UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

December 13, 1979

In Reply Refer to:
NTFTM 791213-03

Dr. Fred Finlayson
Aerospace Corporation
P. O. Box 92957
Los Angeles, California 90009

Dear Dr. Finlayson:

Enclosed is a second draft of the NRC's Special Inquiry Group Staff report on human factors which will form most of the human factors section of Volume II of the report to the Commission. Two sections; evaluation of selection and training, and findings and recommendations, are still being worked on.

Please try to provide any comments you may have by December 20, 1979. If you have enough time, send them in writing; otherwise call in your comments to either me (301/492-8902), or Gordon Chipman (301/492-8924).

Sincerely,

for E. Kevin Cornell, Staff Director
NRC/TMI Special Inquiry Group

Enclosure:
Second draft: Human Factors

8001230388

- o Problems with procedure consistency include:
  - Nomenclature used in the procedure is usually 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.
- o Problems with correctness of procedure:
  - Section B symptoms are not correct. Symptoms for leak or rupture include "rapid continuing decrease of pressurizer level."
- o 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

The Essex Company found that the emergency procedures failed to identify in clear and concise terms what decisions are required of the operator, the information needed by the operator to make the decision, what actions need to be taken to implement the decisions and how the operator varifies the correctness of his decision and actions.

The Essex evaluation of the use of procedures included the following factors:

- . Accessibility of procedures
- . Management of the update of procedures
- . Use of procedures as job performance aids

It found that there was no aid available to access the procedures. The operator must depend on his familiarity with the procedures to know which one is applicable to a given situation in the plant. The procedures should specify the condition of the plant which makes them applicable to the situation, this was not the case at TMI.

would be advisable to do it but Met. Ed. wasn't.

Cheapshot
ignorance mostly
not intentional

Essex concluded that Met Ed has the attitude that "CRO's and SRO's are not all that important in the operation of the plant, and that engineering and management personnel are better qualified to develop the design aids and took to be used by ... (the operators." This conclusion was reached from the fact that there was no formal program for operator input into procedures update or having them identify the problems encountered in their use. Essex felt, and we agree that a mechanism is needed to identify problems with the procedures and enable operator input to the solution of these problems.

In an emergency situation the operators has only three aids available to him to cope with the emergency; emergency procedures, training in similar situations and knowledge of the plant operation and status. The operator must detect and isolate the problem by diagnosis. Essex pointed out that the operator can depend neither on his knowledge of the plant nor his training to make the diagnosis or to determine what action is necessary to isolate the problem. He therefore, must rely on the emergency procedures. For this reason he needs accurate and readily accessible procedures to supplement his knowledge and training. They should provide him with decision criteria and steps to be taken to formulate hypothesis concerning what is happening in the plant and to test the hypothesis employing displayed data and test sequences.

The underlying question is were these procedures available to cope with the situation at TMI on the morning of March 28 and did procedures or lack of procedures have an impact on the accident. Essex found that the procedures were grossly diffic[illegible] in assisting the operator in diagnosing the feedwater system, the emergency feedwater system, the OTSG level response when emergency feedwater pumps were initiated. The procedures were of no help in diagnosing the PORV failure nor did they provide guidance in analyzing the situation of increasing pressurizer level while RC pressure decreased. Furthermore, the procedures gave no guidance regarding overriding the automatically initiated HPI, when to trip the RC pumps while temperature and level are high and pressure is low, and when and how to establish natural circulation.

Perhaps the following statement in the Essex report best characterizes their view of the TMI-2 procedures as compared to the state-of-the-art in this area:

> "It seems ironic that in the day of advanced data processing and photographic technology, nuclear power plant procedures have not progressed out of the stone age."

invites hostility

way behind state of art
~~above~~
not commensurate with ~~gravest~~ gravity of
potential consequences.

12/7/79

2.0 HUMAN FACTORS CONSIDERATIONS IN

THE TMI-2 ACCIDENT

2.1 Introduction

Analysis of the Three Mile Island accident suggests that certain engineering and design aspects coupled with operator training, experience and emergency procedures may have directly influenced the operator actions and inactions which significantly affected the course of the accident. These types of considerations are formally referred to as "human factors."(1) Several of these factors can be singled out as directly causing the accident while others can only be identified as possible contributors to the general confusion of the operators; confusion which impaired their ability to correctly analyze the problem they faced and take appropriate corrective actions.

2.2 Significant Operator "Errors"

Two actions or inactions by operators stand out as having had the greatest impact on the accident. First, they failed to recognize that the pilot-operated relief valve (PORV) on the reactor pressurizer had not automatically closed as it is designed to in the course of recovery from a reactor trip. Consequently, the operators did not close the PORV block valve for over two hours after the events began

and the resulting water loss caused significant damage to the reactor.(2)

A second action which significantly affected the course of the accident was operator throttling (curtailment) of the high pressure injection (HPI) of water into the reactor coolant system. Had the HPI been allowed to function at a high rate, the reactor core would have remained covered and serious core damage would have been prevented.(2)

It is clear that both of these operator actions, failure to close the PORV block valve, and throttling the HPI, significantly contributed to the accident. There is strong evidence, however, that instrumentation, procedures, and training may have led the operators to make both of these mistakes as will be outlined below.

1. Failure to Isolate the PORV

Failure to close the PORV block valve can be attributed to failure to recognize the symptoms spelled out in one of the plant's emergency procedures (Pressurizer System Failure) (3), which, as part of their training, the operators memorize and use as a basis for diagnosing and responding to emergencies. According to this procedure, the operator must recognize the following symptoms.

1. The PORV v[illegible] has failed to close.

2. Elevated reactor coolant drain tank pressure and temperature; and

3. Elevated PORV pipe discharge temperature above the 200^{o}F alarm set point.

For each, there appears to be a logical "human factors" explanation of why the operator failed to notice the symptom and take the appropriate corrective action.

First, failure to directly notice the failed open PORV can be traced to the method of indicating the valve's positon, a single red PORV status indicator light. This light is on when an electrical signal is sent to open the PORV and it is off when the signal is terminated. This light does not, as may be inferred by its labeling, "PORV open and closed," indicate the actual position of the PORV.(4) Consequently, at about 13 seconds into the accident the when PORV indicator light went out and the operator was misled into believing the valve had actually closed when, in fact, it had stuck open.(5) Parenthetically, it is interesting to note that the original TMI-2 control room design contained no indicator light. However, following a March 29, 1978 trip where the PORV had failed open,(6) the existing light and labeling were installed.

A valve indicator system which directly sensed the open and closed position of the valve would not likely fail in a manner which would incorrectly indicate valve closure.(7) Thus, it can reasonably be assumed that, had there been such an indication system directly sensing actual valve position, the operators would have noticed the open valve indication and closed the block valve much earlier, terminating the accident well before any core damage occurred.

The failure of the operators to recognize the second symptom, elevated reactor coolant drain tank temperature and pressure, can also be traced to human engineering and design factors, namely inadequate and poorly placed instrumentation as well as the pre-accident history of a leaking code safety valve.

Water discharged from the pressurizer through the PORV eventually collects in the reactor coolant drain tank (RCDT). Thus, if the PORV fails open, the temperature, pressure and water level in the RCTD are expected to increase. However, at TMI-2, one of the code safety valves (or possibly the PORV) which also drains into the RCTD had been leaking since the fall of 1978, and had been scheduled for repair during the next reactor shutdown.(8)

Thus, it was not unusual for the operators to observe elevated temperature, pressure and level in the RCDT and, in fact, about once every shift operators had been forced to pump the accumulated water from the RCDT.(8) One can logically surmise that an operator having worked under this condition for several months would not have noticed RCDT conditions early in the accident as being abnormal. Added to this problem is the fact that the instrumentation for RCDT conditions and the corresponding alarms are behind the control panel and cannot be read unless the operator leaves his normal operating area in front of the control panel and walks about 50 feet to read the instruments (see Figure ___ in Section ___). To further compound the problem, the RCDT instrumentation on the back panel only gives instantaneous information. It does not record the RCDT parameters which would make available to the operators the previous trends of RCDT temperature, level and pressure. Consequently, when the operator went to check the RCDT status, he had no way of telling whether the RCDT conditions were a result of a single opening and closing of the PORV in combination with a small leak in the code safety valve, or whether they were a result of a longer continuous leak from a stuck open PORV.

In fact, in the period from 10 to 15 minutes into the accident, one operator did check the RCDT and noted that it was full.(9) After the RCDT rupture disc had failed (at about 15 minutes), the shift supervisor from Unit 1 checked the panel and noted that it was empty.(9) This was immediately followed by an increase in reactor building pressure and the sounding of an associated alarm. The shift supervisor consulted with the CR operators and correctly concluded that the RCDT rupture disc had failed. However, they incorrectly concluded that the RCDT has been nearly full of water from the previously leaking code safety valve and that the subsequent momentary opening of the PORV (at the time of reactor trip) had added enough water to overfill the tank, causing its emergency rupture disk to break,(10, 11) and result in the tank indicating empty.(12)

If the RCDT monitoring instrumentation had either been located in normal view of the operators or been recorded, it is more likely that they would have noticed the time trend of RCDT parameters and correctly realized the condition of a stuck open PORV.

The third symptom which the operators failed to notice was the elevated temperature of the discharge pipe from the PORV. As discussed above, the pressurizer code safety valve adjacent to the PORV had been leaking for some months prior to the accident. Because of the proximity of this valve to the PORV, the temperature of the PORV discharge line had been reading high, about 180°F. Earlier in the day on March 28, (13) the safety valve leakage had increased approximately 40 percent and the discharge temperature of the safety valves had increased above the range of 180° to 200° which had been maintained for some time.

As a consequence of this history of operating with a leaky safety valve, the TMI-2 operators were misled into believing that the rise in temperature in the discharge line following the reactor trip was caused by a combination of high temperatures before the accident and a momentary opening of the PORV. There is evidence also that the situation leading the operators to this faulty logic was further compounded by their lack of training in basic engineering. Apparently, operators believed that the highest expected temperature in the discharge line as a result of a stuck open PORV was over 500°F.(14) In fact, because of the throttling action of the PORV relief valve, the maximum achievable temperature was closer to 300°F. The operators were apparently unaware of this fact and the information is not contained in their emergency operating procedures.

Following initiation of the accident, the operators periodically monitored the discharge line temperature and noted temperatures as high as 285°F (15). However, it was almost 2½ hours into the accident when the oncoming shift supervisor noticed the PORV discharge temperature was 229°F, and that it was about 25°F hotter than the code safety discharge temperature, and correctly interpreted the reading which led to closing the PORV block valve (16).

To summarize, there is strong evidence to suggest that the TMI-2 operators' failure to recognize the symptoms of a stuck open PORV valve and to follow the emergency procedure of closing the block valve early in the accident, can be attributed to a combination of deficiencies in instrumentation, control room layout, emergency procedures and training as well as poor reactor maintenance prior to the accident. We recognize however that it was theoretically within the within the capability of the operators to recognize the PORV failure from the information in hand; in fact, the symptoms were eventually recognized. While the delay in recognizing these symptoms was a key element in the severity of the accident, the delay can be attributed to human factors' inadequacies affecting the interface between operator and machine.

2. Throttling of High Pressure Injection

Manual throttling or curtailment of the flow of emergency core cooling water into the reactor coolant system was a second significant operator action that affected the severity of the TMI accident.

At approximately 2 minutes into the accident, operators took manual control of the automatic high pressure injection (HPI) system (which had started when RCS pressure dropped below 1640 psig) and reduced the water flow to the reactor. For most of the first hour-and-a-half, the net flow rate was reduced from about 1,000 gpm to only about 25 gpm. (17) Technical analysis indicates that if this throttling had not occurred, core damage would have been avoided (18)

The factors which caused the operators to take that this action are complex. Similarly to the stuck open PORV recognition problem, they involve improper training, lack of instrumentation and inadequate procedures, as well as a fundamental misunderstanding of reactor thermal hydraulics by the operators, and by portions of Met Ed's management, the industry and the NRC.

The basic mistake made by the operators during the early minutes which led to their throttling HPI and limiting the flow of emergency water to the reactor coolant system, was the failure to recognize that the reactor was experiencing a small loss of coolant accident (LOCA), that could lead to uncovering the core.

The preceding PORV discussion addresses factors involved in their failure to recognize the stuck open PORV, the basic cause of the LOCA. However, the question remains; why, having failed to recognize the PORV failure, the operators did not recognize the other symptoms of a LOCA and take appropriate action. Several additional human factors issues serve as a logical explanation.

First, the TMI plant did not have any means of directly measuring the water level in the reactor. If direct water level or water inventory instrumentation had been available, it is reasonable to expect that the operators would have taken appropriate steps to prevent uncovering of the core, i.e., maintain high HPI flow. (19) The TMI design (as well as most PWR's) relied on a faulty understanding of reactor behavior which served as a basis for operator training and emergency procedures. This involves a misconception that water level in the pressurizer serves as a true indication of total volume of water in the reactor coolant system under all accident conditions. (20) Subsequent analysis (refer to _______) reveals that for the LOCA which occurred at TMI, previously believed relationships of high pressurizer level signifying that the reactor vessel is full of water are not correct. (21) Consequently, much of the operator training and the emergency procedures were invalid and led the operators to mistakenly throttle high pressure injection in an attempt to maintain pressurizer level within the normal range. For example, the emergency procedure dealing with loss of coolant accidents (EP 22021.3) contains two alternative sections, each of which warns the operators to look for a combination of low reactor pressure and low pressurizer level. At TMI, reactor pressure did fall but pressurizer level increased. Having failed to observe the symptoms applicable to this procedure, it is logical that the operators did not follow the prescribed corrective actions that could have prevented the accident.

Lacking unambiguous emergency procedures, operators instead followed other dictates of their training and operating procedures and attempted to control pressurizer level by throttling the HPI system. (22, 23) Not only had the TMI-2 operators been trained to interpret pressurizer level as positive indication of the level of water in the reactor coolant system, apparently they also received strong admonition to avoid taking the pressurizer solid. This admonition was strongly emphasized and reinforced by various documents which clearly define the pressurizer levels to be maintained by the operators. (24)

In summary, there is strong evidence that the combination of inadequate procedures, inadequate training, the failure to incorporate lessons learned and/or the lack of direct water level instrumentation, misled operators to throttle HPI which stands out as a significant factor in the accident. Furthermore, these inadequacies were a result of a basic misconception on the part of the operators, industry and the NRC of how the reactor coolant system would behave.

These actions could be ascribed to "operator error" as was done in NUREG 0600. However, it is our view that the overall system of training, operating, CR design, and maintenance is the major problem--a view that has become more evident as the study of this accident has progressed.

2.3 Other Factors Contributing to the Accident

In addition to the two preceding examples of how inadequate instrumentation, training and procedures may have directly caused the accident, other similar "human factors" had a strong potential for contributing to the general confusion of operators and most likely impaired their ability to correctly respond to the problems being faced.

The Essex Corporation's study contained in ___________ describes a number of these factors. Several examples are illustrative of their findings. First, the confusion of the first hour of the accident was compounded by a discovery that the emergency feedwater block valves were closed. Although technical analysis suggests a closure of these valves did not directly cause the accident, (25) discovery of the closure 8 minutes into the accident and the resultant diversion of operator attention to feedwater problems may have diverted them away from analysis and reaction to more fundamental causes of the accident. (26)

This failure to discover closure of EFW valves can be directly attributed to several human engineering control room deficiencies. First, there was inadequate quality control of valve lineup, which should have lead the operators to discover the closed valves before the accident. Second, the control room did not contain any direct indication of EFW flow. Thus, operators were forced to rely on secondary indication of valve position and pump condition to verify flow status. Third, the indicator lights which tell the operator whether or not the EFW block valves are closed were hidden by one of the out-of-service tags that cluttered the control panel as shown in Figure ______. Fourth, the feedwater control panel is not laid out in a logical fashion such as control locations mimicking actual valve and pump positions in the plant. In fact, the control and display placement on the EFW panel is inconsistent (27) as shown in Figure _____. The absence of any logical panel layout forces operators to rely on memory or random search to locate a particular control. This panel layout problem existed elsewhere in the control room and increased operator workload and probability for mistakes, particularly during emergency conditions.

A second condition that added to the confusion in the control room was the alarm system which hampered the operators during the early stages of the accident. For example, the control room contains over 750 alarms. These alarms are not prioritized and many are difficult to read from normal operator positions. During the first few minutes of the accident, about 100 of these alarms went off. (28) In order not to lose important information on which alarms had been actuated and which had cleared, the operators did not acknowledge any alarms (and silence the audible alarm) for some time into the accident. When asked if there was any way to "shut off the horn and the bell so you can think a little bit," by Representative Carr, Mr. Fredericks said no. (29)

This problem with alarm systems prompted one operator tr write a year before the accident:

> "The alarm system in the control room is so poorly designed that it contributes little in the analysis of a casualty. The other operators and myself have several suggestions on how to improve our alarm system--perhaps we can discuss them sometime--preferably before the system as it is causes severe problems." (30)

On March 28, 1979, the control room alarm system had not changed.

The Essex Corporation found other examples of poor control room design which contributed to confusion. These include poor lighting, numerous examples of illogical panel layout, confusing use of indicator color coding, and situations where operator's ability to read meters and observe indicator lights were impaired.

In addition, the Essex Report found that several operator errors were caused or influenced by expentancy or set. Set is a psychological construct defined as a temporary but often recurrent condition of individuals that orients them toward certain information and events rather than others, and increases the likelihood of certain responses over others. The influence of 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 safety valve had been leaking for some time prior to the accident. 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 the real problems.

Development of these erroneous 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. The importance of operator set in the TMI incident is also 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.

Essex found that the influence of psychological stress as a determinent in the TMI accident was 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 the investigation by Essex or the SIG that would indicate any problems in the reasoning or problem solving capabilities of any of the operators on 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 March 28, scored highest of all TMI operators. The two control room operators for whom scores are available both scored in the upper 50 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.

2. 4 Summary and Conclusions Perhaps the best summary of the overall conclusion reached in this analysis were expressed one year before the accident. A TMI operator in addressing problems experienced during a March 29, 1978 reactor trip stated in a letter to his supervisor:

> "I feel that the mechanical failures, poor system designs and the improperly prepared control systems were very much more the major cause of this incident that was operator action. Although training is always essential and welcome--nothing we study or learn to practice could have prepared us for this unfortunate chain of events...You might well remember this is only the tip of the iceberg and the best operator in the world can't compensate for multiple casualties which are complicated by mechanical and control failures."

This seems to be a fairly accurate description of the problems faced by the operators albeit all of the information necessary for them to have prevented the accident was available. The point here is that many of the actions they took were not a result of a lack of information or stupidity, but were a logical result of the inadequate CR design, operator training and emergency procedures.

The Essex Corporation Study (31) reached a similar conclusion by stating:

> "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."

REFERENCES AND NOTES

1. As used in this report, "human factors" is an interdisciplinary approach to optimizing human performance in the man-machine system. It includes application of principles relating to psychology, physiology, instrumentation, control and workspace design, personnel selection and personnel training.

2. Section II-D, Alternative Accident Sequences, Subsection II-D-1.1.

3. Three Mile Island Nuclear Station Unit #2 Emergency Procedures 2202-1.5, Pressurized System Failure, Revision 3, dated September 29, 1978.

4. This design is a specific violation of accepted human factors principles as contained in Mil-Std-1472B, paragraph 5.2.2.1.5:

   "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."

5. I&E Testimony, TMI-278, page 12.

6. SIG Precursors, Subsection H.

7. Such indicators are commonly controlled by microswitches which sense the position of the relief valve stem. While erroneous position indication is possible with such a design, the likelihood of a false indication of the PORV being shut is small.

8. NUREG 0600, Investigation into the March 28, 1979 Three Mile Island Accident by the Office of Inspection and Enforcement, Section I-1-3.

9. I&E Testimony TMI 198, pages 25-28, TMI 278, pages 6-8.

10. NRC/SIG Testimony, September 11, 1978; Faust, Frederick, Scheimann, Zewe, pages 154 and 155.

11. Oversight Hearings before the Subcommittee on Energy and the Environment, May 9, 10, 11 and 15, 1979. Serial No. 96-8 Part 1, page 170.

12. It was actually reading off scale low (below 60 inches).

13. Reference ~~6~~ 8.

14. NRC/SIG Deposition of Joseph Chwastyk, October 11, 1979, pages 7172.

15. NRC/SIG Sequence of Events, time 24 minutes, 58 seconds.

16. NRC/SIG Sequence of Events, 2 hours, 18 minutes.

17. Reference ~~6~~ 5, Section 4.3.

18. Section II-D Alternative Accident Sequences, Subsection II-D1.1. NOTE: A definitive analysis of the reactor coolant system water balance is not possible with the data that is available.

19. As discussed in Section _____, there had been earlier attempts to require instruments to directly measure water level in the reactor vessel for pressurized water reactors.

20. The analysis of small break LOCA's by NRC and the industry do not include considerations of the vagaries of operator actions.

21. This fact was known before the TMI accident but had not been widely recognized or incorporated. See Section (precursors). Had this information been incorporated, the symptoms indicating false reading of pressurizer level would have been known and the operators would likely have maintained a high HPI flow.

22. Reference ~~8~~ 15, page 123.

23. Public Hearings Before the President's Commission on Three Mile Island, May 30, 1979, page 194.

24. These include: Section 3.4.4 of Appendix A to TMI operating license; OP 2103-1.3 Revision 3, July 19, 1978; Babcock & Wilcox Limits and Precautions for Pressurizer Operations.

25. Section II-D-2.3.

26. Reference ~~8~~ 16, page 124.

27. The negative impact on the operator performance of this inconsistent layout was demonstrated later in the accident. At approximately 90 minutes into the accident, the operator permitted steam generator A to boil dry again because he was trying to add water to the A generator but was actually operating the valve that controls water to the B generator.

28. Hearings Before Committee on Interior and Insular Affairs, Task Force on Three Mile Island, May 11, 1979, page 43.

29. Reference 25, page 44.

30. Letter, Edward Frederick to James Seelinger TMI-2 Superintendent for Technical Support, March, 1979.

31. Essex Report _____________.

12/12/79
To Editor

3.3.2 TMI-2 Control Room Description

General Layout

At the TMI nuclear power plant, the control stations, switches, and indicators necessary to start up, operate and shutdown the nuclear unit are located in one control room. Controls for certain auxiliary systems are located at remote control stations.

As can be seen from Figure 1, and the photograph in Figure 2, the TMI-2 control room is very large and contains a large number of instruments, controls and alarms. The control room consoles are arranged in a U-shaped pattern with vertical panels following the same pattern behind the consoles, separated by a passage aisle. The operator's desk is located in front of the U-shaped console and panel arrangement. Figure 1 shows the floor plan and layout of the control room and a perspective on the size and layout can be obtained from the photo in Figure 2.

According to the TMI-2 Final Safety Analysis Report (FSAR), the control room was to be designed so that one man could supervise operation of the unit during normal steady-state conditions. During abnormal operating conditions, additional operators are expected to be available for assistance. The control room is arranged to include the operating consoles, which house frequently used controls and indicators, as well as startup and emergency controls and indicators. The FSAR also notes that the controls and indicators were to be located in a logical arrangement, making them accessible and readily visible to the operator. Recorders and radiation monitoring equipment, infrequently used

POOR ORIGINAL

control switches, remaining indicators, temperature recorders, annunciators and reactor building isolation valves position indication are mounted on the vertical panels behind the consoles. Table ___ summarizes the functions of the panels which were during the March 28, 1979 accident.

Visible and audible alarm units are incorporated into the control room to warn the operator of unsafe or abnormal conditions. The control room was supposedly designed such that information readouts contain all the necessary indications that are required by the operator for monitoring conditions in the reactor, reactor coolant system, containment and safety-related process systems throughout all operating conditions of the plant.

Plant Computer

The plant computer system is usd for monitoring alarms, plant performance, logging data and performing simple calculations, is located near the center of the control room on one console. This system uses a Bailey 855 computer which is linked to a smaller NOVA computer. The NOVA computer was added to the original design to provide more capacity for monitoring the balance-of-plant conditions.

The computer has two output modes -- an alarm printer and a utility printer. These are both automatic typewriters and if either fails, its output is automatically transferred to the other. A small cathode ray tube display is also provided which duplicates the output of the printers or can be used for independent display.

For all monitored parameters that have an alarm function, the alarm printer automatically prints an alarm message when the parameter has gone into an alarm condition. The computer also samples each parameter -- temperature, pressure, level, etc. --and compares the reading to a preset alarm value. If the reading is found to be outside of acceptable limits, a notation to that effect is typed out on the "alarm printer." When the parameter again comes within acceptable limits, another notation is typed. The alarm printer also makes a record of starting, stopping, or tripping of major equipment.

The computer alarm printout is capable of typing only one line every four seconds. Consequently, in situations where alarms are initiated rapidly, the printer is unable to keep up and alarm printout is delayed. An operator can bring the printout up to real time, but only at the cost of clearing all alarms awaiting printout from the computer memory. At one point during the accident, the alarm printer was over 2 hours behind.

The uitlity printer provides output on request. The value or condition of any monitored parameter can be requested. Special subroutines allow the operator to request output values in specific preprogrammed groups called "Operator Special Summaries" or to trend output values in preprogrammed groups called "Operator Group Trends."

