Progress in Nuclear Energy, Vol. 10, pp. 299-347.
Printed in Great Britain.

0149-1970/82/030299-49$24.50/0

THE HUMAN FACTOR IN NUCLEAR POWER PLANT SAFETY: PROGRESS SINCE THREE MILE ISLAND

STEPHEN H. HANAUER*

8216 Stone Trail Drive, Bethesda, MD 20817, U.S.A.

(*Received 9 February* 1981)

Abstract—Post-Three Mile Island assessments of human factor considerations in nuclear power plant safety are reviewed. The basic ingredients are the capabilities and limitations of people in operation and maintenance activities, and the functional requirements of safe nuclear power plant operation. The roles of the human are to provide for initial equipment functionability and personnel readiness, to minimize the frequency and severity of events that inevitably occur, and to maintain or restore critical safety functions in accident situations. Operations activities to promote these safety roles include qualification and training, procedures, management and information transfer from the plant to the operator. Recent research and operations programs are reviewed.

1. INTRODUCTION

Consideration of the human aspects of nuclear power plant safety did not begin with the Three Mile Island accident. However, it is generally acknowledged that before TMI the entire nuclear enterprise—industry, government, interested public groups—emphasized hardware and neglected people when safety was being considered. In this paper, the post-TMI assessments of the pre-TMI human factors inadequacies are reviewed. A brief discussion is given of the most important aspects of the human capabilities and limitations relevant to nuclear power plant safety. The major portion of this review is a description of the programs now in place and under development to improve the human aspects of nuclear power plant design and operation.

The author of this review has attempted to include the most important programs worldwide, but acknowledges that his experience, and the preponderance of the information available to him, have led him to deal principally with U.S. programs. With a few exceptions, only information available before September 1981 is included.

The role of the human in nuclear power plant safety depends on the allocation of safety-related control functions between automatic devices and manual actions. In current designs worldwide, immediate actions to shut down the neutron chain reaction, cool the reactor core, and close up the barriers to radioactive releases are taken automatically, whereas later activities to remove the core decay heat are designed to be controlled manually. The safety roles of the human operating crew are therefore:

(1) To provide, in advance, equipment functionability and personnel readiness to perform the automatic and manual safety actions if they are needed;
(2) To operate the plant so as to minimize the frequency and severity of the off-normal events that will inevitably occur;
(3) To monitor the automatic safety actions and perform the manual safety actions needed in off-normal events, by maintaining or restoring critical safety functions.

In order to perform these safety roles, the people must be selected, trained, and qualified, they must have and use procedures, they must be supported by an organization and management, and they must be provided with real-time information regarding plant variables, status and alarms.

2. ANALYSES OF THE THREE MILES ISLAND ACCIDENT

2.1. *Human factors in the accident*

The sequence of events at TMI is widely known; see for example Kemeny *et al.*, 1979 and Rogovin, 1980. It includes equipment failures and human errors in a combination that wrecked the reactor core and frightened the country. Table 1, partly taken from

* The author is a member of the U.S. Nuclear Regulatory Commission staff, but this paper is not a USNRC publication. The USNRC has neither approved nor disapproved its technical content.

Table 1. Human errors in Three Mile Island accident sequence*

(1) (Before the accident). Incorrect valve lineup left both block valves closed and prevented delivery of auxiliary feedwate to steam generators to provide normal shutdown cooling.
(2) (Before the accident). Failure to fix leaky valve in condensate demineralizer; the leak probably let water into th instrument air (as it had on two previous occasions) and initiated the accident.
(3) (Before the accident). Operating at power with a leaking power-operated relief valve, and failing to recognize that thi would obscure identification of a stuck-open valve.
(4) Eight-minute delay in diagnosing failure of delivery of auxiliary feedwater and re-opening block valves.
(5) Delay of 2½ hr in recognizing relief valve stuck open and closing block valve.
(6) Throttling back high-pressure emergency core cooling. Failure to recognize an ongoing loss-of-coolant accident, and thus the need for emergency core cooling.
(7) Failure to recognize symptoms of boiling in primary system and its implications: inadequate core cooling; incorrec interpretation that full pressurizer means full reactor; impaired natural circulation.
(8) Failure to diagnose and act on hydrogen combustion or explosion in containment.

* This material is taken principally from Malone *et al.* (1980).

Malone *et al.* (1980), gives a listing of the events that are principally important for the present review. The role of human misunderstanding and error evidently looms large.

Many analysts found that the plant design and operation showed inadequate consideration of people, their capabilities and limitations. Admittedly using 20/20 hindsight, these analyses discuss shortcomings in (1) selection, qualification, and training of operating people, (2) presentation of needed information to the people, (3) maintenance, operating, and emergency procedures used by the people to perform their duties, and (4) organization and management of the people. Industry and government programs were harshly criticized.

2.2. *The Kemeny Commission*

President Carter appointed a Commission to 'conduct a comprehensive study and investigation' of the TMI accident. The Commission held hearings; its sta conducted technical studies. The report of the Con mission given in Kemeny *et al.* (1979) includ conclusions and recommendations related to huma factors. These are summarized in Table 2. The recon mendations are more detailed than the summary giv in the table; they include actions to be taken b industry and government.

The technical staff assembled by the Presiden Commission reported their analysis in Jaffe *et a* (1979). There are reports on the following iten relevant to this review:

TMI-2 site management.
Selection, training, qualification and licensing Three Mile Island operating personnel.
Control room design and performance.
Technical assessment of operating, abnormal an emergency procedures.
Simulators—training and engineering design

Table 2. Summary of the recommendations of the Kemeny commission related to human factors safety

(1) Organization and management
(1.1) Responsibility and accountability for safe plant operations placed on the licensee.
(1.2) Higher organizational and management standards needed to assure utility competence.
(1.3) Each utility should have a separate safety group that reports to high-level management.

(2) Operations personnel
(2.1) Important to attract highly qualified people; pay scales should be high enough.
(2.2) Upgrade NRC licensing functions for operating people.
(2.3) Establish accredited training institutions.
(2.4) Utilities must give plant-specific training initially and continuously.
(2.5) Research and development is needed on improving training simulators.

(3) Man–machine interface
(3.1) Operating people should have the critical information they need to cope with accidents, clearly displayed and continuously recorded.

(4) Procedures
(4.1) Substantially more attention and care must be devoted to the writing, reviewing, and monitoring of plant procedur

The recommendations of the staff, reported in Jaffe *et al.* (1979) are evidently the foundation for, and provide the detailed basis for, the Commission's recommendations. They add up to a revolution in nuclear power plant design and operation, in which the concerns for the people important to safety are to be elevated to an equivalence with hardware safety evaluation.

2.3. *Special Inquiry Group*

A few months after the Three Mile Island accident, the NRC contracted with a Washington law firm to direct an inquiry into the accident, study its implications for other nuclear power plants, and identify areas where further study is recommended. Rogovin *et al.* (1980) report the results of the study. The study directors were outsiders (non-NRC employees), as were the members of the review panels. The full-time technical staff of the study were NRC employees working under the direction of these independent outsiders.

Rogovin *et al.* (1980) give a narrative of the accident and 80 pages of conclusions and recommendations under 12 headings. This Special Inquiry Group concluded that: 'The principal deficiencies in commercial reactor safety today are not hardware problems, they are management problems . . . many nuclear plants are probably operated by management that has failed to make certain that enough properly trained operators and qualified engineers are available. . . . The NRC, for its part, has virtually ignored the critical areas of operating training, human factors engineering, utility management and technical qualifications.' In Volume II, Part 2, Section E, Rogovin *et al.* (1980) give a review of the human factor aspects of the accident, including analyses of the human errors and detailed recommendations. This is based on the work of Malone *et al.* (1980), who studied the accident in detail from this standpoint. 'The primary issue addressed was to what extent was operator performance, or lack of performance, directly caused or influenced by equipment design features, information availability and usability, emergency procedures, selecting and training and control room manning levels.'

The Special Inquiry Group, based on the work of Malone *et al.* (1980), attributed the operator errors to 'important factors not within the operators' control . . . These include inadequate training, poor operator procedures, a lack of diagnostic skill on the part of the entire site management groups, misleading instrumentation, plant deficiencies and poor control room design.'

The author of this review has seen nothing to convince him that this evaluation isn't right on the mark.

2.4. *Other evaluations*

It was inevitable that an accident with the public visibility and economic consequences of Three Mile Island should be analyzed by a large number of organizations. In developing its post-TMI Action Plan, the NRC (1980a) provided cross-reference tables to seven studies, giving item-by-item comparison of the recommendations of these studies with the components of the Action Plan. These cross-references in NRC (1980a, Volume 2) show substantial overlap; that is, similar recommendations were made by the different evaluation groups. The Action Plan, analyzed in Section 4 of this review, is thus a coordinated response to the lessons of the TMI accident, as embodied in these seven studies. There are many more studies of the TMI accident than the seven included in NRC (1980a), but this reviewer knows of no really different and significant technical recommendations in the human factors area to have been brought forth that are not in Action Plan matrices in NRC (1980a), Volume 2.

3. HUMAN CAPABILITIES AND LIMITATIONS

3.1. *Human error*

The safety-related actions required in a nuclear power plant are carried out by machines and people. Allocations of such actions to automatic control (machines) or manual control (people) has in the past been performed by the equipment designers. Whether this allocation has resulted in optimum present designs would be a subject for useful further investigation. For plants already built, changing the allocation from machine to human or human to machine would involve potentially expensive redesign of machines and potentially distracting revision of human training and procedures. NRC (1981a) recommends, for plants already in operation, establishing clearly what the allocation actually is in the plant. Decisions about any changes that may be essential can then be made. For plants still in the design phase, NRC (1981a) sets forth a systems review that includes analysis leading to allocation of safety-related functions to people and machines.

Malone *et al.* (1980) discuss human error:

> 'While the phrase "human error" covers a multitude of sins, it also results from a multitude of causes, not all of which imply a deficiency on the part of the operator. Human errors result from a variety of causes including: the operator himself; conditions

under which he is operating; design of equiment and information required for the performance of tasks; design of procedures which support the completion of task sequences; and training. Specific factors in the incidence of human error in each of these areas are as follows:

Operator factors in human error incidence:
fatigue,
disorientation,
distraction,
motivation,
forgetfulness,
confusion,
expectancy or set,
psychological stress,
inadequate reasoning/problem solving capability,
inadequate skill levels,
inadequate knowledge.

Operational factors in human error incidence:
time constraints,
interfering activities,
poor communications,
excessive workloads,
environmental stress (noise levels, lighting levels, temperature, etc.).

Design factors in human error incidence:
controls/display location,
control/display arrangement,
control/display identification or coding,
control/display operation or response,
information availability,
information readability,
availability of feedback information.

Procedural factors in human error incidence:
erroneous instructions or directives
incomplete or inconsistent instructions,
confusing directives.

Training factors in human error incidence:
inadequate knowledge training,
inadequate skill training.'

3.2. *Human reliability*

The basic problem to be treated in human factors associated with nuclear power plant safety is that of correct action by the person or persons involved. This is conventionally evaluated as human action reliability. Reliability connotes a quantity that characterizes the probability of the correct action occurring. This is studied as 'human reliability', whose practitioners estimate the probabilities of various kinds of human errors and failures in a matrix that places such human errors in the context of nuclear power plant operation and safety. Relevant studies involve data on human performance and reliability, together with models of human behavior, to be used in conjunction with the data in making such predictions. The users of this information include (1) organizations performing probabilistic risk assessments, and (2) organizations developing regulatory requirements.

However, for designers and operators (and government regulators), human reliability transcends estimates of a probability. In the present state of the art, the adequacy of human factors in a given plant is not evaluated by calculating one or more probabilities and comparing with acceptability criteria for probabilities. Instead of this ideal, perhaps realizable in the future, we presently evaluate human performance factors for the plant in question. That is, we look directly at the qualification of personnel, adequacy of procedures, presentation of information, and so forth, without any intermediary probability calculation. This can be done usefully without any modeling at all, probabilistic or otherwise, using empirical knowledge of features that enhance human performance. A more structured approach involves use of a model of human behavior to organize the data and their application.

3.3. *Human function in the man–machine system*

A model of human function in the man–machine system context was given by Rasmussen (1979). He states:

> '*Man as a system component.* Design of systems depends on descriptions of man and machines which are compatible in structure and concepts. For automated systems, information processing concepts are natural choices for integrated *functional design.* Functional properties of man depend, however, on emotional features of work situation.
>
> '*System as man's work environment.* Consideration during design of *subjective values and preferences* demands a description of work situation in psychological terms, relating features of the situation to subjective values and emotional states.
>
> 'Two separate descriptions are then needed for compatability with engineering and psychology. Parameters and variables suitable for description of their interaction must be found. Descriptions of human mental functions typically depend on situation analysis and information process models. Descriptions of subjective values and preferences typically depend on factor and scaling analysis and emotional state models.'

In Fig. 1, Rasmussen (1979) shows a model of the human data-processing and actions. He identifies

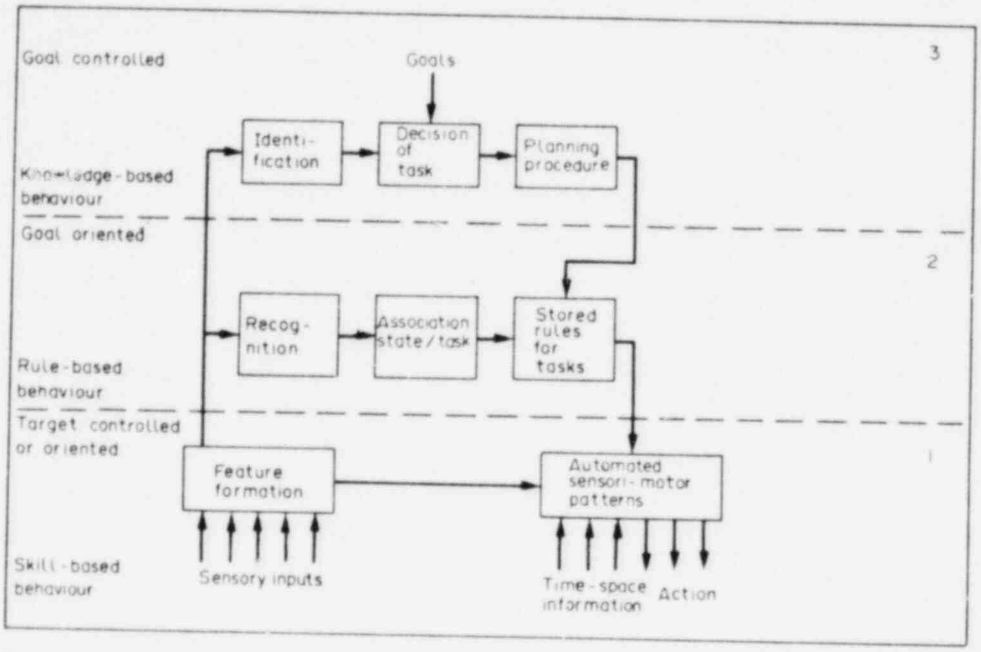

Fig. 1. Schematic illustration of different categories of human data processing. From Rasmussen (1979).

three levels at which human data processing takes place and the types of models which can be used to describe the data processing:

Level (3) Heuristic problem solving strategies; artificial intelligence models.

Level (2) Natural language models; decision tables; associative nets; fuzzy sets.

Level (1) Control theoretic models; bandwidth-gain-descriptions; sampling and queueing theory.

'The output of a human data processor in interaction with a physical system always consists of actions, i.e. changes of the spatial arrangements of things, i.e. the body and external objects. Actions have extensions in time, and decompositions of a current activity into a sequence of actions can be done in many ways. . . .

'This is the first trick for coping with complexity: temporal integration of the interaction of body and environment into behavioral units serving familiar intentions with transfer of control to the high capacity subconscious system; level 1.

'To cope with less familiar situations, a sequence of such actions must be controlled by a conscious linking together of a sequence of proper intentions which then can activate the related actions. In the following discussion, a sequence of intentions and actions designed to bring the environment into a specified state is called a *procedure*. Such a procedure generally contains a sequence of statements of system states separated by specification of actions which will bring the system into the next state. A procedure implicitly contains elements of a model of the physical function of the system in that it specifies the relation between events induced by human actions and the consequent state of the system, which is then related to the next action of the procedure. However, it is a very rudimentary model, linked to a restricted flow of events which are valid under special conditions and purposes.

'The procedure used in a specific man-machine interaction can be based on a stored set of *rules* which are empirically collected during previous occasions and thereafter selected and stored as successful sequences; or they can be generated by some other person and prescribed in the form of work *instructions*. In both cases, we are in the domain of stereotyped, *rule-controlled* performance, level 2.

'In new situations when appropriate procedures have not yet evolved or cannot be composed of familiar subsequences, the task must be accomplished by *goal-controlled* performance, i.e. the proper sequence must be selected from trial and error or based on causal functional mental operations.' Reasoning of this type is at level 3.

The relevance of Rasmussen's model to nuclear power plant operation is generally accepted. Memorization of 'immediate action procedures' and simulator training are intended to form the basis for level 1 response. With the written procedures, they also provide for level 2. Provision for level 3 is the understanding by the operator of the processes in the plant, and is the product of the people's intelligence, education and training.

Human errors, therefore, are the result of incorrect functioning of the human data processor at one, or more, of the levels of response. If the human error rate is unacceptable, improvements are sought appropriate to the level at which the error occurred.

Malone *et al.* (1980) give a detailed listing of the many studies carried out over 30 yr related to human factors and human errors. This work was directed principally at military and aerospace problems. Other compendia of non-nuclear human factors information are given by Price *et al.* (1980b), IEAL (1980) and IEEE (1980). The last two emphasize technology transfer and potential nuclear power plant applications. Hagan and Mays (1981) have reviewed some relevant information of the same kind as directly applicable to nuclear plants. Mallory *et al.* (1980) give a compendium of guidelines proposed for nuclear power plant control rooms, based on the material previously developed for military and aerospace problems. Seminara and his co-workers (1977, 1979a, 1979b, 1980a, 1980b) also give bibliographies related to control rooms. Other recent, shorter bibliographies include those in Fuchs, Engelschall and Imlay (1981a) for procedures, and Price *et al.* (1980a) for staffing. Swain and Guttman (1980) provide an extensive bibliography related to human reliability; that is, the analysis of human error rates or probabilities.

3.4. *Analysis of human error rate*

A methodology for analyzing human errors in nuclear power plants is given in Swain and Guttman (1980). This work is based on the earlier work of these authors and others in the Reactor Safety Study (WASH-1400, 1975) and many other studies. The authors give as its purpose 'to furnish methods, models, and estimated human error probabilities (HEPs) to enable competent analysts to make quantitative or qualitative assessments of ocurrences of human errors in nuclear power plants that affect the availability of operational reliability of engineered safety systems and components. A second purpose of the handbook is to show the user how to recognize error-likely equipment design, operating policies and practices, written procedures, and other human factor problems so that improvements can be considered.'

Swain and Guttman (1980) describe the 'Sandia Human Reliability Model':

> 'THERP (Technique for Human Error Rate Prediction) is a method to predict human error rates (i.e., human error probabilities) and so evaluate the degradation of a man-machine system likely to be caused by human errors alone or in connection with functioning equipment, operational procedures and practices, or other system and human characteristics that influence system behavior.'

Human error can involve a person's action initiating an event sequence, or a person's failure to act when needed. The context of such failures is the *event tree* of WASH-1400 (1975). For each initiating event, many sequences can ensue, depending upon the actions of people and machinery. The analyst lists all the actions or functions or systems important to the outcome of the event sequences. The tree can be organized in terms of any of these; which to use depends on the needs of the analysis. As an example, 'plant transient' is an initiating event and 'reactivity control', 'reactor primary system coolant inventory', 'heat removal from primary system', 'containment isolation' are some of the functions important to the outcome. Some of the possible outcomes are 'core remains cooled', 'core releases gap activity', 'core melts with containment intact', 'containment valve leaks'.

Human error or equipment failure can initiate the transient; likewise, function, system, or action success or failure depends on humans and machines. THERP enables the analyst to estimate the propensity for human error to contribute to the likelihood of the various event sequences, and thus to evaluate the role of human error in nuclear power plant safety.

The steps in THERP are given by Swain and Guttman as follows:

(1) Define appropriate system failure(s). These are the system functions which may be influenced by human errors and for which error probabilities are to be estimated.

(2) List and analyze the related human operations. This step is the task analysis (described in Section 4) that considers the performance shaping factors in Section 3.

(3) Estimate the relevant error probabilities.

(4) Estimate the effects of human errors on the system failure events of interest. This step usually involves integration of the human reliability analysis with a system reliability analysis.

(5) Recommend changes to the system and calculate new system failure probabilities. (The procedure is iterative.)

The above five steps typify the use of human error analysis as a tool in system design. For assessments only, Step 5 is not required.

The following parameters are estimated by THERP:

(1) *Task Reliability*—the probability that it will be completed successfully within some allotted period of time.
(2) *Error Correction*—the probability of detecting and correcting incorrect task performance in time to avoid any undesirable consequences.
(3) *Task Effects*—the probability that incorrect and uncorrected task performance will result in undesirable consequences.
(4) *Importance of Effects*—this is often a value judgement.

THERP is used to generate quantitative estimates of the first three parameters based on the dependences among human performances, equipment performance, other system events, and outside influences. Thus, estimates of human error probabilities for all but an initiating task represent conditional probabilities.

It is evident from the foregoing that a key to the analysis of human error is the resolution of system (function, action) operation into equipment operation and human operation. 'System failure' in Step 1 above determines the course of the event sequence. In the 'plant transient' example given earlier, the 'reactivity control' function includes the 'chemical volume control system (CVCS)' which, among other things, can be used to add boron to the primary coolant water to reduce reactivity. 'Failure' of the CVCS means that the boron is not injected with the rate, quantity, and timing needed to provide the reactivity control in the event sequence under consideration. Such 'failure' can arise from equipment inadequacies (design inadequate, component fails, power not available) or from human errors (failure to initiate, turn off, mismanipulation of controls).

Fault trees are used to investigate the topology of system failures. (Other methods are available). The components of system success and failure are the adequate and inadequate operation of the equipment and human tasks necessary to achieving system success. In the complex and redundant safety-related systems of nuclear power plants, the fault trees are correspondingly complex. Human error analysis requires consideration of each human task on the tree.

Although we have several sets of nuclear power plant fault trees, most of them do not explicitly include the full set of human tasks, so we do not yet have a detailed job and task analysis for the control-room operating staff. We do not even have task information on such related jobs as maintenance, surveillance, testing, and operations outside the control room. Presumably, the limiting case of significance to safety is operation during the most severely taxing sequence of events in which the operating crew can mitigate the public safety aspects of the accident. We do not know which event sequence, or which sequences, represent the most severe challenge. Such analysis, sorely needed, would presumably form the information and requirements for all human factor considerations of the operating crew—training, qualifications, procedures, control-room information displays, organization and management. Some portions of job task analysis are given in Malone *et al.* (1980) and Mallory *et al.* (1980); Davis *et al.* (1981) have also reported a task analysis, but at a level so general that the result is an outline of the needed knowledges and skills, rather than a specific list.

INPO (1981) has published a two-volume job/task analysis of the shift supervisor position in nuclear power plants. The purpose was to define the 'real job requirements (i.e. tasks performed) plus the skills and knowledge required for safe and efficient operation of the plant'. The knowledge requirements thus developed are compared by the authors with academic curricula content and with the contents of representative training programs.

This work was a limited special-purpose study of the need for academic education for shift supervisors. A more comprehensive study that includes many operating positions is under way under INPO and U.S. Department of Energy auspices, scheduled for completion in 1982.

Although the INPO analysis may well be useful for input into control room review or procedure development, application of these results outside the original knowledge-training area has not yet been analyzed.

The NRC guidelines for control room human factors reviews (NRC, 1981a, 1981d, 1981c) and emergency operating procedures development (NRC, 1981c) require use of task analysis results in performing human factors analysis.

Development of human performance models is a widespread activity. Swain and Guttman (1980) review the literature before 1980. Some additional recent unpublished discussions and presentations are summarized below by the author of this review.

(1) Human behavior in nuclear power plants can be divided into (a) known or foreseen events and sequences, in which human errors can occur, and (b) unknown and unforeseen events and sequences that must be analyzed in real time by the operating crew. The latter—rare events—call for a different order of knowledge and understanding than those foreseen and prepared for with procedures and training.

Therefore, selection, training, procedures and equipment design should take into account the importance of solving unforeseen kinds of problems. This includes methods of information display, analysis and decision making not currently included in training and procedures, and also training in coping with stress (see below).

(2) The stresses of coping with unforeseen or dangerous event sequences, or sequences which appear to be dangerous, are performance shaping factors that must be included in human performance levels. The qualitative aspects of performance under stress and the counter-productive potential responses (rigidity, regression, etc.) must be considered; training, procedures and equipment should be forgiving of such actions to the extent practical. Selection of personnel should include evaluation of performance under stress.

(3) THERP is an input–output model dependent on data or expert prediction of error probability under the given conditions (task, stress, etc.). For the most important tasks, in rare sequences, data are sparse or nonexistent and estimates are necessarily suspect. More detailed models, under development, analyze the space between input and output. This enables more structured estimation of failure probability and also helps to guide designers, trainers and procedure-writers where to put their resources.

(4) More and better data are needed on human performance and reliability, particularly for knowledge-based activity. But statistically significant input–output data are not going to be obtained for the rare, most serious events. Therefore, we must learn all we can from the event data we do get, must get the maximum information from nuclear plant simulation and from non-nuclear data, and must develop models to improve our understanding and application of the data we can obtain.

It seems evident to the author of this review that humans have limitations in responding at all levels of data processing (Fig. 1). Some of these are inherent limits of human capability; others can be improved by training and working environment (data presentation, procedure usability, etc.) at a cost.

Resources are required to develop better procedures or install improved instrument displays. Upgrading qualifications and training takes valuable time and attention and decreases the available manpower pool. Overtraining leads to diminishing returns or even decreased safety. The possibility of tradeoffs and the necessity for realistic cost–benefit–risk studies are evident; but only with the technological basis—largely missing today—can we make such decisions scientifically, and improve on today's intuition.

4. HUMAN FACTORS IMPROVEMENTS IN THE NRC ACTION PLAN

4.1. *General description of the Action Plan*

The Action Plan was developed by the NRC (1980a) to bring together all the recommendations for changes as a consequence of the lessons of Three Mile Island. The objective of developing the Action Plan was to respond responsibly to every TMI-related recommendation within the purview of the NRC. This purview includes actions to be taken by the NRC, an agency of the U.S. Government, in its role as (1) establisher of standards and requirements, (2) reviewer and decision maker on licensing applications, (3) inspector of ongoing non-government activities and enforcer of government requirements, and (4) supporter and manager of research to obtain the technical data needed for the other agency functions. The purview of the NRC also extends to its regulation of the nuclear power industry. Many recommendations, and thus many Action Plan items, involve new or revised NRC requirements and new or revised industry actions to meet these requirements.

The table of contents of the Action Plan is given in Table 3. The Action Plan was first synthesized from all the recommendations received. When it was assembled, the mass of work it represented was obviously beyond the resources then believed to be available to NRC and the industry. Both the industry and the NRC worked to assign priorities to the various items, and look for those which, however desirable, could be deferred without an undue impact on public safety. Appendix B of NRC (1980a) gives the rationale and the results of this effort.

Many of the Action Plan items are new or revised requirements. For example, the Action Plan mandates new instrumentation which will result in the addition of approximately 100 new indicators in the control room. Plant owners must attain and demonstrate compliance with them. These requirements have been set forth in a number of documents, not all of them consistent. The current tabulation at the time of writing is that in NRC (1980b). However, it is becoming evident that even this list of required actions is requiring inordinate resources at the operating nuclear power plants and those nearing completion. The NRC staff reported (NRC 1981b) that completing the required extensive plant changes on the schedules in NRC (1980b) would involve repeated plant shutdowns. This results from the optimistic and uncoordi-

Table 3. Contents of the Action Plan*

CHAPTER I—Operational Safety

- (A) Operating personnel
  - (1) Operating personnel and staffing
  - (2) Training and qualification of operating personnel
  - (3) Licensing and requalification of operating personnel
  - (4) Simulator use and development
- (B) Support personnel
  - (1) Management for operations
  - (2) Inspection of operating reactors
- (C) Operating procedures
- (D) Control room design
- (E) Analysis and dissemination of operating experience
- (F) Quality assurance
- (G) Preoperational and low-power testing

CHAPTER II—Siting and Design

- (A) Siting
- (B) Consideration of degraded or melted cores in safety review
- (C) Reliability engineering and risk assessment
- (D) Reactor coolant system relief and safety valves
- (E) System design
  - (1) Auxiliary feedwater system
  - (2) Emergency core cooling system
  - (3) Decay heat removal
  - (4) Containment design
  - (5) Design sensitivity of B&W reactors
  - (6) *In situ* testing of valves
- (F) Instrumentation and controls
- (G) Electrical power
- (H) TMI-2 Cleanup and examination
- (J) General implications of TMI for design and construction activities
  - (1) Vendor inspection program
  - (2) Construction inspection program
  - (3) Management for design and construction
  - (4) Revise deficiency reporting requirements
- (K) Measures to mitigate small-break loss-of-coolant accidents and loss of feedwater accidents

CHAPTER III—Emergency Preparedness and Radiation Effects

- (A) NRC and licensee preparedness
  - (1) Improve licensee emergency preparedness—short term
  - (2) Improving licensee emergency preparedness—long term
  - (3) Improving NRC emergency preparedness
- (B) Emergency preparedness of state and local governments
- (C) Public information
- (D) Radiation protection
  - (1) Radiation source control
  - (2) Public radiation protection improvement
  - (3) Worker radiation protection improvement

CHAPTER IV—Practices and Procedures

- (A) Strengthen enforcement process
- (B) Issuance of instructions and information to licensees

Table 3—*continued*

(C) Extend lessons learned to licensed activities other than power reactors
(D) NRC staff training
(E) Safety decision-making
(F) Financial disincentives to safety
(G) Improve safety rulemaking procedures
(H) NRC participation in the radiation policy council

CHAPTER V—NRC POLICY, ORGANIZATION AND MANAGEMENT

(A) Development of safety policy
(B) Possible elimination of nonsafety responsibilities
(C) Advisory committees
(D) Licensing process
(E) Legislative needs
(F) Organization and management
(G) Consolidation of NRC locations

APPENDIX A—Near-term operating license requirements in the TMI action plan

APPENDIX B—Relative priorities of action items

APPENDIX C—Recommendations and requirements based on IE bulletins and orders and commission orders

APPENDIX D—Glossary

APPENDIX E—Key to references

Comparative table

* From NRC (1980a).

nated completion dates assembled into the Action Plan. Recently, improved co-ordination of requirements for each plant has been undertaken.

4.2. *Action Plan human factors items*

Section 1 of the Action Plan (in Table 3) sets forth the human factors items in the Action Plan. This is an outline of the human factors program today for nuclear power plants in the United States. A few programs not included in the Action Plan are research task being pursued by American and foreign organizations. Sections 5–8 in this paper give technical reviews of the most important human factors operations and research programs and the improvements now under way at the plants. The requirements currently being applied are intended to provide the upgrading in human factors safety shown to be needed by analysis of the Three Mile Island accident. The research programs are aimed at improved future technical knowledge leading to whatever changes in requirements are shown to be needed and validation of requirements not in need of changing.

5. OPERATORS AND OTHER PERSONNEL

5.1. *Introduction*

In this section are summarized the selection, qualification and training of operations personnel, with a brief discussion of non-operations personnel. Programs in these areas were in place before the Three Mile Island accident. However, the reviews following the accident (see Section 2, above) found important weaknesses. Since 1979, programs of regulation and research have been enlarged and redirected.

5.2. *Role of operator*

The mistakes at Three Mile Island (Section 2) have evoked a reconsideration of the role of the human operator in nuclear power plants.

It should be remarked at the outset that 'th operator' is a convenient misnomer. Current U.S. on shift staffing requirements (see Section 6, below include the 10 persons listed in Table 4 (NRC, 1980d This operating crew is augmented as needed wit

Table 4. Minimum staffing requirements for U.S. plants for nuclear power plant emergencies (from NRC (1980d)

Major functional area	Major tasks	Position title or expertise	On shift*	Capability for additions	
				30 min	60 min
Plant operations and assessment of operational aspects		Shift supervisor (SRO)	1	—	—
		Shift foreman (SRO)	1	—	—
		Control room operators (RO)	2	—	—
		Au:iliary operators	2	—	—
Emergency direction and control (emergency coordinator)‡		Shift technical advisor, shift supervisor or designated facility manager	1†	—	—
Notification/ communication§	Notify licensee, state local and federal personnel and maintain communication		1	1	2
Radiological accident assessment and support of operational accident assessment	Emergency operations facility (EOF) director	Senior manager,	—	—	1
	offsite dose assessment	senior health physics (HP) expertise	—	1	
	Offsite surveys		—	2	2
	Onsite (out-of-plant)				
	In-plant surveys	HP technicians	1	1	1
	Chemistry/radio-chemistry	Rad/chem technicians	1	—	1
Plant system, engineering, repair and corrective actions	Technical support	Shift technical advisor	1	—	—
		Core/thermal hydraulics	—	1	
		Electrical	—	—	1
		Mechanical	—	—	1
	Repair and corrective actions	Mechanical maintenance/rad waste operator	1†	—	1
		Electrical maintenance	1†	1	1
		Instrument and control (I&C) technician	—	1	—
Protective actions (in-plant)	Radiation protection: (a) Access control (b) HP coverage for repair, corrective actions, search and rescue first-aid and firefighting (c) Personnel monitoring (d) Dosimetry	HP technicians	2†	2	2
Firefighting	—	—	Fire brigade per technical specifications	Local support	
Rescue operations and first-aid	—	—	2†	Local support	
Site access control and personnel accountability	Security, firefighting communications, personnel accountability	Security personnel	All per security plan		
		Total	10	11	15

* For each unaffected nuclear unit in operation, maintain at least one shift foreman, one control room operator and one auxiliary operator except that units sharing a control room may share a shift foreman if all functions are covered.

† May be provided by shift personnel assigned other functions.

‡ Overall direction of facility response to be assumed by EOF director when all centers are fully manned. Director of minute-to-minute facility operations remains with senior manager in technical support center or control room.

§ May be performed by engineering aide to shift supervisor.

technicians, craftsmen, engineers and managers called in for emergencies. By 'operator' the author means, in particular, the licensed Shift Supervisor, Shift Foreman and Control Room Operators. But the roles of the other team members, in particular the Shift Technical Advisor, are also included as appropriate in this discussion.

Everyone knows what the operator does: he operates. The U.S. Code of Federal Regulations states (10 CFR 55.4):

(d) *Operator* is any individual who manipulates a control of a facility. An individual is deemed to manipulate a control if he directs another to manipulate a control.

(e) *Senior operator* is any individual designated by a facility licensee under Part 50 of this chapter to direct the licensed operators.

An IAEA (1979) Safety Guide says, 'The Control Room Operator is responsible for the manipulations of controls in the control room in accordance with the relevant operating instructions and procedures.'

Wirstad (1981a) and Andersson (1981) give a general analysis of the operator's role, as composed of eight 'Describing Factors' and four 'Steering Factors'. One wonders whether a complete set of specifications of these factors would tell us what the essential safety role of the operator really is.

Another approach to describing the operator's role is through analysis of his tasks. Such a task analysis is given by Davis *et al.* (1981), but the entries are general and categorical. An example is given in Table 5. Here these authors give 'carry out emergency operating procedures', rather than implementing a specific named procedure. The authors recognize this generality. They state (page 2-9):

> 'an element of a particular task for a particular plant might be to "implement emergency procedure XX after recognizing the symptoms of a loss-of-coolant accident" while the associated generic element would be "carry out appropriate actions after recognizing plant conditions requiring implementation of emergency operating procedures".'

These generalized analyses were based on plant-specific data, collected at specific sites, and validated at specific sites. Generic results were derived from the specific data.

The behavior, knowledge and skills required for a generalized task such as the example of Table 5, and the procedure that should be written to accomplish it, are all generalized too. Much insight can be gained from such generalized analysis, but specifics, even specific examples, are not given. Moreover, the task analysis at this level of generality is stripped of all technical content. The tasks, elements, behaviors and training objectives are those of any complex process. Not a word suggests the nuclear power plant.

Mallory *et al.* (1980) give an outline of task analysis procedure aimed principally at control room evaluation. Their Figure 2.5 gives an example of specific information; instrument variables like high containment pressure and potential operator errors are given. But no results are included.

Malone *et al.* (1980) present (their Appendix C) a detailed chronology of the operators' actions during the Three Mile Island accident. The tasks actually performed, and those omitted, are an important specific data sequence ripe for task analysis.

A detailed, but partial, control room task analysis is given by INPO (1981). This initial report precedes a comprehensive job and task analysis underway under the aegis of INPO and the U.S. Department of Energy for many operating positions. The 1981 report is 'a limited study for the special purpose of defining the job of the shift supervisor in terms of the real requirements (i.e., tasks performed, plus the skills and knowledge required of the shift supervisor) for safe and efficient operation of the plant. This effort was intended to outline the body of knowledge, rather than develop an exhaustive list of job knowledges'.

Initially, a series of surveys and interviews was conducted to elicit the tasks actually performed or required of shift supervisors as viewed by the incumbents. Data regarding the attributes of incumbent population were also collected and analyzed. A sample size of 40 out of the 604 shift supervisors in the U.S. was used.

In addition to the tasks as defined by the incumbents, the INPO (1981) analysis includes a detailed analysis of 75 emergency and abnormal conditions presently available from the ongoing long-term program.

A 'jury of experts' selected a total of 300 tasks for detailed analysis out of an estimated total of 1500. The selection was based on importance, difficulty and relative time spent in training, since this partial task analysis was directed specifically at education and training requirements. Table 6 gives a few examples from the list of tasks. The analysis of the 300 tasks was performed by teams of subject matter experts and instructional technologists. The analysis method is summarized in Table 7.

The results of the analysis of individual tasks is a 'menu' of knowledge a shift supervisor requires to perform his job, as defined by the analyzed tasks. Study of this work provides a comprehensive listing ('menu') of the role of the shift supervisor and, by implication, delimits also the role of the operating crew of which he is the leader. Along with his detailed operating tasks ('Start up the reactor coolant waste evaporator') and his emergency tasks ('Determine if indications of core damage are present') are supervisory and leadership items ('Schedule maintenance activities'; 'Direct action of the fire brigade').

Task analysis methods for nuclear operations are also discussed by Andersson *et al.* (1979); the approaches are similar and reference is given to detailed results.

A complementary viewpoint of the role of the operator has been given by Corcoran *et al.* (1980a,

Table 5. Example task analysis results (Task: carry out emergency operating procedures) (From: Davis, Mazour and Zaret (1981)

Elements	Behaviors required	Individual responsible		Training objectives
		RO or SRO	SRO only	
(1) Recognize plant conditions requiring implementation of emergency operating procedurrs	Perceptual processes			Operator should recognize all conditions requiring implementation of emergency operating procedures without reference to plant procedures
	!dentify cues requiring implementation of emergency operating procedures [Note: any one of five (5) senses may identify symptoms]			
	Cognitive processes			
	Determine applicable emergency operating procedure	X		
(2) Recognize automatic actions	Perceptual processes			Operator should recognize automatic actions associated with all plant emergencies ·ithout reference to procedures
	Locate and read indicators and annunciators	X		
	Identify display meanings and relationships	X		
	Cognitive processes			
	Compare and verify indications	X		
(3) Carry immediate operator actions	Perceptual processes			Operator should carry out, for all plant emergency conditions, immediate operator actions without reference to applicable procedures
	Locate and read indicators and annunciators	X		
	Identify display meanings and relationships	X		
	Locate controls	X		
	Identify technical specifications limiting conditions for operations	X		
	Cognitive processes			
	Compare and verify indications	X		
	Coordinate actions of all shift personnel		X	
	Analyze plant conditions	X		
	Maintain good judgement and problem-solving performance under stressful and/or physically hazardous environment	X		
	Establish priorities		X	
	Maintain overall perspec'ive; do *not* become totally involved in a single operation		X	
	Communication processes			
	Inform appropriate personnel	X		
	Direct actions	X		
	Receive verbal reports	X		
	Motor processes			
	Position components (valves, switches, etc.)	X		
	Control system parameters (pressures, levels, etc.)	X		
	Take manual (backup) control of normally automatic functions	X		
	Operate controls		X	

Table 5—*continued*

Elements	Behaviors required	Individual responsible		Training objectives
		RO or SRO	SRO only	
(4) Carry out subsequent operator actions	Perceptual processes			Operator should carry out, through reference to applicable procedures, subsequent operator actions of all emergency operating procesures
	Locate and read indicators and annunciators	X		
	Identify display meaning and relationships	X		
	Locate controls	X		
	Identify technical specifications limiting conditions for operation	X		
	Cognitive processes			
	Maintain good judgement and problem-solving performance under stressful and/or physically hazardous environment	X		
	Compare and verify indications	X		
	Establish priorities		X	
	Coordinate actions		X	
	Maintain overall perspective; do *not* become totally involved in a single operation		X	
	Analyze plant conditions	X		
	Determine additional equipment and/or support required		X	
	Determine steps or procedures required to recover from emergency		X	
	Communication processes			
	Inform personnel	X		
	Direct actions	X		
	Receive verbal reports	X		
	Recall personnel		X	
	Recommend action to appropriate authorities		X	
	Receive advice from STA and other technical personnel		X	
	Maintain written logs/reports	X		
	Motor processes			
	Position components (valves, switches, etc.)	X		
	Control system parameters (pressure, levels, etc.)	X		
	Take manual (backup) control of normally automatic functions	X		
	Operate controls	X		

1980b). They suggest that the safety-related roles for the operator are:

(1) Keep the plant set up so that it will respond properly to disturbances.

(2) Operate the plant so as to minimize the likelihood and severity of event initiators and disturbances, and

(3) Assist in accomplishing safety functions during the event.

The connection with the TMI accident is evident; see for example Section 2 and Table 1 of this review.

A key concept in the recommendations of Corcoran *et al.* (1980a, 1980b) is the *Critical Safety Function*. This is defined by them as,

> 'one or more actions that prevent core melt or minimize radiation releases to the general public. Actions may result from automatic or manual actuation of a system (e.g., reactor protection system generates a trip, operator aligns the shutdown cooling system), from passive system performance (safety injection tanks feed water to the reactor coolant system), or from natural feedback inherent in the plant design (control of reactivity by voiding in the reactor)'.

For one class of plants, Corcoran *et al.* give the 10

Table 6. Tasks analyzed in study from INPO (1981) (this table forms a small sample)

Task no.	Task title	Task no.	Task title
1.1	Establish initial conditions at the operator panel for a reactor startup	124.16	Direct shift personnel actions during major plant evolutions
1.1M	Perform control rod exercise	124.17	Estimate completion times of shift evolutions
1.2	Perform estimating critical position calculations	124.19	Recall which safety limits, safety system settings and limiting operating conditions are addressed by technical specifications
1.2M	Perform control rod programming verification		
1.3M	Perform the full length control rod assembly drop time test	124.20	Apply technical specifications directions for safety limits, safety system settings and limiting conditions for operation
1.4	Perform shutdown margin calculations		
1.4M	Disconnect and connect control rod drive mechanism from control rod	124.25	Monitor plant chemistry to ensure conformance to specifications
1.6	Perform rod group latching and position indication alignment	125.1	Direct emergency response as site emergency coordinator (emergency plan)
1.7	Perform safety group transfer operations between the DC hold and auxiliary power supplies	125.2	Classify emergency events requiring emergency plan implementation
		125.3	Direct action of the fire brigade
1.8	Operate control rods to shape axial power	125.4	Analyze indications to determine that an emergency/abnormal plant event is in progress
1.11	Perform individual rod transfer operations between normal and auxiliary power supplies	125.5	Direct shift personnel actions to ensure plant safety during an emergency/abnormal event
1.12	Perform regulating group transfer operations between the normal and auxiliary power supplies		

Table 7. Task analysis methodology. (From INPO (1981))

(A) Analysis of selected tasks:
   (1) Treat each task from the original survey including write-in tasks and write-in of tools and equipment.
   (2) Treat each task suggested for addition by the writing team.
(B) Construct performance objectives that include conditions (normal, off-normal), actions and standards.
(C) Construct performance steps and performance aids.
(D) Construct tool and equipment lists to include:
(1) Composite list.
(2) Tool and equipment by task statements.
(E) Identify task conditions (normal, off-normal, transient and emergency).
(F) Identify safety and regulatory requirements.
(G) Identify reference documents and training manuals.
(H) Specify methods of instruction.
(I) Write job performance measures and skills, knowledges and abilities.
(J) Identify task clusters across engineering systems.
(K) Compile the original draft and organize the task into a hierarchy for each engineering system.

critical safety functions listed in Table 8. Such a list is not uniquely determined, even for a single plant. Grouping or subdividing functions leads to shorter or longer lists, technically correct also. There are many unpublished examples of such lists. One is given here:

A suggested set of safety functions for Boiling Water Reactors is:

Reactivity.
Reactor Water Level.
Containment.

A suggested set of safety functions for Pressurized Water Reactors is:

Reactivity.
Core Cooling and Inventory.
Primary Pressure.
Heat Sink.
Containment.

The role of the operator during an abnormal or emergency event sequence is to maintain or restore adequate performance of the critical safety functions.

Table 8. Critical safety functions. Example from Corcoran *et al.* (1980b)

Safety functions	Purpose
Reactivity control	Shut reactor down to reduce heat production.
Reactor coolant system inventory control	Maintain a coolant medium around core.
Reactor coolant system pressure control	Maintain the coolant in the proper state.
Core heat removal	Transfer heat from core to a coolant.
Reactor coolant system heat removal	Transfer heat from the core coolant.
Contaimment isolation	Close openings in containment to prevent radiation releases.
Containment temperature and pressure control	Keep from damaging containment and equipment.
Combustible gas control	Remove and redistribute hydrogen to prevent explosion inside containment.
Maintenance of vital auxiliaries	Maintain operability of systems needed to support safety systems.
Indirect radioactivity release control	Contain miscellaneous stored radioactivity to protect public and avoid distracting operators from protection of larger sources.

This has the advantage of not requiring diagnosis of the event sequences or ultimate causes of the observed problems. At the same time that he is controlling the plant to ensure adequate safety functions, the operator will attempt to diagnose the problem and initiate recovery of the plant to normal operation or, if that is impossible, orderly shutdown.

Corcoran *et al.* (1980a) point out that multiple success paths exist to restore safety functions under a wide variety of circumstances.

The role of the operator is summarized by Corcoran *et al.* (1980b) in the 'Quality Operation' goals shown in Table 9.

Pew, Miller and Feeher (1981) have analyzed actual operator decisions during four events that occurred in nuclear plants. For each (of several dozen) decision, they analyze the information, knowledge and alternatives available to the operating crew. The result is a taxonomy of decision making, as well as recommended human factors improvements.

The role of the operators, as perceived by the operators (shift supervisors, etc.) themselves, has been studied by several authors. INPO (1981) includes the results of a questionnaire. N. Morley (private communication) has surveyed operators' perceptions of probabilities and decision criteria. Holmgren (1980) follows the evolution of the operator's perception of the job, from task orientation, through evaluation of malfunctions, to a 'differentiated process feeling', an analytic approach that now includes intuition.

The TMI experience should make us wary of the

Table 9. Quality operation goals and benefits (from Corcoran *et al.* (1980b)

Goals	Benefits
Keep the plant running	Reduces safety function challenges. Reduces plant cycles thus generally increases equipment lifetime. Improved economics. More stable operation. Service to the public.
Shut the plant down when safety may be compromised	Reduces safety function challenges. Reduces probability of serious events. Minimize consequences of events. Positive factor in public acceptance of nuclear power.
Mitigate the consequences of operational transients and accidents	Overall safety enhanced. Minimizes economic losses. Positive factor in public acceptance of nuclear power.
Conduct planned outages safely and efficiently	Increases safety. Improves economics. Reduces radiation exposure to workers.

limits of intuition, as Holmgren (1981) also warns. The INPO (1981) results show a heavy load of knowledge-based tasks in abnormal and emergency situations, with an impressive menu of required knowledge. This is consistent with the views expressed by Corcoran *et al.* (1980a, 1980b) on the essential role of the operator in controlling critical safety functions.

5.3. *Qualification of operators*

The countries having nuclear power plants have varied requirements for the qualifications of operators. Moreover, there have been substantial recent changes in these requirements, made as the result of the TMI accident.

The IAEA (1979) Safety Guide, a pre-TMI document, provides guidance for experience and training of professionals, operators and technicians. In addition, certain positions are to be 'authorized' before they are allowed to perform duties having an immediate bearing on safety.

In most nuclear countries, requirements have been established for at least some members of the operating crew. Licensing of individuals is required in some countries, the positions requiring licensed incumbents also varying from country to country. A recent survey has been conducted by NRC (1981f). CSNI (1981) recently conducted a Specialists Meeting on the subject.

The Swedish program is summarized by Wirstad and Andersson (1980).

In the United States, the current requirements are given by the Code of Federal Regulations (1981), 10 CFR55, augmented by Regulatory Guide 1.8 (NRC, 1975), 'Personnel Qualification and Training', and by additional requirements established since TMI; see Denton (1980) and Table 10.

The current shift staffing of U.S. Plants was established by NRC (1980d) and is given in Table 4. Readiness for severe emergencies dictates the operating shift complement of ten, exclusive of security forces. Of these ten people, two must hold SRO (Senior Reactor Operator) licenses and two, RO (Reactor Operator) licenses. The requirements for these are given in 10CFR55, Regulatory Guide 1.80, and Denton (1980). These people typically have a high school education. For shift supervisors, INPO (1981) found the average education to be 13.0 yr (High School plus [illegible] yr), with 14% having a college degree (5% Associate; [illegible]% Bachelor; 1% Master, 0% Doctor).

Licensed individuals have completed rigorous training programs that include classroom, simulator, and on-the-job components. Annual requalification is required, consisting of refresher training and examinations. Several accredited colleges have joint programs with utility training centers; these training programs have been evaluated as equivalent to 1–2 yr of college education (private communication).

Following completion of the training program, candidates for licenses must pass an NRC examination. This consists of three parts:

(1) A 1-day written examination covering technology, procedures, features and behavior of the plant and radiological protection.
(2) An oral examination, typically 4 hr, including discussion questions, plant walk-through and control room.
(3) A simulator exercise, typically 2 hr, responding to a series of abnormal events and combinations of malfunctions.

The technical content of these examinations is given in Table 10.

The changes made since TMI in this program have been mostly to raise the quality level rather than to change the nature of the program. Table 11 lists all changes already implemented plus those already decided for the future.

The present requirements are based on intuition and experience; the recently decided changes are based on the experience at Three Mile Island. To date, little specific technical basis exists on which to decide whether the present requirements are inadequate, just right or perhaps excessive. (This is true of most college curricula, also).

The task analyses reviewed in Section 5.2 above, and the more comprehensive ones under way, are intended to provide this specific technical basis. But there are larger questions, believed by the author not to be amenable to task analysis. An example of such larger questions is the current effort to develop long-range goals and requirements for licensed operators. Some of the publicly available papers are listed in NRC (1981g). The proximate reason for these papers was a proposed NRC rulemaking proceeding to revise operator licensing requirements. Denton (1980) had foreshadowed such rule changes in promulgating the short-term requirement changes. A proposal to embody Denton's changes in the rules (Item 1 in NRC, 1980g) was rejected, and superseded by more far-reaching proposed changes (NRC, 1980g) to require college-level education for licensed operators, as well as training and experience. Some of the alternative proposals were: (1) require all new RO licences to have 45 college credits; new SRO licenses, 60 credits; (2) require college credits on a sliding scale, with licensing experience substituting for some required credits for operators already licensed; (3) require a university degree in science or engineering for all new shift

Table 10. Technical content of operator licensing examinations in the U.S. 10 CFR 55

WRITTEN EXAMINATIONS AND OPERATING TESTS

§55.20 Scope of examinations

The written examination and operating test for a license as an operator or a senior operator are designed to test the applicant's understanding of the facility design and his familiarity with the controls and operating procedures of the facility. The written examination is based in part on information in the final safety analysis report, operating manuals, and license for the facility.

§55.21 Content of operator written examination

The operator written examination, to the extent applicable to the facility, will include questions on:

(a) Fundamentals of reactor theory, including fission process, neutron multiplication, source effects, control rod effects and criticality indications.
(b) General design features of the core, including core structure, fuel elements, control rods, core instrumentation and coolant flow.
(c) Mechanical design features of the reactor primary system.
(d) Auxiliary systems which affect the facility.
(e) General operating characteristics, including causes and effects of temperature, pressure and reactivity changes, effects of load changes and operating limitations and reasons for them.
(f) Design, components and functions of reactivity control mechanisms and instrumentation.
(g) Design, components and functions of safety systems, including instrumentation, signals, interlocks, automatic and manual features.
(h) Components, capacity and functions of reserve and emergency systems.
(i) Shielding, isolation and containment design features, including access limitations.
(j) Standard and emergency operating procedures for the facility and plant.
(k) Purpose and operation of radiation monitoring system, including alarm and survey equipment.
(l) Radiological safety principles and procedures.

§55.22 Content of senior operator written examination

The senior operator written examination, to the extent applicable to the facility, will include questions on the items specified in §55.21 and in addition on the following:

(a) Conditions and limitations in the facility license.
(b) Design and operating limitations in the technical specifications for the facility.
(c) Facility licensee procedures required to obtain authority for design and operating changes in the facility.
(d) Radiation hazards which may arise during the performance of experiments, shielding alterations, maintenance activities and various contamination conditions.
(e) Reactor theory, including details of fission process, neutron multiplication, source effects, control rod effects and criticality indications.
(f) Specific operating characteristics, including coolant chemistry and causes and effects of temperature, pressure and reactivity changes.
(g) Procedures and limitations involved in initial core loading, alterations in core configuration, control rod programming and determination of various internal and external effects on core reactivity.
(h) Fuel handling facilities and procedures.
(i) Procedures and equipment available for handling and disposal of radioactive materials and effluents.

§55.23 Scope of operator and senior operator operating tests

The operating tests administered to applicants for operator and senior operator licenses are generally similar in scope. The operating test, to the extent applicable to the facility requires the applicant to demonstrate an understanding of:

(a) Pre-start-up procedures for the facility, including associated plant equipment which could affect reactivity.
(b) Required manipulation of console controls to bring the facility from shut-down to designated power levels.
(c) The source and significance of annunciator signals and condition-indicating signals and remedial action responsive thereto.
(d) The instrumentation system and the source and significance of reactor instrument readings.
(e) The behavior characteristics of the facility.
(f) The control manipulation required to obtain desired operating results during normal, abnormal and emergency situations.
(g) The operation of the facility's heat removal systems, including primary coolant, emergency coolant, and decay heat removal systems, and the relation of the proper operation of these systems to the operation of the facility.
(h) The operation of the facility's auxiliary systems which could affect reactivity.

Table 10—*continued*

(i) The use and function of the facility's radiation monitoring systems, including fixed radiation monitors and alarms, portable survey instruments and personnel monitoring equipment.
(j) The significance of radiation hazards, including permissible levels of radiation, levels in excess of those authorized and procedures to reduce excessive levels of radiation and to guard against personnel exposure.
(k) The emergency plan for the facility, including the operator's or senior operator's responsibility to decide whether the plan should be executed and the duties assigned under the plan.
(l) The necessity for a careful approach to the responsibility associated with the safe operation of the facility.

Table 11. Training curriculum. From TVA (1981).This curriculum comprises the 'Student Operator' block on Fig. 2. 'POTC' is the TVA Power Operations Training Center at Soddy-Daisy, TN, U.S.A.

STUDENT 1	STUDENT 2	STUDENT 3	STUDENT 4
STEP 1 (POTC) Orientation Safety First aid Math Physics Chemistry (10 weeks)	STEP 1 (POTC) Electrical theory AC and DC circuits Motors Generator Principals of solid state Composition I (13 weeks)	STEP 1A (POTC) Reactor theory Fuel core design BWR and PWR Thermal hydraulics Health physics Fuel loading and startup Power operation and shutdown Industrial psychology (9 weeks)	(Assigned plant) On the job training Plant familiarization (20 weeks)
STEP 2 (POTC) Plant systems Pumps Heat exchangers Systems designs Thermodynamics Calculus and analytic geometry Oral and communication (19 weeks)	STEP 2 (POTC) Turbines Design Operations Precautions Control Report writing (12 weeks)	STEP 1B (POTC) Reactor technology Instrumentation Systems Fire training Reactor internals Reactor coolant systems Accident and transient analysis (8 weeks)	
		STEP 2 (Assigned plant) Plant systems Plant procedures Electrical training (22 weeks)	
Total—29 weeks	Total—25 weeks	Total—39 weeks	Total—20 weeks

supervisors; (4) require a degree in science or engineering for 25% or 50% of all new licenses after some cutoff date; the eventual goal being 100%; (5) provide separate career paths for college-trained and non-college people; (6) various ways of giving present licensees full, partial, or phased exemption from new requirements.

Responses from the nuclear power industry and from operators (all unpublished) were negative and strong. They assert that the present cadre of licensed operators (3000 in the U.S.) is knowledgeable and experienced. This is true, in the author's opinion. Proponents of enhanced requirements point to operator errors at TMI (Table 1) and elsewhere. The author must agree.

The INPO (1981) study of shift-supervisor training requirements, based on task analysis, was published to bear on this problem. The authors of that study conclude:

'The body of knowledge required for the shift supervisor is diverse, including both general topics

> as well as technically complex concepts and applications. With most of the required knowledge being plant systems, their components and operating characteristics, the study found utility training programs and on-the-job training to be the most applicable. An examination of the knowledge of physical sciences showed the shift supervisor needing to be more familiar with the application of concepts than the theory of these concepts. The comparison of knowledges offered in degreed programs with those required of the shift supervisor showed, in most cases, the level of knowledge required for the shift supervisor did not exceed selected topics in lower division level college courses.
>
> 'From this study there appeared to be no universally applicable academic curricula to meet the knowledge requirements of the shift supervisor. Little evidence exists to indicate that a unilateral requirement for a bachelor of science or associate of science degree could contribute significantly to the job performance of the shift supervisor.'

Let us suppose this study (which had just been published at the time of writing this review) to be technically correct, and the conclusions quoted above to be solidly based on the technical results. There remain, nevertheless, issues in operator qualification that many people believe cannot be resolved by task analysis. Most of these issues have been the subject of unpublished letters and discussions; some are discussed or implied in NRC (1980g). The principal issues are the following:

(1) How to achieve a long-term improvement in operator qualifications, if improvement is needed, without losing the knowledge and experience of the 3000 operators now working—a valuable resource, irreplaceable in the short term.

(2) How to provide career paths for both college graduates and people who don't aspire to college degrees.

(3) How, if college graduates are to be used in operations, to attract and hold college graduates long enough to have the desired experience in operations jobs that involve shiftwork. The career path is central to this problem.

(4) How to compare technical training and experience with college credits.

(5) How to foster the gradual rising of technically qualified people experienced in operations into the engineering and management ranks at the plants and the corporate offices.

(6) How to provide for adequate qualification of the initial operating staff at a new plant.

These are social questions as well as technical ones. The person in charge of a nuclear power plant, or shift, must make emergency decisions affecting lives and property on a large scale. His technical capability is only a part—an essential part—of his qualifications to make such decisions. His leadership ability, inside and outside the plant, his credibility, his behavior pattern under pressure, will determine the acceptability of his actions in addition to the technological quality of these actions. It remains to be determined whether a substantial change will be initiated in the qualifications and careers of nuclear power operators in the U.S.

5.4. *Training*

In the U.S. training programs are under the direction of the electric company. Some companies perform the entire program; others use contracts with reactor vendors, who operate simulator centers, training companies like General Physics Corp., and educational institutions to perform part of the required training.

An example of a program performed entirely by the electric company is given in Fig. 2 and Table 11, from TVA (1981). The incoming neophyte must have a high school education, be in good health, and score acceptably on a battery of aptitude tests for mathematics, science, mechanics and electrical technology.

Table 11 evidences the breadth of the initial training program. As shown in Fig 4. additional simulator training is associated with the steps in the career path; not shown on Fig. 4 are additional classroom and on-the-job training modules associated with the simulator training, including special classes for candidates for licensing examinations.

The TVA program is accredited by Chattanooga State Technical Community College. After a student has completed the 'Student 3' module (Table 11), the University will allow 70 quarter-hours of credit for the TVA-taught technological subjects and 42 quarter-hours for the academic subjects (Math, Chemistry, Speech, Thermodynamics, etc.) taught in conjunction with the University. A few more university-level courses will earn the student an Associate Degree.

The contents of the training program have changed recently for two reasons:

(1) Improvements shown to be necessary or desirable by the TMI accident; see Table 12.

(2) Desire to accredit the training program for college-level equivalence, in view of foreseen requirements for college education for operators, as in NRC (1981g). Both these trends are apparent in the TVA program (Fig. 2 and Table 11, TVA, 1981).

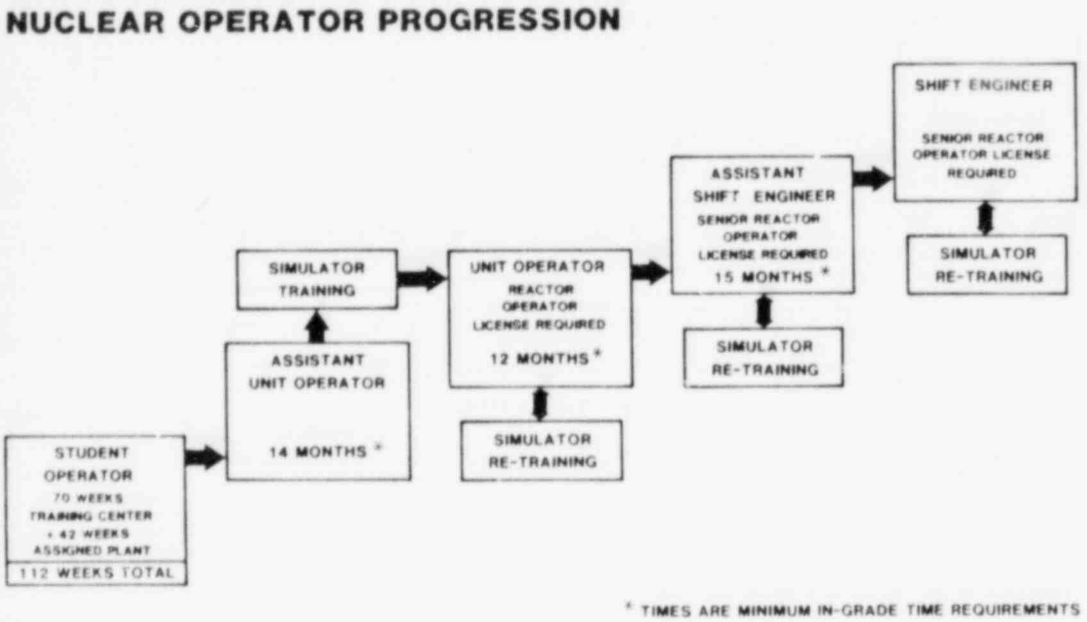

Fig. 2. Training in operator career path. From TVA (1981).

The task analysis of INPO (1981) compares the knowledge required of a shift supervisor with college curricula at the Associate and Bachelor levels. Not given, but recommended for the further work, is re-review of industry training programs as compared with the knowledge required.

5.4.1. *Use of simulators in training.* In recent years, use of simulators in training program has burgeoned. Aircraft and spacecraft simulators are common-place. The author participated in simulator training programs for reactor experiments at Oak Ridge National Laboratory (unpublished) in the 1950s. A rudimentary 'operator's console' with three control levers was connected to the 200-amplifier analog computer used for reactor and plant dynamic studies. The console was placed in front of the bank of 12 pen recorders used as computer output readouts.

The first full-scale power reactor simulator in the U.S. was built in the mid 1960s by General Electric Company near the Dresden Nuclear Power Station. The replica control room, essentially complete, is connected to a digital computer. An instructor's console provides for command of the simulated operation (initial conditions, hold, time compression) and also for introducing off-normal events into the simulation.

It should be noted that the word 'simulator' is also used by computer analysts for computer programs that calculate dynamic response for all purposes, including safety analysis. In this report, 'simulator' is used only for the training device consisting of a real-time calculation of dynamic system behavior and a real-time interactive man-machine interface.

The use of simulators for operator training has recently been reviewed by Jones *et al.* (1980). Hetrick and Bailey (1981) report on a conference held 26–28 January 1981, on simulation methods. The Halden Project conference on (among other things) application of process computers includes papers on simulator models (Halden, 1980).

The digital computer modeling needed to make a simulator work has received much recent attention; see for example Hetrick and Bailey (1981). Research programs in this area are under way in many countries, and are included in the U.S. TMI Action Plan (NRC, 1980a, Item I.A.4.2).

In view of the complexity of nuclear power plants, real-time detailed mathematical modeling of all phenomena is beyond the capabilities of the highest performance computer. For example, such phenomena as three-dimensional reactor core power distribution, coupling of space- and time-dependence of core dynamics, two-phase fluid swelling in partially filled vessels and pipes, cocurrent and countercurrent flow of separated fluid phases, behavior of the core and primary system under inadequate cooling conditions, are not modelled in simulator computers. Any one of

Table 12. Operator-related changes in U.S. plants since the TMI accident

(A) *Very short term actions* (NRC (1980e))

(1) Retrain all operators to understand the TMI accident including revised simulator small-break demonstrations and hands-on exercises; loss of coolant accident analyses; revised procedures for small-break loss of coolant accidents.

(2) Develop guidelines, procedures, and retrain operators in use of existing instrumentation and equipment in identifying and mitigating events involving inadequate core cooling.

(B) *Short term actions* (Eisenhut (1979))

(3) Inaugurate shift technical advisor.
(4) Realign responsibilities of shift supervisor.
(5) Inaugurate formal shift turnover procedures.
(6) Improve access control for control room.

(C) *Medium term actions* (Eisenhut (1980))

(7) Increased experience requirements for SRO candidates.
(8) Require 3 months on-shift training of all candidates.
(9) Augment training and requalification programs and licensing examinations in the areas of heat transfer, thermodynamics, fluid flow, transient behavior, mitigation of inadequate core cooling.
(10) Require SRO equivalent examinations of training instructors who teach systems, integrated response, transients and similar courses.
(11) Require requalification programs for instructors.
(12) Require certification of licensing candidates to be signed by high level corporate manager; require candidates to permit (under U.S. Privacy laws) NRC to inform company regarding details of examination performance.
(13) Impose time limits for written examinations; increase passing grade; require passing grade on each category.
(14) Require two SRO on shift, one in control room area at all times.
(15) Give guidance on allowable overtime.
(16) Provide resources and procedures for feedback of operating experience to operating staff.
(17) Revise procedures to provide independent checkout of manual ex-control room manipulation of safety equipment.

(D) *Medium and long term Activities* (NRC 1980a, 1980b))

(18) Re-analyze transients and accidents; revise procedures and training.
(19) Review organization, management, resources of electric companies and plants.
(20 Perform human factors and safety function reviews of control rooms and implement needed modifications.
(21) Design and install Safety Parameter Display System.
(22) Expand initial testing to include realistic drills for verifying equipment performance, procedures and operating crew training.

these phenomena can be modelled on a computer, but not necessarily in real time, and the best models have approximations in them. It is also possible to provide simulated sequences by storing scenarios and playing back these stored values. The earlier simulators made considerable use of stored scenarios, but the current trend is toward dynamic calculation where possible, based on the equations that describe the dynamic behavior of the system. The dynamic modeling is much to be preferred over the stored scenarios. Dynamic modeling allows the simulator to respond realistically to all event sequences, including a variety of errors and failures. To include all these sequences in a stored scenario would require, first, analyzing the course of each sequence; and, second, storing all the scenario variations together with a selection logic for determining which to play back. Since the essence of simulation is real-time modeling, choices must be made on how to use the available computing capability. Some phenomena are not included in the model; some others are approximated or represented by stored scenarios; others are modeled dynamically.

The importance of modeling is illustrated by one of the lessons of TMI. After the accident, investigations of operator knowledge and understanding focused on the inability of the simulator used in the training of the TMI operators to represent the sequence of events actually experienced in the accident. A key phenomenon—flashing in the primary system—was not represented. All PWR simulators were reviewed by Jones *et al.* (1980) in this respect:

'Prior to the TMI-2 event, little or no thought was given by the nuclear training industry to modeling in a training simulator the response of a PWR primary loop with saturated conditions. In general, operation of a safety systems is assumed to preclude vapor formation in the primary system. The possibility for a slowly developing loss-of-coolant accident proceeding unrecognized for a considerable time period without adequate core cooling was considered as not credible and/or the consequences were assumed to be bounded by those of the large LOCA.

'Since the TMI-2 event, most of the PWR simulator operators have attempted to reproduce, with varying degrees of success, the significant effects on plant monitors that would result from a saturated primary coolant. However, none can truly model two-phase primary coolant flow and its interactive effects on the many associated reactor systems. Accurate and thorough models of two-phase flow in a PWR system following a transient are still in developmental stages. Computer codes in use are large and (relatively) very time-consuming for use in dynamic modeling with real-time simulation.'

It is evident that allocation of computing resources is necessary and trade-offs must be evaluated.

Starting with the GE Dresden simulator, the U.S. nuclear simulators have comprised full-scale control room replicas and full-plant calculations. Other formats are possible and useful. Blomberg, Josefsson and Åkerhielm (1977) and C/E Studsvik (undated) have described a 'Compact Nuclear Simulator', with a panel about 2 m long plus three CRT readouts, connected to a digital computer. This 'medium fidelity' simulator gives the student training in plant dynamics, without the distractions (or the advantages) of the detailed, multiple function plant control room. The readouts and control devices on the "Compact Simulator' are schematic and functional only, but the computer model of the plant dynamics can be as detailed and elaborate as computing resources permit.

Rouse (unpublished discussion, 1981) has suggested a hierarchy of 'high-fidelity, medium fidelity, low fidelity' simulators for different aspects of training. Although this idea was not stated by Rouse to be new, the author has found no published U.S. nuclear references. Rouse identified two kinds of rules for operations:

(1) Symptomatic rules, to use for responding to familiar patterns of symptoms;
(2) Topographic rules, to use with knowledge of the process to understand and respond to unfamiliar patterns of symptoms.

Low and medium fidelity part-task simulators are principally useful for enhancing understanding of the plant, and gaining experience in applying topographic problem solving techniques, whereas high-fidelity, full-task simulators (such as the Dresden simulator) are used to provide training on symptomatic rules.

Generic simulators (low fidelity) were described by Green and Myerscough (1977) and Cocquyt *et al.* (1977). An Oak Ridge National Laboratory program, yet unpublished, includes these ideas; one hopes they will publish references to sources. IEEE (1980) includes mention of 'Part Task Simulators' but no published references are given. IEAL (1980) contains brief discussions of part-task simulators and an undifferentiated bibliography on this and many other topics. The U.S. nuclear power plant industry makes almost no use of part-task simulators at present. C/E Studsvik (undated) state that the Compact Simulator is used for training in Sweden.

5.4.2. *Use of simulator to measure performance.* Netland (1979), and Stokke (1981) and Bott *et al.* (1981) have described use of training simulators to collect data on operator performance. It seems evident that, while not completely realistic, the full-scope training simulator reproduces most aspects of the control-room situation. Only the stress of 'the real situation' is missing. Comparison of alternative design approaches, measurement of response times and accuracy, identification of confusing indications or procedures are easily performed. This appears to be a fruitful path for future research. Further discussion is given in Section 8.5 of this review.

6. ORGANIZATION AND MANAGEMENT

General guidance on management and organization is given by IAEA (1979, 1980b) and Allenspach and Crocker (1980). Both the onsite plant organization and the offsite corporate and outside support for the plant must be considered.

The TMI accident has been analyzed to show strong evidence of management and organizational inadequacies. Since the TMI accident, a number of important changes have taken place in the plants, in the electric utility companies, and in the U.S. nuclear power industry as a whole.

6.1. *Organization and staffing at the plant*

Single-unit plants used to operate with less than 100 employees on site. Nowadays, increased workload and increased regulatory requirements have increased the minimum number to 200 or more. Allenspach and Crocker (1980) have published guidelines. The following discussion is based substantially on their work.

Operations.—The minimum shift complement is given in Table 4, from NRC (1980d). The need for 10 operations people on each shift, plus security forces, is based on functions of the onsite forces in an emergency. The required Emergency Plan must provide coverage of the major functional areas of Table 4.

Five or (preferably) six shift teams are employed. This provides for continuous shift coverage, plus time off and extra time for continuing training and education.

Maintenance.—Staff and supervision must be available for routine preventive maintenance as well as unscheduled repairs. The maintenance staff has an especially heavy workload when the plant is shut down for periodic major overhaul and refueling.

Technical.—Support is required for the operations and maintenance staffs in the areas of reactor and other engineering, chemistry, radiation protection and instrumentation. Included is analysis of operations; that is, a continuing evaluation of the performance of the plant, with special attention to errors and failures, and unexpected behavior. Because of the importance of radiation protection to plant safety and to personnel safety, this function is made independent of operations.

Traini g.—The tiaining requirements of the plant staff include on-site (in-plant) and off-site (classroom, simulator) components. Some on-site training resources are needed.

Security.

Administrative Service.

Audit and review.—The safety operation of a nuclear power plant is the subject of a variety of reviews and audits, discussed in Section 6.3 below.

6.1.1. *Changes since the TMI accident.* Operating plants in the U.S. have been required to make a number of changes in organization and management as a result of the TMI accident. These are listed in Table 13. They represent a short-term program to improve the plant staffing and management in the areas identified by the TMI accident reviews.

For new plants, coming into operation since the TMI accident, the requirements of Table 13 have been applied. In addition, these plants have also been required to have an independent safety engineering group. In addition, a review of organization, staffing and management competence at plant and corporate levels is conducted by a multidisciplinary NRC team, using primarily interviews and reviews of administrative documents. The objective is to evaluate the capability of the organization to operate the plant safety. This is not a quantified variable susceptible to measurement. Some guidelines have been given by IAEA (1979, 1980b), Allenspach and Crocker (1980), NRC (1981h), Podonsky *et al.* (1980) and INPO (1981c).

One change of greater long-term significance is the inauguration of the Shift Technical Advisor. The STA is discussed by NRC (1979), Denton (1979), Eisenhut (1979) and INPO (1981b). The reviews of the TMI accident concluded that the operating crew did not understand what was happening. They had been trained to recognize and cope with certain specific event sequences. Their emergency operating procedures were organized to cope with these design basis sequences.

It was therefore proposed to add a shift crew member who would be educated to understand power plant science (e.g., thermodynamics) as well as trained to know the plant and its behavior. The STA position was inaugurated as a method of immediately improving the plant operating staff's capability for response to off-normal conditions. He is required to have college level education in engineering or science as well as training in reactor operations. While he is a member of the operating crew, he has no routine operating

Table 13. Organization and management changes in U.S. operating plants since the TMI accident (NRC (1980b)

(1) Add shift technical advisor around the clock, to add engineering capability to control room.
(2) Clearly define shift supervisor responsibilities and delegate administrative duties and some communications to others to avoid unnecessary distraction from his safety role.
(3) Limit routine overtime and manage necessary non-routine overtime.
(4) Additional senior operator on shift crew (effective 1 July 1982).
(5) Establish formal shift turnover procedure and checklist.
(6) Establish improved formal control over access to control room by other people.
(7) Establish organizational component and procedures to feed back operating experience at all plants to the operating and management people.
(8) Establish procedure for direct verification of all safety operations; in longer term, implement safety system status monitoring systems.
(9) Increase shift staffing and on-call assistance as required for emergency response; see Table 4 of this review.

duties that would interfere with his primary emergency role of diagnosing events and advising the control room supervisor.

6.1.2. *Capability of management evaluation.* A principal problem is the lack of objective measures of performance in this area. That is, we don't have a good index of 'the safety of plant operation', except where an accident occurs. Some unpublished approaches have been attempted, using, for example, the rate of occurrence of reportable events, enforcement actions, unscheduled outage data, etc. These are, at best, remote measures of 'the safety of plant operation'. Other approaches that have been used are subjective and qualitative. The NRC (1981i) has the 'Systematic Analysis of Licensee Performance', but the validity and timeliness of this largely subjective rating scheme have recently been questioned.

The Institute of Nuclear Power Operations has issued (INPO, 1981c) performance objectives and criteria for the evaluations conducted by the Institute's teams of each U.S. nuclear power plant, and for nuclear utilities to use in self-evaluation. Fifty-one objectives are given in the areas of organization and administration, training and qualification, operations, maintenance, radiation protection, chemistry, emergency preparedness, and technical support. The criteria are specific, but not quantitative. In their evaluations published so far INPO has not given a summary rating, relative, absolute, or quantitative.

Lacking quantitative measures of 'the safety of plant operation', one is forced to rely on the qualitative guidelines and criteria mentioned earlier, and thus on qualitative judgements of management and organizational adequacy. It is to be hoped that future studies will result in the development of better, more nearly quantitative measures, leading to improvement in the management of the plants.

6.1.3. *Importance of management capability.* All our experience, and all the TMI accident reviews, emphasize the importance of management in the safe operation of nuclear power plants. The experience of the author in nuclear plant safety reviews over many years, and in supervising the NRC management reviews recently, supports the view that the quality of management is essential to the safety of plant operation. In each plant there is one, or a very small number, of key individuals who actually run the plant. Often, but not always, these key people are the incumbents of the top supervisory positions. Everyone, at all levels, knows what kinds of actions are rewarded, what you have to do to get promoted or earn a bonus. These desiderata may be, but are not always, the principal objectives and priorities set forth in published company policy directives.

Moray (private communication) has surveyed some control room operators and plant engineers regarding difficult operating-safety choices. An example is the decision to initiate plant shutdown quickly, but perhaps unnecessarily, on detecting an indicated abnormal value of a plant variable. The people surveyed gave answers that varied by several orders of magnitude on the 'values' of truly required shutdowns, shutdowns required but not executed, and unnecessary shutdowns. They are, presumably, reacting to their perceptions of how the key leaders in their plants view people who shut the plant down unnecessarily compared to people who miss needed shutdowns. Of course, the people surveyed are the people who make such decisions routinely. If they decide wrongly, management may well be blamed, and management may well deserve the blame.

6.2. *The nuclear company*

Allenspach and Crocker (1980) set forth some guidelines regarding the utility company. The overall management and support of the nuclear plants in a company should be integrated. A corporate official should have the responsibility for the nuclear operation and safety; this official should be at a sufficiently high level that he can command the necessary resources as required.

Several different organizational structures have been used successfully:

(i) Single vice-president in charge of nuclear operation and safety; see for example NRC (1981j), Docket No. 50-387.

(ii) Separate vice-presidents for operations and engineering; an example is in NRC (1981j) Docket No. 50-369. Successful application requires close working ties between the nuclear segments of the operation and engineering organizations.

(iii) 'Matrix' organization with managers of operations and managers of technology (radiation protection, engineering, training); an example is discussed in NRC (1981j) Docket No. 50-400.

The simplest pattern is (i), with a single corporate management of nuclear operations having command of all the resources. The more complex arrangements like (ii) and (iii) require more coordination, but some companies prefer them and some make them function acceptably.

Since the TMI accident, the NRC has been much more aggressive in its review of management structure and resources for the plants coming on line. Detailed reviews can be found for each plant in NRC (1981j).

For the operating plants, NRC has not yet decided on the depth or timing of a management re-review. Indeed, although such a review program is foreseen in the Action Plan NRC (1980a, item I.B.1.1), its implementation is still undecided.

With the very large number of new plants scheduled to come on line in the U.S. during the 1980–1985 period, the cadre of experienced managers and senior operators will be severely taxed. Current projections start at approx. 70 operating units in 1980, growing to approx. 120 in 1985 and approx. 150 by 1990. Some cancellations and long-term deferrals have been announced since this projection. However, the number of operating plants will still almost double in the next few years. For utilities with operating nuclear units, a massive recruiting and training program is in order. For a utility bringing on line its first plant, the problem is to acquire enough experienced managers and shift supervisors to form an adequate cadre. An example of this problem is given in NRC (1981j), Docket No. 50-382. This plant, the first for this company, was reviewed about 18 months before its projected nuclear operating date. The severe shortage of qualified, experienced senior people had resulted in a corporate management group entirely lacking in nuclear operating experience, and a plant management with many key positions vacant—Assistant Plant Manager-Operations and Maintenance, Plant Operation Superintendent, Plant Engineering Department Supervisor, General Support Superintendent, Nuclear Training Director, six Shift Supervisors. It is not yet clear whether the necessary qualified people can be acquired and trained in time for this plant to achieve its projected operation schedule.

The qualifications of the corporate managers and staff are difficult to establish specifically: what are the measurable attributes of a successful manager for safe operations? Allenspach and Crocker (1980) give what guidance is feasible and refer to some not very useful U.S. standards documents.

6.3. *Management review and audit*

Because of the importance to public safety of correct nuclear power plant operation, a system of reviews and audits has been established to assure attention to safety. All of this structure except the Independent Safety Engineering Group (Item 3, below) was in place before the TMI accident, and so it will be described only briefly.

6.3.1. *Operational quality assurance.* Each company, and each plant, in the U.S. is required to establish a quality assurance program for operations, maintenance, modifications and all other activities potentially affecting public safety. The requirements are in 10CFR50, Appendix B, and NRC (1981h), Section 17.2. A comprehensive program includes verification of activities by trained and qualified individuals, independent of the organization responsible for performing the task, free from the direct pressures of costs and schedules, reporting to a management official with authority to resolve disputes and enforce decisions.

6.3.2. *Plant staff review group.* This comprises a working committee, whose members are members of plant staff management. The group reviews and approves plans and procedures and changes to them, equipment changes, and reportable events, plus exercising an operations safety review function.

6.3.3. *Independent safety engineering group.* This is a new organizational module, so far required in the U.S. only on plants coming online since the TMI accident. The requirements are given in NRC (1980f), Appendix A, and Allenspach and Crocker (1980). The Group is an additional group of five dedicated, full-time, site-based engineers, who report off-site to a technically oriented high level corporate official not responsible for power production. The function of the group is to examine safety information regarding the plant and also safety information from off-site, and to develop recommendations for changes that would improve safety. The group does not do detailed audits of operations and does not have sign-off responsibility. The review functions of the Independent Safety Engineering Group include the following:

Evaluation for technical adequacy and clarity of all procedures important to the safe operation of the facility.

Evaluation of plant operations from a safety perspective.

Evaluation of the effectiveness of the quality assurance program.

Comparison of the operating experience of the plant and plants of a similar design.

Assessment of the plant performance regarding conformance to requirements related to safety.

Any other matter involving safe operation of the nuclear power plant that an independent review deems appropriate for consideration.

Assessment of plant safety.

The group performing this function should be composed of individuals with varied backgrounds and disciplines related to nuclear power plants.

Such groups are functioning at about a dozen plants. After experience is gained, the decision will be made whether to require these groups at all operating plants.

6.3.4 *Independent review and audit group.* This comprises a high-level committee that provides a safety overview of the whole plant, including the recommendations of the quality assurance, plant staff, and independent safety engineering groups. For many utility companies, it is appropriate to include knowledgeable and experienced outside consultants to enhance the expertise and independence of the group.

6.4. *Working hours*

Nuclear power plant operations are required around the clock. A number of developments have combined to create a situation where overtime work—beyond the 8-hr shift, 40-hr week—is a commonplace occurrence in nuclear power plant operating crews:

(1) The shortage of trained and qualified people; see Section 6.2.

(2) The increased number of shift crew people required at each plant since the TMI accident; see Tables 4 and 14.

(3) The increasing number of operating plants.

(4) The increased workload on the shift operating crews imposed by post-TMI requirements for augmented training, surveillance of operations, testing and maintenance and plant modifications.

This combination of increased workload and shortage of qualified people naturally tends toward longer work weeks for the people. Since the operating crews are already working rotating shifts (universal practice in the U.S.), the situation is characterized by increased length of the rotating shifts. The author and his colleagues, participating in the management reviews discussed above in Section 6.1, were told by control room operating personnel that they were tired as a result of routine overtime required of them over months and even years caused by the workloads and shortages. A discussion is given in NRC (1981j), Docket 50-311.

Human circadian rhythms are well known and much studied, as are the effects of night work and long work periods. Holley *et al.* (1981) give a 66-page review, plus 2084 references no older than 1972, with emphasis on pilot performance. Experiences reported by pilots and air traffic controllers are compiled by Lyman and Orlady (1980). In 77 reported incidents, the reporter associated fatigue with the occurrence.

Shift work, which upsets circadian rhythms, is necessary for technical reasons in some industries that involve continuous processes, in transportation, and in vigilance activities. Increasingly, shift work is being used to enhance the use of invested capital, even where no technical necessity exists for it.

A selected bibliography directed at shift work and overtime in nuclear power plants is given by Wallace *et al.* (1980a). Since the present emphasis is on overtime of shift workers, some materials developed in connection with 12-hr shifts are relevant. In fact, the tired workers referred to earlier were routinely working 12-hr shifts.

Twelve-hour shifts as a routine alternative to 8-hr

Table 14. U.S. overtime guidelines (NRC (1980b))[*]

In the event that overtime must be used (excluding extended periods of shutdown for refueling, major maintenance or major plant modifications), the following overtime restrictions should be followed:

(1) An individual should not be permitted to work more than 12 hr straight (not including shift turnover time).

(2) There should be a break of at least 12 hr (which can include shift turnover time) between all work periods.

(3) An individual should not work more than 72 hr in any 7-day period.

(4) An individual should not be required to work more than 14 consecutive days without having 2 consecutive days off.

However, recognizing that circumstances may arise requiring deviations from the above restrictions, such deviation shall be authorized by the plant manager or his deputy, or higher levels of management in accordance with published procedures and with appropriate documentation of the cause.

If a reactor operator or senior reactor operator has been working more than 12 hr during periods of extended shutdown (e.g., at duties away from the control board), such individuals shall not be assigned shift duty in the control room without at least a 12-hr break preceding such an assignment.

NRC encourages the development of a staffing policy that would permit the licensed reactor operators and senior reactor operators to be periodically assigned to other duties away from the control board during their normal tours of duty.

If a reactor operator is required to work in excess of 8 continuous hours, he shall be periodically relieved of primary duties at the control board, such that periods of duty at the board do not exceed about 4 hr at a time.

The guidelines on overtime do not apply to the shift technical advisor provided he or she is provided sleeping accommodations and a 10-min availability is assured.

[*] Note added in proof. NRC recently published (*Federal Register* **47,** 7352 (18 February 1982)) revised guidance; Item 1 was changed to 16 hr, item 2 to 8 hr, and other changes were made.

shifts have been investigated in 50 chemical plants by Wilson and Rose (1978). In many ways, chemical plant operators have duties similar to nuclear plant operators. They concluded that there was some preference by workers for the social and familial advantages of rotating 12-hr shifts in a 40-hr average week (thus, no long-range overtime). Drawbacks include increased fatigue and inability to use double shifts to cover for illness and other absence. Fatigue was studied using workers' perceptions and also accident rates. Most workers reported overall decreased fatigue from fewer 12-hr shifts per week, even on night shifts. The author implies that the accident rate did not change, but no data are given.

Joaquin *et al.* (1981) studied 12-hr shift experience at the Ontario Hydro Bruce Heavy Water Plant, a chemical operation associated with, and co-located with the Bruce Nuclear Power Station. The Bruce Heavy Water Plant (but not the nuclear power plant) went on 12-hr shifts in January 1979. The workers surveyed experienced some additional fatigue, but believed their physical condition to be unchanged (64%) or improved (30%). They perceived no effect (56%) or small positive effect (38%) on their work performance. No effect of the 12-hr shift was detected on sick leave rates, except for mechanical maintainers, where the rate increased.

More recently, Ontario Hydro announced that the 12-hr shift would not be implemented at their nuclear stations. (Strickert *et al.*, 1981).

Price *et al.* (1980a) studied some possible tradeoffs for coping with the conditions leading to chronic overtime. They considered three options:

(1) Changing from an 8-hr rotating shift to a 12-hr rotating shift.
(2) Reducing the number of reactor operators and/or senior reactor operators required in the control room on a shift.
(3) Utilizing lesser trained and/or experienced personnel in the control room.

They concluded that none of these options is desirable for new units. This is particularly the case in view of the report by Joos *et al.* (1979) that indicates that human error rates are higher during the first months of plant operations.

In order to control the perceived fatigue in operating crews, NRC has issued overtime guidelines. A representative set is given in NRC (1980b), and is reproduced in Table 14. These guidelines are not working very well; they are too prescriptive. For example, the requirement that the plant manager or his deputy approve all deviations results in a large paper workload during refueling, without a compensating safety benefit. More work is obviously needed which one hopes is based better on available data.

7. PROCEDURES

7.1. *Procedures in nuclear power plants*

A nuclear power plant is a complex physical system operated, maintained and modified by several hundred people. Information transfer among these people is by means of technical data and procedures. The interaction between procedures and people (those who write them and those who read and use them) is included in human factors considerations in nuclear power plants. (The presentation of technical information to operating people is included in Section 8 in this review).

A vast number and variety of procedures facilitate and encumbers operation of a present-day nuclear station. Management directives and administrative procedures are part of the subject of Section 6 of this review. Procedures for normal operation, while important to plant availability, and as components of initiating events leading to plant transients and accidents, are not included in this review. This chapter deals with the emergency operating procedures to be used by the plant operating crew in coping with abnormal plant operation, including severe transients and accidents; testing and maintenance procedures are discussed in Section 8. Off-site emergency preparedness, plans and procedures are the subject of an accompanying paper (Grimes and Ramos, 1982).

7.2. *Emergency operating procedures—general*

The Emergency Operating Procedure is a written document (it may some day be stored in a computer memory) intended for the operating crew to consult and use in abnormal situations. The role of the operator in such an event (Section 5.2 of this review) is twofold:

(1) To maintain or restore adequate performance of the critical safety functions;
(2) To diagnose the problem and initiate recovery of the plant to normal operation or, if that is impossible, to orderly shutdown.

The procedures should therefore be oriented to the dual task of the operation crew. For task 1, the procedures should describe the symptoms by which performance of the critical safety functions can be evaluated, and guide the operator to success paths for restoration of the functions if the symptoms show the need. For task 2, the procedures should include a diagnosis procedure and guidance for recovery.

If the preceding analysis of operator tasks and procedure needs is correct (it is the author's, based primarily on Corcoran *et al.*, 1980a and 1980b), then present-day emergency operating procedures in U.S. nuclear power plants are in need of upgrading. An upgrading program is under way.

The reviews of the TMI accident contain severe criticisms of the emergency operating procedures available to those operators. Kemeny *et al.* (1979) state:

> 'Some of the key TMI-2 operating and emergency procedures in use on 28 March were inadequate, including the procedures for a LOCA and for pressurizer operation. Deficiencies in these procedures could cause operator confusion or incorrect action.'
>
> 'There were deficiencies in the review, approval and implementation of TMI-2 plant procedures . . .
>
> 'Substantially more attention and care must be devoted to the writing, reviewing and monitoring of plant procedures . . .'

The review of Rogovin *et al.* (1980) includes the following:

> 'The underlying questions are: were there procedures available to cope with the situation at TMI on the morning of 28 March 1979, and did procedures or lack of procedures have an impact on the accident. We believe that the procedures were grossly deficient in assisting the operator in diagnosing problems with the feedwater system, the emergency feedwater system, and OTSG level responses when emergency feedwater pumps were activated. The procedures were of no help in diagnosing the PORV failure, nor did they provide guidance in analyzing the situation of pressurizer level increasing 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 (Malone *et al.* (1980)).'

The Action Plan by NRC (1980a) includes (Items I.C.1, 7, 8 and 9 in Table 3) a program for procedure improvement. In the short term, small-break loss-of-coolant accidents were re-analyzed, using realistic computer codes, as compared to the highly conservative codes previously relied on. This change is important, since operator actions should be based on the transient behavior as it is actually experienced, rather than on design-basis calculations performed for bounding cases.

The combinations of events included were also broadened, from previous such work, to include the operation of non-safety equipment that might help in preventing accidents from developing or mitigating their consequences if they do occur. This change is analogous to the change in computer codes from conservative bounding models (assuming for design purposes that only safety equipment will function) to realistic codes (allowing for operation, or failure, of any relevant equipment).

The actual behavior will, of course, depend on what sequence of events actually occurs; that is, which among the large number of possible combinations of successes and failures of equipment, plus correct operations and errors, will take place in the specific case. The new analyses are being broadened to include enough representative combinations to provide guidance to procedure development.

All plants were required to revise their procedures as needed to make them consistent with the revised analyses. In addition to the small-break loss-of-coolant accidents, analysis was performed for all plants, and procedures developed, for recognizing symptoms of the approach to, and the course of, inadequate core cooling, using instrumentation presently installed. The procedures also include mitigating such situations, to the extent this can be done with the existing plant systems.

For plants coming online since the TMI accident, improved procedures have been developed, still mostly using the traditional approaches. These have been based on improved technical guidelines that take into account the analyses described earlier. These procedures have been audited using walkthroughs in the plants as well as real-time simulator exercises.

For the future, all plants will develop completely revised emergency operating procedures, based on improved technical guidelines (Section 7.3) and also on human factors guidelines (Section 7.4) for improved application under emergency conditions.

The program of analysis for procedure development bases is being broadened from the initial emphasis on small-break loss-of-coolant accidents and inadequate core cooling recognition, to a comprehensive analysis of plant transients and accidents. This work, now under way for U.S. plants, is necessarily based on a taxonomy of transient and accident sequences. Event trees (see Section 2.4 of this review) are a way of organizing these sequences. To make the analysis task manageable, the possible sequences, candidates for analysis, must be screened. Some screening factors include:

(a) Whether a sequence has actually occurred in some plant;

(b) Judgement, plus any available data, regarding the probability of a failure or error, or of a sequence taken as a whole;

(c) Whether the failure or error is likely to be rectified, and thus its effect nullified;

(d) Whether alternate success paths are available if a failure or error occurs;

(e) Whether the sequences produce symptoms that are confusing or are likely to evoke an incorrect operation response;

(f) The consequences or risk associated with a given sequence.

The sequences which survive screening are analyzed, using as realistic a computer model as practical. The results of the analysis are values of plant variables as functions of time. In applying these results to procedure development, one looks for similarities of symptom patterns, and alternative success paths to terminate the sequence successfully or mitigate its consequences.

The development of procedures is thus intimately related to the analysis of plant behavior. In addition, the information available to the operating crew is essential to their response, and therefore to the procedures that govern their response. Thus the review of the man-machine interface, particularly the control room (Section 8 of this review), must be done in conjunction with procedure evaluation. In order to effect substantial improvement in control rooms and procedures, the control room analysis must be performed with good procedures; procedure validation must be done in a good control room.

Finally, the qualifications and training of the operating people must be included in analyzing the procedures and the control room. These inter-related factors—control room, procedures, qualification and training of the people—must all be analyzed together. The programs of improvement in human factors safety will have to deal with all the components of the contributions people make to nuclear power plant safety and risk.

7.3. *Technical guidelines for emergency operating procedures*

The 'Technical Guidelines' of this section read like procedures; that is, they are technical documents stating what the operator should do in various circumstances. They differ from actual procedures in (1) their generic nature and (2) their presentation.

The generic nature of procedure technical guidelines arises in the generic nature of the analysis on which they are based. This is done for economy, for plants sufficiently similar that the analyses, and guidelines, are valid. The guidelines are given in terms of systems and functions, whereas the procedures must deal with the actual plant controls and equipment that must be manipulated.

The guidelines are technical documents to be used as a basis for procedure writing, whereas the procedures themselves must be used in real time, so to speak, by the operating crew, under stress, in the actual transient or accident. The guidelines are therefore technical documents containing technical information, while the procedures are written, or should be written, with the use in view. Existing procedures in the U.S. and therefore existing procedure guidelines, are universally event oriented. They are keyed to an initiating event, like reactor trip (scram), or pipe break (loss-of-coolant accident). Since there are several kinds of initiating events, there are several emergency operating procedures in each plant. The better ones begin with the symptoms by which the operator can recognize the particular event, then follow with the operating steps to be performed.

Many reviewers have observed that procedures, and procedure guidelines, developed with this event orientation are poorly related to the most urgent and most difficult parts of the operating crews' emergency tasks. They do not focus on maintenance or restoration of the critical safety functions, and they do not focus on diagnosing the source of the problem to enable recovery of the plant. Thus although these procedure guidelines contain, if correct technically, the ingredients of the operating crews' need for guidance, they do not provide readily usable, organized guidance for what has to be done.

Longer-term procedure development programs have been mandated by NRC (1980a), item I.C.1 and I.C.9. The objective of this program is to develop procedures better suited to the operator's role and tasks, and better arranged for control room use.

Emergency Operating Procedure Guidelines are under development in the U.S. for all classes of plants now operating and under construction. None of these has yet been published in finished form. General Electric Owners' Group (1980) has published draft guidelines for (Reactor Vessel Water) 'Level Control', (cold) 'shutdown', and 'Containment Control' (Suppression pool water level and temperature, drywell atmosphere temperature and pressure). Reactivity control guidelines have not yet been published for GE plants. It is evident that these new guidelines are organized to correspond to critical safety functions.

Each guideline starts with 'entry conditions'—a short outline of symptoms showing the need for attention to the associated critical safety function. As an example, entry conditions for the Reactor Vessel Water Level guideline are:

[redacted]

(1) Water level indicated below a predetermined value; or

(2) Drywell pressure indicated above a predetermined value; or

(3) Containment Isolation valves close.

The guideline then lists, in order, the required operator actions. There is a great deal of branching, dependent upon the success or failure of the measures undertaken by the automatic systems and the operator. The branch points are associated with symptoms—values of variables—and criteria—predetermined levels at which the operator should take alternate or additional action.

Contingency guidelines are provided for six sets of symptoms of increasing severity. The Level Control, etc., guidelines contain transfers to the Contingency guidelines. The Contingency guidelines are symptom oriented also, and include steps for the operating crew to take in degraded situations (systems don't work) or those with inconsistent symptoms (instruments don't work or the combination of circumstances is unforeseen or not understood). They thus comprise the guidelines for inadequate core cooling.

Several sets of plant-specific emergency operating procedures have been developed from the guidelines in General Electric Owners' Group (1980). These have been subjected to several simulator exercises, in which operating crews have used the procedures in real time to respond to a wide variety of simulated event sequences, including multiple failures and instrument failures leading to inconsistent symptoms. The effectiveness of the approach, and the basic technical correctness of the guidelines, have been validated, in large measure, by these simulations.

Although the shutdown guideline takes the plant to cold shutdown, and thus fulfills the requirement for plant recovery (the second basic function of the operating crew), the guidelines in their present form do not explicitly provide for diagnosis. Experience will tell us whether such provision is needed.

The owners' groups for pressurized water reactors in the U.S. are also developing improved procedure guidelines. However, none has yet been brought to the state of the General Electric Owners' Group (1980) report. An example of the present state of development is given in Combustion Engineering (1981). These guidelines are organized overall by function: Reactivity Control, Primary System Inventory and Pressure control, Primary System Heat Removal and Inadequate Core Cooling. Within these functional categories, the guidelines are organized by events: loss of feedwater, loss of forced reactor coolant flow and steam line break, for example, under Primary System Heat Removal. Each guideline begins with a three-page discussion of the event and its symptoms, and then the operator action guidelines follow. More work is required, in the author's opinion, before these and other current draft PWR guidelines will be in shape to support the writing of plant-specific procedures that promote the successful accomplishment of the two basic functions of the operating crew.

7.4. *Human factor aspects of emergency operating procedures*

The human factor shortcomings of the existing procedures at Three Mile Island have been reviewed by Rogovin *et al.* (1980) and Malone *et al.* (1980). Besides the technical inadequacies discussed in the preceding section of this review, the procedures are not well suited to use in emergencies, under stress, in the control room. Their physical form, layout, format and mode of expression need to be brought into conformance with the needs and limitations of the human readers who must use them.

NRC (1981c) gives a bibliography of over 100 references, mostly directed toward readability and usability. Fuchs, Engelschall and Imlay (1981a, 1981b) and Morgenstern *et al.* (1981) have given recommendations. NRC (1981c) has published, for public comment, criteria for procedures. Topics covered include organization, format, style and content.

Intuition suggests that there must be many acceptable, convenient, usable ways to organize, format and style a set of emergency operating procedures. The authors of the publications referenced in the preceding paragraph each present a single way of doing this as a directive or a strongly recommended example. The recommendations are different, and in some respects inconsistent.

Brune and Weinstein (1981) give a checklist for emergency operating procedures. The 46 questions are based on an analysis by the authors of some typical procedures of current types (*not* the symptom-based procedures under development), and analysis of 1641 event reports classified as operator or procedural errors. Of these, 329 involved procedure-related operator performance deviations.

Each checklist item is rated according to its (subjectively assessed) probability to induce performance deviation under low, medium and high stress as defined in Swain and Guttman (1980).

While some of the checklist questions are clearly particularized to event-oriented procedures, and to the shortcomings of today's procedure books, others are more widely applicable.

Airliner cockpits are furnished with procedures manuals for emergencies. Because of the faster time response of the jet aircraft compared to a nuclear power plant, the aircraft emergency procedures manuals are necessarily concise, easy to read and follow, with crisp clear style. The author suggests that a jet aircraft is as complicated a machine as a nuclear power plant, less amenable to manual control improvisation or on-stream repair, with a higher operator (pilot) workload, and a more difficult problem of achieving a safe shutdown state (landing and stopping) in an emergency. (There are, of course, other significant differences). The nuclear plants have, in the author's opinion, much to learn from a study of airliner emergency procedures manuals.

It is to be hoped that the future procedures to be written from the guidelines now under development will be presented in a form usable by the operating crew in an emergency. Some beginnings of advanced methods are summarized in the next section.

7.5. *Potential improved forms of procedures*

The traditional picture of a book of typewritten procedures is virtually universal, yet better forms may soon be available.

Malone *et al.* (1980) mention (Volume 1, page 76) use of procedure pages projected onto a large screen in the middle of a U.S. nuclear plant control panel. The author has seen (unpublished) a decision tree requiring five sheets of 2 m^2 each to depict. The direct use of such large drawings seems intuitively impractical in the control room, but is being pursued. The problem would seem to be to recover the correct path on the tree as the aspects of the decision boxes change during the course of the event sequence.

The potential for implementing such a decision tree on a computer seems obvious Halden (1981, 1981b) has begun studies on the use of computer presentation of operation manual materials. The two referenced reports include a computer terminal and program to watch over compliance with equipment outage technical specifications (Halden, 1981) and the basic structure of a computer program for presenting sequences of instructions. Further work is left for the future.

8. CONTROL ROOMS AND OTHER DESIGN ASPECTS OF THE MAN–MACHINE INTERFACE

8.1. *Introduction*

The traditional 'human factors' concern, to the outsider at least, is the presentation of information to the operator in the control room. This topic is the principal subject of the present chapter. Related areas are alarms, status monitoring of safety systems, monitoring of critical safety functions, and disturbance analysis systems. Maintenance is also reviewed briefly.

Following the Three Mile Island accident, Malone *et al.* (1980) assessed the control room at that plant, along with other aspects of the man–machine interface. These authors' conclusions are given here verbatim:

> 'The primary conclusion reached on the basis of this investigation was that the human errors experienced during the TMI incident were not due to operator deficiencies but rather to inadequacies in equipment design, information presentation, emergency procedures and training.
>
> 'This general conclusion is supported by several more specific conclusions which are:
>
> (1) TMI-2 was designed and built without a central concept or philosophy for man–machine integration.
>
> (2) Lack of a central man–machine concept resulted in lack of definition of the role of operators during emergency situations.
>
> (3) In the absence of a detailed analysis of information requirements by operator tasks, some critical parameters were not displayed, some were not immediately available to the operator because of location, and the operators were burdened with unnecessary information.
>
> (4) The control room panel design at TMI-2 violates a number of human engineering principles resulting in excessive operator motion, workload, error probability and response time.
>
> (5) The emergency procedures at TMI-2 were deficient as aids to the operators primarily due to a failure to provide a systematic method of problem diagnosis.
>
> (6) Operator training failed to provide the operators with the skills necessary to diagnose the incident and take appropriate action.
>
> (7) Conflicting implications between instrument information, training, and procedures precluded timely diagnosis of and effective response to the incident.'

Control room designs and requirements generally are discussed by Malone *et al.* (1980), as well as maintenance. Prior to Three Mile Island there was some increasing attention being paid to human factors in nuclear power plant control rooms; see for example the work of Seminara and his collaborators (1977, 1979a, 1979b, 1980a, 1980b, 1981). Current programs for control room improvement, and recent technology developments, are reviewed in the following subsections.

8.2. *Human factor principles for control room design*

A discussion of general references for human capabilities and man–machine interfaces is given in Chapter 3 of this review. Military and other data directly relevant to nuclear control rooms are referenced in Appendix A of NRC (1981d). Many—most—of the precepts of this document are applicable to control rooms in general. How, then, can the designer or reviewer tell that there is a nuclear power plant connected to this particular control room? The short answer is that human capabilities are not significantly different for nuclear power plant operators. The information needs, the characteristics of the process and the particulars of the procedures will determine the technical content; thus, these things reflect the special behavior of the nuclear plant. Aside from the systems and functions analysis performed to determine the required technical content, the nuclear plant control room design process is the same as for any other control station of comparable complexity.

Appendix B of NRC (1981d) describes 'Systems/Operations Design Analysis Techniques' applicable to nuclear power plant control room design. Systems/Operations analysis is stated by the author to be the basic tool used in establishing design requirements, by 'systematically defining the equipment, personnel, and procedural data requirements to meet all functional objectives of the control room, including safe operation of the plant'. This reference gives a complete design process, suitable for new plants or control rooms if there are ever to be any. The concepts are also useful in performing a review of an existing plant, as described in the next sub-section. The central focus of the design or review process is a review of system functions and an analysis of the tasks required of the control room operating crew. Job and task analysis are discussed generally in Section 3 of this review. Task analysis should be the basis for the control room design. It was neglect of this precept that evidently led to the deficiencies in the Three Mile Island, Unit 2, control room so severely criticized by Malone *et al.* (1980).

8.3. *Control room reviews*

The shortcomings of U.S. nuclear power plant control rooms made evident by Three Mile Island showed the need for a program of review and improvements. Such a program is set forth in the TMI Action Plan (NRC 1980a, 1980b). Detailed design reviews are to be conducted for the control rooms of all plants, old and new. The changes shown by these reviews to be necessary will be implemented in conjunction with concomitant improvements in emergency operating procedures and operating crew training and installation of a Safety Parameter Display System (see next sub-section). The review and evaluation process is shown in Figs 3, 4 and 5.

The control room review is built on the technical basis furnished by the function and task analysis described in the last sub-section. Surveys of knowledgeable people and reviews of previous human errors are used, in addition to the function and task analysis, to identify potential problem areas for review. A survey of the information available and the arrangement, labeling, etc., of the displayed information is used to identify 'Human Engineering Discrepancies' (HEDs) where improvement may be needed. The functional and performance capabilities should be verified by walk-through/talk-through exercises simulating responses of an operating crew to postulated event sequences. The result of this process is a list of HEDs.

The close connection between the control room design and review and the training of the operating crew and the emergency operating procedures they use is evident. Preliminary assessments already conducted by the author of this review and his colleagues show how this connection operates. Often, an HED observed has been attributed to shortcomings in procedure or training rather than (or in addition to) the control room information presentation.

If a plant-specific simulator is available with a control room identical to the plant's, then the validation can be done in real time—an obvious advantage.

Figures 4 and 5 outline the process of assessing the HEDs identified in the review. Both the propensity for causing an operator error and the consequences of the error are considered in the assessment (NRC 1981e). Neither of these factors can be precisely determined. The probability of an error depends on many variables. The success shown by some operators in coping with abominably mis-designed boards (see for example Malone *et al.*, 1980, and Seminara *et al.*, 1977) amply demonstrates this. The consequences of an error depend on the sequence in progress and on the effect of other operator actions that can mitigate or aggravate the event. Seminara *et al.* (1979a) have shown how 'enhancement' changes—improved labeling, color coding, demarcation, and other changes that leave the instrumentation and control hardware unchanged—can improve control panel readability and usability. Figures 6a and 6b, taken from this reference, show graphically what can be done. The improvement is obvious.

An interesting and important question can be illustrated from Fig. 6b. The main steam trip and bypass valves (right side of panel) and the two sets of

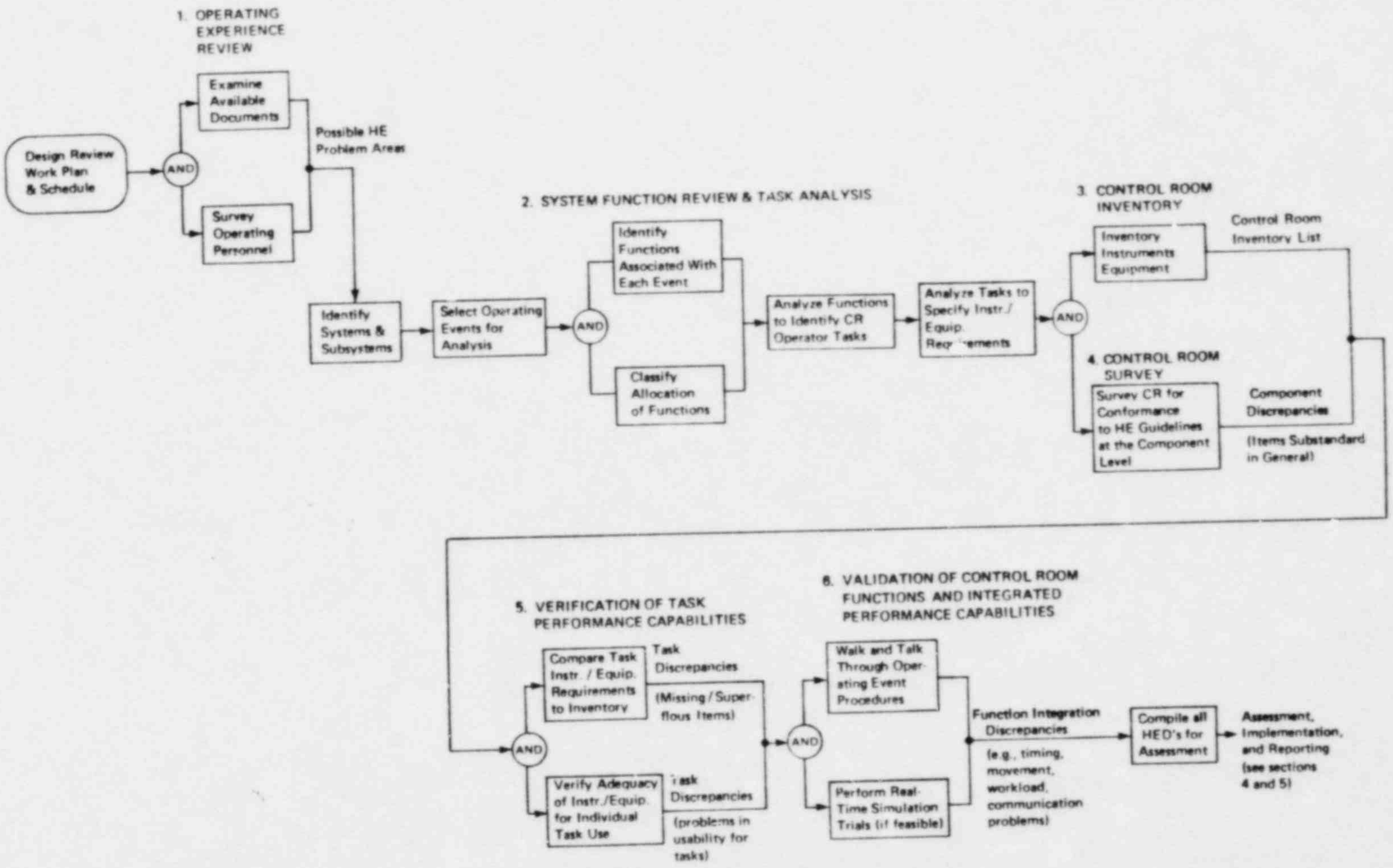
Design Review Work Plan & Schedule
AND
1. OPERATING EXPERIENCE REVIEW
Examine Available Documents
Survey Operating Personnel
Possible HE Problem Areas
Identify Systems & Subsystems
Select Operating Events for Analysis
2. SYSTEM FUNCTION REVIEW & TASK ANALYSIS
AND
Identify Functions Associated With Each Event
Classify Allocation of Functions
Analyze Functions to Identify CR Operator Tasks
Analyze Tasks to Specify Instr./Equip. Requirements
AND
3. CONTROL ROOM INVENTORY
Inventory Instruments Equipment
Control Room Inventory List
4. CONTROL ROOM SURVEY
Survey CR for Conformance to HE Guidelines at the Component Level
Component Discrepancies
(Items Substandard in General)
5. VERIFICATION OF TASK PERFORMANCE CAPABILITIES
AND
Compare Task Instr. / Equip. Requirements to Inventory
Task Discrepancies
(Missing / Superflous Items)
Verify Adequacy of Instr./Equip. for Individual Task Use
Task Discrepancies
(problems in usability for tasks)
6. VALIDATION OF CONTROL ROOM FUNCTIONS AND INTEGRATED PERFORMANCE CAPABILITIES
AND
Walk and Talk Through Operating Event Procedures
Perform Real-Time Simulation Trials (if feasible)
Function Integration Discrepancies
(e.g., timing, movement, workload, communication problems)
Compile all HED's for Assessment
Assessment, Implementation, and Reporting (see sections 4 and 5)

Exhibit 3-1. Review processes.

Fig. 3. Control room review process: determination of human engineering discrepancies From NRC (1981d).

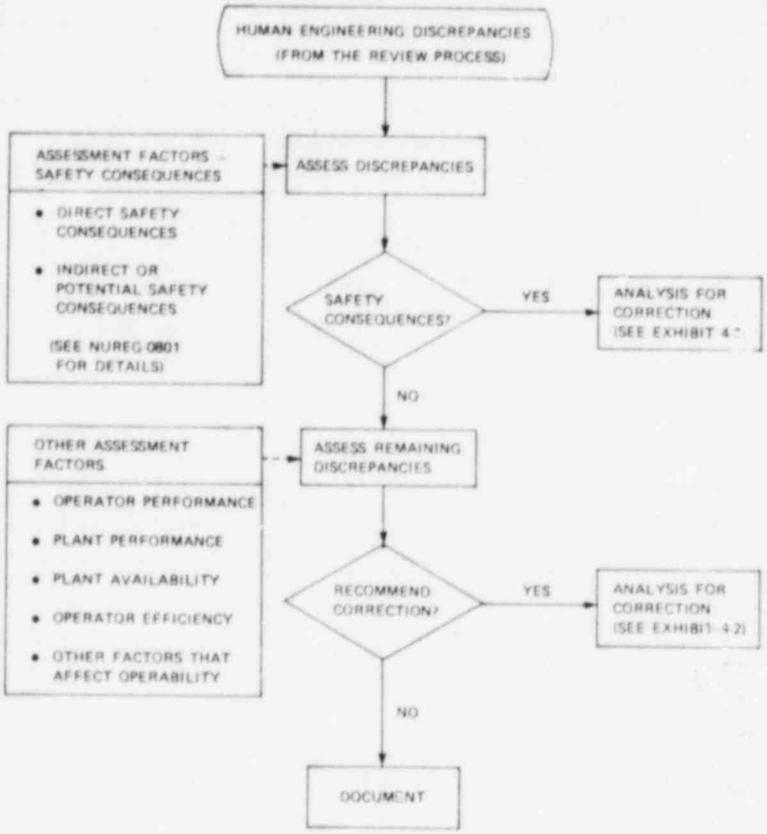
HUMAN ENGINEERING DISCREPANCIES (FROM THE REVIEW PROCESS)
ASSESSMENT FACTORS – SAFETY CONSEQUENCES
• DIRECT SAFETY CONSEQUENCES
• INDIRECT OR POTENTIAL SAFETY CONSEQUENCES
(SEE NUREG-0801 FOR DETAILS)
ASSESS DISCREPANCIES
SAFETY CONSEQUENCES?
YES
ANALYSIS FOR CORRECTION (SEE EXHIBIT 4-2)
NO
OTHER ASSESSMENT FACTORS
• OPERATOR PERFORMANCE
• PLANT PERFORMANCE
• PLANT AVAILABILITY
• OPERATOR EFFICIENCY
• OTHER FACTORS THAT AFFECT OPERABILITY
ASSESS REMAINING DISCREPANCIES
RECOMMEND CORRECTION?
YES
ANALYSIS FOR CORRECTION (SEE EXHIBIT 4-2)
NO
DOCUMENT

Exhibit 4-1. The assessment process. Selection of HEDS to be analyzed for correction.

ig. 4. Control room review process: selection of human engineering discrepancies to be analyzed. From NRC (1981d).

ain regulating valves (lower left) are arranged A–B–C from left to right. The auxiliary throttle valves center) are C–B–A with C on top, and the main solation valves (upper left) are A–B–C with A on top. At least you can read this on Fig. 6b, whereas the riginal labels in Fig. 6a are unreadable (and, in the uthor's experience, are often incomprehensible if you nanage to read them). The question is, should the panel be rearranged so all the A–B–C's are similarly aid out? The advantage is obvious. Not so obvious is he potential for error after the change for the operator who has learned the old layout. There is a need for btaining relevant, valid experimental data on this point.

The changes implemented as a result of the review hould be validated, by a process similar to that used or the earlier control room validation. This validation process should also be used to determine how much rearrangement should be done.

If extensive improvement is required, a better as well s cheaper solution may be the addition of a new console into the existing control room. The new panels, incorporating cathode-ray tube displays and computer formats, would be used for certain functions, with the old panels, perhaps with enhancement, serving as a backup.

No review and improvement program is known to the author to have been carried out and implemented with the scope and depth given in NRC (1981d, 1981e).

Pew *et al.* (1981) have evaluated some possible areas for human factors improvement, using analysis of four actual nuclear power plant transients. The analysis method was based on the critical decision elements actually made by the operating crews involved, categorized as detection, interpretation, etc. For 18 innovations (training, display improvement, addition of personnel, etc.), the analysis gives ratings based on ranking by a panel of experts and also on decision diagrams. Some results from this reference are given in Table 15. Training is ranked highest, with control room monitoring of basic safety functions, display improvement, and workspace layout judged very

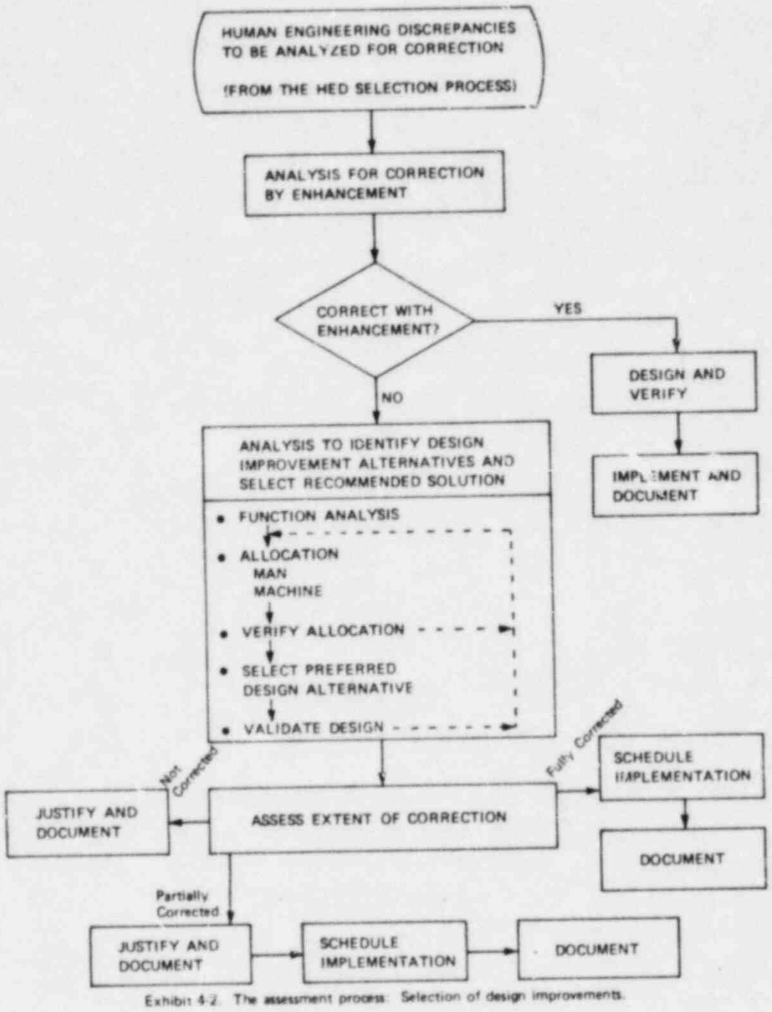
HUMAN ENGINEERING DISCREPANCIES TO BE ANALYZED FOR CORRECTION
(FROM THE HED SELECTION PROCESS)
ANALYSIS FOR CORRECTION BY ENHANCEMENT
CORRECT WITH ENHANCEMENT?
YES
NO
DESIGN AND VERIFY
IMPLEMENT AND DOCUMENT
ANALYSIS TO IDENTIFY DESIGN IMPROVEMENT ALTERNATIVES AND SELECT RECOMMENDED SOLUTION
• FUNCTION ANALYSIS
• ALLOCATION MAN MACHINE
• VERIFY ALLOCATION
• SELECT PREFERRED DESIGN ALTERNATIVE
• VALIDATE DESIGN
Not Corrected
Fully Corrected
JUSTIFY AND DOCUMENT
ASSESS EXTENT OF CORRECTION
SCHEDULE IMPLEMENTATION
DOCUMENT
Partially Corrected
JUSTIFY AND DOCUMENT
SCHEDULE IMPLEMENTATION
DOCUMENT

Exhibit 4-2. The assessment process: Selection of design improvements.

Fig. 5. Control room review process: analysis and correction of selected human engineering discrepancies. From NRC (1981d).

helpful. This reference also includes valuable insight on operating crew knowledge-based behavior and decision processes.

8.4. *Information presentation in the control room*

The general principles of information display are well known and have been adapted to nuclear power plant control rooms by Mallory *et al.* (1980) and NRC (1981a, 1981d, especially Appendix A of 1981d). The last reference contains a detailed cross-reference of the 'Control Room Human Engineering Guidelines' to an extensive bibliography. Besides these general and particular guidelines, a number of special areas have been studied recently; these are reviewed in the following subsections.

8.4.1. *Control room alarms.* A principal control room man–machine interface is embodied in the alarm system. Its basic function is to call the operator's attention to situations requiring such attention. In current control rooms, the alarm system is judged to have severe shortcomings, in need of substantial improvement.

Visuri *et al.* (1981) have discussed the alarm system in a hierarchy of operator support. All these systems—the definitions can overlap—assist the operators' decision making:

(1) Safety Panel (Sub-section 8.4.3 of this review) displays recent time histories of approx. 20 key safety parameters in one place for monitoring the safety status of the plant.

(2) Safety Console (8.4.3). An enhanced safety panel

[redacted]

Table 15. Rating by a panel of experts of the impact of improvements on operator decision making (1 = not helpful; 7 = extremely helpful) from Pew, Miller and Feeher (1981)

	Mean	Std. dev
STAFF ORGANIZATION		
(1) Availability of additional personnel	2.88	1.45
(2) Prior definition of operator responsibilities	2.13	0.93
(3) Addition of shift technical advisor to crew	3.50	1.87
TRAINING		
(4) Skill training	4.25	0.83
(5) Understanding standard and emergency procedures	5.75	0.43
(6) Knowledge of specific plant characteristics	6.00	0.87
(7) Knowledge of power plant fundamentals	4.63	1.11
(8) Training in decision skills	4.88	1.45
COMPUTERIZED SUPPORT SYSTEMS		
(9) Monitoring basic safety and availability functions	5.63	0.48
(10) Disturbance detection and classification	4.13	1.36
(11) Information integration	3.50	1.32
(12) Action identification	1.75	0.66
(13) Preditive simulation	2.00	1.00
WRITTEN PROCEDURES		
(14) Procedure accessibility and accuracy	5.75	1.20
CONTROLS AND DISPLAYS		
(15) Display improvement	5.25	1.39
(16) Control improvement	3.75	1.71
(17) Control-display integration	4.75	1.39
(18) Workspace layout	5.25	1.20

with access to greater than 100 signals to support diagnosis and action selection and verification in addition to safety status monitoring.

(3) Critical Function Monitoring System (8.4.3). A safety console with logic that relates safety status to maintaining or restoring critical safety functions (see Section 7).

(4) Disturbance Analysis System (8.4.4). Computer software to determine the cause of a disturbance, analyze and predict its development and present corrective actions.

(5) Disturbance Analysis and Surveillance System (8.4.4). A Disturbance Analysis System to which is added surveillance of safety status, system availability, safety procedure and technical specifications. The scope of this is still under consideration, and these systems are highly developmental today.

(6) Alarm Handling System. Extracts relevant alarms out of the large amount of process signals.

(7) Alarms are indications of either correctly performed safety functions or changes in plant operating mode caused by the disturbance. Presenting only exceptions to normal patterns would relieve the operators from extraneous information. (Visuri *et al.*, 1981).

The traditional alarm component in power plant control rooms is the *annunciators*, comprising one or more audible alarms and panels of multiple, backlighted tiles for the individual functions. The visual aspect of each tile (dark, lit, flashing) gives the status of the function; the audible alarm calls the operator's attention to changes in status.

For single component failures or errors, the system works well. If (for example) the level controller on one steam generator malfunctions, the resulting incorrect water level is annunciated and the operator is directed to the subsystem for troubleshooting.

For many plant transients, a large number of annunciators light up nearly simultaneously. The feedwater trip sequence that initiated the accident at Three Mile Island, like most such sequences, tripped over 100 annunciators in the first few minutes (Kemeny, 1979). Many normal or frequently encountered situations are in this class; the fact that operators can make any sense out of such an array is remarkable.

In the author's experience, there are upwards of 1000 annunciator tiles in a single-unit control room.

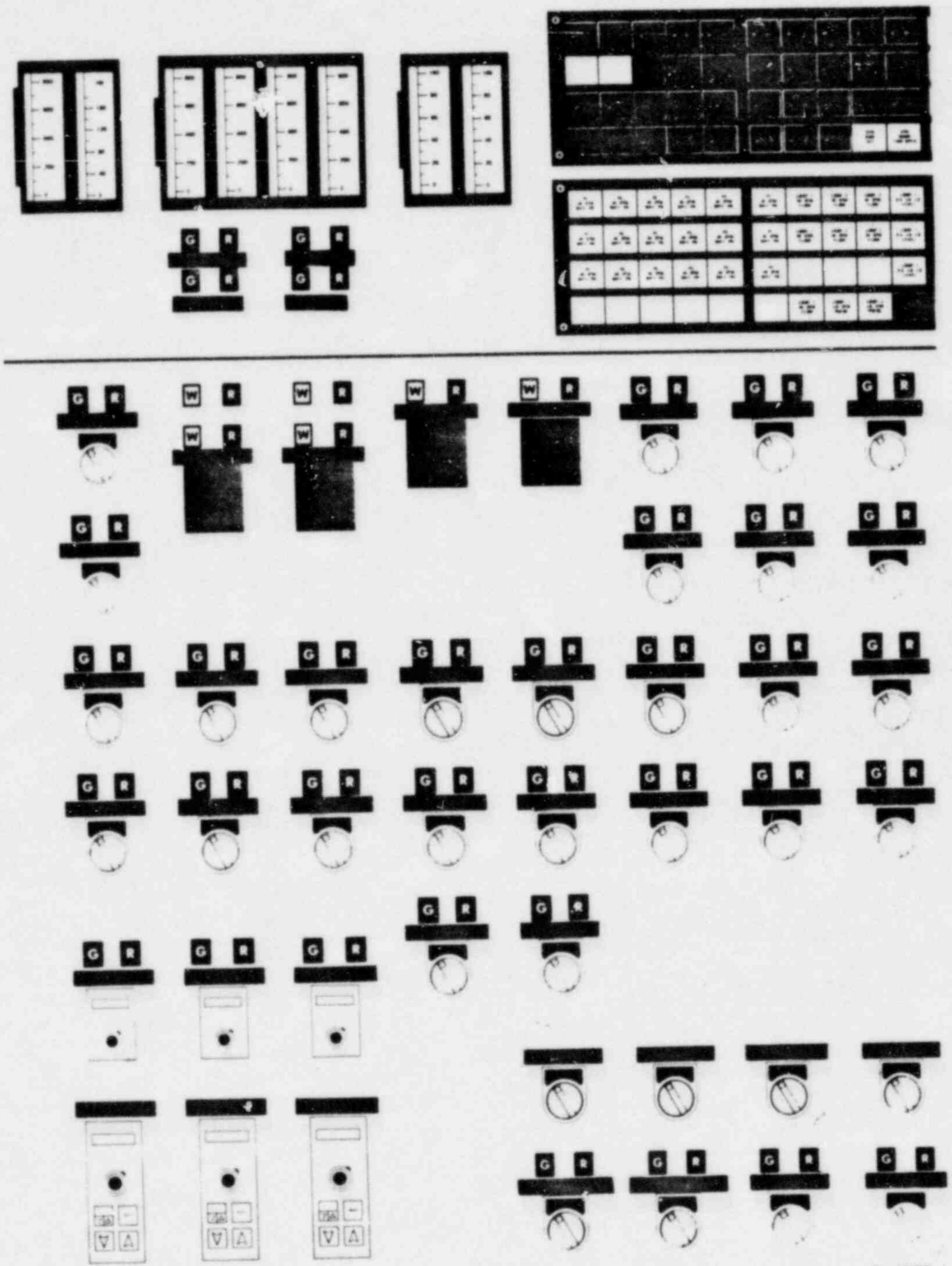

Fig. 6a. Before and after panel layouts illustrating human factors enhancement. From Seminara *et al.* (1979a).

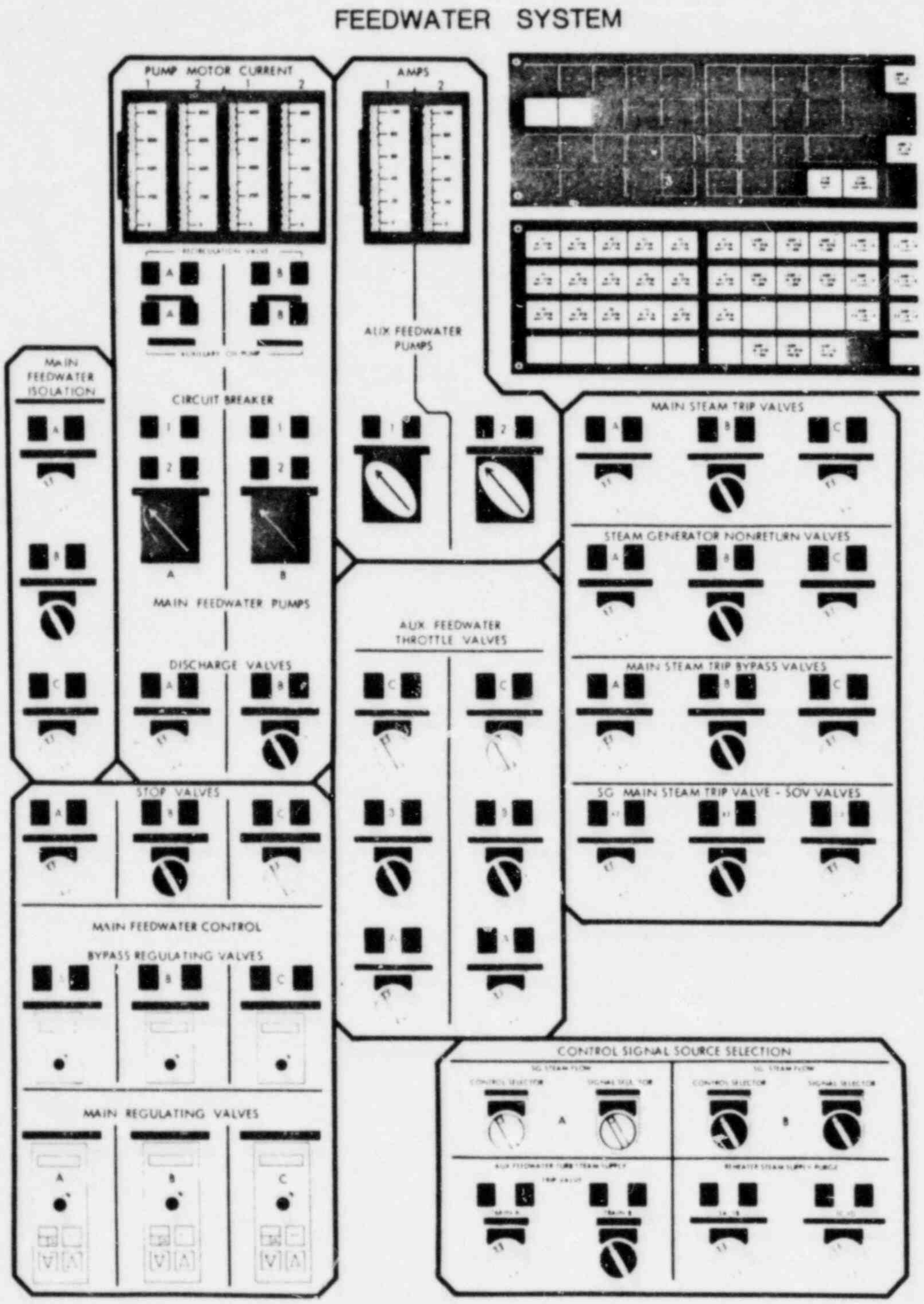

Fig. 6b. Before and after panel layouts illustrating human factors enhancement. From Seminara *et al.* (1979a).

Moreover, he has never seen fewer than 40 tiles lit, even during operation deemed to be normal and uneventful.

Banks and Boone (1981) have surveyed some of the problems of existing annunciator systems. They note the presence of inexcusable flaws:

(1) The legend on the tiles was small, or otherwise unreadable, confusing, cryptic, with abbreviations inconsistent with labels on associated instruments and procedures.

(2) Many annunciators alarm rcutinely. In one plant, 46 tiles relate to doors, they alarm each time a door is opened, although the control room operating crew has no action to take when a door opens. Many other distracting alarms are present. Some are alarmed for normal conditions.

(3) In one plant, there are 12 separate audible alarms—horns, bells, buzzers, warbling tones. When a certain fuse blows, they all sound!

(4) The layout, arrangement, hierarchy and demarcation of the tiles is poor.

But even in well-designed systems, 1000-plus tiles with legends are little help to the operator in diagnosing and mitigating sequences that alarm 100-plus tiles in a few minutes, with a fresh alarm every few seconds.

The use of printers and CRT displays for alarm indication and recording is well established. Yet 100-plus lines of alarms on a printer or CRT is even less useful to the operator in real time than the pattern—perhaps recognizable—of lit and flashing tiles.

A diagnostic aid easily implemented in computer-based systems is precise time-ordering of alarms to facilitate deciding what came first, thus helping to identify the cause of the event.

A number of recent studies have been aimed at improving the usefulness of alarm information for the operator coping with a major transient. All are based on computer logic and CRT display. Jervis (1980) states as the basic objectives: 'to integrate the data and alarms on a plant area basis and make them readily accessible by the operator'. This author gives five essential features:

(i) An overview which gives a quick assessment;

(ii) Time order of detection of alarms;

(iii) Delineation of plant areas and systems in alarm state;

(iv) Permanent record of alarms;

(v) Cross-referencing of data and alarms.

Jervis (1980) describes several existing systems and gives a formal functional specification of one. The central idea of this system is classification of alarm signals and presentation to the operator of an overview of the alarm status of the plant. Alarms are suppressed (from the visual display) by software logic whose technical basis is not given by the author. Wahlström (1980) suggests a logic involving the various states of the plant. As an example, a low pressure alarm on a pump discharge pipe would be inhibited when the pump in not running or not supposed to be running, or not required to run. Bürger and Végh have extended the concept to include display of 'the alarm trees, showing the operator the "alarm patterns" from which the deduction were made'. Černý (1980) describes briefly a hierarchical classification of 930 alarm variables in a fossil power plant.

Visuri *et al.* (1981) give a detailed discussion of a developmental alarm handling system, with details in the related paper by Visuri and Øwre (1981). Both *a priori* data and on-line process data are edited and translated by the computer program into process status and alarms. The authors identify two classes of alarms:

(i) Automatic functions that should follow a trip that are not carried out;

(ii) Off-normal signals which would be presented as alarms in a conventional system, with normal consequences and multiple signals suppressed.

Two classes of displays are described:

(a) Color-coded process layout diagram at various levels of detail;

(b) Chronological lists of alarms selected by degree of urgency.

A computer program embodying these principles was developed for a 660 MW Finnish BWR. Simulation of a pipe break in the primary coolant cleanup system showed 140 alarms in 10 sec, 210 in 30 sec. The alarm handling program gave 10 and 23 high-priority alarms—a reduction of about a factor of 10. 'The alarms indicating the location of the break by high room temperature and water on the floor were the 11th and the 22nd among the filtered alarms, but 174th and 93rd in the all alarms list.'

8.4.2. *Status monitoring.* This topic is here limited to techniques for presenting to the operator a condensed picture of the readiness of systems he may call on during transient and accident sequences. The work reported up to now has been limited to safety systems for plant shutdown and cooling.

Not reviewed here is an extensive literature in the technology of trouble monitoring, for example by on-line analysis of acoustic noise or neutron fluctuations.

All safety systems—all systems—include information presented to the operator for his use in controlling the action of the systems. For safety systems, most of which have no function during normal operation, the initial information needed by the operator is system readiness; that is, availability of the system to function if needed. At various levels of sophistication this can include, (1) cognizance of equipment deliberately removed from service for testing and maintenance, (2) checking for correct lineup of valves and circuit breakers, (3) monitoring of essential support functions like energy, cooling and lubrication, (4) keeping up with required testing intervals and allowable reductions in redundancy, (5) on-line monitoring of the safety function success as evidenced by critical variables. The last, item (5), is discussed separately in sub-sections 8.4.3 and 8.4.4, below.

Administrative procedures are universally applied in implementing safety system monitoring. A long list of reported lapses testify to the need for improvement in this monitoring. The auxiliary feedwater system at Three Mile Island was valved out of service before the accident, and its non-availability was not recognized until 8 min into the sequence of events.

The author has been shown many computer-based systems for keeping up with required surveillance tests and equipment out of service. These are basically accounting systems to improve the effectiveness of administrative controls. We lack quantitative data on the effectiveness of such controls and the improvement provided by the computer systems.

NRC (1973) has published a Regulatory Guide on safety system status monitoring, recommending installation of information readout in the control room to supplement and facilitate administrative control. The TMI Action Plan (NRC 1980a, Item I.D.3) includes status monitoring as an item for future consideration. A commitment to implement the guide has been included in a proposed rule by NRC (1981m).

Brown and Von Herrmann (1981) evaluated existing U.S. monitoring schemes using a system ranking based on risk importance. They used the following hypothesis: 'The ability of the operating crew to efficiently determine the status of a safety related system or component is commensurate with the safety significance of that system or component.' Their measure of 'safety significance' was based on probabilistic risk assessment. The Reactor Safety Study (NRC 1975b) risk model was used, with the increment in core melt frequency from the unavailability of the system under consideration used as the measure of safety significance.

The relative effectiveness of various safety status monitoring techniques was assessed by judgemental analysis of how well the status is *transmitted* to the operator; capability of the operator to *receive* the information (training, procedures) was not included.

The effectiveness of status monitoring was found not to be consistent with the risk significance of the systems and components in the plants studied. Undesirable features of present designs were noted, similar to the alarm system reviews of Banks and Boone (1981).

A program to develop an automated safety system status monitoring system has been described by Nadelik and Roggenbauer (1980) and by Haubert and Stokke (1980). Graae (1981) has reported a pilot experiment, applying some developmental software from this program in an operating nuclear plant.

The basis of the system is a set of decision matrices for possible combinations of first and second failures in highly redundant systems. Allowable outage times, determined by plant-specific rules (in the U.S., technical specifications) that may be based on probability considerations, are the constraints on the system. The information displayed includes the system status, applicable rules, and mandated actions. If prompt action is not required, the operator is kept aware of times available for repair options.

The testing time of a few months reported by Graae (1981) for the pilot experiment involved only a few real faults, but simulation testing provided additional operating experience. The referenced author concluded, 'the experiment has given evidence enough to provide that a system of this type is of real benefit for the operation of a nuclear power plant. The experiment has also outlined how a system in full scale should look like to meet the practical needs of the operating staff'.

8.4.3. *Monitoring of plant safety status.* Whereas the previous sub-section treated monitoring of the readiness of safety system hardware, this sub-section considers the monitoring of the plant process. Thus we consider here the Safety Console, Safety Panel and Critical Function Monitor of Visuri *et al.* (1981).

'Safety' as a real-time variable has not been well defined. It is obviously insufficient to monitor only radioactive releases; plant 'safety', although basically defined as freedom from releases, involves prevention and mitigation of accidents that lead to releases. On the other hand, it is impractical to monitor all variables that could possibly lead to situations involving potential releases. A most useful concept is that of 'critical safety functions', discussed in sub-sections 5.2 and 5.7 of this review. The monitoring of the variable 'safety' can, in this view, be reduced to monitoring the values of a limited number of plant variables—a 'state vector' for safety.

Unique, complete sets of variables comprising a Safety State Vector have not been published. NRC (1981) gives only general guidance relating the variables to Critical Safety Functions.

Honeycutt *et al.* (1981) give a set of 21 variables for a PWR, which (with redundancy) means handling 36 signals. For a BWR, these authors suggest that a somewhat shorter list would be appropriate, based on the work of Levy (1980).

Yamazaki *et al.* (1980) have described a safety console for BWR application with 12 variables.

A much larger set of variables comprises the instrumentation needed to follow the course of an accident. This has been defined by NRC (1980g); five categories of variables are given:

(1) Primary information for control room operator to accomplish manual actions for design basis accidents;
(2) Information whether safety functions are bei. g accompiished;
(3) Information to indicate potential or actual breach of barriers to fission product release;
(4) Information on operation of safety systems;
(5) Information to monitor and assess any radioactive releases.

The Safety State Vector contains a much smaller number, since its function is monitoring Critical Safety Functions rather than the whole course of an accident sequence. A still smaller set of variables is used for the Safety Console, whose primary function is 'to aid the operator in the rapid detection of abnormal operating conditions' (NRC (1981)). Most Safety Console preliminary designs the author has seen have a cluster of 10 or fewer plant variables for a primary display. Since these are displayed on a CRT, many additional 'pages' of information are readily accessible, so long as it is in the underlying data base. The design trend in the U.S. is a large data base, encompassing over 100 variables, with a large number of varied formats available on the operator's request. The front page, normally displayed, is the Safety Panel.

The potential of this system seems limited only by the data base and by the ability of the operating crew to receive and use the information. Development of additional programming and operational uses is to be expected, in the author's opinion. Possibilities include safety system status monitoring and disturbance analysis. Further development, simulator studies, and operational experience must all be acquired before the actual, realizable potential of this group of systems will be determined.

NRC (1981k, 1981l) and Ramos (1981) have given criteria for a Safety Parameter Display System—a Safety Console integrated into a control room, but used in conjunction with other emergency response facilities in coping with accidents. Meijer (1980) described a 'Critical Function Monitoring System' that includes a Safety Console. Many designs are under development.

8.4.4. *Disturbance analysis.* Disturbance analysis has been considered generally by Johansson (1980) who gives the following definition:

> 'Disturbance analysis is an automated method for the surveillance of a process, especially concerning its deviations from normal operating conditions, and with the purpose to give the process operator information about these deviations. This task is accomplished through a comparison of the actual process information with that obtained from an *a priori* analysis of the process.'

The objective, of course, is to improve the operator's knowledge and understanding of what is going on and thus to improve the probability of the correct actions being taken.

Dowling *et al.* (1981) have reported a detailed feasibility study of a Disturbance Analysis System (DAS—in this review, no distinction is made between DAS and similar systems that also include surveillance, sometimes called DASS). The 500-plus page report includes goals and functions, design procedures, and a developed design specification.

These authors approach the DAS in terms of plant states. The DAS is to generate target plant states, determine the actual plant state, and identify 'disturbances' as differences between the target and actual states. Plant functions and conditions (requirements) were defined for each of 22 subsystems giving 235 possible DAS functions. Of these, 194 were selected using cost/value considerations. Additional DAS functions can be added as modules.

The overall goals, in order of descending priority, were given as:

(1) Achieving safe shutdown,
(2) Monitoring for trip surface assumption violations,
(3) Keeping the plant running,
(4) Achieving a damage-free shutdown.

It can be seen that DAS can be an aid to achieving these goals, which are also the goals of other design and operational activities.

A single reference PWR was used to develop a specific proposed DAS system. An example of a plant function is 'fluid mass inventory in the pressurizer and reactor coolant subsystem are to be determined from hot and cold leg temperatures, hot leg pressure, and the water level and temperature in the pressurizer . . . For this application, the range of operation was limited to subcooled conditions in the reactor coolant system, four-pump operation, and the water level in the pressurizer between the upper and lower limits of measurement . . . The intention is to obtain information on leaks before conditions deteriorate to the point where flashing occurs in the coolant'. Algorithms are given for the value of inventory and its uncertainty. A display format (mass vs time, linear plot) is proposed.

Computer studies gave 'better' operation and quicker recognition of the events with the developmental DAS.

A Germany group has been developing the STAR, a DAS, for several years. The most recent report is Buttner *et al.* (1981); see also Buttner *et al.* (1980).

A STAR system has been installed and tested in the Grafnerheinfeld nuclear power station, but operation of the plant has been delayed. The plant variable data base is scanned every 5 sec and parameters outside of predetermined limits (high level, low flow, etc.) are alarmed. A model of the plant, embodied in cause-consequence diagrams, is used to digest the information.

The cause consequence diagram proceeds from prime causes (plant disturbances, for example pump switched off, controller failure, tube break) through changes in plant variables outside limits, to messages to the operator that give instructions for manual actions or information about pending or actual automatic actions. Possible interactive intermediate steps include questions to be answered by the operator giving the computer additional information not available in the data base. To develop a set of cause consequence diagrams is the most complicated and critical task. As a byproduct, such development may reveal system or instrumentation inadequacies.

The operator receives from STAR (1) an alarm summary—the messages and instructions, and questions, from the DAS; (2) a more detailed presentation of the subsystem where the trouble is located.

Buttner *et al.* (1981) give the results of 5 yr work on the development of this system. Several improvements are foreseen, including trending analysis to inform the operator about a disturbance before the first limit is exceeded.

Meijer *et al.* (1980) describe a developmental DAS that also is based on cause consequence diagrams. Much attention was paid to development of display formats to enhance operator understanding. Information displayed includes identification of the affected system, the disturbance as inferred with the prime cause, suggested recovery action, and anticipated consequences if the disturbance is not corrected. A demonstration system with 98 input signals was tested on a PWR simulator. Systems included were feedwater and component cooling water. The DAS improved operator response and provided guidance for additional system development. Cause consequence diagrams were also developed and the simulator operated to successfully track the Three Mile Island accident; the DAS messages would likely have aided in avoiding the serious later events in the TMI sequence.

Yamazaki *et al.* (1980) describe a simplified DAS based on errors between the values of 16 signals from the plant, compared to calculated values for these signals from a linear dynamic model.

Long (1980) has cautioned developers and users of DAS projects of the need for reliability and robustness in the DAS function, in order that the operator be truly assisted rather than distracted or confused. The need for simulator verification and operational experience is emphasized.

8.5. *Experimental measurements*

In several connections, it is highly useful to obtain experimental operational information. Examples of this need include evaluation of control room and procedure changes to avoid safety decrements, comparison and verification of proposed operator aids and validation of training.

Although data from actual control room evolutions would in principle be best, it is impractical to wait for incidents to occur in plant operation. Rare events would be unavailable. It is therefore advantageous to use simulation techniques to obtain such data, even though stress factors would be different (presumably, more severe) in real accident sequences. Bott *et al.* (1981) describe an experimental facility for such measurements. The basic tool is a full-scope nuclear power plant simulator with a control room that duplicates that of the power plant. To this is added a Performance Measurement System, a computer software system developed by General Physics Corporation for the Electric Power Research Institute. This consists of on-line recording of data of the control room inputs (the aspects of control devices manipulated by the operators) and the simulated plant behavior as displayed on the control room readout devices. The recorded data are analyzed for event sequence and any off-normal variable behavior.

The initial experiments described by Bott *et al.* (1981) analyzed operator trainee responses to seven initiating events that had actually occurred in operating plants, for future comparison of simulator data with experience. The results include insight into operating problems and time-response data; the latter fit log-normal distributions.

8.6. *Advanced control rooms*

The development of reliable on-line computers and large-screen cathode-ray tube terminals provide an obvious potential for man–machine interface improvement. Around the world, advanced control rooms have been developed, using the new technology to achieve display functions not previously possible.

While the earlier applications simply use the CRT displays to substitute for hard-wired indicators, more recently proposals have been made to embody alarms, safety panels, safety consoles, DAS, and other 'smart' functions into the computer–CRT complex. The preceding sections of this chapter include many references to such proposals.

The basics of advanced control rooms are simple enough. A number of CRT displays (the author has seen as few as five and as many as 16) are grouped into a suitable console or panel along with hard-wired displays and controls. A critical computer, or pair of computers for reliability, or distributed microprocessor system, provide the data handling and display formatting.

The hard-wired display indicators are used to back up the computers so plant availability is not controlled by computer reliability, and to provide qualified (seismic, environmental) safety-grade indicators for safety functions.

Present practice is to use conventional hard-wired control devices (switches, push-buttons, knob adjustments) rather than keyboard inputs via the computer.

Although many operating control rooms have a few CRT displays sprinkled over the control panel, only a few plants in operation have full CRT boards with hard-wired backup instruments. To date, operational and simulator experience have been highly promising.

The interested reader is referred to Halden (1980) and GRS (1980) for recent reviews.

8.7. *The man–machine interface outside the control room*

Although the principal, traditional focus on 'human engineering' is on the control room, many events testify to the incident potential of operations outside the control room. Many plant operations, much testing, and most maintenance is performed outside the control room. Control-type operations designed to be conducted at stations outside the control room are governed by the same principles as those in the control room.

Testing and maintenance activities are conducted by non-licensed operators and crafts people, without the planning and discipline of a control room, yet have a high potential for affecting safety. Failure to restore the auxiliary feedwater system to operability after testing contributed to the Three Mile Island accident.

IAEA (1980a) has in preparation a Safety Guide on maintenance in nuclear power plants. This guide includes recommendations on program scope, organization, administrative controls, facilities and audits.

Seminara and Parsons (1981) have performed an extensive review of the human factors aspects of maintenance in nuclear power plants. These authors conclude that, although the military establishment has developed criteria and procedures for maintainability in design and maintenance program guidelines, the U.S. nuclear power designers seem not to have maintenance in mind. 'The magnitude and nature of the deficiencies that were found do strongly suggest the need for a systematic and concerted effort to design power plants that are maintainable in a more reliable, safe, effective and economic fashion. This need is far more acute in nuclear than in fossil plants. Design for maintainability requires deliberate, specialized, and integrated concern for human factors from concept development to system implementation.' Brune and Weinstein (1980) have developed a checklist for evaluating procedures for maintenance and testing. This work is aimed principally at performing these tasks more safely at operating plants, whereas Seminara and Parsons (1981) deal with design and operation.

The author believes that design, procedures, and operation aspects of maintenance and testing are all in need of improvement.

As a result of the Three Mile Island accident, a check by an independent qualified person is required whenever a safety-related system is manipulated outside the control room (NRC 1980a, Item I.C.6). We need a study to see whether error data show any improvement attributable to this requirement. The safety system status monitor should also provide improvement in assuring restoration after maintenance and testing.

9. CONCLUDING REMARKS

This paper provides a review of the most important programs aimed at improving the contribution of people to nuclear power plant safety. They range from long-range research projects to applications now being implemented at operating plants. The latter include substantial changes, accomplished or imminent, in personnel qualifications, procedures and control room designs. These seem to the author to be likely to provide considerable improvement in the safety performance of the people involved. A note of caution, however: neither a quantitative measure of the actual safety improvement to be realized, nor a model of behavior capable of providing quantitative estimates, is yet available. Such measures and models are under development. They are needed, together with operational and experimental data to support them. Development and implementation of changes in operating plants should be accompanied by programs of verification and validation, using the best models and data available, and with ongoing surveillance of operational safety as revealed by plant experience. In this way, needed timely improvement can be achieved in the human aspect of nuclear power plant safety.

REFERENCES

Allenspach F. R. and Crocker L. P. (1980) Guidelines for utility management structure and technical resources, Draft Report for Interim Use and Comment, NUREG-0731, U.S. Nuclear Regulatory Commission.

Andersson H., Bäck P. and Wirstad J. (1979) Job analysis for training design and evaluation, Report No. 6, Swedish Nuclear Power Inspectorate.

Andersson H. (1981) An approach for operators role in complex process operation, in HPR-269, see Halden (1980).

Banks W. W. (1981) Human engineering CRT display development guidelines, EG & G Idaho, Inc. (in press).

Banks W. W. and Boone M. P. (1981) Nuclear control room annunciators: problems and recommendations, NUREG/CR-2147, U.S. Nuclear Regulatory Commission.

Bjørlo T. J. and Trengereid J. K. (1979) Coordination of operator supporting systems and procedures, Paper presented at IAEA-NPPCI Meeting 'Procedures and Systems for Assisting an Operator during Normal and Anomalous Nuclear Power Plant Situations', Munich, 5–7 December 1979.

Blomberg P. E., Josefsson R. and Åkerhielm F. (1977) Experience with the use of the Studsvik compact simulator, Paper 3.2 in Proceedings of IAEA Specialists Meeting, Simulators for Training of Nuclear Power Plant Operators and Technical Staff, 27–29 October 1976, S-546, Aktiebolaget Atomenergi, Studsvik, Nyköping, Sweden.

Bohr E., Hennig, J., Preuss W. and Thau G. (1977) Human factors in the nuclear power plant, RS 13-510, 321/31-SR-100, TÜV Rheinland, Germany; NRC Translation 460, Vol. I and II, U.S. Nuclear Regulatory Commission.

Borghese Joseph B. (1978) Human performance using column and star format multivariate color CRT displays. Man–Machine Systems Laboratory, Massachusetts Institute of Technology.

Bott T. F. *et al.* (1981) Criteria for safety related nuclear power plant operator actions: initial pressurized water reactor (PWR) simulator exercises. NUREG/CR-1908, U.S. Nuclear Regulatory Commission.

Brown R. G. and Von Herrmann J. (1981a) Boiling water reactor status monitoring during accident conditions, NUREG/CR-2100, U.S. Nuclear Regulatory Commission.

Brown R. G. and Von Herrmann J. (1981b) Light water reactor safety features status monitoring final report, NUREG/CR-2278, U.S. Nuclear Regulatory Commission.

Brune R. L. and Weinstein M. (1980) Development of a checklist for evaluating maintenance, test and calibration procedures used in nuclear power plants, NUREG/CR-1368, and Procedures evaluation checklist for maintenance, test and calibration procedures, NUREG/CR-1369, U.S. Nuclear Regulatory Commission.

Brune R. L. and Weinstein M. (1981) Development of a checklist for evaluating emergency procedures used in nuclear power plants, NUREG/CR-1970 and Checklist for evaluating emergency procedures used in nuclear power plants, NUREG/CR-2005, U.S. Nuclear Regulatory Commission.

Bürger L. and Végh E. (1980) Man–machine communication in experimental reactor control room, pp. 247–260 of IAEA/NPPCI Specialists meeting on procedures and systems for assisting an operator during normal and anomalous nuclear power plant operation situations, GRS-19, Gesselschaft für Reaktorsicherheit, Cologne, Germany.

Büttner W. E. *et al.* (1980) Functions and design characteristics of the STAR disturbance analysis system, paper presented at IAEA-NPPCI meeting Procedures and systems for assisting an operator during normal and anomalous nuclear power plant situations, Munich, 5–7 December 1979; GRS-19, Gesellschaft für Reaktorsicherheit, Cologne, Germany; see also Felkel L. *et al.*, Analytical methods and performance evaluation of the STAR application in the Grafenrheinfeld nuclear power plant, in the same volume.

Büttner W. E. *et al.* (1981) Disturbance analysis and alarm handling, a current review of requirements based on experience with the STAR system, Paper C1-1 of Halden Project Meeting at Fredrikstad, Gesellschaft für Reaktorsicherheit, Cologne, Germany.

CE/Studsvik (undated) Compact nuclear simulator, an innovative classroom size training device . . . , Combustion Engineering, Inc., Windsor, CT 06095, U.S.A.

Černý R. (1980) The dynamic classification and reduction of alarms in computer-based information systems, Session V of IAEA/NPPCI specialists meeting on Procedures and systems for assisting an operator during normal and anomalous nuclear power plant operation situations, GRS-19 Gesellschaft für Reaktorsicherheit mbH, Cologne, Germany.

Cocquyt G. *et al.* (1977) Training exercises for basic understanding of the dynamics of PWR power plants, Paper 3.3 in Proceedings of IAEA specialists meeting, Simulators for training of nuclear power plant operators and technical staff, 27–29 October 1976, S-546, Aktiebolaget Atomenergi, Studsvik, Nyköping, Sweden.

Code of Federal Regulations (1981) Title 10 (Energy) Parts 1–199, Office of the Federal Register, Washington DC. Abbreviated as 'CFR' in citations; '10 CFR 55.20' means Code of Federal Regulations, Title 10, Part 55, Section 20.

Combustion Engineering (1981) Emergency procedure guidelines, CEN-152, and emergency procedure guidelines development, CEN-156, Combustion Engineering, Inc., Windsor, CT 06095, U.S.A.

Corcoran W. R. *et al.* (1980a) The operator's role and safety functions, TIS-6555, Combustion Engineering, Inc., Windsor, CT 06095, U.S.A.

Corcoran W. R. *et al.* (1980b) The critical safety functions and plant operation, Paper presented at IAEA International Conference on Current nuclear power plant safety issues, Stockholm 2–24 October 1980, TIS 6743, Combustion Engineering, Inc., Windsor, CT 06095, U.S.A.

CSNI (1981) CSNI specialist meeting on Operator training and qualifications, abstracts, SINDOC (81) 8, OECD

Nuclear Energy Agency. The proceedings of this conference have not yet been published.

Danchak M. M. (1981) Techniques for displaying multivariate data on cathode ray tubes with applications to nuclear process control NUREG/CR-1994, U.S. Nuclear Regulatory Commission.

Davis L., Mazour T. and Zaret R. (1981) Analysis, conclusions and recommendations concerning operator licensing, NUREG/CR-1750, U.S. Nuclear Regulatory Commission.

Denton H. (1979) Letter to all operating nuclear power plants; Subject: discussion of lessons learned short term requirements, 30 October 1979, U.S. Nuclear Regulatory Commission.

Denton H. (1980) Letter to all power reactor applicants and licensees, Subject: qualifications of reactor operators, 28 March 1980, U.S. Nuclear Regulatory Commission.

Dowling E. F., Benedict B. J. and Snidow N. L. (1981) Disturbance Analysis and surveillance system scoping and feasibility study-final report, ALO-139, U.S. Department of Energy.

DSN (1981) Position des opérateurs sur la formalisation des procédures I et A (Incidents et Accidents) DSN No. 415, Commisariat à l'Energie Atomique, Départment de Sûreté Nucléaire, France.

Duncan K. D. (1981) Training for fault diagnosis in industrial process plant, in Rasmussen (ed.) *Human Detection and Diagnosis*, Plenum Press, 1981.

Edsberg E. and Thomassen B. B. (1981) Functioning of the operating crew in a complex control system, HWR-29, OECD Halden Reactor Project.

Ehret C. (1980) New approaches to chronohygiene for the shift worker in the nuclear power industry, to appear in Night and shift work: a multidisciplinary approach (Vth Symposium on Night and Shift Work, Rouen, 12–16 May 1980, Pergamon Press.

Eisenhut D. (1979) Letter to all operating nuclear power plants; subject: followup actions resulting from the NRC staff reviews regarding the Three Mile Island Unit 2 accident, 13 September 1979, U.S. Nuclear Regulatory Commission.

Eisenhut D. (1980) Letter to all licensees of operating plants and applicants for operating licenses and holders of construction permits, subject: interim criteria for shift staffing, 31 July 1980, U.S. Nuclear Regulatory Commission.

Fechner J. B. (1980) Qualifikation, Fachkunde, Weiterbildung—schutzbarriere Mensch in Kernkraftwerk—anforderungen aus der Sich des Bundesministers des Innern, Bonn, Bundesministers des Innern; NRC Translation 865 as Qualifications, professionalism, in-service training—the human shield in the nuclear power plant.

Fuchs F., Engelschall J. and Imlay G. (1981a) Evaluation of emergency operating procedures for nuclear power plants, NUREG/CR-1875, U.S. Nuclear Regulatory Commission.

Fuchs F., Engelschall J. and Imlay G. (1981b) Human engineering guidelines for use in preparing emergency operating procedures for nuclear power plants, NUREG/CR-1999, U.S. Nuclear Regulatory Commission.

General Electric Owners Group (1980) Emergency procedure guidelines, Revision 10 Draft dated 10 June 1980, was used in writing this review. This can be obtained from U.S. Nuclear Regulatory Commission.

Graae T. (1981) Implementation of an automated status analysis system in an operating nuclear power plant—experiment in pilot scale, Paper presented at the Halden Meeting, June 1981, in Fredrikstad, ASEA-ATOM.

Green J. F. and Myerscough P. B. (1977) The design of a simulator for the training of operating engineers in advanced gas cooled reactor stations (AGR), Paper 3.4 in Proceedings of IAEA specialists meeting, Simulators for training of nuclear power plant operators and technical staff, 27–29 October 1976, Aktiebolaget Atomenergi, Studsvik, Nyköping, Sweden.

Grimes B. K., Ramos S. L. and Weiss B. H. (1982) Emergency planning and preparedness since Three Mile Island, *Prog. Nucl. Energy* (to be published).

GRS (1980) Procedures and systems for assisting an operator during normal and anomalous nuclear power plant operation situations, GRS-19, Gesellschaft für Reaktorsicherheit, Cologne, Germany.

Hagan E. W. and Mays G. T. (1981 Human factors engineering in the U.S. nuclear arena, *Nuclear Safety* **22,** 337–346.

Halden (1980) Enlarged HPG meeting on water reactor fuel performance, and application of process computers in reactor operation; a compilation of non-project papers presented at the first two sessions (total five) on computer applications, Lillehammer 1980, HPR 269 and 270, OECD Halden Reactor Project.

Halden (1981) Computerized operation manual for safety technical specifications, HWR-30, OECD Halden Reactor Project, Norway.

Halden (1981b) Potentials of computer-assisted operation manuals, HPR-280, OECD Halden Research Project.

Haubert R. and Stokke R. (1980) Monitoring readiness of safety relevant devices in nuclear power plants by means of CRT—colour displays, pp. 365–379 of IAEA/NPPCI specialists meeting on Procedures and systems for assisting an operator during normal and anomalous nuclear power plant operation situations, GRS-19, Gesellschaft für Reaktorsicherheit, Cologne, Germany.

Heimbürger H. (1981) Technical features of principle and full scope simulators, Paper presented at NKA/KRU conference on control room design, operator training and human reliability, 15–18 June 1981, Fredrikstad, Norway.

Hetrick D. L. and Bailey P. G. (Editor) (1981) Simulation methods for nuclear power systems, EPRI WS-81-212, Electric Power Research Institute.

Hol J. Ø. Øhra G., Edsberg E. and Petterson F. (1981) Retrofitting of control rooms with computer based systems, HWR-25, OECD Halden Reactor Project.

Hol J. Ø., Øhra G. and Netland K. (1978) Design of pictures and use of colours and symbols for a CRT based supervision system, Paper presented at Enlarged Halden Programme Group Meeting, Loen, 5–9 June 1978, OECD Halden Reactor Project.

Holley *et al.* (1981) Effects of cricadian rhythm phase alteration on physiological and psychological variables: implications to pilot performance; NASA TM-81277, National Aeronautics and Space Administration.

Holmgren M. (1980) The development of 'process feeling' and problem solving behaviour in computer based control rooms, Paper No. 8 in HPR 269; see Halden (1980).

Holgren M. (1981) Experience from VDU-presented information, HWR-35, OECD Halden Reactor Project.

Honeycutt F. *et al.* (1981) Design and hardware alternatives for a safety parameter display system, NSAC-34, Electric Power Research Institute.

IAEA (1979) Staffing of nuclear power plants and the recruitment, training and authorization of operating personnel; a safety guide, 50-SG-01, International Atomic Energy Agency, Vienna.

IAEA (1980a) Maintenance of nuclear power plants; a safety guide, 50-SG-07, International Atomie Energy Agency, Vienna (available in draft; date given is for 'Rev. 7').

IAEA (1980b) Management of nuclear power plants for safe operation, Safety Series No. 50-SG-09, International Atomic Energy Agency, Vienna (available in draft; date given is for 'TRC-1, September 1980').

IAEA (1980c) Proceedings of IAEA/NPPCI specialists' meeting on Procedures and systems for assisting an operator during normal and anomalous nuclear power plant situations, GRS-19, Gesellschaft für Reaktorsicherheit mbH, Cologne, Germany.

IEAL (1980) Application of space and aviation technology to improve the safety and reliability of nuclear power plant operations, International Energy Associates, Limited, DOE/TIC-11143, U.S. Department of Energy.

IEEE (1980) Working conference on advanced electrotechnology applications to nuclear power plants, executive summary, IEEE Cat. No. TH 0077-8, Record, IEEE Cat. No. TH 0073-7, New York, Institute of Electrical and Electronics Engineers, Inc.

INPO (1981) The shift supervisor position in the nuclear power industry, 2 Vol., Institute of Nuclear Power Operations.

INPO (1981b) Nuclear power plant shift technical advisor, GPG-01, Rev. 1, 28 April 1981, Institute of Nuclear Power Operations.

INPO (1981c) Performance objectives and criteria for plant evaluations, preliminary, Institute of Nuclear Power Operations.

Jaffe L. *et al.* (1979) Reports of the technical assessment task force, staff reports to the president's commision on the accident at Three Mile Island, U.S. Government Printing Office. Some of this material was reprinted in *Prog. Nucl. Energy* **6,** (1–3), 1–325 (1980).

Jervis M. W. (1980) Integrated data and alarm systems for central control rooms, in Halden (1980).

Joaquin J., Mullins R. and Wagner K. (1981) BHWP 12-hour shift reports, 974/08005, Ontario Hydro.

Johansson O. (1980) The general structure of a disturbance analysis system, Paper No. 1 in Halden (1980).

Jones D. W. *et al.* (1980) Nuclear power plant simulators: their use in operator training and requalification, NUREG/CR-1482, U.S. Nuclear Regulatory Commission.

Joos D. W., Sabri Z. A. and Husseiny A. A. (1979) Analysis of gross error rates in operation of commercial nuclear power stations. *Nuclear Engineering and Design* **52,** 265.

Kemeny J. *et al.* (1979) Report of the president's commission on the accident at Three Mile Island, U.S. Government Printing Office.

Kisner R. A., Fullerton A. M., Frey P. R. and Dougherty E. M. (1981) A taxonomy of the nuclear power plant operator's role, Oak Ridge National Laboratory.

Levy S. (1980) Fundamental safety parameter set for boiling water reactors, NSAC-21, Electric Power Research Institute.

Long A. B. (1980) Disturbance analysis and surveillance systems—critical appraisal and future prospects, