per leg
  - control makeup
  - bring RC system under control
  - bring pressure and temperature back to normal
  - reduce FW to produce 15% neutron power level
  - control rods to produce 15% neutron power level
  - control Tave, RC pressure, steam header pressure
  - control pressurizer level to 240"
  - control OTSGs to 30"
  - control reactor power to zero
  - control OTSG levels using EFW system
  - control heater drain pumps
  - maintain the vacuum
  - maintain seal oil temperature
- Respond to faults and system status changes
  - respond to loss of FW to one OTSG
  - respond to loss of FW to both OTSGs
  - respond to loss of FW due to valves closing
  - respond to turbine trip
  - respond to inoperative PORV
  - respond to reactor trip
  - respond to leak or rupture in RCS.

TABLE 5 PRIMARY SKILLS AND KNOWLEDGE BY TRAINING OBJECTIVE CATEGORIES

Training Objective Cateogory	Skills	Knowledge
Detect and isolate a fault or off normal condition	● Diagnostic	● Principles of system operation ● Decision rules (fault cues) ● Procedures (correct responses)
Detect and isolate causes for changes in systems status	● Diagnostic	● Principles of systems operation ● Principles of change (causes)
Verify that system response is correct	● Diagnostic ● Memory	● Facts (limits) ● Facts (automatic responses)
Control system status	● Control ● Procedural	● Facts (rate of response) ● Facts (correct response) ● Procedures
Respond to faults and system status changes	● Procedural ● Perceptual	● Facts (rate of response) ● Facts (correct response) ● Procedures

Evaluation of Simulator Training

An assessment was made of the distribution of training time to skills acquisition and knowledge acquisition for the training of the crew of four who were on duty at TMI the night of 28 March 1979. This assessment involved determining the proportion of total training time given over to skills and knowledge acquisition. It was determined that 16% of the hours devoted to training were concerned with skills acquisition. Furthermore, less than 6% of the total time devoted to the initial training of specific crew members was devoted to simulation training. A similar analysis of general AO and cold license training conducted by Met. Ed. revealed that 17% of the training hours were devoted to skills acquisition training and about 5% of total training time was devoted to simulation training.

The relative importance of different operator skills was determined for the procedures of importance by identifying the number of training objectives requiring each skill. The proportion of training objectives associated with each type of skill is as follows:

Diagnostic skill - 49% of training objectives
Control skill - 34%
Procedural skill - 34%
Procedural skill and/or control skill - 50%
Perceptual skill - 16%

The essential feature of diagnostic skill training is the ability to reproduce the symptoms of a fault condition and require the operator to detect and isolate the problem based on his understanding of what is happening in the plant. Diagnostic skill training, therefore, requires a simulator which has high fidelity to the operator's control room in terms of systems response, cue patterning, and format of the information available to the operator for diagnosis. The simulator need not be of high fidelity with the represented control room in terms of physical characteristics (console size and shape; panel arrangement; control and display arrangement; control size, shape, location and orientation to the operator; display size, shape, scaling and orientation). Therefore, to the degree that it accurately simulates system initial condition, system responses, symptoms, rates of change, failure effects, and responses to operator inputs, the B&W Lynchburg simulator should serve as an effective training tool for diagnostic skill acquisition even though it does not physically represent the TMI-2 panel configuration.

As indicated above, half of the training objectives for selected procedures are associated with diagnostic skills acquisition, and half are associated with procedural and control skill acquisition. Procedural skill acquisition refers to the development of skills for following sequences of activity, determining what to do next, and following procedures. Control skills involve development of perceptual-motor capabilities associated with making precise control manipulations while monitoring displays. Control skills also involve generation of expectations concerning what the system will be doing, leading to the development of anticipations of what the system will be doing prior to initiation of the system response. For these types of skill acquisition high fidelity simulation is required for both console configuration and system response. Acquisition of these skills, which account for 50% of the training objectives associated with relevant procedures, cannot be accomplished through the use of the B&W simulation facility due to its lack of physical fidelity with the TMI-2 control room.

Operators do not receive sufficient simulator training to enable acquisition of the range of diagnostic skills, control skills and procedural skills associated with the performance of tasks within relevant procedures. A sufficient amount of simulator training must be identified in terms of skills to be acquired rather than with respect to a minimum number of hours of exposure to the simulator. What simulation training the operators do receive is only partly appropriate for the kinds of skills being acquired. The B&W simulator is more applicable to the development of diagnostic skills than it is for acquisition of control and procedural skills.

Another problem with the simulator training provided for the operators is the use of the simulator. A simulator can be used to demonstrate what happens in a reactor system when specified failures occur. A simulator can also be used to provide practice in control techniques, procedural sequences, fault isolation, and integration of displays. Finally, a simulator can be used to measure operator performance capability in terms of reaction time, time to complete specific sequences or operations, probability of success, number and types of errors, and control precision.

It is obvious that the simulator training afforded the TMI operators emphasized the first of these applications, use of the simulator to demonstrate plant responses to the operator. This conclusion is based on the fact that the shift supervisor on duty at TMI at the time of the accident had undergone requalification training on the B&W simulator in March 1979. During the 20 hours of simulator operations, a total of 19 different evaluations and emergencies were simulated. Of these, 14 were only performed once and only one was performed as often as three times. This would indicate that the simulator is being used to illustrate for the operator what a selected emergency looks like in terms of display readings and plant reactions. It is not being used to allow the operator to acquire skills through practice in responding to faults and formulating hypotheses concerning what is happening in the plant. In this regard, the simulation training is judged insufficient.

The simulator is supposedly used to assess operator performance capability. However, what assessments that are made are based on the subjective opinion of the instructor concerning operator performance capability level rather than on quantitative measurements of operator performance or selected parameters, such as time to diagnose and correct a fault condition, accuracy of procedures following accuracy of control input, etc.

Evaluation of On-The-Job Training

A second method of presenting skills acquisition training at Three Mile Island is through on-the-job training (OJT). While simulator training accounted for about 5% of the time the accident crew spent in training, formal OJT accounted for about 10% of their training time. As stated in the FSAR, the OJT program requires that an operator will have experienced certain specified events during the two year term of his license. Specifically, he must participate in a minimum of 10 reactivity manipulations. The reactivity manipulations which were judged to demonstrate skill and familiarity with reactivity control systems and which were credited as meeting the OJT requirement include but are not limited to:

- Power change of greater than 10% full power with the reactor control station in manual
- Control rod manipulation from subcritical to the point of adding nuclear heat
- Boration and deboration maneuvers involving control rod manipulation
- Turbine startup and shutdown
- Reactor trips and subsequent actions.

While the use of OJT to enhance and solidify the acquisition of skills is an excellent follow-up training approach due to the high fidelity of the control room configuration, system response, procedures, etc., it should not constitute a major approach for the acquisition of skills. The primary limitation of OJT for skills acquisition is the inherent lack of experimental control in terms of selection of events, selection of initial conditions, and selection of time of onset. In OJT, the operators must respond to what is happening during actual operation. Their expectancies concerning systems response is therefore built on the events that they happened to experience during the OJT period. The FSAR does not ensure a breadth of experience over the reactivity manipulations in that it only requires that an operator experience 10 events. The 10 events can comprise the same event experienced 10 times. It does state in the FSAR that participation of licensed personnel in the OJT program will be reviewed quarterly by supervisors to ensure that operators participate in a variety of evaluations. If diversity of operations is lacking, specific assignments may be made to ensure wide operator experience.

Evaluation of Classroom Training

Classroom training constitutes the use of lectures and lesson plan handouts for self study. The TMI-2 training course description states that 81% of the total of 2647 hours for auxiliary operator training and cold license training be given over to classroom instruction. The crew on duty at the time of the accident spent an average of 85% of their training time in classroom instruction.

Classroom instruction, therefore, constitutes the major training method for initial operator training. As the operator progresses to the hot license training phase, he spends all of his training time either in attending training sessions during his training shift, or in self study for a minimum of two hours of each shift.

In either training approach, lecture or self study, the critical factors from a training evaluation standpoint are the completeness and accuracy of the content, and the readability and clarity of the lesson plan format.

The lesson plan, designated lecture outline, for the feedwater system was critically reviewed. The outline had no access number or code, no statement of revisions, and no date of preparation. The contents of the outline were: objectives, system functions, general system description, operational description, and appendices including a fact sheet, interlocks, important parameters, technical specifications, flow diagrams, and references.

The outline contains 14 pages of text. The objectives, which appear to comprise a portion of the training objectives (what the trainee must be able to do with no indication of standards or conditions of performance) are as follows:

- To know the purpose of the system.
- To be able to draw a one-line diagram of the feedwater system showing all major valves, components, instruments and connecting lines.
- To know the value of the major operating parameters.
- To be able to trace the system out in the plant.

The general system description comprises about a page of text describing the overall feedwater system and emergency feedwater system. The operational description is 5-1/2 pages of straight text describing procedures for startup, normal operation, shutdown, and two special or infrequent operations (loss of feedwater heater and condensate/condensate booster pump set trip). The appendix labeled Flow Diagrams comprises three pages of handdrawn diagrams.

In terms of content, the outline is very general and addresses only normal operations (except for a very brief description of two abnormal situations). The training objectives derived from the relevant emergency procedures, listed in Table 3, include 12 objectives which are directly related to the feedwater system. Not one of these objectives is addressed in the lecture outline on feedwater systems.

In terms of format, the outline presents information in blocks of text. Such a presentation is difficult to read and retain. Flow diagrams are hand drawn and are also difficult to read. It is obvious that while the author of the outline knew feedwater systems, he did not display any expertise in terms of training material presentation to enhance trainee interest and retention.

A similar evaluation of the lecture outline for the reactor coolant system which was used by the accident crew during their training yielded identical results. Not one of the 20 training objectives concerned with RCS in Table 3 are addressed in the outline. The outline is primarily concerned with system normal operation but does list operating transient cycles for a number of transients. An inoperative or failed PORV and a LOCA are not included in the list.

The lesson plans and outlines have been assembled into a B&W Training Manual, published in 1974. This manual presents detailed descriptions of TMI systems. The section on the reactor coolant system runs 16 pages and does not address any emergency modes or failure conditions whatsoever. The section on OTSGs runs 25 pages with 2 pages given to tube leak detection and location. None of the relevant training objectives (Table 3) are addressed. The section on RC pumps and motors is 8 pages long and is totally devoid of information on failures or emergencies.

An assessment of the content of the TMI-2 training program in terms of the training requirements presented in Appendix H was not possible due to the difficulty in obtaining complete descriptions of the course content.

3.4.2.4 Evaluation of Training Measures — One of the most important aspects of a training program is the adequacy of the training effectiveness evaluation methods and measures. With a good set of measures to establish operator performance capability in terms of job requirements, the training system itself must benefit by virtue of the feedback concerning effectiveness of different methods, materials, content areas, etc.

The only real measure of operator capability at Three Mile Island is the NRC Licensing Examination. In fact, operators claim that the total thrust of training is to assist them in passing this examination. The NRC examination was evaluated in several ways. A count was made of the number of training objectives associated with accident relevant procedures which were included in samples of the examination. An average of 1.2 of the 53 identified training objectives were addressed over a sample of three RO examinations and two SRO examinations. If, in truth, the operators are trained to pass the NRC exam, they did not receive much training at all on the training objectives associated with accident-related emergency procedures.

While the B&W simulator should be capable of scoring operators on selected performance parameters, the only measure associated with simulation exercises in use is instructors' judgement. Such judgement is usually made in terms of a dichotomy, pass or fail. The student does not benefit from such an assessment.

The Met. Ed. Training Division has established a number of written and oral tests such as evaluation quizzes concerning the content of operational review lectures, written quizzes on the fundamentals and system review program, an annual evaluation examination, written and oral (simulating the examination normally administered by NRC), and examinations conducted every three and six weeks of the nine month training period leading to a hot plant license.

The approach to test construction appears to be too informal as is the approach to the entire training program. Tests should reflect job requirements and should be based on specific training objectives. They are not. Tests should be performance based and criterion referenced. They are not. Tests should comprise methods of presenting feedback to operators as to their performance strengths and weaknesses. They do not. Tests should measure both operator knowledges and skills, including the capability to diagnose a transient and identify causal factors, the capability to control plant systems, the capability of following procedures, the capability to anticipate the response of slowly reacting systems, and the capability to understand what is going on in the plant. They do not.

3.4.2.5 Evaluation of Training Management — The primary problems noted with Three Mile Island training management are as follows:

- There is no formal method to evaluate the effectiveness of courses, the currency and accuracy of material, and the adequacy of materials, media and measures.
- There is no formal method for upgrading and updating training methods, techniques, content and materials.
- There is no selection criteria or instruction program for instructors which emphasizes instructional skills rather than plant control skills.
- There is too much concern for the administrative aspects of the course (record keeping, conduct of evaluations, etc.) and too little concern for ensuring that the training provided the operators is directly related to the skills and knowledge required to meet specific job requirements.

3.4.2.6 Summary — Even though the Met. Ed. Training Program was noted to be in full compliance with industry training standards, the program has a number of significant problems. These include:

- Too little application of simulation for skill acquisition
- Inappropriate use of simulation as a demonstration tool rather than a training device
- Failure to use simulation to measure operator performance capabilities
- Reliance on on-the-job training for skills acquisition
- Use of training materials and manuals which are too specific in terms of system description, and not sufficiently specific in terms of emergency modes
- Failure to develop and validate real measures of performance capability and knowledge
- Failure to formally review and update training program elements
- Failure to train instructors in instruction skills.

The overall problem with TMI training is the same problem with information display in the TMI control room application of an approach which innundates the operator with information and requires him to expend the effort to determine what is meaningful.

3.4.2.7 Conclusions — While it is true that the Met. Ed. training program met the criteria, guides, requirements and recommended practices established by NRC, ANSI, and the industry, the evaluation of the training program determined that it was almost totally deficient. The approach to training paralleled the TMI-2 approach to information display — which is to provide the operator with everything that he may ever need and let him determine what is meaningful.

In their numerous interviews and depositions, whenever any member of the crew was asked what he needed in the early morning hours of 28 March 1979, his response was invariably some way of knowing what was going on in the plant. To a large extent this is an information display problem. To a similar extent it is a training problem. The process by which an understanding of plant status is developed is through an integration of displays, diagnosis of plant status and performance, and reference to diagnostic procedures. No training was provided to operators to assist them in integrating display readouts. No training was provided to enable development of skills in diagnosing plant status and performance and certainly no diagnostic procedures were available to the operators.

Training at TMI-2 was deficient in that is was not directed at the skills and knowledges required of the operators to satisfy job requirements. It is not even apparent that selection of training methods was based on an analysis of operator skills and knowledges or even that training objectives were developed which directed the selection of training course content.

Training at TMI-2 was deficient because every training objective associated with relevant procedures identified requirements for skills which could only be acquired through the application of simulation, and less than 5% percent of the crew's training time was spent in simulation. Not only was simulation largely ignored, but where it was used it was misused. The little simulation training provided the operators was used to demonstrate selected faults rather than provide the operators the opportunity to practice diagnosing the fault and selecting a response.

Training at TMI-2 was deficient in that it failed to provide the operators with the skills they needed on 28 March, i.e., skills in development of a hypothesis and acquisition of feedback data to verify the accuracy of the hypothesis. Training received by the operators generally ignored emergency conditions, presumably on the premise that the system was sufficiently reliable so as to hardly ever require operator fault detection and isolation.

Training at TMI-2 was especially deficient in its failure to provide for measurement of operator capabilities. Even if the remainder of the training program was totally unsatisfactory and methods and measures for operator capability assessment were provided, decisions could be made concerning the readiness of the operators. Without these measures the TMI training program makes the assumption that since a trainee has been exposed to material, he has learned it. The assumption is naive and, in the case of TMI-2, almost castastrophic.

Training at TMI-2 is deficient in its training of instructors. Instructors were selected for their knowledge of systems, components and operations. Instructors received no instruction in how to instruct, how to reinforce lesson objectives, or how to assist trainees in understanding the system.

Training at TMI-2 was deficient in its archaic approach to learning. No applications of instructional technology are included in the program. Self study is by the book, including learning everything there is to now about system structure and function. Self study exercises do not apply any of the proven techniques of self paced, individualized instruction, including programmed instruction, pictorial scenarios, graphic depiction of procedures, and frequent self examination. Simulation exercises, as stated above, are almost totally deficient, even though they are cited by operators as the most meaningful element of their training. Classroom instruction is by lock step lecture (straight lecture with no student interaction), inundating the trainee with verbose descriptions of unrelated facts, incomplete sequences, and uncoordinated operating principles.

Training at TMI-2 was deficient in that it was not closely associated with procedures used by the operators. No guidance at all is provided the operators in what to do if procedures do not apply, or if the situation faced in the plant is counter to what the procedures describe. The Met. Ed. training division is on record as stating that procedures are only guidelines and what the operator must rely on is his training.

Training at TMI-2 was deficient in that it totally ignored the fact that operators are dealing with a slowly responding system. Nowhere in the training program were trainees advised of plant response time and what to do to ensure that errors are not made on the basis of this slow response. Given such training the operators would have been better equipped to cope with the closure of the emergency feedwater block valves.

Training at TMI-2 was deficient in that it did not provide for formal updating and upgrading of training methods, materials, and content. No formal techniques had been established wherein insights and experiences of operators were used to update the training program. The Met. Ed. training program viewed operators as people to be trained, and failed to see the other side of the two way street.

Training at TMI-2 was deficient, above all other considerations, because it failed to establish in the crew the readiness necessary for effective and efficient performance.

Operators were exposed to training material, but they certainly were not trained. They were exposed to simulators for the purpose of developing plant operation skills, but they were not skilled in the important skill areas of diagnostics, hypothesis formation, and control technique. They were deluged with detail, yet they did not understand what was happening. The accident at TMI-2 on 28 March 1979 reflected a training disaster.

3.5 Findings

The findings of this investigation concerning the human factors engineering aspects of the TMI control room and operations include the following:

Control Room Design

- Information required by operators is too often non-existent, poorly located, ambiguous, or difficult to.read.
- Annunciators are poorly organized, are not color coded, are often difficult to read, and are not arranged in priority order.
- For the RCS, Pressurizer and Secondary System sub-panels of Panel 4, a total of 84% of applicable human engineering criteria for displays were not met.
- At TMI there are 1900 displays located on the vertical panels. Of these, 503 or 26% cannot be seen by a 5th percentile operator standing at the front panels.
- Labeling of controls and displays is in many cases inadequate or ambiguous, as indicated by the 800 changes made by the operators to the labels provided.
- For the RCS, Pressurizer and Secondary System sub-panels of Panel 4, a total of 68% of applicable human engineering criteria for labels were not met.

Control Room Development

- Human engineering planning at TMI-2 was virtually nonexistent.
- NRC and the nuclear industry have virtually ignored concerns for human error.
- Where operator - oriented control panel design bases were used (Calvert Cliffs and Oconee) the result was more effective man-machine integration.

Procedures

- A detailed asssessment of EP 2202-1.3 "Loss of Reactor Coolant/ Reactor Coolant System Pressure" revealed serious deficiencies in content and format.
- There is little consistency between nomenclature used in procedures and that used on panel components.

- Instructions for control actions seldom provide an indication of the correct (or incorrect) system response.
- Procedures place an excessive burden on operator short-term memory.
- Charts and graphs are not integrated with the text.
- It is not clear which procedures apply to which situations.
- There is no formal method for getting operator inputs into updates of procedures.
- Procedures were grossly deficient in assisting the operators in diagnosing the feedwater system, diagnosing the PORV failure, determining when to override HPI, and determining when to go to natural circulation.

Training

- The Met. Ed. training program was in full compliance with government imposed standards concerning training.
- TMI-2 training was deficient in that it was not directed at the skills and knowledges required of the operators to safety job requirements.
- The essential operator skill is to be able to diagnose what is happening in the plant. The most effective training method of acquiring this skill is simulation. Only 5 percent of training time is used for simulation training.
- Training in emergency procedures was deficient.
- Training at TMI-2 was deficient in its failure to provide for measurement of operator capabilities.
- Training at TMI-2 was deficient in its training of instructors.
- Training at TMI-2 was deficient in its archaic approach to learning.
- Training at TMI-2 was deficient in that it was not closely associated with procedures.
- Training at TMI-2 was deficient in ignoring the fact that operators are dealing with a slowly responding system.
- The training program at TMI-2 did not provide for formal updating and upgrading of methods, materials, and course content.
- Training at TMI-2 failed to establish in the crew the readiness necessary for effective and efficient performance.

3.6 Conclusions

Section 2.2 described specific operator actions and inactions which caused or contributed to the March 28, 1979, accident at TMI-2. Clearly, operator error was a major factor in the accident. To let the matter rest, however, with an assessment that the accident was due to operator error is to miss one of the most important lessons which can be learned from TMI-2.

The operator errors in question were largely caused in turn by the man-machine interface of the TMI-2 facility. In fact operator actions were, in the main, a direct consequence of aspects of the operating system including:

- Human engineering characteristics of the control room
- Content of the operator training program
- Content of the emergency procedures.

The most general conclusion reached as a result of this study is that aspects of control room design, training and procedures caused certain operator actions/inactions to take place and that these were then causative factors in the accident sequence.

This general conclusion is supported by several more specific conclusions which are:

- TMI-2 was designed and built without a central concept for man-machine integration.
- Lack of a central man-machine concept resulted in lack of definition of the role of operators during emergency situations.
- In the absence of a detailed analysis of information requirements by operator tasks, some critical parameters were not displayed, some were not immediately available to the operator because of location, and the operators were burdened with unnecessary information.
- The control room panel design at TMI-2 violates a number of human engineering principles resulting in excessive operator motion, workload, error probability, and response time.
- The emergency procedures at TMI-2 were deficient as aids to the operators primarily due to a failure to provide a systematic method of problem diagnosis.
- Operator training failed to provide the operators with the skills necessary to diagnose the incident and take appropriate action.
- Conflicting implications between instrument information, training, and procedures precluded timely diagnosis of and effective response to the incident.

3.6.1 Conclusion 1: TMI-2 was designed and built without a central concept for man-machine integration.

This conclusion is warranted by the results of interviews with the system developers which describe the development process and by evaluation of the development product — the control room itself. In terms of the development process, currently accepted man-machine system design requires at least the following general steps:

- Identification of all system functions
- Allocation of those functions to man or machine
- Definition of operator tasks
- Task analysis in terms of information requirements, decision requirements and action requirements
- Analysis of workstation and manning requirements
- Preliminary design
- Design evaluation using workstation mockups
- Review and revision of designs using evaluation data
- Final design
- Test and evaluation of system capabilities against the original functional requirements.

As documented in Section 3.2, this process was not rigorously followed in the TMI-2 design process. A few facts serve to demonstrate lack of application of accepted system design procedures. Among these are the following:

- No task analysis was performed
- No mockups of the control room design was constructed
- No walk-throughs of operator activities were conducted
- No critical design review was held.

3.6.2 Conclusion 2: Lack of a central man-machine concept resulted in lack of definition of the role of operators during the incident.

The systems approach to man-machine interface development described earlier is intended to define the roles and responsibilities of operators under both nominal and off-nominal circumstances. Operator roles under normal operation are beyond the scope of this report. In regard to the March 28 incident, however, there is little evidence that operator roles during off-normal events was systematically addressed. One distinguishing characteristic which is applied in current system development approaches is the operating role versus the maintenance role. The TMI operator role includes both. A gross separation of these roles can be stated as follows:

- In the operating role, one is concerned with the major output variables of the system being controlled and with the means of controlling them.
- In the maintenance role, one is concerned with diagnosis of system failure and the means of rectifying these.

The operator role in a particular system can also vary in the degree to which judgement and knowledge of the system are required. This aspect varies from the system manager role at one end of the spectrum to the procedure follower at the other.

Analysis of the TMI-2 operator training approach brought forth the assertion that "The operators are supposed to think and to understand the system." This implies that the system manager operator role is the basic concept. This is hard to credit, however, given the control room design, the specific instrumentation, and certain aspects of operator training.

The system manager concept implies the following:

- In the system manager role, the operator constantly monitors a small number of critical system output variables. In the case of a nuclear reactor, these would largely correspond to the variables controlled by the ICS. These would be grouped into a single station. No action would be required as long as the ICS performed acceptably. During any unusual event, the manager role would require that the operator be able to observe the behavior of the critical parameters and command appropriate action when required.
- The manager role implies control of and immediate feedback on resources available to accomplish the assigned task.
- The manager role requires the ability to make decisions concerning system performance, and the commands necessary to obtain it. This generally requires supporting aids for hypothesis testing and evaluation of alternative courses of action.

The TMI-2 man-machine system does not support the above definition of the operator role and yet various investigative efforts have found fault with the on-duty operators for failing to assume this role.

Critical operating parameters are not grouped into a single station but are scattered throughout the control room according to subsystem. At the system manager role level, the subsystem concept is not particularly valuable for organization particularly when it results in separation of critical parameter display. Examples of this problem include:

- Compensated pressurizer level and RCS pressure cannot be read from the secondary station despite the fact that secondary system commands influenced both parameters.
- Steam generator level and pressure cannot be read from panel 5 when the turbine bypass valves are being used to control generator pressure.

In both cases, problems result from segmenting the panels by subsystem rather than functionally. The functional, or cause-effect, relationship between controlled and output parameters constitute the primary information which the operator requires while in the system manager role.

A key deficiency in the area of functional relationships between parameters is the topic of saturation in the primary system. As far as core integrity is concerned, maintenance of RCS pressure above the saturation pressure is the most important function in the plant. No suitable display of this relationship is provided. Operators would have to note RCS pressure and hot leg temperature and enter steam tables to obtain this information. In fact, however, operators were not trained in this procedure and did not appear to regard RCS pressure as being as important as pressurizer level. Stability of RCS pressure (at a value of 1100-1200 psig) was interpreted by operators to imply that they had plant control.

The second aspect of the system manager operator role is the control and monitoring of resources. The major resource available is water. The plant is controlled mainly by transferring water from one place to another. Selected displays of flow rate, container level, pump operation, etc. are provided. These, however, are insufficient for the operators to carry out any systematic procedure of coolant management. Status information on how much water had been pumped from one place to another would have immediately led to a LOCA diagnosis. Instead, operators knew that some water had been transferred from the RCS to the RCDT and the RB sump but did not know how much. They knew that water would enter the RCDT from other sources but did not know how much had in fact entered. These indications are more in the nature of heuristics or "clues" than variables entering into a positive coolant management scheme. In fact, the control room indications are so unenlightening from the coolant management standpoint that CROs frequently find that water has appeared in an unexpected place, as noted by an AO, and are then obliged to trace valve line-ups and check tank levels to find out how the water got there.

Third, the system manager role requires support in the form of decision aids in the evaluation of alternate courses of action. Today this frequently involves the use of computers to organize disparate information and to predict system performance. The performance of the alarm printer and the inadequacies of rapid access to data experienced by the operators show this aid to have been overlooked in planning the system.

A second aid is the emergency procedure. Unfortunately, the emergency procedures tell what you should do after you have identified the cause of the problem. EPs are organized by fault (LOCA, steam line break, etc.). Symptoms are listed for each EP, which is not much help in inferring a fault from known symptoms.

The operators on duty during the incident have reported examining five or six EP's at the same time and attempting to spot some grouping which would account for the observed symptoms.

Operator training also involves simulation of various emergency situations. Simulation capability has recently been expanded to cover the TMI-2 incident. The problem is that this approach requires that every failure be identified previously and practiced by the operator. The same problem exists with respect to the EPs. A separate EP must be written for each contingency.

The conclusion seems warranted that the TMI-2 man-machine integration and design does not support the operator in the system manager role.

When the operator is viewed as filling the maintenance or procedure following role, the design shows greater consistency with the rôle concept. The mantenance role does not require a great deal of panel organization because the maintenance function is operator-paced rather than machine-paced. While pressure may exist to complete the maintenance function as rapidly as possible, the maintenance operator does not have to respond in real time to the operating system's behavior. This real time rapid reaction to operating events is the reason for attention to human engineering principles in panel design. These principles are essential for error-free and timely response in the system manager role while controlling an operating system. Panel organization is less critical in maintenance functions. Lack of a functional panel layout may increase task time but is not likely to result in errors because the task proceeds at the operator's pace.

The organization of the EPs too is consistent with the maintenance role of the operator. This organization proceeds from known problems to confirming symptoms, preventive and corrective steps.

The man-machine integration in the TMI-2 plant is, therefore, consistent only with support of the maintenance/procedure following concept of the operator's role. Despite the assertion on the part of the system developers that the system manager role of the operator is the organizing concept, the training program and the man-machine interface aspects of the CR are inadequate to support the operator in this role. Evaluations of the operators' actions against a standard which assumes that the system manager role should have been carried out will fail to reach a fundamental problem of the TMI-2 system which is man-machine integration. Proposed quick fixes involving an instrument here or an EP there will also fail to address this fundamental problem.

3.6.3 Conclusion 3: In the absence of a detailed analysis of information requirements by operator tasks, some critical parameters were not displayed, some were not immediately available to the operator because of location, and the operators were burdened with unnecessary information.

Information items which were critical to the accident but not displayed in the control room include:

- Total primary system inventory
- RCS pressure and hot leg temperature in relation to saturation valves
- Indication of total flow or flow rate from pressurizer to RCDT
- Emergency feedwater flow rate.

Displays not readily available to the operator due to placement include:

- RCDT parameters which are displayed on panel 8A (see Figure 10)
- Compensated pressurizer level which cannot be seen from the feedwater station but which can be influenced by feedwater controls via primary to secondary heat transfer
- OTSG levels which cannot be read from the turbine control station.

An excellent example of operator overload is furnished by the annunciator system. Annunciators are grouped by subsystem but within annunciator panels there is no apparent separation or coding by priority. There are approximately 750 alarm annunciators in the TMI-2 control room. During the accident, a majority of these were in alarm. This presents a perceptual overload in terms of detecting critical alarms and time/sequence of alarms — particularly in view of the lag and subsequent failure of the alarm printer.

3.6.4 Conclusion 4: The control room panel design at TMI-2 violates a number of human engineering principles resulting in excessive operator motion, workload, error probability and response time.

Examples of human engineering principles which are required for military systems (24) are listed below with characteristics of the TMI-2 control room which violate these principles.

- System status must be indicated by a positive status light. Absence of a light as an indication is unacceptable. The PORV open/close indicator violates this principle and the false close indication was a major factor in the delay in the isolating the PORV.
- Meters which show system parameters should be in close proximity to the control for those parameters. The emergency make-up flow rate

meters are located on panel 8 while the make-up valve controls are on panel 4. The location makes the flow rate difficult to view from the primary station as evidenced by the fact that operators have placed tape strips across the meter faces to indicate 250 gpm.

- Panel layout and position of controls/displays should facilitate selection of proper control by grouping according to frequency of use, function, and criticality. The TMI-2 controls and displays are grouped into panel stations according to subsystems. Within stations, however, the layouts are deficient in organization. Lack of a logical arrangement of feedwater displays resulted in delay in discovering the block valves EF-12A&B to be closed. The operator was obliged to review the line-up twice to determine the reason for lack of feedwater flow.
- Conventions for control/display placement and control operation should be followed consistently. Physical relationships between A loop and B loop controls and displays are not consistent (e.g., A loop components are sometimes located above B loop components, sometimes below, and sometimes beside. The A loop/B loop positioning of the EF-V12A&B valves is opposite to that of the EF-V11A&B valves.) It is thought that this inconsistency contributed to the operator error at 91 minutes when the A loop OTSG boiled dry for the second time.

3.6.5 Conclusion 5: The emergency procedures at TMI-2 were deficient as aids to the operators primarily due to a failure to provide a systematic method of problem diagnosis.

Impact of the EPs on operator actions during the accident is discussed in Section 3.3. The primary deficiency is that the EPs are written in a form which assumes that the cause of the emergency is known. Each EP corresponds to a given problem cause (e.g., loss-of-coolant). Symptoms associated with a LOCA and required operator actions are given. What is not provided is a systematic procedure for diagnosing a problem given the symptoms. The operators reported that they were reviewing four or five EPs attempting to compare symptoms so as to find a failure mode that would account for the observed plant events.

In short, the EPs provide guidance once one knows the accident cause but are of little use in diagnosing the cause from the symptoms.

3.6.6 Conclusion 6: Operator training failed to provide the operators with the skills and knowledges necessary to diagnose the incident and take appropriate action.

Operator actions during the TMI-2 accident were generally consistent with the content of training received.

- Operators were trained to exercise control of make-up flow and let down flow to maintain a pressurizer bubble. Operator concentration on pressurizer level and avoidance of a solid pressurizer was consistent with training.

- Operators were not trained to attend to RCS pressure in relation to saturation conditions. In the accident, given high pressurizer level and low RCS pressure, they attended largely to level.
- Operator skills in the area of hypothesis formation and testing are central to diagnosis of causes of abnormal plant response. Development of these skills would require presentation of "canned problems" via simulator with the operators then practicing a systematic diagnosis procedure. Training exercises of this type were included in the training program but the number and types of such exercises were insufficient.

3.6.7 Conclusion 7: Conflicting implications between instrument information, training, and procedures precluded timely diagnosis of and effective response to the incident.

The major factor in the TMI-2 incident was the failure of the PORV to close, the delay in diagnosing this problem, and the throttling of HPI during the period. While numerous indications existed of a LOCA in general and failed PORV in particular, instrument/training/procedures conflicts were largely the cause of operator actions.

LOCA related symptoms known to the operator included:

- Low RCS pressure
- High PORV discharge temperature relative to code safety valve temperatures
- Ruptured RCDT diaphragm due to filling from the PORV discharge line.

These indications were in conflict with:

- False closed indication of the PORV status light
- High pressurizer level.

LOCA EP procedures state that high RCS pressure and low pressurizer level are symptoms of loss-of-coolant. Given this conflict and training emphasis on avoiding pressurizer level, operators bypassed ESF and reduced make-up flow in an attempt to control level. The alternative would have been to leave HPI on. This would conflict with training and procedures dictating avoidance of solid operation. Operators had also been trained to consider high pressurizer level to be a positive indicator of core coverage.

Filling of the RCDT and rupture of the diaphragm were ambiguous indications to the operators. The flow to the RCDT and the reactor building sump were attributed to the initial opening of the PORV and later considered as symptoms of a OTSG tube leak.

High PORV tailpipe temperatures also appear to have been interpreted as ambiguous. The temperature in question had been running higher than normal and this appears to have masked the implications of the quantitative temperature valve. The difference in temperature between PORV outlet and code safety valve outlet suggested a PORV leak and was, in fact, the cue which eventually led to the correct diagnosis. During the period prior to PORV isolation, however, the temperature differences appear to have been attributed to the fact that the PORV opened but the code safety valves did not.

Statements to the effect that the operator had indications of a leaking PORV and were at fault for not realizing it must be considered in light of the conflicting indications and conflicting implications resulting from emergency procedures and training content.

4.0 HUMAN FACTORS IN THE NUCLEAR POWER INDUSTRY

Recently American (38) and German (74) studies have pinpointed human error as the single most likely causes for nuclear power plant accidents. Other studies (75, 76) estimates that at least 25% of the unplanned outages of power plants (nuclear and fossil) are caused by human error. Clearly then, it can be seen that human error severely compromises the safety and profitability of nuclear power plants. Major gains in both areas could be achieved if the frequency of operator mistakes could be reduced.

Most engineers, administrators and managers involved in the nuclear power industry are quite familiar with human error — it occurs when an operator makes a mistake. The not-so-subtle implication of this definition is that the operator is responsible for the mistakes (since he makes or "creates" it). The mistake is then a function of training, stupidity (selection), fatigue, or perhaps some poltergeist in the head of the guilty operator.

While training, selection, scheduling, etc. contribute to the quality of operator performance; a more complete list of potential causes can be obtained by slightly revising the definition of human error. Human errors occur when the operator's response is unacceptable to the system (i.e., wrong). The key word here is response. The operator is responding incorrectly to something. While the response may be wrong because of poor selection or training, it could be wrong also because the operator could not see an important display (i.e., poor design) or the component nomenclature in his procedures differed from panel labels (i.e., poor procedures).

In general, the first (limited) definition of human error holds the operator responsible for most mistakes and has one pervasive remedy for errors — more, and more effective, training. The operator is expected to learn how to operate control panels regardless of the quality of panel design or procedures. However, when errors occur where poor design or procedures are causal factors, improved or increased training will not of itself resolve the problem.

The limited definition has one rather obvious advantage in that it quickly places the blame for an accident or incident, and by changing operators or by immediate retraining the public and government is supposedly assured that the human error will never occur again.

The second (broad) definition recognizes that "human errors" can be and are frequently caused by the operator's environment (e.g., panel layout and procedures), his experience (e.g., day-to-day operations, training) and personal (e.g., physiological, medical and psychological) factors. Operating under this definition human factors engineering participates in the system design and development process to prevent human error by systematically eliminating identified design, procedural, and selection and training causes for error.

Assuming that some 30 years of intensive research coupled with wide acceptance throughout the military and aerospace communities qualifies human factors engineering as a systems discipline needed for the prevention of human error; and recognizing that human factors engineering as a discipline played no identifiable role in power plants designed in the late 1960's; what steps has the NRC and the nuclear power industry at large taken to include human factors engineering in criteria applicable to more recent plants? This question is addressed in the following section (Control Room Design, Control Room Development, Operator Selection and Training, and Operator Procedures).

In addition to this study, the NRC and the Electrical Power Research Institute (EPRI) have sponsored several studies surveying the human factors engineering of nuclear power plants. These studies are summarized in Section 4.5.

4.1 Control Room Design

In order for a nuclear power plant to be licensed for operation its control room must meet the criteria contained in Title 10 of the Code of Federal Regulations in the Standard Review Plan, and in NRC's Regulatory Guides. In addition, the Regulatory Guides and industry standards (IEEE, ANS) provide design guidelines and standards that supplement mandatory NRC criteria.

When taken together, these regulations, guides and standards include all of the design requirements placed, across-the-board, on all nuclear power plants. If human factors engineering design criteria are currently being used as a means to prevent human error in nuclear power plants, these criteria would be found somewhere in the regulations, guides, and standards. Historically, human factors engineering design criteria have been written in two basic forms: an authoritative source for human engineering criteria (e.g., MIL-STD- 1472B) is referenced; or engineering criteria specifying how to design equipment for human operation, are described. Performance criteria, specifying how well the man-machine system must operate are used at times when minimum acceptable performance levels can be determined early in the design process or when established human factors engineering criteria may be irrelevant because of special design considerations (e.g., operating environments).

4.1.1 10 Code of Federal Regulations (10CFR)

10CFR lists all of the general regulations and design criteria that nuclear power plants must meet to be licensed for operation in the United States of America. For instance:

> Appendix A "General Design Criteria for Nuclear Power Plants," II. Protection by Multiple Fission Product Barriers, page 354.
>
> Criterion 19 — Control room. A control room shall be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss-of-coolant accidents. Adequate radiation protrection shall be provided to permit access and occupancy of the control room under accident conditions without personnel receiving radiation exposures in excess of 5 rem whole body, or its equivalent to any part of the body, for the duration of the accident.
>
> Equipment at appropriate locations outside the contorl room shall be provided (1) with a design capability for prompt hot shutdown of the reactor, including necessary instrumentation and controls to maintain the unit in a safe condition during hot shutdown, and (2) with a potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures.

According to Appendix J, 10CFR has some 26 criteria and regulations that pertain to the design of the control room.

1. None of the regulations or criteria references human factors engineering sources for design criteria or data.

2. All of the regulations are far too general to specify how to design equipment for human operation.

3. Performance criteria do little more than state that the power plant will remain safe under all conditions. While the role of the operator in system safety is implicit in some criteria, no attempt is made to deal directly with man-system design as a source of errors that compromise system safety.

Thus the 10CFR published in 1979 (13) does not provide the guidance, authority, or criteria needed to design control rooms to prevent human error. Operator training, licensing, and the use of licensed operators in the control room are the only human factors engineering issues addressed in the code.

4.1.2 Standard Review Plan (SRP)

In 1975 the NRC consolidated its regulations concerning the planning, design, testing and operation of nuclear power plants into one document to be used by the Commission in reviewing the Safety Analysis Reports prepared by utilities desiring to operate a nuclear power plant.

While the SRP is somewhat out-of-date, it still provides the most comprehensive review of criteria, regulations, and standards applicable to power plant design. As shown in Appendix I, the SRP has some 142 criteria applicable to control room design.

1. None of the criteria or regulations makes reference to human factors engineering sources for design criteria or data.

2. Design criteria aimed at preventing human error are limited to providing the operator with sufficient information, control, and time-to-perform.

3. Few criteria (e.g., SRP-OC-24, Appendix I) recognize the role of design in preventing human error. How the man/system interface is designed is ignored for the most part.

4. Environmental design (SRP-CC-1 through 19, Appendix I) generally ignores lighting, noise, and special garments as potential causes for human error.

5. There is no evidence of a concerted attempt to develop control rooms designed to prevent human error. This fact is well established by the separation of responsibility in reviewing operator functions.

   Section 15.1.5 Spectrum of Steam System Piping Failures Inside and Outside of Containment (PWR), page 15.1.5-2.

   The sequence of events described in the applicant's safety analysis report (SAR) is reviewed by both RSB and EICSB. The RSB reviewer concentrates on the need for the reactor protection system, the engineered safety systems, and operator action to secure and maintain the reactor in a safe condition. The EICSB reviewer concentrates on the instrumentation and controls aspects of the sequence described in the SAR to evaluate whether the reactor and plant protection and safeguards controls and instrumentation systems will function as assumed in the safety analysis with regard to automatic actuation, remote sensing, indication, control and interlocks with auxiliary or shared systems. EICSB also evaluates potential bypass modes and the possibility of manual control by the operator.

   Equivalent Statement:

   Section 15.2.6 Loss of Non-Emergency A-C Power to the Station Auxiliaries, page 15.2.6-1.

Section 15.2.7 Loss of Normal Feedwater Flow, page 15.2.7-1.

Section 15.2.8 Feedwater System Pipe Breaks Inside and Outside Containment (PWR), page 15.2.8-2.

Section 15.3.1 Loss of Forced Reactor Coolant Flow Including Trip of Pump and Flow Controller Malfunctions, page 15.3.1-2.

Section 15.3.3 Reactor Coolant Pump Rotor Seizure and Reactor Coolant Pump Shaft Break, page 15.3.3-2.

Section 15.4.4 Startup of an Inactive Loop or Recirculation Loop at an Incorrect Temperature, and Flow Controller Malfunction Causing an Increase in BWR CORE FLOW RATE, page 15.4.4-2.

Section 15.4.6 Chemical and Volume Control System Malfunction That Results in a Decrease in the Boron Concentration in the Reactor Coolant (PWR), page 15.4.6-1.

Section 15.5.1 Inadvertent Operation of ECCS and Chemical and Volume Control System Malfunction That Increases Reactor Coolant Inventory, page 15.5.1-2.

Section 15.6.1 Inadvertent Opening of a PWR Pressurizer Safety/Relief Valve or a BWR Safety/Relief Valve, page 15.6.1-1.

Section 15.8 Anticipated Transients Without Scram, page 15.8-1.

For all of its impressive size and scope, the SRP provides no effective criteria or guidelines for human engineering design of control rooms.

4.1.3 Industry Standards

Since the beginning of the commerical use of nuclear power, the various industries involved in manufacturing power have been on the leading edge of standardization and criteria development. From a human factors engineering standpoint IEEE 279 "Criteria for Nuclear Power Plant Protection Systems," published in 1969 was the first recognition that control room design could impact operator performance and, therefore, safe plant operations.

Since IEEE 279 several standards relevant to control room human engineering design have been published (Appendix N).

Among the more prominant are:

- "Design Basis Criteria for Safety Systems in Nuclear Power Generating Station," ANSI/ANS-4.1, 1978.
- "Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants," ANS 51.1, 1973.
- "IEEE Recommended Practice for the Design of Display and Control Facilities for Central CR's of Nuclear Power Power Plant Generating Stations," IEEE STD-566, 1977.

- Proposed American National Standard "Criteria for Safety-Related Operator Actions," ANSI N660/ANS-51.4, 1977.
- IEEE Trial-Use Standard "Criteria for Safety Systems for Nuclear Power Generating Stations," IEEE STD 603, 1977. This contains many of the standards found in IEEE 279.

Of these industry standards, IEEE STD-566 is the only one to deal exclusively with control room human engineering issues; therefore, IEEE STD-566 is reviewed separately in paragraph 4.1.4 below.

Several of the other standards are worthy of review.

a. ANS 51.1, 1973, Design Criteria, page 9

> 5.3.4.4 The data displayed and controls located in the control room shall be adequate:
>
> (1) to regulate the process variables within their normal limits
>
> (2) to cope with malfunctions or accidents
>
> (3) to assess accidents and perform necessary actions for recovery.

On the surface, this standard appears quite powerful, however, two problems leave it basically impotent. First, the term "adequate" could never be accurately defined. Second, there is no prescribed means to judge adequacy. Is it determined by the control room designer based on his experience, or through simulations using operators and realistic procedures, etc.?

b. IEEE 497, 1977, 5. General Requirements, page 8

> 5.3.2 Location and Identification. Post accident monitoring displays shall be located accessible tothe operator during the post accident period and shall be distinguishable from other displays. Post accident monitoring displays which enable the operator to determine when conditions exist that require specified manual actions, or monitoring the results of those actions, shall be located in the vicinity of the control stations used to effect the actions.

This standard has several weaknesses. First, there is no reference point for "accessible." Does it mean accessible when the operator is three feet from the display or perhaps 10 feet from the display? Second, "distinguishable" seems like an acceptable criteria; however, distinguishable only means that two displays are noticably different is some way. Several identical displays can be arranged in a matrix and each will be distinguishable from the other by its position in the matrix. However, there is likely to be significant confusion in identifying displays in the middle of the matrix. Distinguishability is not a sufficient criteria to prevent human error.

c. ANS 51.4, 1977, 7.0 Information Availability, page 14

> 7.1 The operator shall be provided with clearly presented readout information, at the required time for him to assess the need for a particular protective action without significant diagnoses.

The obvious question is, would any designer intentionally provide the operator with an unclearly presented readout?

d. ANS 51.4, 1977, 7.0 Information Availability, page 15

> 7.5 Readout information shall be provided which indicates that each action controlled by an operator manipulation has been correctly initiated.

Is there no readout when it has been initiated incorrectly? Are there no constraints on the location of feedback displays?

1. The vast majority of control room design standards specify the information to be displayed and control to be maintained from the control room.

2. None of the industry standards reviewed contained definitive, quantitative human engineering design criteria; however, some standards obviously recognized the role of design in operator performance.

3. There seems to be a movement within the nuclear power industry to consolidate human engineering criteria and standards. Unfortunately, IEE STD-566 notwithstanding, this movement has failed to realize that prevention of human error is absolutely essential to the power industry and that ambiguous, qualitative standards are categorically unacceptable for control room design.

4.1.4 Review of IEEE Standard 566-1977

IEEE 566 is an IEEE Recommended Practice containing eleven (11) pages devoted to providing "uniform guidelines for the functional selection, coordination and organization of control and information systems in a nuclear power plant central control room." According to its Scope:

> This document establishes guidelines to be used by power plant system designers in selecting information and control devices to be made available in the central control room, and in determining how and where they shall be made available so that they can most reliably and quickly be used by the operator. The guide addresses the functional requirements of the information systems, controls, and displays, but not the selection of specific devices or equipment. It does not apply to the physical design of the control room enclosure or structures mounted therein.

The primary recommendations are contained in Section 5, 6 and 7 entitled, Design Bases, Usage Analysis and Functional "Considerations" respectively.

Design Bases — Rather than suggesting design bases for control rooms, 566 provides a list and description of the design bases that should be established prior to design. This is quite appropriate for some bases (e.g., number of operators, functional arrangement of the control room, etc.) which are specific to a given plant; however, other more general bases could and should be specified. For instance operator anthropometric bases should be generally the same between plants. One of the bases in 566 will be quite difficult for the control room designer to specify, that is the "limiting number of display devices which can be active at the same time. . .to avoid operator sensory saturation." 566 provides no guidance on how to determine this limiting number.

From a human factors engineering standpoint several bases are missing from the 566 list. These include:

a) A set of operator procedures (albeit draft).

b) A complete analysis of the tasks operators must perform, including steps to be taken, time limits, types of instrument interfaces, etc.

c) The human engineering standards (e.g., MIL-STD-1472B) to be employed.

d) Failure Modes and Effects Analyses/Fault Trees relevant to operator errors.

Usage Analysis — The "Usage Analysis" is a means to systematically document judgments and facts concerning how often and under what circumstances particular control panel components and systems will be used. Then, based on these judgments and facts, the Usage Analysis permits the designer to assign components and systems to various sections of the control room.

This analysis is most likely to work for a very gross grouping of controls and displays. Such grouping could be made without the "Usage Analysis" but the worksheets for this analysis document the logic as assignment decisions.

Functional Considerations — In Section 7, Functional "Considerations" take the place of what would be usually called standards. The 21 "Considerations" occupy about 1½ pages. A review of the human errors involved in the TMI-2 accident found it unlikely that any of the errors would have been prevented, if the 566 "Considerations" were available during the late 1960's.

The 566 "Considerations" are often ambiguous, very general and in some cases, questionable technically (see Table 6 entitled "Review of Some Functional Considerations from IEEE-STD-566," below). Furthermore, they overlook a whole host of human engineering criteria important to preventing operator error, including:

1) A criterion suggesting that status indicators (e.g., valve position indicators) give positive, rather than derived, indication of status.
2) Control/Display layout conventions.
3) Label placement and sizing conventions.
4) Alarm placement rules, etc.

Generalizations and ambiguities and oversights such as these make it hard to see how the contents of 566, if implemented, would help prevent operator error. Since most of the 566 Functional "Considerations" should be known, and to some extent practiced already by most control panel designers, it seems that the purpose of this document is to admonish the designer to consider the operator. Unfortunately 566 provides little guidance on just how to prevent operator error.

4.1.5 NRC Regulatory Guides

Many of the design standards promulgated by nuclear industry associations have been reviewed and modified, where necessary, and published by the NRC as Regulatory Guides. While "Reg. Guides" sometimes contain design criteria (regulations) they more frequently contain design guidelines, acceptable means to meet design criteria, and interpretations of criteria (Appendix K).

As was the case with standards, the number of operator-oriented design criteria and guidelines included in Reg. Guides has been on the increase since the mid-1970's. For instance:

1. RG 1.114 Guidance on Being Operator at the Controls of a Nuclear Power Plant, Revision 1, November 1976, page 1.

   1. The operator at the controls of a nuclear power plant should have an unobstructed view of and access to the operational control panels, including instrumentation displays and alarms, in order to be able to initiate prompt corrective action, when necessary, on receipt of any indication (instrument movement or alarm) of a changing condition.

2. RG 1.97 Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant Conditions During and Following an Accident, Revision 1, August 1977, page 4.

   17. The instrumentation should be designed to facilitate the recognition, location, replacement, repair, or adjustment of malfunctioning components or modules.

TABLE 6

REVIEW OF SOME FUNCTIONAL "CONSIDERATIONS"

FROM IEEE-STD-566

	Functional "Considerations"	Comment
1.	"7.2 Display Facilities. In support of the operator needs, the control room designer should arrange the display facilities so that the operator can readily observe the displays and analyze the status of any system."	"Readily" is very difficult to define, some possible meanings might include: a. Observable from any place within the control room without need for walking to the vacinity of the displays, b. Observable from in front of the panel containing the display, b. Observable from workstations where the operator will use the information from the display.
2.	"7.6.2 Redundant and Diverse Information. Where a number of critical parameters require redundant or diverse displays as a means of checking the reasonability of information, the alternative information sources should be located to allow the operator to use both sources in arriving at a conclusion."	Does this suggest that two redundant displays be placed: a. Within the foveal area of an operator at some optimum distance? b. At some maximum distance apart? c. Within the field-of-view of some stationary operator at some optimum distance? d. So that the operator can walk from one display to the other to check values? e. So that one operator can ask another to read a distant display and then check the "reasonability of information."

3. "7.8 Device Arrangement. Individual devices or groups of individual devices should be arranged to minimize operator motion including changes in direction of vision."

This consideration has several flaws, including:

   a. "Minimum" may be impossible to define since different procedures will often require different switch operation and display reading sequences.

   b. "Minimum" could lead to control/display crowding which can lead to inadvertant actuation and problems in display identification from a distance.

   c. Within wide limits, distance moved is not nearly as important to operator error as direction and changes in direction of motion.

4. "7.9 Equipment or System Status. Consideration should be given to provide indication when non-safety-related equipment is taken out of service for maintenance, calibration, or inspection, and when it is returned to service."

It would be helpful if this consideration provided some criteria concerning when or under what circumstances indications should be provided.

3. RG 1.97 Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant Conditions During and Following an Accident, Revision 1, August 1977, page 3.

   10. The accident-monitoring instrumentation should be specifically identified on control panels so that the operator can easily discern that they are intended for use under accident conditions.

4. RG 1.97 Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant Conditions During and Following an Accident, Revision 1, August 1977, page 4.

   16. The accident-monitoring instrumentation design should minimize the development of conditions that would cause meters, annunciators, recorders, alarms, etc., to give anomalous indications confusing to the operator.

While these guidelines demonstrate an ever increasing concern for the needs of the operator, none provides any information on how these needs are to be met (i.e., how to design the control room). As is often the case in nuclear criteria, ambiguous phrases like "easily discern," "indications confusing to the operator," "initiate prompt corrective action," "facilitate recognition" are used in place of definitive, quantitative criteria.

Guidelines such as these have two notable shortcomings: first, their interpretations are unbounded; second, the designer who makes and applies his own interpretation is lulled into believing that he has "human engineered" the control panel. It is questionable whether these guidelines, if applied as they stand, would result in any reduction in human error potential.

1. The Reg. Guides published since the mid-1970's show increasing concern for human factors engineering design issues.

2. None of the Reg. Guides makes reference to human factors engineering sources for design criteria, engineering solutions or performance data.

3. While some ambiguous guidelines are included, no Reg. Guides contain definitive, quantitative human factors engineering guidelines or criteria.

4. The Reg. Guides reflect no coordinated NRC effort to prevent human error in nuclear power plant operations.

4.2 Control Room Development

Well human engineered control panels are a result of an active human engineering program throughout all phases of system development.

1. System Planning
    - Participate in Early Cost/Benefit Trade-Offs
    - Man-Machine Function Allocation
    - Identification and Analysis of Personnel Function/Tasks
2. Design
    - Workplace Layout and Equipment Design
    - Design for Maintenance
    - Job Aids (Procedures)
    - Design of the Work Environment
    - Job Design and Manning
    - Design of Training Programs and Devices
    - Personnel Selection and Classification Program
3. Testing
    - Man-System Interface Verification
    - Identification of Alterations/Backfits
    - Development of Performance Expectancy Measures (time to complete tasks; error rates; etc.)
4. Operations
    - Performance Monitoring (Operator-System)
    - Investigations into Outages and Incidents
    - Recommendations for Backfits
    - Personnel Evaluation.

The NRC Standard Review Plan, 10CFR, Industry Standards, and NRC Regulatory Guides were examined to determine the degree to which designers, utilities, and NSSS vendors are required to implement human engineering during nuclear power plant system development.

1. Human engineering by name and by intent is showing up with increasing frequency in NRC and nuclear industry Control Room Development criteria. For instance:

    - The SRP includes:

      Section 13.1.1 Management and Technical Support Organization, page 13.1.1-2.

      2. Preoperational Responsibilities
         These are functions which should be substantially accomplished before preoperational testing begins and generally before submittal of the final safety analysis report (FSAR).

a. Development of human engineering design objectives and design phase review of proposed control layouts.

- IEEE STD-338

  4. Basis, page 8.

  Interrelationship among the systems, components, and human factors in each phase of the test activity shall be considered and reflected in the system design and layout.

The intent of human engineering (to prevent human error) is frequently found in testing criteria for procedures and equipment.

- RG 1.101 Emergency Planning for Nuclear Power Plants, Revision 1, March 1977, page 10.

  This section should describe provision for the conduct of periodic drills and exercises to test the adequacy of timing and content of implementing procedures and methods, to test emergency equipment, and to ensure that emergency organization personnel are familiar with their duties. Preplanned descriptions or simulations of accidents or similar events should be used to prepare scenarios appropriate to the objective of each drill or exercise.

- 10CFR

  Appendix A, "General Design Criteria for Nuclear Power Plants," IV. Fluid Systems, page 356.

  Criterion 37 — Testing of emergency core cooling system. The emergency core cooling system shall be designed to permit appropriate periodic pressure and functional testing to assure (1) the structural and leaktight integrity of its components, (2) the operability and performance of the active components of the system, and (3) the operability of the system as a whole and, under conditions as close to design as practical, the performance of the full operational sequence that brings the system into operation, including operation of applicable portions of the protection system, the transfer between normal and emergency power sources, and the operation of the associated cooling water system.

Operational phase human engineering criteria include reporting on human error as a cause for accidents.

RG 1.16 Reporting of Operating Information — Appendix A Technical Specifications, Revision 4, August 1975, page 3-4.

Information provided on the licensee event report form should be supplemented, as needed, by additional narrative material to provide complete explanation of the circumstances surrounding the event.

(6) Personnel error or procedural inadequacy which prevents or could prevent, by itself, the fulfillment of the functional requirements of systems required to cope with accidents analyzed in the SAR. The following are examples:

(a) Failure to restore a safety system to operability following test or maintenance.

(b) Improper procedure leading to incorrect valve lineup which resulted in closure of one manual valve in each of two redundant safety injection subsystems and would have prevented injection on demand.

2. While there is no coherent approach to human engineering in Control Room Development, some elements of such a program are peppered among the SRP, 10CFR, Reg. Guides, and industrial criteria.

4.3 Operator Selection and Training

Standards and guides currently exist providing the nuclear power industry with guidelines in the selection and training of control room operators which were not extant during the planning phases of the TMI-2 staffing and training program. Adjustments to selection policy or training program approach are more easily facilitated and less costly than changes which would involve redesign of hardware or control room layout. Based on an analysis of Met. Ed.'s current selection criteria and training program description it appears that the Met. Ed. training staff has updated their training program, incorporating the requirements and guidelines as they were developed by industry and regulating bodies (Appendices F and G). Criteria for selection and training which currently exist are fairly comprehensive and offer a basis for program development and implementation with only minor inadequacies.

Selection Criteria — Selection Criteria are stipulated in a number of sources available to industry. Among them are 10CFR-Energy; ANS 3.4/ANSI N546 Medical Certification and Monitoring of Personnel Requiring Operator Licenses for Nuclear Power Plants; ANS 3.1, American National Standard for Selection and Training of Nuclear Power Plant Personnel; Regulatory Guide 1.8 Personnel Selection and Training, and Proposed Revision 2; and Regulatory Guide 1.134. ANS 3.1 American National Standard for Selection and Training of Nuclear Power Plant Personnel stipulates general requirements for the selection of Nuclear Power Plant Control Room operators (Section 4, page 5):

> . . .operators to be licensed by the NRC shall have a high school diploma or equivalent, two years of power plant experience and should possess a high degree of manual dexterity and mature judgment.

There exists some ambiguity about the "equivalent" of a high school diploma and its particular relevance. Some utilities, including Met. Ed., administer written selection tests, though there is little evidence that these tests have been validated as predictors of trainability or job performance, or that they are indeed utilized as tools for selection. The industry should undertake, individually or as a whole, an analysis of the requirements of the job of nuclear power plant control room operator and determine valid, relevant and effective predictors of successful trainability and ensuing job performance.

Health requirements and disqualifying conditions are listed in ANS 3.4 (Section 5, page 4) in addition to being stated more generally in other documents, such as 10CFR-Energy, ANS 3.1 and Regulatory Guide 1.134. Some of the requirements are stated in clear concise language, i.e., in ANS 3.4 (Section 5, page 4), the requirement for eyes is:

1. "Near and distant visual acuity 20/40 in better eye, corrected or uncorrected.

2. Peripheral visual fields by confrontation to 120° or greater.

3. Color vision adequate to distinguish among red, green and orange-yellow signal lamps, and any other coding required for safe operation of the particular facility as defined by the facility operator.

4. Adequate depth perception, either by stereopsis or secondary cues as demonstrated by practical test."

In other cases, the language used is somewhat ambiguous, and, therefore, difficult to put into practice. For example, requirement for a "high degree of manual dexterity" could be interpreted to mean the passing of a standardized test of manual dexterity or simply a degree of dexterity and coordination perceived during a personal interview. "Mature judgment," also a stipulated requirement for control room operation, is a broad general construct very difficult to measure. Other documents, such as Regulatory Guide 1.134, stipulate very general requirements that "physical condition and general health. . .are not such as might cause operational errors endangering public health and safety." (Reg. Guide 1.134, Section A, page 1)

The major inadequacy of the existing criteria and standards dealing with nuclear power plant personnel selection is a lack of specificity which can best be solved when specific requirements and demands of the control room operators job are more fully understood.

Training Criteria — Criteria and guides for the training of nuclear power plant personnel have been developed by industry and the NRC. In 10CFR-Energy (Part 55) are listed those aspects of nuclear power plant reactor operation on which operators will be tested in the license application process. ANS 3.1 (Section 5, pages 7-8) lists general categories which are required in cold or hot license training, including: principles of reactor operation; design features of the nuclear power plant; instrument action and control systems; etc. There is a heavy emphasis in 10CFR-Energy (Part 55) on operator requalification training, reflecting the importance of maintaining the proficiency of operations personnel. ANS 3.1 American National Standard for Selection and Training of Nuclear Power Plant Personnel, describes requirements for providing review of procedures, training in facility or procedural change and the participation by each licensed operator in specific control manipulations, in addition to an annual written requalification examination. The requirements for simulators to be used in the training of nuclear power plant personnel are presented most fully in ANS 3.5 Nuclear Power Plant Simulators for Use in Operator Training. Plant evolution which must be among the capabilities of each simulator are stipulated (Section 3.1, page 2), including normal as well as abnormal plant functions. If a simulator is to be used in requalification training to provide experience in specific control manipulators, 10CFR-Energy (Part 55, page 416) requires that that simulator:

> shall accurately reproduce the operating characteristics of the facility involved and the arrangement of the instrumentation and controls of the simulator shall closely parallel that of the facility involved.

To determine effectivness of the transfer of training, indeed to rule out negative transfer, using a plant-specific vs a similar control room configuration, an in-depth study needs to be conducted.

The Standard Review Plan requires that the Final Safety Analysis Report include a description of the means for evaluating the effectiveness of the training for each trainee. This is carried out by examining the test scores, licensing exam scores and on-the-job performance of each operator. A recommended practice of Regulatory Guide 1.101 Emergency Planning for Nuclear Power Plants suggests that emergency response training be evaluated for program effectiveness (Paragraph 2.3.4, page 1.101-14). This kind of program evaluation should be conducted of all training programs on a continuing basis. Trainee scores and job performance can be collected, analyzed, and compared to determine areas of strength and weakness in each utilities training program.

A complete job analysis should be undertaken by the industry as a whole to identify components of the control room operator's job. At that point, standards, guides and criteria which currently exist can be validated, more specific guidelines developed and therefore, more support given to the utility in the process of developing and implementing its nuclear power plant personnel training programs.

4.4 Operator Procedures

Even the best designed control rooms produce unacceptable levels of human error when operator procedures are not suited to the tasks. Poorly organized procedures can cause delays in accession; poorly formatted procedures can cause the operator to lose his place and skip steps.

Human engineering standards for procedures must include:

1. Document Fidelity
    - Completeness
    - Correspondence of procedures to actual tasks
    - Correspondence of procedural nomenclature to actual nomenclature
    - Provisions for informing operator or display changes resulting from correct operations, etc.
2. Accessibility
    - Document indexing and table of contents organization
    - Information organization
    - Correspondence of information available to operator for accession, to accession information requirements, etc.
3. Legibility and Readability
    - Size, spacing, font of letters
    - Use of special emphasis markings
    - Page layout
    - Sentence, complexity, and length
    - Level of language
    - Letter/background contrast
    - Design of charts, figures, tables, etc.
4. Usability
    - Provisions for checklisting
    - Level of proceduralization

- Memory (short and long term) requirements
- Physical handling of procedures documents, etc.

The NRC Standard Review Plan, 10CFR, Industry Standards, and NRC Regulatory Guides were examined to locate criteria for Operator Procedures.

1. The criteria and guidelines for operator procedures paralleled those for "Control Room Design." The emphasis was on the contents of procedures, with virtually no attention to their design. While information completeness was covered and some attention was given to information organization, operator responsibility, task/procedure correspondence, and document maintenance, the other Fidelity considerations as well as Accessibility, Legibility and Readability, and Usability were almost completely ignored.
2. None of the standards or guidelines suggested or required the use of human engineering criteria or data in the preparation of procedures.
3. The most recent SRP, 10CFR, Regulatory Guides and Nuclear Industrial Standards, taken together, do not provide the criteria necessary to prepare procedures that will minimize the probability of human error.
4. There appears to be little, if any, concern over procedures as a potential cause of human error.

4.5 Adequacy of the Application of Human Factors Engineering Technology in Nuclear Power Plants

The purpose of this section is to review some major issues that pertain to the adequacy of human factors engineering in the nuclear power plant industry. Since this report is investigatory in nature, it may appear to be negative. This report is only concerned with problem areas, therefore, areas with adequate or excellent human factors engineering are not mentioned; except in passing here to say that the efforts of Westinghouse, General Electric (Nuclenet) and some others utilizing computers and advanced display and control technologies, are to be commended for recognizing the role of the operator in the control room design process. Without passing too quickly, however, it should be noted that standardization of symbology and software should be undertaken immediately, otherwise a profileration will result just as it did in the aerospace and aviation industry a few years ago.

A recent synopsis of human factors and the power industry by Seminara (35) reveals that actually a considerable amount of attention has been devoted to the subject since the 1960's. In the early 1970's the WASH-1400 Reactor Safety Study (38) was initiated which contains considerable information regarding control room design, as well as discussion of human error. In Appendix III (p. III-59 ff) of WASH-1400, an attempt was made to calculate the probability of human error in the control room, taking into account varying degrees of (poor) human factors engineering, e.g., the likelihood of poorly placed switches resulting in confusion and error.

The Electric Power Research Institute (EPRI), in the mid-1970's recognized the need for investigation of human factors aspects of control rooms and initiated a research program in the human factors area. A Lockheed Missile and Space Company, Inc., Human Factors Team (J.L. Seminara, W. Gonzalez and S.O. Parsons) was contracted to review five operational control rooms and corresponding simulators. The results of this study (45) present a rather bleak picture of nuclear power human factors engineering when compared to aerospace and military industries.

The Nuclear Regulatory Commission (NRC), meanwhile contracted with the Aerospace Corporation (F.C. Finlayson, T.A. Hussman, K.R. Smith, R.L. Crolius and W.W. Willis) to study human factors engineering of nuclear power plant control rooms and the effects on operator performance. As a result of this study, it was concluded (46) that operator characteristics, job performance guides and control room and system design influence operator performance.

The issue of human error has received a great deal of attention. Sandia Labs, particularly Alan Swain, has published well over 50 reports on human error and reliability since the early '60's. At least five of these reports, including Section 6.1 of Appendix III of WASH-1400 (38), are directly concerned with nuclear power operations. Swain (36) assessed human reliability in nuclear reactor plants and Swain and Guttman (37) discussed the application of human reliability to nuclear power. Later, Swain (39) did a preliminary human factors analysis of the Zion nuclear power plant and identified human factors engineering design, training and written instruction shortcomings. Merren, Esterling and Swain (40) investigated the uses of reliability techniques in evaluation of nuclear power plants.

Human error in control room operation is a complex issue because, aside from the fact that it is difficult to measure, it is difficult to differentiate between human and design error. In the Babcock and Wilcox explanation of the TMI-2 accident (47), it is pointed out, for example, that the operators failed to recognize the open PORV for two and one-half hours and that the blocked feedwater valves were not recognized for eight minutes. What is not pointed out is that the operator did have an indication that the PORV was closed (although there was other evidence that it was open) and that a tag hung above one of the emergency feedwater valve indications obscured it from the operator's sight.

Seminara, et al., (45) used the critical incident technique in an attempt to discover the role of human error in nuclear power plant operations. The results of that study reveal only one incident where human error was attributed directly to training. That was a case where the operator wondered what would happen if he pushed a pushbutton. (One wonders, even in that case, whether the pushbutton was properly labeled.) On the other hand, Adams et al., (1979), by analysis of Licensee Event Reports (LER) to determine operator error in nuclear power plants, found that 30 percent of the errors were attributable to the operator. In any event, Finlayson, et al., (46) noted that although the incidence of human error in nuclear power plant operations is low, the number of potential control room operator related incidents is not trivial as control rooms become larger and more complex.

One of the major issues that needs to be raised is the lack of good human factors engineering guidelines for control room design. Adams et al., (1979) makes the point that, because of complexities, operation of the nuclear power plant entails monitoring and control tasks that require an integrated team of highly trained individuals who can perform complex tasks involving multiple inputs of information and analytical decision making in a disciplined manner, however, most control rooms reflect design concepts evolved, not from the system requirements, but from traditional fossil-fuel or water power plant control room. The authors believe that this blend of old design concepts with new requirements has resulted in many human factors engineering deficiencies.

The need for a human factors engineering design guide for control room design was raised by Finlayson et al., (46) and reemphasized by Seminara, et al., (35) who concluded that there is not only an urgent need for a human factors engineering design guide, tailored to the special demands of the utility industry, but also for a human factors engineering standard to be used for specifying, developing and evaluating new control designs. It was also noted that human factors engineering principles developed by military and space programs to ensure operator effectiveness and reliability have not generally been applied to the design of power plant workstations.

The results of the present study reveal workstations with displays incorrectly located, inadequate color coding, confusing annunciator components, anthropometric, visual scan and walking requirements which do not conform with operator capabilities and labeling inconsistencies, which could all have been prevented, or at least alleviated, by adequate regulations and standards. It is, therfore, recommended that NRC and the utilities initiate actions to publish and enforce human factors engineering regulations and standards. Adaptation and tailoring of DOD and NASA documents would probably be the best way to begin.

Human factors engineering aspects of maintenance, along with training, is an area that is frequently overlooked in long-range planning, even in industries such as aerospace, that normally do consider human factors engineering in the design process. In his appearance before the Presidents Commission (1979), Elliott (47) indicated that utilities have too few maintenance personnel and while he does not address maintenance specifically, he does recommend increased training for the Nuclear Power Generating Division in order to provide systems orientation so that personnel in narrow areas of specialization have an overview of how and where they fit in, especially in emergency situations. In his appearance, Rickover (17) maintains that a major factor in the successful safety record of Navy nuclear vessels is the disciplined approach to maintenance.

Seminara, et al., (35) has documented a magnitude of problems, with photographic evidence, in the area of power plant maintenance and confirms the above impressions that inadequate maintenance has resulted in underestimations of maintenance manning requirements, much more so for nuclear than for fossil-fuel operations.

The U.S. Air Force has recognized that difficulties in properly emphasizing human resources and logistics factors in system development has created both operational problems and less than desired efficiency in training and in maintenance expenditures. Therefore, the Air Force has developed a design morphology for fault detection and dispatch activities of maintenance control in the operations control center of a prototype MX system (Ostrofsky, et al., 1979). Although the mission of a nuclear power plant and a missile are vastly different, the roles and functions of the control room operator, auxiliary operator and maintenance personnel have counterparts in missile systems. The type of approach to long range maintenance and operation planning for advanced missile systems may well lend itself to advanced nuclear technological systems.

By comparison with the nuclear power industry, the application of human factors engineering technology to design and development of complex man-machine systems in the weapon system and aerospace industries seems excellent. The factors that have led DOD and NASA to develop better systems from a human factors engineering (human factors engineering point of view include the following:

- Human Factors Engineering Standards and Specifications: MIL-H-46855B (25) states the unequivocal requirement for human factors engineering in Section 3.1.1 where it states:

  Human engineering shall be applied during development and acquisition of military systems, equipment and facilities to achieve the effective integration of personnel into the design of the system. A human engineering effort shall be provided to develop or improve the crew-equipment/software interface and to achieve required effectiveness of human performance during system operation/maintenance/control and to make economical demands upon personnel resources, skills, training and costs. The human engineering effort shall include, but not necessarily be limited to, active participation in the three major interrelated areas of system development: analysis, design and development, and test and evaluation.

  MIL-STD-1472B (24) establishes general human factors engineering criteria for design and development of military systems, equipment and facilities. Its stated purpose is to present human factors engineering design criteria, principles and practices to be applied in the design of systems, equipment and facilities so as to:
  - achieve required performance by operator, control and maintenance personnel
  - minimize skill and personnel requirements and training time
  - achieve required reliability of personnel-equipment combinations
  - foster design standardization within and among systems.

- Human Factors Engineering Design Process: Requirements for application of human factors engineering methods and criteria at each step of the system development process is addressed by MIL-H-46855B and is described in detail by Baker, *et al.*, (1978) (70) for weapon systems and Malone, *et al.*, (1979) for ship. Within DOD there are agreed upon human factors engineering activities and events required at each stage of the system acquisition process. The application of the human factors engineering design process ensures integration of the human element with system hardware, software, environments, and information.

- Human Factors Engineering Design Criteria: Each military service and NASA have compiled handbooks of human factors engineering design criteria comparable to the tri-service 1972 Guide to Equipment Design (28).

- Use of Simulation: The military services, particularly those involved with aviation systems, as well as NASA, have relied heavily on man-in-the-loop simulation to develop design concepts, compare attributes of competing concepts, and to validat the effective design of selected concepts. Use of such simulation ensures that operator and maintainer requirements and capabilities are considered prior to the actual fabrication of system hardware.

- Human Factors Engineering Test and Evaluation: The area where human factors engineering has had its major impact on military systems is in human factors engineering test and evaluation. The U.S. Army Test and Evaluation Command has implemented a Test Operating Procedure (TOP) for human factors engineering which must be applied to all systems and equipment procured by the Army. This TOP (26) contains guidance on human factors engineering test and evaluation methods and includes test and evaluation measures and criteria in the Human Engineering Data Guide for Evaluation (HEDGE). A comparable approach has been taken by the Navy in the Human Factors Test and Evaluation Manual (HFTEMAN) (73). With DOD directives requiring test and evaluation to be applied throughout the development of a system, from its earliest stages forward, and with the strong influence of human factors engineering in the test and evaluation process, it is guaranteed that human factors engineering will be addressed from the earliest phases of system acquisition.

The central and focal factor in the application of human factors engineering principles, methods and data to aerospace and weapon systems is the concern for the human component during system development. Without this orientation the integration of man with hardware and software will be incomplete at best. The key principle that the nuclear industry can learn form the military-aerospace industry regarding human factors engineering is simply that people will perform more effectively in the operation of systems when they have been considered in the development of such systems. Human factors engineering need not always receive highest priority in system trade-offs, but it does need to be considered in the trade-offs. The military services and NASA have recognized this fact and are therefore fielding systems which far excel Three Mile Island 2 in terms of operability, maintainability and safety.

LIST OF ACRONYMS

LIST OF ACRONYMS

AB	Auxiliary Building
A-E	Architect-Engineer
AO	Auxiliary Operator
B-O-P	Balance-of-Plant
B&R	Burns and Roe
B&W	Babcock and Wilcox
BWST	Borated Water Storage Tank
CFR	Code of Federal Regulations
CO	Condensate (Pump, Valve, Etc.)
CR	Control Room
CRO	Control Room Operator
CRT	Cathode Ray Tube
CW	Circulating Water
DB	Design Bases
DH	Decay Heat
ECCS	Emergency Core Cooling System
EF	Emergency Feed Water (valve)
EFW	Emergency Feed Water
EMOV	Electromatic Relief Valve
EP	Emergency Procedure
EPRI	Electric Power Research Institute
ES	Emergency System
ESF	Engineered Safety Feature
FSAR	Final Safety Analysis Report

FW	Feed Water
GPM	Gallons-Per-Minute
GPU	General Public Utilities
HE	Human Engineering
HF	Human Factors
HFE	Human Factors Engineering
HPI	High Pressure Injection
HV&AC	High Voltage, Alternating Current
IC	Intermediate Cooling
I&E	Inspection and Enforcement
IEEE	Institute, Electrical and Electronic Engineering
JCPL	Jersey Central Power and Light Company
JPA	Job-Performance-Aid
LOCA	Loss-of-Coolant Accident
MET ED	Metropolitan Edison
MS	Main Steam
MU	Make-Up (Pump, Valve, Etc.)
NI	Nuclear Instrumentation
NPSH	Net Positive Suction Head
NRC	Nuclear Regulatory Commission
NSSS	Nuclear Steam Supply System
OC-2	Oyster Creek, Unit Two
OJT	On-the-Job Training
OTSG	Once-Through Steam Generator
P	Pump
PORV	Power Operated Relief Valve

PSAR	Preliminary Safety Analysis Report
psi	Pounds-Per-Square Inch
psig	Pounds-Per-Square Inch, Gauge
PZR	Pressurizer
RAD	Radiation
RB	Reactor Building
RC	Reactor Coolant
RCDT	Reactor Coolant Drain Tank
RCS	Reactor Coolant System
RM	Reactor Monitor
RTM	Reactor Technology Memoranda
SBM	J-Handle Switch Used Throughout Nuclear Industry
SI	Safety Injection
SF	Shift Foreman
SRO	Senior Reactor Operator
SRP	Standard Review Plan
SS	Shift Supervisor
Tave	Temperature, Average
T&E	Test and Evaluation
Th	Temperature, Hot
TMI	Three Mile Island
TMI-1	Three Mile Island, Unit One
TMI-2	Three Mile Island, Unit Two
TOP	Test Operating Procedure
V	Valve

REFERENCES

REFERENCES

1 Three Mile Island Special Inquiry Deposition of: Salvatore Charles Gottilla, September 17, 1979

2 Three Mile Island Special Inquiry Deposition of: Edward J. Gahan, September 26, 1979

3 Unpublished Essex Personnel Interview of Duke Power Co. Personnel, September 18, 1979

4 Unpublished Essex Personnel Interview of Combustion Engineering Corporation Personnel, Windsor, Conn., September 14, 1979

5 Unpublished Essex Personnel Interview of Bechtel Corporation Personnel, Gaithersburg, Md., September 25, 1979

6 Unpublished Essex Personnel Interview of Baltimore Gas and Electric Company, Baltimore, Md., September 28, 1979

7 Unpublished Essex Personnel Interview of General Public Utilities Corporation Personnel, September 6, 1979

8 Final Safety Analysis Report for the Three Mile Island Nuclear Station - Unit 2, Volumes 1-13, by Metropolitan Edison Company, Jersey Central Power and Light Company, and Pennsylvania Electric Company, 1974

9 Final Safety Analysis Report for the Oconee Nuclear Power Plant - Units 1-3, Duke Power Co.

10 Final Safety Analysis Report for the Calvert Cliffs Nuclear Power Plant Units 1 and 2, Volumes 1-3, by Baltimore Gas and Electric Company, January 1971

11 Preliminary Safety Analysis Report for the Three Mile Island Nuclear Station - Unit 2, Volumes 1-4, by Metropolitan Edison Company, and Jersey Central Power and Light Company, October 28, 1971

12 Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, by the Office of Nuclear Reactor Regulation, September 1975

13 Code of Federal Regulations, Title 10 - Energy, January 1, 1979

14 Federal Register, Volume 31, No. 190, September 30, 1966

15 President's Commission on the Accident at Three Mile Island Deposition of Burns and Roe, Inc., by Edward J. Gahan, August 6, 1979

16 President's Commission on the Accident at Three Mile Island Deposition of Burns and Roe, Inc., by Pio Nardone, August 8, 1979

17 Comments by Admiral H. G. Rickover, USN Director Naval Nuclear Propulsion Program in Meeting with Members of The President's Commission on the Accident at Three Mile Island, July 23, 1979

18 President's Commission on the Accident at Three Mile Island Deposition of Thomas A. Ippolito, August 9, 1979

19 Human Factors Methods for Nuclear Control Room Design, by Lockheed Missiles and Space Co., Inc., EPRI Summary Report, June 1979

20 President's Commission on the Accident at Three Mile Island Deposition of Ronald L. Williams, August 9, 1979

21 Proposed IEEE Standard, Nuclear Power Plant Protection Systems, by IEEE/NSG/ Reactor, Instrumentation and Controls and Committee/Standards Subcommittee, September 13, 1966

22 Safety Criteria for Reactor Instrumentation, by Voss A. Moore, Jr., U.S. Atomic Energy Commission, April 16, 1968

23 Anthropometric Source Book, Volume 1-3, NASA Reference Publication 1024, July 1978

24 U.S. Military Standard 1472B, Human Engineering Design Criteria for Military Systems, Equipment and Facilities, December 31, 1974

25 U.S. Military Specification 46855, Human Engineering Requirements for Military Systems, Equipment and Facilities

26 U.S. Army Test and Evaluation Command Test Operations Procedures (TOP) Human Factors Engineering, Perkins and Maxey (TECOM), Malone, Shenk and Kirkpatrick (Essex Corporation), December 20, 1977

27 Human Factors Engineering Third Edition, Ernest J. McCormick, McGraw-Hill Book Co., 1970

28 Human Engineerng Guide to Equipment Design (Revised Edition), Harold P. Vancott and Robert G. Kinkade, 1972

29 Job Analysis for Training Design and Evaluation, Hakan Andersson, Per Back and Jan Wirstad, Report No. 6, January 1979

30 Diagnosis of Plant Failures from a Control Panel: A Comparison of Three Training Methods by A. Shepherd, E. C. Marshall, Ann Turner, and K. D. Duncan, Ergonomics, Volume 20, No. 4, pp. 347-361, 1977

31 ANSI N18.1, Selection and Training of Nuclear Power Plant Personnel, March 8, 1971

32 ANSI/ANS 3.5, American National Standard for Nuclear Power Plant Simulators for Use in Operator Training, January 29, 1979

33 Investigation into the March 28, 1979 Three Mile Island Accident, by Office of Inspection and Enforcement, NUREG-0600, August 1979

34 NASA Publication MSFC 512

35 Human Factors Aspects of Nuclear and Fossil Fuel Power Plant Maintainability, Seminara, Parsons and Parris, from the Proceedings of the Human Factors Society 23rd Annual Meeting, 1979

36 Human Reliability Assessment in Nuclear Reactor Plants, SCR-69-1236, Swain, A.D., April 1969

37 "Human Reliability Analysis Applied to Nuclear Power," Swain, A.D. and Guttmann, H.E. in Proceedings of the 14th Annual Reliability and Maintainability Conference, Institute of Electrical and Electronic Engineers, New York, January 1975, 116-119 (also SAND74-5379)

38 WASH-1400 (NUREG-75/014): Reactor Safety Study - An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, U.S. Nuclear Regulatory Commission, Washington, D.C., October 1975

39 Preliminary Human Factors Analysis of Zion Nuclear Power Plant, SAND76-0324 (NUREG76-6503), Swain, A.D., October 1975, 81 pages (available only in reading room, U.S. Nuclear Regulatory Commission)

40 Uses of Reliability Techniques in Evaluation of Nuclear Power Plants, SAND76-0325 (NUREG76-6504), Merren, G.T., Esterling, R.G., and Swain, A.D., October 1975, 1936 pages (available only in reading room, U.S. Nuclear Regulatory Commission)

41 Systems Psychology, Kenyon B. DeGreene (ed.), McGraw-Hill, Inc., 1970

42 Updates to Chronology Prepared by NRC Special Inquiry Group

43 Preliminary Annotated Sequence of Events March 28, 1979, TMI-2 by Met. Ed.

44 Metropolitan Edison Transcripts of Interviews with TMI-2 Operators, May 14, 1979

45 Human Factors Review of Nuclear Power Plant Control Room Design, EPRI NP-309, Seminara, Gonzalez, and Parsons, Lockheed Missiles and Space Co., November 1976

46 Human Engineering of Nuclear Power Plant Control Rooms and Its Effects on Operator Performance, Finlayson, Hussman, Smith, Crolius and Willis of the Aerospace Corporation, February 1977

47 President's Commission on the Accident at Three Mile Island Deposition of Babcock and Wilcox by Lind, Kosiba, Elliott and McMillan, July 3, 1979

48 Report of the President's Commission on the Accident at Three Mile Island, The Need for Change: The Legacy of TMI, October 1979

49 ANSI N720/ANS 55.4 Gaseous Radioactive Waste Processing Systems for Light Water Reactor Plants, January 1977

50 ANSI N271/ANS 56.2, Containment Isolation Provisions for Fluid Systems, Draft 3, November 1974

51 IEEE Standard 338, Criteria for the Periodic Testing of Nuclear Power Generating Station Class 1E Power and Protection Systems, 1975

52 ANSI N193/ANS 56.3, Overpressure Protection of Low Pressure Systems Connected to the Reactor Coolant Pressure Boundary, 1st Draft, Revision 2, October 1974

53 ANS 56.6/N277, Pressurized Water Reactor Containment Ventilation Systems, 3rd Draft, Revision 3, July 1977

54 ANS 3.7.2, Emergency Control Centers for Nuclear Power Plants, June 1978

55 ANSI N18.5/ANS 2.2, Earthquake Instrumentation Criteria for Nuclear Power Plants, Revision 1, January 1977

56 IEEE Standard 279, Nuclear Power Plant Protection Systems, 1968

57 Code of Federal Regulations, Title 10 - Energy, January 1, 1971

58 Code of Federal Regulations, Title 10 - Energy, January 1, 1969

59 Code of Federal Regulations, Title 10 - Energy, January 1, 1967

60 Federal Register, Vol. 33, No. 244, December 16, 1968

61. Federal Register, Vol. 32, No. 132, July 11, 1967

62 Federal Register, Vol. 35, No. 125, June 27, 1970

63 Federal Register, Vol. 35, No. 249, December 24, 1970

64 RG 1.33, Quality Assurance Program Requirements (Operation), Revision 1, January 1977

65 RG 1.97, Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant Condition During and Following an Accident, December 1975

66 RG 1.70, Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants, February 1972

67 RG 1.68.2, Initial Startup Test Program to Demonstrate Remote Shutdown Capability for Water-Cooled Nuclear Power Plants, January 1977

68 RG 1.108, Periodic Testing of Diesel Generator Units Used as Onsite Electric Power Systems at Nuclear Power Plants, August 1976

69 RG 1.95, Protection of Nuclear Power Plant Control Room Operators Against an Accidental Chlorine Release, February 1975

70 HFE Technology for Navy Weapon Systems Acqusition, C.C. Baker, J.H. Johnson, M.T. Malone and T.B. Malone, Naval Sea Systems Command, July 1979

71 Human Factors Engineering Technology for Ships, T.B. Malone, Naval Sea Systems Command, 1979 (in press)

72 Oversight Hearings of the Ninety-Sixth Congress on the Accident at the Three Mile Island Power Plant, Middletown, PA, Serial No. 96-8, Part I

73 Human Factors Test and Evaluation Manual, T.B. Malone and S.W. Shenk, Naval Air Systems Command, October 1976

74 Nuclear Power and the Public Risk, Robert Sugarman (ed.), IEEE Spectrum, November 1979

75 Human Factors in Utility Reliability, J.A. Prestele and R.W. Pack, 1979 Reliability Conference for the Electric Power Industry, 1979

76 Operator Error in Nuclear Power Plants: A Preliminary Assessment, S.K. Adams, Z.A. Sabri and A.A. Husseiny, Presented at the Annual Meeting of the Human Factors Society, November 1979