The computer is also programmed to record automatically all changes in state of a predesignated group of parameters called "Sequence of Events" inputs. These event inputs are stored in the computer and can be printed on request. The sequence is started by any one of the "Sequence of Events" inputs changing state and continues until printed by the operator.

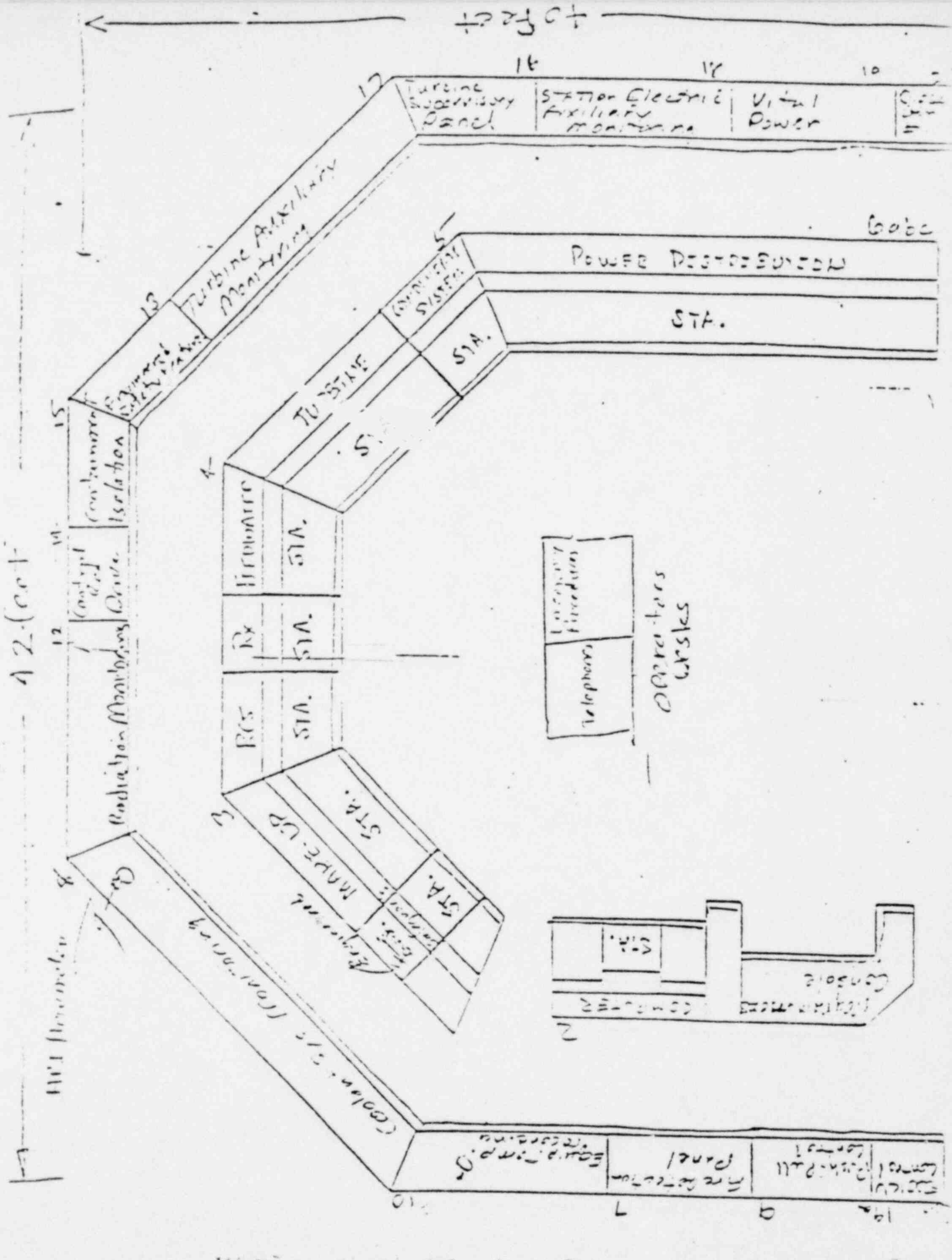
The plant computer provides the operator with an efficient means of keeping logs and showing trends on a large number of plant parameters under normal operating conditions. The computer was not designed to accommodate the data needs of the operator in an accident situation. Using the computer in an accident situation requires that the operator leave his control panels in order to request computer output; it takes the computer several seconds to supply the requested output; and, as pointed out above, the automatic alarm printout can be several minutes, or even hours, behind real time. All of these tend to limit the computer's usefulness in an accident situation. If properly designed and programmed, the computer can provide information useful for diagnosing and responding to an emergency situation. However, the TMI computer was not programmed to establish a hierarchy of critical parameters to be monitored in the event of an emergency. Thus, during the March 28, 1979 accident, the large number of unimportant alarms and the resulting backlog made the computer nearly useless as a diagnostic tool.

TABLE ___

TMI-2 CONTROL ROOM KEY PANEL DESCRIPTIONS*

Panel	Description
2	Computer console
3	Reactor coolant makeup and purification system and the control room equipment related to the safety features actuation system.
4,5,6	Controllers, recorders, and indications necessary for control and supervision of the reactor power output, feedwater, condensate, steam generators, and turbine generator.
7	Indicates a fire in the unit and the automatic steps being taken to control it.
8	Annunciators and indication for status of the various nuclear and conventional cooling systems of the unit.
10	Records temperatures of major equipment, reactor vent valves, control rod drives, a self-powered neutron detector tubes; each temperature monitored is alarmed if the temperature exceeds a preset limit.
13	Status of the engineered safety features panel.
14	Individual control rod position, fault lights, and inserted and withdrawn limit lights.
15	Graphic panel that shows the position of all reactor building isolation valves.
21	Station radiation monitoring equipment and recorders; including equipment required to annunciate and indicate the status of equipment and interlocks intended to prevent any release to the environment that exceeds present limits.

*Panel numbers refer to those shown in Figure 1.



POOR ORIGINAL

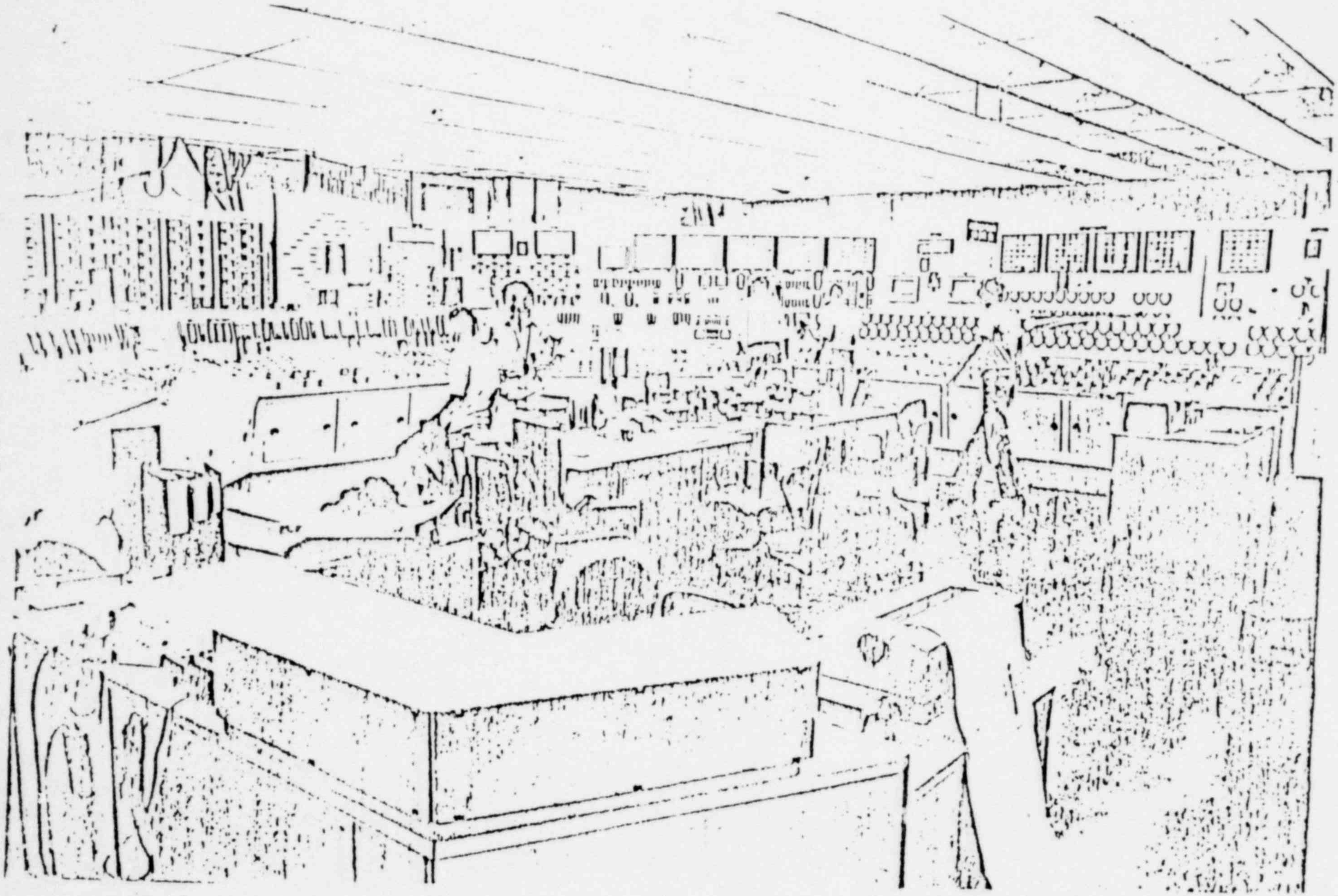


FIGURE 2 - TMI-2 CONTROL

12/17/79
To Editor

Human Engineering Criteria and TMI-2

The AEC (NRC) review and approval of the application for a construction permit, submitted by Met Ed for TMI-2 in April of 1968, was completed and the TMI-2 construction permit (CP) was issued in November 1969. (1) The primary criteria which were used in the AEC staff review of that permit are found in Title 10 of the Code of Federal Regulations. At the time of the CP review of TMI-2, the criteria most relevant to control room design were found in the proposed Appendix A to 10 CFR Part 50, "General Design Criteria for Nuclear Power Plants. (2) Typical examples of these criteria indicate that Federal regulations for control rooms were vague, lacked specificity and contained little, if any, indication of concern for human engineering issues associated with the interface between operators and the control room. For example, criterion 12[2] requires that "Instrumentation and Controls shall be provided as required to monitor and maintain variables within prescribed operating ranges." Another example is criteria 11[2] which states in part:

> "The facility shall be provided with a control room from which actions to maintain safe operational status of the plant can be controlled."

While these criteria were only proposed by the AEC at the time, they were published with the notation that they "would not add any new requirements, but are intended to describe more clearly present Commission requirements..."[2] Thus they were in effect AEC requirements. In addition to these Federal regulations, te industry had also developed standards which could have affected the human engineering of the TMI-2 control room. One example which was referenced in the TMI PSAR application, was IEEE standard 279 which required that:

> "If the protective actions 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."[3]

POOR ORIGINAL

The thrust of this standard was to provide an effective means of warning operators of an inoperative system. It should be noted, however, that this standard applied only to the Reactor Protection System and not to safety systems such as the emergency core cooling system.

Another industry standard (IEEE 603) which exhibited a concern for human engineering was entitled, "Displays for Protective Actions Initialed by Manual Means."(4) This standard did apply to other safety systems and suggested that the display instrumentation provided for the manually initiated protective actions required for a safety system should be part of the safety system, and that the design should minimize the possibility of anomalous indications which could be confusing to the operator. It should be noted, however, that unlike IEEE-279, this standard was not required for the control room design and was not referenced in the TMI PSAR.

In addition to these standards, Section 7.4 of the TMI-2 PSAR outlines the general philosophy to be used in designing the TMI-2 control room. Similar to the standards described above, this general design philosophy contains only a vague and general reference to the man-machine interface problem.

Section 7.4 provides that all controls and instruments were to be located in one room. This room was to be designed so that one operator would suffice during normal operations. During "other than normal steady state operating conditions," other operators were to be available to assist the control operator. This section also contains general prescriptions for the shape of the control room, the relative placement of various systems, brief description of an audible alarm system, requirements to allow occupancy during abnormal conditions such as fire protection, radiation shielding, and ventilation, provisions related to evacuation of the control room and provisions for auxiliary control stations.

The final portion of Section 7.4 provides a typical example of the general nature of the specifications provided in the PSAR and the limited extent to which they addressed the human engineering problems. It stated in part(11):

> "7.4.7 SAFETY FEATURES
>
> The primary objectives in the control room layout are to provide the necessary controls to start, operate, and shut down the nuclear unit with sufficient information display and alarm monitoring to insure safe and reliable operation under normal and accident conditions. Special emphasis will be given to maintaining control integrity during accident conditions. The layout of te engineered safety features section of the control board will be designed to minimize the time required for the operator to evaluate the system performance under accident conditions. Any deviations from predetermined conditions will be alarmed so that the operator may take corrective action using the controls provided on the control panel."

In the time period from 1970 to 1978, there was a significant growth in the number of requirements and guidance related to control room design within both the NRC and the nuclear industry. As shown in the Essex report, a large number of these criteria were found to be related to human engineering. While these requirements and guidelines provided more substance than previously existed, the majority of these criteria still suffer from the same deficiency identified previously. That is, they were too vague and too general to require the direct application of human engineering technology which had been extensively developed in other fields(5).

During this time period, the NRC issued a number of documents for use by the nuclear industry containing recommended practices or guidance in safety matters starting with Reactor Technology Memoranda followed by Safety Guides and then Regulatory Guides. In 1975, the NRC consolidated its criteria in a Standard Review Plan(6) aimed at providing guidance to its technical staff who review and approve applications for nuclear power plant licenses.

The more substantive of these criteria include the following:

- Requirement of IEEE-279 that bypasses be indicated was expaned in Regulatory Guide 1.47[7] to include safety systems.

- Regulatory Guide 1.97 "Instrumentation for Light Water Cooled Nuclear Power Plants to Assess Plant Conditions During and Following an Accident" included a provision for analysis of what instruments are required. While not so identified in the Regulatory Guide, this provision is similar to the use within the human engineering discipline of a task analysis to determine what needs to be done and what must be provided to the operators so that they can effectively accomplish their tasks. However, without more specifity, this Regulatory Guide was not interpreted by the NRC or the industry to cover the use of a task analysis as in some other industries.[13] (See discussion on the limited implementation of RG 1.97 in Section on Operating License Review Issues Concerning TMI-2).

- A third regulatory guide entitled, "Guidance on Being Operator at the Controls of a Nuclear Power Plant"(8) also provides insight into NRC regulatory attempts to address the man-machine interface. The basic thrust of this regulatory guide is to place the onus on the CR operator for safe operation of the plant. It assumes, but does not establish the

POOR ORIGINAL

basis for further assumption, that the control room will provide the operator with all the aids needed to perform his job. For example, the guide states:

> "The operator of the controls of a nuclear power plant should have an unobstructed view of and access to the operational control panels, including instrumentation displas 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;"
>
> and that:
>
> "The operator at the controls should not normally leave the area where continuous attention (including visual surveillance of safety-related annunciators and instrumentation) can be given to reactor operating conditions and where he has access to the reactor controls. For example, the operator should not routinely enter areas behind control panels where plant performance cannot be monitored.

In spite of this analysis of the control room at TMI and operator actions performed during the early stages of the accident clearly suggest, in fact, that the TMI-2 was not designed so that operators would have an unobstructed view of instrumentation displays and alarms (See Section___). Furthermore, operators had to enter the area behind reactor controls in order to observe the reactor drain tank instrumentation critical to an assessment of the accident.

The detailed review conducted by Essex of these regulations, Reg. Guides, Standard Review Plan, found no examples of criteria which were written with a clear intent to include human engineering considerations in the licensing and regulatory system.

The expansion in guidance related to human factors from pre-1970 to pre-1978, that was experienced by the NRC also occurred in the codes and standards of the industry. Essex found that a significant number of industry standards developed during this time period relating to human factors. As in the other cases discussed above, however, few of these standards were thought to be important and they were too vague to effectively require the application of human engineering in the design process. Rather they were narrowly drawn guidelines addressing a specific component or group of components and did not adequately address the man-machine interface problems.

The most significant industry guidelines in existence during the operating license review of TMI-2 are found in IEEE Standard "Recommended Practice for the Design of Display and Control Facilities and Central Control Rooms of Nuclear Power Generating Stations" Standard 566, 1977.[9] While this standard contains guidance directly related to human engineering, a detailed review of this standard by the Essex Corporation found serious deficiencies. Essex noted that the standard was incomplete and that it did not include guidance on the use of some very powerful human factors tools such as the use of task analyses. In addition, they found that some of the specific guidelines in the standard were contrary to standard human engineering practices.

[Example]

Essex did find, however, one standard IEEE 338, 1977, "Standard Criteria for the Periodic Testing of Nuclear Power Generating Stations Safety Systems" which included an explicit recognition of human engineering by noting that "interrelationships 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."[10]

Nearly all of the industry standards available during this time frame, were published after the application on the operating license for TMI-2 had been submitted to the NRC in 1974. Thus, the more recent standards were not applied to the TMI-2 design except as deemed necessary by the NRC on the utility to address "significant" safety issues.

Conformance of TMI-2 to Human Factors Criteria and Standards

As we previously noted, the TMI-2 design was found by the AEC to meet the applicable criteria prior to issuance of the construction permit in 1968. Furthermore, the design development by the utility and its contractors, and the review of this design by the AEC were conducted with essentially no human engineering resources (See Section___). As will be discussed in the following section, TMI-2 was found by NRC to satisfy the existing criteria even though a review of the current design today by human engineering specialists against these limited criteria would find serious deficiencies.

When a nuclear power plant application is received by the NRC for an operating license, the practice has been to require conformance of the design to the criteria specified at the time of issuance of the construction permit and to address the necessity for meeting subsequent criteria on a case-by-case basis. The necessity to conform to post-CP criteria is determined by the NRC on the basis of a perceived level of safety improvement which can be achieved by such conformance and on a similar basis by the industry. (See Section___ on the Regulatory Requirements Review Committee.) The absence of any human engineering expertise on the NRC staff suggests that no need was perceived in this area.

In summary, we found a lack of substantive human engineering criteria and guidance, both within the NRC (AEC) and the nuclear industry, and more importantly, a lack of appreciation for the importance of human engineering to the safe operation of nuclear power plants. Furthermore, the resources to employ the techniques of human factors engineering that would be required to implement even the existing criteria did not exist within the NRC and in only a limited way within the nuclear industry.

Human Engineering Criteria and TMI-2 References

1. NUREG-0380, U.S. Nuclear Regulatory Commission Program Summary Report, Vol. 3, No. 5, May 18, 1979, p. 3-2.

2. Proposed Amendment to 10 CFR Part 50, "Licensing of Production and Utilization Facilities" to add Appendix A, "General Design Criteria for Nuclear Power Plant Construction Permits" (32 F.R. 10213) July 11, 1967. Pages 10213 through 10216.

3. Institute of Electrical and Electronic Engineers "Proposed IEEE Criteria for Nuclear Power Plant Protective Systems" IEEE 279, August 1968. Section 4.13 Indication of Bypass.

4. Institute of Electrical and Electronic Engineers "Displays for Protective Actions Initiated by Manual Means" IEEE 603, 1968.

5. For example: U.S. Military Standard 1472B, Human Engineering Requirements for Military Systems, Equipment and Facilities December 31, 1974. This standard includes detailed design guidelines, principles and requirements.

6. NUREG-75/087 "Standard Review Plant for the Review of Safety Analysis Reports for Nuclear Power Plants," LWR Edition.

7. Regulatory Guide 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems," May 1973.

8. Regulatory Guide 1.114 "Guidance on Being Operator at the Controls of a Nuclear Power Plant," Rev. 1, Nov. 1976.

9. IEEE Std. 566-1977, "IEEE Recommended Practice for the Design of Displays and Control Facilities for Central Control Rooms of Nuclear Power Generating Stations," Nuclear Power Engineering Committee of the IEEE Engineering Committee, 1977.

10. IEEE Standard (338), "Criteria for the Periodic Testing of Nuclear Power Generating Station Class IE Power and Protection System, 1975, p. 8.

11. Preliminary Safety Analysis Report, Three Mile Island Nuclear Station-Unit 2, Section 7.4.

12. MIL H-46855, Military Specification "Human Engineering Requirements for Military Systems, Equipment and Facilities" May 2, 1972., para. 3.2.1.3.

6/12/79
TO Edi...

TMI-2 Control Room Design Evaluation

The likelihood of operator actions such as those which exacerbated the March 28 accident can be reduced by the systematic integration of the human factors engineering into the planning and design of a plant. To determine the extent to which TMI-2 was designed to prevent or minimize operator errors, the Essex Corporation evaluated the TMI-2 control room and compared it with human factors engineering criteria and guidelines generally applied to other industries. The following discussion of human engineering aspects of the TMI Control Room design have been divided into categories which reflect different aspects of the design. They summarize the findings of the Essex Report.

Workstation Desing

One of the fundamental tenets of human factors engineering is that workstation design should facilitate operator performance and reduce the probability of operat r error. To accomplish t is, controls and displays should be logically organized according to function, sequence, or in relation to the system they control (i.e., mimic). Furthermore, controls should be placed to minimize the operator's need for reaching and to shorten the visual span between the operator and the instruments he must read, thus reducing time to locate and manipulate specific controls or displays.

Essex found that little, if any, attention was paid to this aspect of workstation layout. Apparently no analysis was made of the tasks which must be performed at the various TMI-2 workstations, or the capabilities and limitations of the operators performing such tasks. The following deficiencies are indicative of their findings:

- o In many cases, workstation design appears to <u>maximize</u> visual scan, reach and walking requirements. (Refer to Figure___ of Section___.)

  -- RC pump seal pressure is on panel 10, seal temperature on panel 8, while the pump controls are on panel 4.

  -- Makeup control is panel 3 while makeup flow indication is displayed on panel 8. See Figure ___.

- o Controls and displays are not logically or consistently sequenced.

  -- Pressurizer heater controls: 3, 5, 2, 4 1 See Figure ___.

  -- Pressurizer narrow range indicators: B, A

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

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.

Essex examined the benchboards and the attached vertical panels in TMI-2 for reaching requirements. The levels of excessive reach requirements were defined using the stature of the fifth percentile male (street clothes) as a basis.[1]

---

[1] Ninety-five percent of all males are taller than the fifth percentile male. USAF surveys conducted in the early 1950's were used as a basis ( ).

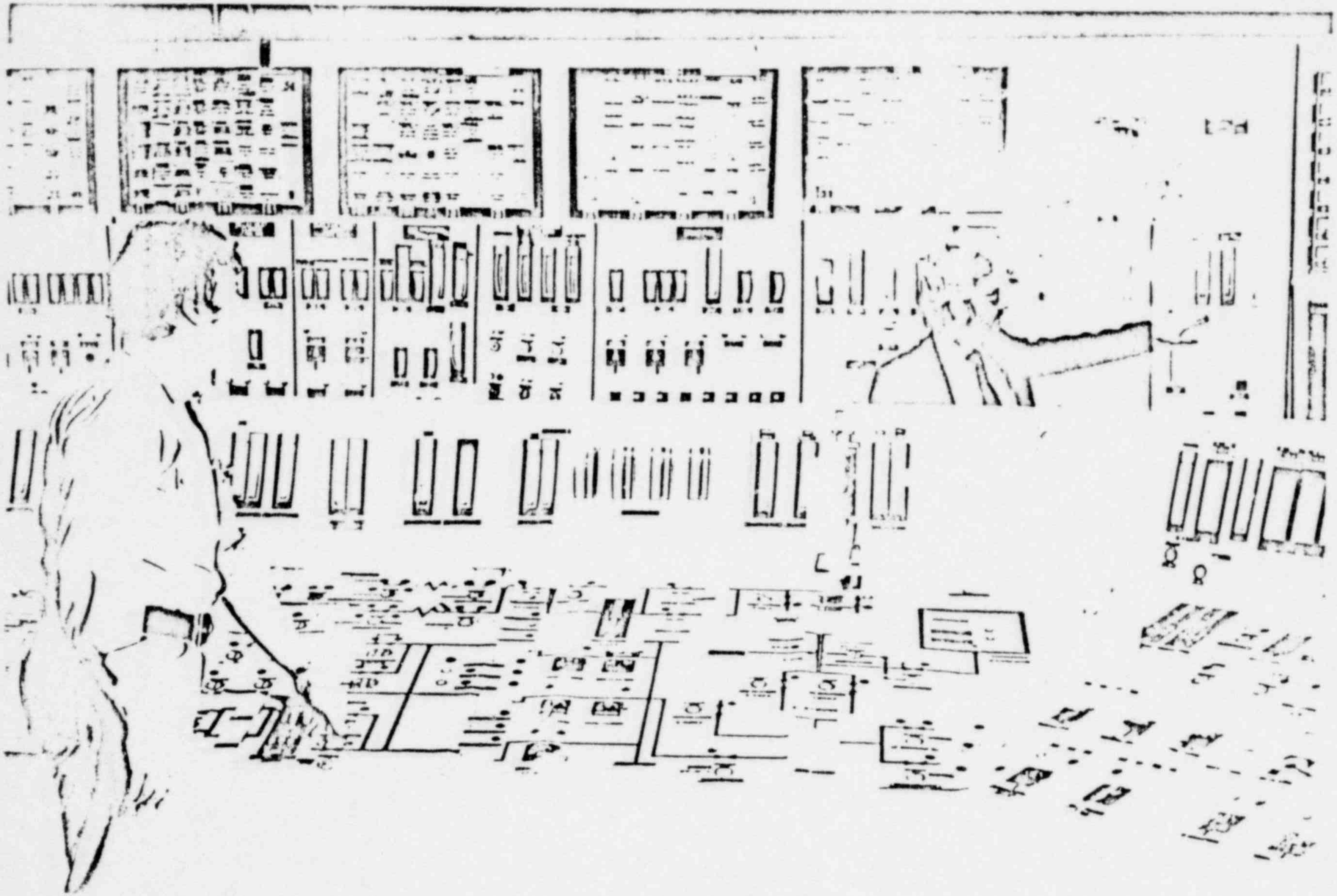


Figure — Example of [illegible] arrangement layout*

* Operator at left is controlling makeup/[illegible] flow while operator at right is monitoring the flow

POOR ORIGINAL

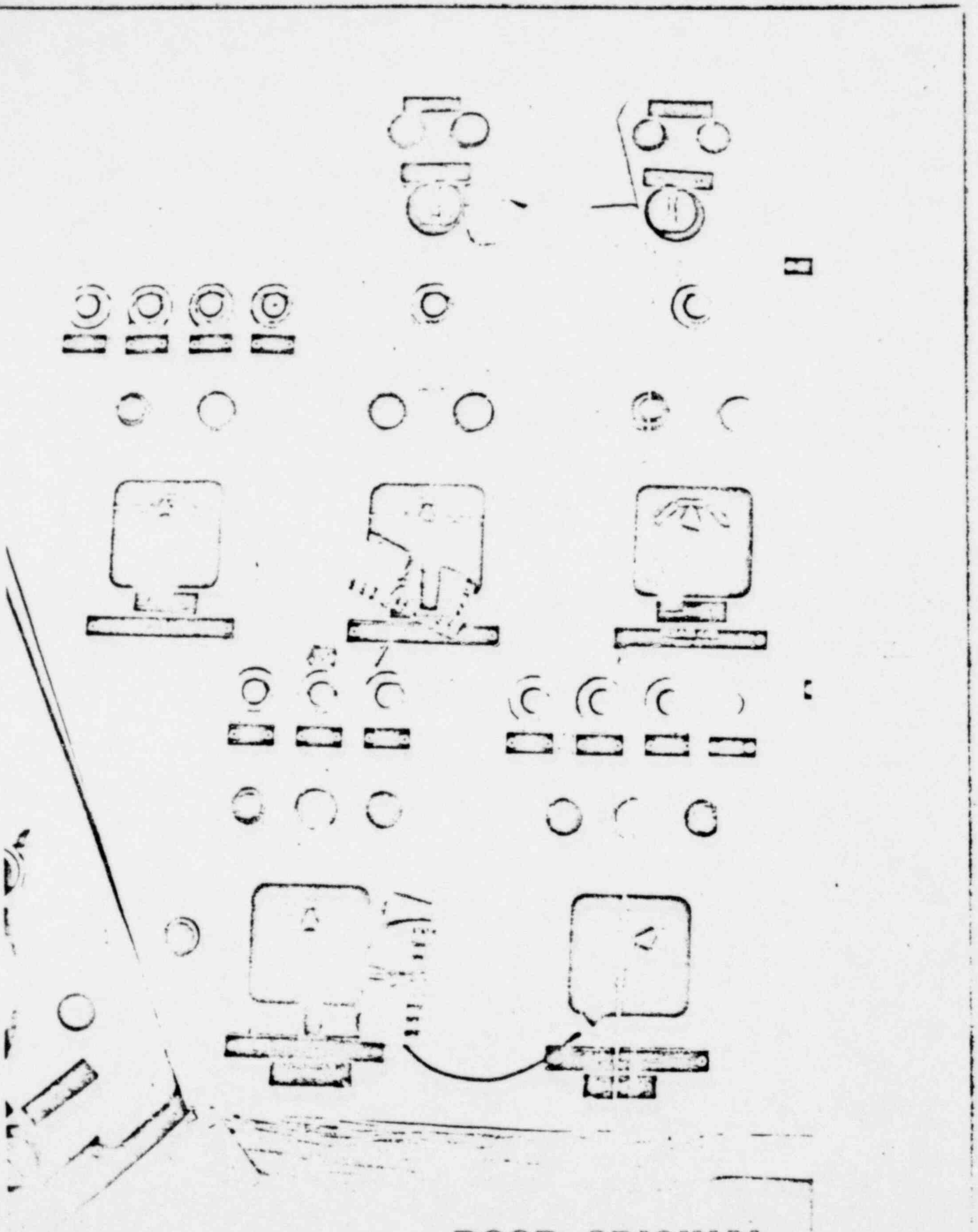


FIGURE — TMI-2 PRESSURIZER HEATER CONTROLS

They found that 18 chart recorders, 10 control stations (10 switches) and 31 switches (most with frequent use) required a reach of 10"-14" greater than that of the fifth percentile male standing erect, necessitating him to bend over the panel to actuate the control or switch.

Control and Display Design

Poor selection of control and displays can impede the performance of tasks assigned to a particular workstation. The Essex evaluation of the TMI-2 control room identified several such deficiencies in the control and display design at TMI. Examples include:

- o 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.
- o Displays have been selected without concern for the nformation 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.
- o Bulbs are difficult to change in pushbuttom/legend light control-indicators --in some cases resulting in shorting out of switch. (Note: CROs stated that the process is so unmanageable that they generally wait until the plant is shut down before attempting to replace burned out bulbs ( )).
- o Auditory displays associated with annunciators are not prioritized to assist the operator in discriminating critical alarms.
- o In some cases for controls having common operating modes (i.e., automatic and manual), control is turned clockwise to place system in manual, in other cases, counterclockwise. See example in Figure ___.

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 perform tasks 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.

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

- o 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.
  - -- There is no displayed indication of flow through the pressurizer relief valve discharge line.
  - -- There is no displayed indication that the system has reached saturation condition.

- o 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 on back panel 10, approximately 20 feet from the RC pump controls on panel 4.

-- 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. See Figure___.

-- RCDT instrumentation is located on panel 8A which is completely outside the main operating area. See Figure___.

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

-- Strip charts are overloaded, in some cases displaying up to 72 separate channels on the same chart.

-- 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").

o 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 ___ for an example of one alarm panel out of some 20 of a similar size.

o Extinguished lights are used as positive indication of system status (e.g., EMOV seated).

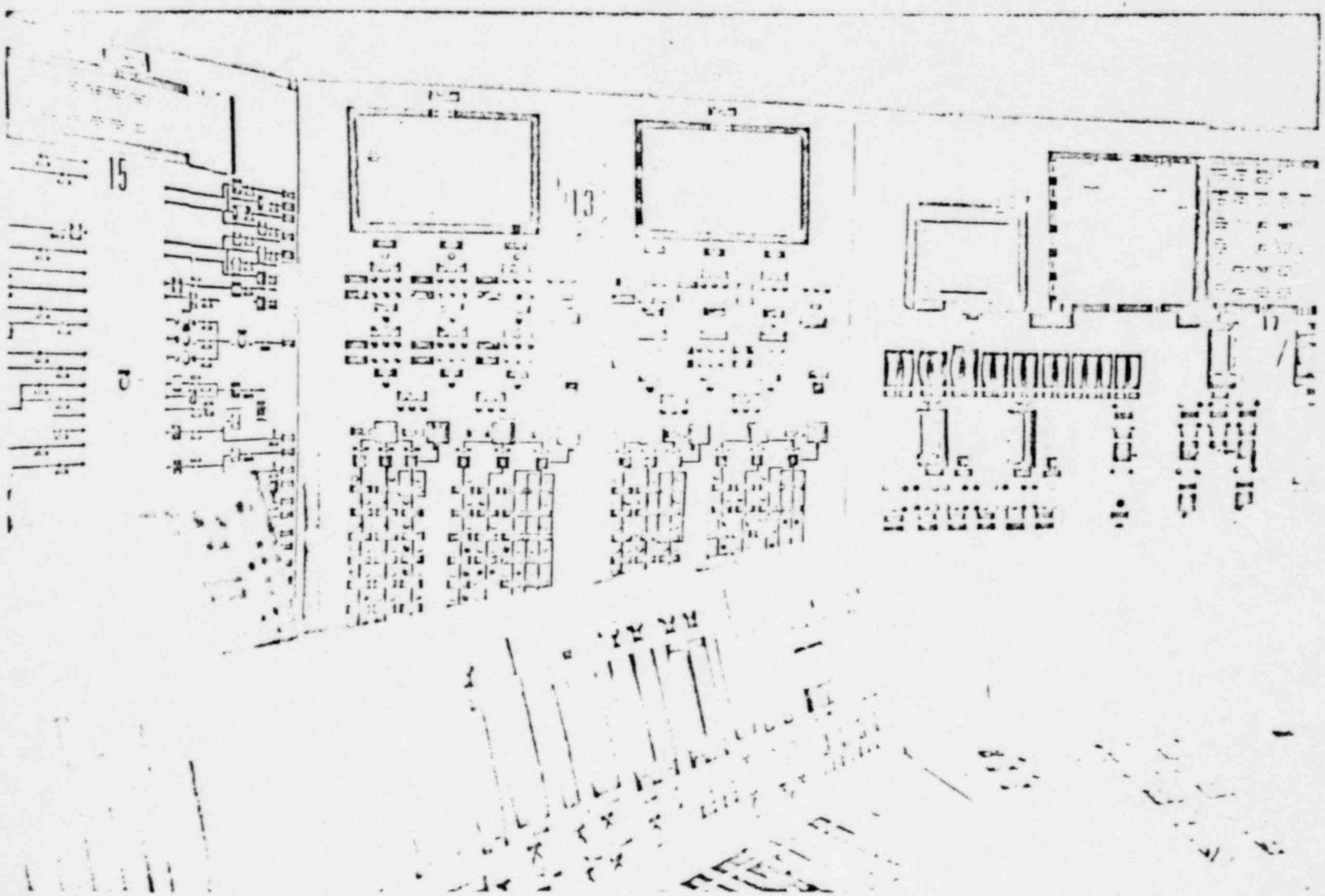


FIGURE —— ESF STATUS INDICATOR BOARD*

*As seen by a 6 foot operator standing at the Engineered Safeguards Actuation Station

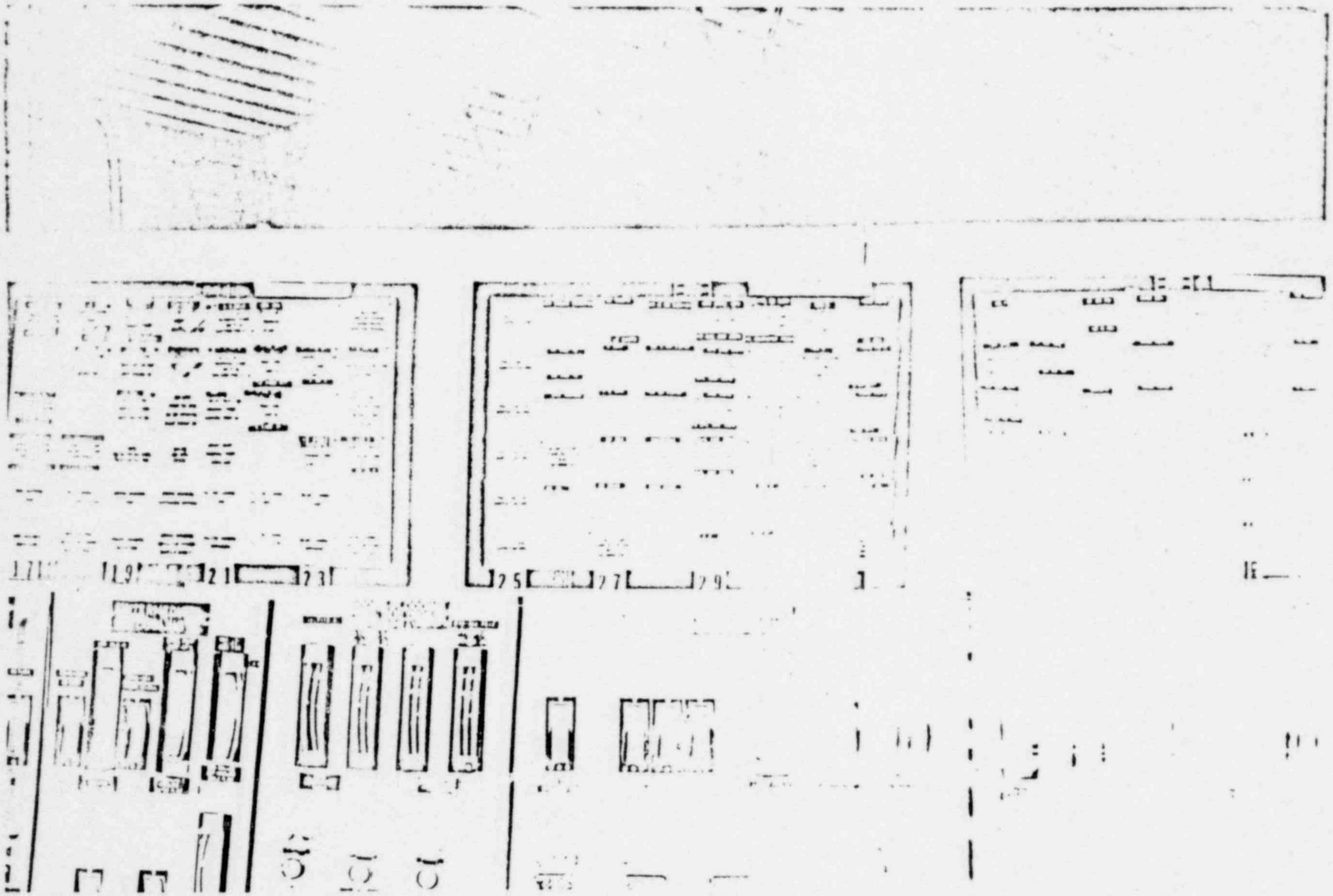


Figure — Type 2 Example of Alarm Panel

- o Displays on several panels were evaluated against standard human engineering criteria. Some 39 deficiencies were found in evaluating three systems on Panel 4.

Parallax

In the TMI-2 CR there is 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 problems will occur. This parallax problem will produce a difference between the actual and the perceived indicator reading. With vertical indicators, parallax will occur when the indicator is placed too high or too low on the panel.

Aside from placing the vertical indicator on the panel so it can be read easily, parallax can be minimized by using a mirrored backing so that the operator can line up the pointer with its scaled image and be confident that his reading is accurate.

The parallax survey done by Essex identified 115 vertical meters in the primary area above the eye level of the fifth percentile male, none of which had mirrored scales.

Obscured Displays

To support primary operations, TMI-2 uses vertical panels behind the benchboard, which contain some 1900 displays, including indicator lights. Depending on their mounting height, displays on the vertical panels can be obscured by the vertical portion of the front benchboard, from viewing by an operator standing at the benchboard.

Essex found a large number of displays below the line of sight of a fifth percentile male standing at the benchboard and looking directly at the vertical panel. Specifically, the following were obscured:

- -- 470 indicator lights
- -- 24 Legend Switches
- -- 3 C/D Units
- -- 3 Vertical Indicators
- -- 1 Stripchart
- -- 1 Dial
- -- 1 Counter

Viewing Distance

While Essex did not have the opportunity to conduct a thorough analysis of display viewing distance there are some strong indications that the TMI-2 control panel presents many opportunities for misreading displays. For example, Three Mile Island-2 presents at least 250 meters located on vertical panels which must be viewed from minimum reading distance is about 10-1/2 feet from the primary benchboard.

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

POOR ORIGINAL

Color Coding

Essex noted that human engineering, growing out of the military and aerospace tradition, is somewhat at odds with the color coding practices evidenced at TMI. The design of the TMI control room sharply reduced the value of color coding to the operator. The number of meanings associated with each color as well as te number of colored lights combine to produce considerable ambiguity in the man/machine communication link.

The color coding deficiencies noted by Essex, including the following:

- A large number of meanings and nomenclature were attached to each color. Specifically, for red-14, for green-11, for amber-11.

- Annunciators, when alarming, intend to draw attention to the window of interest. TMI-2 uses flashing white on a white background. Contrast is particularly bad if several lights are on around the alarming window.

- 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.

The Essex findings are summarized below:

- TMI-2 control room was designed and built witout an appreciation of the needs and limitations of the operator particularly during emergency situation.

- 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.

V. Application of Human Factors Principles by the Nuclear Industry

A. Evaluation of Specific Plants

In order to assess the adequacy of the application of human factors principles to control room (CR) design in the nuclear industry and to compare these CR's with the TMI-2 CR, the Essex Corporation studied two additional plants. The plants chosen for the investigation were Calvert Cliffs 1 and Oconee 2. Both of these plants are pressurized water reactors of approximately the same power output and the same vintage as TMI-2. However, these plants had different architect-engineers and utilities, and the management philosophy utilized in the CR design were different from that employed at TMI-2. At TMI-2, the CR's layout was the responsibility of a senior engineer on the staff of the architect-engineers and all decisions were made by him. On the other hand, Calvert Cliffs 1 and Oconee-1 were designed by a management/operator team. No changes were made to the CR or indicator arrangement without management/operator team approval after all had an opportunity to criticize the change. Furthermore, these two CR's were developed with the aid of a mockup.

The comparison between TMI-2 and the other two plants included a human factors assessment of features such as reach and visibility, and the placement , the readability of meters and indicators in the control rooms.

The ability of the control room operators to easily reach controls and see displays from operational distance is basic to reliable and timely performance. In comparison, the reach survey of the control room indicated that Calvert Cliffs was better than the other two. It had fewer switches and controls beyond the reach of the fifth percentile male standing at the control boards. Oconee was the worst offender with some 22 recorders and 74 switches and controls beyond 10 inches of the reach of the fifth percentile male. In the TMI-2 control room, 18 recorders and 41 switches beyond the 10 inch measurement.

The parallax survey of the three plants focused on vertical meters in the primary area above the eye level of the fifth percentile male. Oconee was better than the other two having only one indicator above the limit while Calvert Cliffs had 75 indicators above the level; however, to minimize the parallax problem, all had mirrored scales and 25 of these had limit switches. TMI-2 had 115 vertical indicators above the eye level, none of which had mirrored scales or limit switches.

Depending on their mounting height, displays on the vertical panels can be obscured by the vertical position portion of the bench board from viewing by an operator standing at the bench. To determine the degree to which displays are obscured, those displays below the sight of a fifth percentile male standing at the bench board looking directly at the vertical panels were counted. Calvert Cliffs and Oconee were better than TMI-2 in this regard. Calvert Cliffs had no obscured displays although there were some displays on back panels and Oconee had only two indicator lights which were obscured. In the Three Mile Island Unit #2 control room, there were 470 indicator lights which were obscured as well as a number of other switches and indicators.

It seems clear that the TMI-2 design gives less attention to the requirements for reach and visibility than either Calvert Cliffs or Oconee 3. Under normal conditions, operators are likely to compensate for design inadequacies such as these. However, under pressure, the operators may take risks with reaching and display reading due to time constraints that could create or compound the problem.

The three plants were also compared for the adequacy of the aids provided for the CRO such as lables, color coding, procedures, and the means to display the procedures provided to assist the operator in running the plant.

The Essex survey of control room labeling found significant and comparable deficiencies in all three plants. For example, labels were left off some components, not attached in any consistent order, and so poorly planned that 34 to 65 percent of the panel components needed backfits.—

For all three plants, the survey study found:

"Deciding where to use colored lights seems to be a matter of tradition rather than reason...The "Christmas Tres" 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 evaluating the color code practice, it was found that all three plants attached several meanings to each color used. In fact, the operator in many cases would have to know the specific component being observed to know how to interpret the color, since in many instances the colors have contradictory meanings.

A summary of the results of the Essex color survey are shown in Table __. As can be seen, the TMI-2 control room attached more meanings to each color than do each of the other two plants.

TABLE ___

NUMBER OF DIFFERENT MEANING & nomenclature

GIVEN TO EACH COLOR

	Red	Green	Amber
Calvert Cliffs	6	4	5
Oconee-3	4	3	4
TMI-2	14	11	11

In summary, the Essex's limited review of the features that aid the operator in reliability and timely performance pointed to Calvert

Cliffs 1 and Oconee 3 as superior in human engineering to TMI-2. Despite their good features, however, Oconee 3 and Calvert Cliffs 1 had some major shortcomings (such as mirror imaging at CC) and a detailed analysis would no doubt uncover more.—

In light of the advancement in human factors in the aerospace industry at the time that the three plants were being designed, it appears that none took advantage of the technology available. The limitations of the Essex study to the two additional nuclear power plants does not permit a conclusive decision as to the state of the nuclear power plant control rooms in general. Therefore, the EPRI study of five additional power plants was reviewed, as well as the Sandia Laboratories analysis of the Zion Nuclear Power Plant.

B. Evaluation of Additional Plants

1. EPRI Report NP-309

In November, 1976, the Electric Power Research Institute (EPRI) published a report, EPRI NP-309, of a 16-month study of five nuclear power plants. EPRI had contracted with the Lockheed Missiles and Space Company, Inc., of Sunnyvale, California, to conduct the study and write the report. The intent of the study was to uncover general problem areas where human factors guidelines could profitably be applied to the next generation of nuclear power plants. A secondary objective was to identify problems within existing power plants where minor modifications at low cost would upgrade the quality of the man-machine interface. A review of this study allows a better evaluation of the TMI-2 control room design in comparison with the state-of-the-art in the nuclear industry and permits a better evaluation of the nuclear power plant CR design.

The EPRI study made the following findings:

a. Control Room Design

The report concluded that insufficient attention is paid to the abilities and limitations of the operator in developing the control room configuration. Serious difficulty in the plants' normal and emergency operations resulted from the poor positioning of controls and instruments on back or remote panels requiring the operators to leave their primary operating station to utilize these controls or monitor these instruments. In addition, the study found illumination evaluation in four of the five plants was inadequate due to glare and reflections on instruments.—

b. Control Board Design

In general, the control board designs were too large requiring too great a visual and control span for the operators and they were not optimized for minimum manning. Control boards had arrays of identical components which are not discriminated into clearly identified panels and subpanels containing related elements. Additionally, closely related controls and displays were often widely separated. Although some mimicing is provided by the designer, there usually is not enough to satisfy the operators so that some operators attempt to modify panels with tape to super-impose mimic logic.

c. Control Placement

Although no data on the physical dimensions of typical control room operators was available, the placement of instruments was too high or too low for convenience. This problem was predominant on the back panels and peripheral consoles. Foot stools and ladders were often required to permit the operators' reach and visual access to these controls and displays.

Placement of controls were found to make them susceptible to accidental activation. Adjacent controls having identical appearance, shape and texture but different functions can result in inadvertent operation. Some controls are placed in a manner which make them suscepible to accidental contact and disturbance from operators and visitors to the control room.

d. Meters

Meters currently utilized in nuclear power plants have a tremendous potential for human factors improvements. The most common problems observed in the five plants examined were improper scale markings in association with scale numerals, selection of scale numeral progressions that were difficult to interpret, parallax problems resulting from placing the meters above or below eye level, meters that fail with the pointer reading in the normal operating band of the scale and glare and reflection from overhead illumination.

The most serious problem observed in all of the plants was lack of meter coding to allow the operator to readily differentiate between normal, marginal and out-of-limits segments of the meter scale.

e. Annunciator-Warning Systems

All five control rooms were provided with an actuation warning system consisting of a horizontal band of hundreds of indicators spanning the uppermost segment of the control board. These systems were too complex and had become a catch-all for a wide variety of qualitative indicators compounding the difficulty to diagnose malfunctions as abnormal situations. When emergencies occurred, the excessively large number of indicators that were illuminated in concert with blaring horns, startle the operator and overload his sensory mechanisms rather than shed light on the problems at hand.

f. Indicator Lights and Color Coding

Indicator reliability is a problem in the nuclear power plant control display. There were a suprising number of burned-out single-lamp indicators at any given time. The replacement of these lamps was difficult and presented problems for the operator. There are examples in the plants of negative indications (the absence of indication to convey information to the operator).

The control room designs under-utilize coding techniques that could help the operator discern plant status and prevent misidentification of control elements. Color codes have not been applied symmetrically and code meanings vary from panel to panel. Present coding of indicators tell the operator whether a valve is closed or open but do not convey any information as to whether the valve should or should not be closed.

g. <u>Labeling</u>

Labels were not placed consistently above or below the panel elements being identified which could result in misidentification of the panel element. Some labels were obscured by adjacent control levers. The best indication of labeling inadequacies is the extensive handmade labeling that operators add to the consoles to clarify identification of given controls or clarify its operation.

2. NUREG 766503, October 1975

The NRC contracted with the Sandia Laboratories to conduct a study of the Zion Nuclear Power Plant. The scope of the study was limited to the human factors problems associated with engineered safety panels in the control room and associated procedures for coping with a LOCA. The Sandia report was published as NUREG-76-6503 in October 1975.

Sandia Laboratories reported that in the Zion situation, as in other nuclear power plants stations we have visited, little attention was paid by the designers to the human engineering practices that have maximized reliable human performance in other complex systems.[1] The report lists the following design features which deviate from sound engineering practices and are regarding as error likely:

---

[1] NUREG-76-5503

- o Poor layout of controls and displays;
- o Poor and inconsistent color philosophy;
- o Too many annunciators;
- o Too many exceptions to the go/no go coding scheme employed for rapid assessment of monitor panel status;
- o Labeling which provides little or no location aid;
- o Misleading labeling due to violation of populational stereotypes; and
- o Insufficient labeling of valves.

It can be seen that the design problems existing at the Zion Plant are similar to those enumerated in the Essex report on TMI-2.

A broader base of investigation might be needed to compare TMI-2 with the state-of-the-art in the nuclear industry in the late 1960's, but from the limited study of Essex of three plants, the five plants studied by EPRI and the study of the Zion plant by Sandia Laboratories, it can be concluded that TMI-2 control room is representative of its contemporary nuclear plants, and that there is a serious human factor problem throughout the nuclear industry.

Human Factors Precursors

Introduction

Prior to March 28, 1979, accident precursors, in the form of reports of reactor instances, Congressional testimony, and correspondence, contained warnings that an accident of the type that occurred at TMI-2 could happen. Another chapter of this report addresses precursors relating to the design and function of the TMI-2 reactor. This section addresses those precursors relating specifically to the "human factors" application in control room design, operator training, emergency procedures and the issue of the man-machine interface.

This discussion and analysis documents the fact that, before the accident, the NRC and the industry had been alerted to the "human factors" problems, many of which existed at TMI-2.

Evaluation of Incidents of Primary Coolant Release from Operating Boiling Water Reactors. WASH-1260

In May 1972, the Atomic Energy Commission appointed a seven member study group[1] under the auspices of the Office of Operations Evaluation to conduct an evaluation of incidents involving the unintentional discharge of significant release of reactor coolant from the primary coolant system operating nuclear power plants. Of 50 reported inadvertent releases on leakages, the study group identified and studied eight. On October 30, 1972, the AEC published the study group report WASH-1260.

The study group made many findings and recommendations, several of which dealt with control room design, manning of the control room, operator training, operating procedures and feedback of operational experience.

Control Room Design

The study group found that insufficient consideration has been given to displaying information on control panels and to the location of controls in relation to each other, particularly when only one operator is required in the control room during operation.[2] The group recommended that the industry develop control panel and control room design standards or guides that address the human engineering aspects of reactor operation during abnormal operating occurrences.[3]

The report discussed the need for further consideration, during the control room design phase, for the instrumentation and controls and their layout, taking into consideration the number of operators, the information required by them to rapidly diagnose and take proper corrective action in response to unusual occurrences, and other human engineering aspects of plant control system design.↑4↓ The study group made specific recommendations addressing the instrumentation needed to provide the operator with the information essential to reaching proper operating decisions during transients and postulated accidents.↑5↓

Control Room Manning

The regulation requires that only one licensed operator be on duty in the control room during operation. In view of this requirement and the fact that more than one licensed operator was on duty in each instance, the study group found that the number of personnel in the control room was not a factor. It was pointed out that the General Electric Company recommended that the power plant be manned by "a shift supervisor on site and two qualified reactor operators in the main control room."↑6↓

The study group recommended that a guide be developed to assist in evaluating the number of reactor operators needed to cope with anticipated transients. They listed the criteria to be taken into account in determining the size of the control room staff. They further recommended that utilities of currently operating plants and applicants for new plants should be required to evaluate their control room manning needs based on the enumerated criteria.

Personnel Training

It was found that the training and experience of the reactor operators in the eight incidents studied appeared to be adequate and met the AEC guides and standards.↑8↓ They also found, however, that the transients studied tended to be aggravated and prolonged by operator actions. The study group felt that one of the causes for this could have been insufficient training.↑9↓

It was recommended that the licensees and applicants should, to the extent practicable, use simulations to train and evaluate operator performance and verify the adequacy of operating procedures. Simulators should also be utilized to evaluate operator performance and adequacy of training during operator licensing.↑10↓

Additionally, the report contained a recommendation that licensees and applicants for licenses be required to submit plans and schedules for training of technicians and repairmen engaged in the testing and maintenance of safety related systems and components.↑11↓

Operating Procedures

During the incidents studied, a number of deviations from operating procedures and technical specifications were experienced.↑12↓ The report indicated that operating procedures were either incomplete or deficient for coping with anticipated transients and although some improvements had been made, further improvements were needed.↑13↓

Feedback of Operational Experience

The report indicated that there was insufficient information available to determine whether incident reports were disseminated between facilities in a timely manner or whether corrective action was taken or planned to minimize the probability of recurrence in the plant where the transient occurred.↑14↓

The study group made a number of recommendations regarding reporting and dissemination of operating experience. It recommended that a system be developed and implemented to fully inform licensees of incidents and unusual occurrences. It further recommended that an incident reporting guide be developed by the AEC, and enumerated specific information to be reported.↑15↓ Finally, it recommended that regulatory policies and procedures be revised to identify more clearly the responsibility for review, decision making, investigation and documentation with respect to incidents and unusual occurrences.↑16↓

On November 28, 1972, the Director of Regulation, in a memorandum to three directors, indicated that the recommendations of WASH-1250 are to be implemented by the appropriate Regulatory Directorates.T17↓

Some actions were taken to implement the recommendations of WASH-1250, including the following:

1. The NRC contracted with Sandia Laboratories to conduct a study of human factors problems of the Zion Nuclear Power Plant.T18↓ This will be discussed in Section VI of this report.
2. The AEC interacted with industry to develop industry standards for control room displays.T19↓ However, to date these standards have not been endorsed by the NRC.
3. Incident and abnormal occurrence reporting requirements underwent evolutionary changes regarding reporting times and information requirements; however, the details and mechanism for utility review of events at other facilities do not appear to have been addressed by the NRC regulations. Furthermore, circumstances surrounding the handling of the 1977 incident of the Davis Besse plant indicate the existing process fell short of the recommendation.T20↓
4. Regarding information available to the operator at a nuclear power plant during and subsequent to a transient or accident, the NRC has written Regulatory Guide 1.97 "Instrumentation to Follow the Course of an Accident." However, as of March 28, 1979 this standard had not been fully implemented in either old

plants or those undergoing licensing review.

5. Reactor simulators have found widespread use. However, the recommendations of WASH-1260 in the area of simulators have not been implemented; i.e., the NRC has virtually no requirements regarding simulators. They are not used to evaluate reactor operators' performance; they are not generally used to verify operating procedures for coping with anticipated transients;T21↓ the NRC examiners seldom observe and evaluate operators on the simulator for their licensing examination, and receive only scant information regarding specific operators' performance. Furthermore, the licensees do not use the simulator as a basis for modifying operating procedures or for evaluating the need for operator training or retraining.

Human Performance March 13, 1975, Memorandum from Hanauer to Commissioner Gilinsky

On March 13, 1975, Dr. Stephen H. Hanauer, Technical Advisor to the Executive Director for Operations of the NRC, initiated a memorandum to Commissioner Gilinsky to which he attached his views on important technical reactor safety issues facing the Commission and reactor safety policy issues.

In his list of technical reactor safety issues, Hanauer addressed the subject of human performance, stating:

"Present designs do not make adequate provision for the limitations of people. Means must be found to improve the performance of the people on whom we depend and to improve the design of equipment so that it is less dependent on human performances...

"The relative roles of human operation and automation (both with and without on-line computers) should be clarified. Criteria are needed regarding allowable computerized safety-related functions and computer hardware and software requirements for safety-related applications."T224

At the time of the TMI-2 accident, no substantive action had been taken by the NRC as a result of this memorandum addressing the human performance issue. No criteria have been developed by the NRC regarding the roles of human operation and automation or computer aids for the operator.

Hearings before the Joint Committee on Atomic Energy, Congress of the United States, February 18, 23, and 24; and March 2 and 4, 1976

Three former General Electric employees, Dale G. Bridenbaugh, Richard B. Hubbard and Gregory C. Minor (BH&M) testified before the

Joint Committee on Atomic Energy citing numerous examples of human factor deficiencies in the nuclear power industry. They pointed to numerous examples of incidents resulting from human error which could have resulted in major accidents. To minimize these errors, they made specific recommendations in the area of control room design, the availability of up-to-date simulators and their utilization for more frequent training of control room operators, the adequacy of operational and maintenance procedures and the training of operators to use these procedures. The NRC, on March 2, 1976, testified before the Joint Committee, rebutting the testimony of BH&M.

The NRC concluded that nuclear reactors are designed to keep the likelihood of operator errors relatively low and took issue with the statement that the human error which has occurred "has seriously jeopardized plant and public safety," because "... the engineered safety features, redundant systems and containment design features have always, singly and in combination, been available to protect plant and public safety."[23]

BH&M testified that improvements in control room design were one method of reducing the likelihood of human error. They noted the complexity of nuclear power plant control rooms, the differences in control room layout throughout the industry and the utilization of mirror images in common control rooms for two nuclear units. They also maintained that "Standardization of control rooms is a vital element of safety..."

The NRC response supported standardization in general but claimed that standardization of control rooms and controls and displays had not been demonstrated to have a significant impact on operator performance.T24↓ The NRC testimony also pointed to studies sponsored by the NRC and industry to evaluate control room design and indicated that the IEEE was developing a standard guide for design and control facilities for control rooms.T25↓

In discussing control room design, the NRC stated that due to the automatic initiation of the engineered safety features, the consequences of an accident are mitigated and the only function of the operator is to assure that these systems function properly and to initiate any action which failed to occur. It therefore concluded that "... the control room design arrangement or operator-process interface is not as critical (or vital) to safety as may be inferred from the February 18, 1976 testimony."T26↓

The NRC did, however, recognize the importance of human engineering principles, control room design standardization and optional arrangement of design to minimize the probability of human error.T27↓

BH&M testified that providing up-to-date simulators and more frequent training of operators is another method of reducing the likelihood of human error. Specifically, they indicated that the present simulators were outdated and did not represent the control philosophy which has evolved over the last ten years. Additionally, they questioned the ability of the operator to remember the accident procedures through time without very frequent update, indicating that retraining periods are too infrequent to keep the operator aware of his special procedures under accident conditions.[28]

In response, the NRC disagreed with the contention that the simulators are outdated for training programs, pointing out that the design philosophy for data display and plant control for operating plants and those in the operating licensing stage of review are very similar to the design philosophy of existing nuclear power plant simulators.[29]

The NRC pointed out that there was no requirement for simulator training and if simulators are used the operator is also trained at the plant for which he seeks his license. The NRC testified that it assures that transition from simulator to plant has been made by the trainee through examination at the facility for which the individual seeks a license.[30]

The NRC agreed that it is unrealistic to expect the operator to remember details of accident procedures over a long period of time. In 1973, the NRC promulgated an amendment to 10CFR 55 by adding an Appendix A, Requalification Programs for Licensed Operators of Production and Utilization Facilities. This program requires periodic review of all abnormal and emergency procedures. The NRC has not conducted any tests nor are they aware of any tests by others to determine how long an operator is able to retain procedural details.[31]

BH&M further testified, "Most human errors in reactor plants result from one of two causes: inadequate procedures or insufficient knowledge of existing procedures."↑32↓ They recommended that the NRC review operational and maintenance procedures to ensure adequacy of both scope and content and that it step up its surveillance of training processes to ensure that the procedures are fully understood and implemented.↑33↓

The NRC responded that guidance in the preparation of procedures is provided to the applicant in Regulatory Guide 1.33 which incorporates industry standards. It pointed out that the utility plans are reviewed to assure compliance with this guide and that NRC inspectors conduct an audit of the detailed procedures to assure their completeness prior to the issuance of an operating license.↑34↓ Review and approval of procedures and amendments thereto is conducted by utility management according to the NRC testimony.↑35↓

The NRC testified that training programs are reviewed to ensure that all personnel receive satisfactory training on all procedures appropriate to their respective job classification and responsibility. Additionally, the requalification program includes lectures on procedures, annual written examinations which include a section on procedures, requirements for licensed individuals to review procedure changes, and an evaluation by supervisors of licensed individuals to assure proficiency in plant procedures.↑36↓

In reviewing the foregoing testimony, the SIG staff believes that it provides a useful insight into the NRC's attitude towards human factors in relation to nuclear reactor safety. In essence, the NRC staff's response is that operators are well trained, there have been no serious accidents, and that automated systems can be depended upon to assure plant and public safety. Other than the fact that there were ongoing studies in the area of human factors application to control room design, the NRC did not develop programs responsive to the BH&M recommendation because the agency maintained human error was not a danger to safe operation of nuclear power plants.

Although the NRC stated that it would implement the recommendations resulting from the aforementioned studies, virtually none of these recommendations for improvement in control room design, operator training and procedure improvement have been implemented by regulations as of March 28, 1979

"Preliminary Human Factors Analysis of Zion Nuclear Power Plant"
NUREG 76-6503, October 1976

The NRC contracted with the Sandia Laboratories to conduct a study of the Zion nuclear plant. The scope of this study was limited to the human factors problems associated with engineered safety panels in the control room and associated procedures for coping with a LOCA. The NRC published the Sandia report in October 1976.↑37↓

The report contained a number of significant conclusions and recommendations for improvement, from a human factors standpoint, in the Zion plant which are equally applicable to other nuclear power plants. It was found that the control panels and other man-machine interfaces deviated from accepted human engineering standards and increased the probability of human error. Improvement in human performance could be achieved by relatively minor and inexpensive changes to the control room, practicing for emergencies, and changes in format and content of written procedures. The report concluded that industry-wide standards covering all aspects of human reliability could serve to materially improve the impact of human performance on system availability and safety.↑38↓

The study found that the major human engineering problems fell into seven major areas.

- o Poor layout of controls and displays
- o Poor and inconsistent color philosophy
- o Too many annunciators
- o Too many exceptions to the go/no go coding scheme employed for rapid assessment of monitor panel status
- o Labeling which provides little or no location aid to controls and displays
- o Misleading labeling due to violation of populational sterotypes
- o Insufficient labeling on valves↑39↓

The report also pointed out that the human factors problems uncovered in the study were not peculiar to the Zion Nuclear Power Plant. Previous visits to other plants by the same investigators revealed similar human factors problems in each plant.T40↓

The report contained the following four recommendations for consideration by the NRC:

1. "Investigate the need for additional human factors data, and develop, on an exploratory basis, a method for acquiring the necessary information. Part of the study should be the determination of what level of information is needed. Whatever level of human error data collection system is deemed necessary, the suggested study should include the procedures and data forms for collecting human performance information.T41↓
2. "Develop the procedures and format for incorporating human performance information (as determined in above item) into the NPRDS.T41↓
3. "Perform a complete human factors analysis at the Zion Plant (that is, expand the present preliminary analysis) to:

    -- Identify all major error-likely situations related to the safeguards systems.
    -- Estimate the relative likelihood of human errors and associated recovery factors for those errors identified as

important by the reliability models.

-- Provide recommendations (based on the above) for improving human reliability at the Zion (and similar) plant(s) and for design of future plants.

-- Develop a procedure for a human factors analysis of nuclear power plants which could be used during all phases of design and development to improve human reliability consistent with other systems engineering requirements.[41]

4. "Upon satisfactory completion of item 3 above, develop industry-wide standards for human engineering of equipment, written procedures, operating methods, and onsite training and practice provisions in nuclear power plants to insure the highest levels of human reliability consistent with other system requirements."[42]

We found that the human factors problems identified in this study are similar to those identified in other studies that predate the TMI-2 accident* and those found in subsequent studies by ESSEX Corp. On August 24, 1976, the Chairman of the NRC, Marcus A. Rowden wrote to the Honorable Virginia H. Knauer, Special Assistant to the President for Consumer Affairs. In his letter Chairman Rowden stated in part, "We believe that human error analyses must not be neglecte' and indeed a special research review group on human error assessments has been established to coordinate and expedite our efforts. Programs are underway to systematize human error analysis and human error data evaluations through contracts, including that with Dr. Swain at Sandia Laboratory. If the results of these programs or actual experience with operating reactors indicate situations in which equipment design or operator interfaces should be improved, we will, in accordance with our statutory responsibilities and our implementing review procedures, require changes to the design or operation of the plants as required."

---

*See Section VIII of this report.

To date, virtually none of the report's recommendations have been implemented. It should be noted that even though the 1976 Sandia report on the Zion plant found that minor inexpensive improvements would enhance plant safety and operations, to our knowledge not one has been implemented, and as of March 28, 1979, none had been planned for implementation.

Plan for Research to Improve the Safety of Light Water Nuclear Power Plants, NUREG-0438

On April 12, 1978, the NRC made its first annual report to Congress on its recommendations for research on improving the safety of light water nuclear power plants. Among the recommendations was one dealing with improved in-plant accident response.

The research recommendation covered operator response during an accident situation, information available to the operator on plant status, operator training and procedures, and human response under stress conditions. It was proposed that the research include not only operators in the control room, but also personnel involved in the testing and maintenance of the plant. It was pointed out that analyses have shown components may be left in an unavailable state by test and maintenance personnel through carelessness, improper training, use of improper procedures or failure to follow procedures.[43]

The proposed research would encompass computerized processing of data, control room layout and data presentation and attention to human factors in the design of annunciators, warning lights and display panels.

This research project was assigned a high priority by the NRC report because of its high potential for risk reduction and its low cost. The report proposed a project to review studies completed and in process on the following topics to establish the need for further research:[44]

- Human error in testing and maintenance.
- Monitoring and diagnostic systems to assist the operator under accident conditions.

- Operating and emergency procedures for responding to accident situations.
- Improved use of simulators in studying operator response to accident situations and for related training.
- Man-machine interface, information presentation, pattern recognition, control-room design, and automatic controls for safety systems.
- Human initiation of accidents.

This research project was scheduled to start up in early FY 1980. The TMI-2 accident reinforced the need for high priority which resulted in accelerating the project initiation to the end of FY 1979.

The SIG staff noted that the purpose of this research project was to identify new areas for research in human factors while ignoring the large body of information being utilized by other industries which could be readily adaptable to the nuclear power plant industry.

1978 Review of Evaluation of the Nuclear Regulatory Commission Safety Research Program, NUREG-0496

In December 1978, the Advisory Committee on Reactor Safeguards sent to the Congress its evaluation of the NRC safety research program. This evaluation recommended research be conducted on a high priority basis in the area of the man-machine interface. Such research would include an examination of the potential for and consequences of human errors. Furthermore, the ACRS recommended exploration of computer-controlled automation in the control room and that control room equipment emphasize diagnostic information that would simplify decision making. The ACRS indicated that along with development of advanced computers and graphic displays for the control room by industry, independent NRC research is necessary, i.e., research to support the "licensing review" of the advanced control room designs and to develop criteria, guides and standards. ACRS also recommended that the NRC conduct a more systematic review and evaluation of operational experiences at U.S. and foreign nuclear power plants.

Analysis of the TMI-2 accident, in our opinion, has highlighted the importance of the application of human factors principles to control room design, operator training and procedures. Although additional research in this area may be justified, the time has come to write standards and modify existing and new power plant control room design, procedures and training programs.

Other Precursors

In addition to the precursors discussed previously, others should be mentioned. The Electric Power Research Institute (EPRI) has sponsored a number of research projects to evaluate the application of human factors in control room design. One such report is EPRI NP-309 of November 1976, which describes a study conducted by the Lockheed Missiles and Space Company, Inc. of Sunnyvale, California. Lockheed evaluated five recently operational nuclear power plants using human engineering expertise and standards developed in other industries.[45]

The report discusses various deficiencies found in the five plants studied. The findings are typical of those in the precursors discussed earlier. These include lack of attention to control room design, poor designs of individual control panels, inappropriate placement of instruments and controls, unreliable indicators and use of negative indications, complexity of the annunciator-warning systems, underuse of proven coding techniques and inconsistencies in labeling.

The EPRI report concluded that:

> "As first priority, a detailed set of applicable human factors standards must be developed and industry-wide acceptance should be promoted... In addition to a comprehensive set of standards, a need is perceived for human factors engineering design guides specific to the needs of the nuclear power industry."[46]

Another study "<u>Human Engineering of Nuclear Power Plant Control</u>

Rooms and its Effects on Operator Performance," prepared for the NRC by the Aerospace Corporation of El Segundo, California, was published during February 1977 as Aerospace Report No. ATR-77(2815)-1. The Aerospace Corporation evaluated the effects of human engineering on operator performance in the control room. It specifically examined what Aerospace considered to be the three general groups of factors which influence operator performance in fulfilling their responsibilities in the control room:T47↓

- o Control Room and Control System Design
- o Operator Characteristics
- o Job Performance Guides

In conducting its study, the Aerospace Corporation's study group visited ten facilities containing eighteen control rooms and three control room simulators.T48↓

As a result of its study, Aerospace Corporation made three recommendations to NRC:

1. Development of a Regulatory Guide to provide directions to the utilities in human engineering of control rooms; the guide should be designed to encourage an increased rate of incorporation of advanced control and display concepts.T49↓
2. A thorough analysis of LER data on personnel errors to establish meaningful cross-correlation of results of plant status in

relation to licensing at the time of the accident, operational power levels, equipment and control elements involved, event significance, radioactivity release, etc.T50↓

3. A detailed study of the programmed malfunctions provided in the software routines of current simulators to determine whether they have the capability to provide student operators with the level of training needed to minimize operator errors under conditions of severe stress. It was further recommended that the study evaluate the effectiveness of operator training in severe accidents on a simulator that does not realistically model the control board layout of the plant for which the operator is to be licensed or relicensed.T51↓

The SIG staff found that virtually no action had been taken by the NRC to implement these recommendations.

↑1↓ WASH-1260, Appendix A

↑2↓ WASH-1260, page 43

↑3↓ WASH-1260, page 44

↑4↓ WASH-1250, page 29

↑5↓ WASH-1260, page 43

↑6↓ WASH-1260, page 27

↑7↓ WASH-1260, page 44

↑8↓ WASH-1260, page 28

↑9↓ WASH-1260, page 28

↑10↓ WASH-1260, page 43

↑11↓ WASH-1260, page 42

↑12↓ WASH-1260, page 28

↑13↓ WASH-1260, page 43

↑14↓ WASH-1260, page 44

↑15↓ WASH-1260, page 45

↑16↓ WASH-1260, page 46

↑17↓ Memorandum from L. M. Muntzing, Director of Regulation, F. E. Kruesi, Director of Regulatory Operations, J.F. O'Leary, Director of Licensing, and L. Rogers, Director of Regulatory Standards. Subject: Implementation of Recommendations of the Regulatory Study Group, dated November 26, 1972.

↑18↓ NUREG 76-6503, October 1976

↑19↓ IEEE 566

↑20↓ Reference precursor section in S16

↑21↓

↑22↓ Page 2 of Attachment "Technical Issues..." to Memorandum from S. H. Hanauer, Technical Advisor EDO, NRC to Commissioner Gilinsky, NRC, Subject Technical Issues, dated March 13, 1975.

↑23↓ Report of J.C. on AEC Hearing, page 913

↑24↓ Report JC on AEC Hearing, page 929

↑25↓ Report JC on AEC Hearing, page 930

↑26↓ Report JC on AEC Hearing, page 930

↑27↓ Report JC on AEC Hearing, page 930

↑28↓ Report JC on AEC Hearing, page 554

↑29↓ Report JC on AEC Hearing, page 934

↑30↓ Report JC on AEC Hearing, page 935

↑31↓ Report JC on AEC Hearing, page 936

↑32↓ Report JC on AEC Hearing, page 555

↑33↓ Report JC on AEC Hearing, page 556

↑34↓ Report JC on AEC Hearing, page 937

↑35↓ Report JC on AEC Hearing, page 938

↑36↓ Report JC on AEC Hearing, page 938

↑37↓ U.S. Nuclear Regulatory Commission: Preliminary Human Factors Analysis of Zion Nuclear Power Plant (NUREG 76-6503), October 1975

↑38↓ NUREG 76-6503, page 3

↑39↓ NUREG 76-6503, page 6

↑40↓ NUREG 76-6503, page 1

↑41↓ NUREG 76-6503, page 10

↑42↓ NUREG 76-6503, page 11

↑43↓ NUREG-0438, page 23

↑44↓ NUREG-0438, page 42

↑45↓ EPRI-NP-309, page v.

↑46↓ EPRI-NP-309, pages 1-28

↑47↓ ATR-77(2815), page 1-1

↑48↓ ATR=77(2815)-1, Table 1-1

↑49↓ ATR-77(2815)-1, page 7-13

↑50↓ ATR-77(2815)-1, page 7-14

↑51↓ ATR-77(2815)-1, page 7-15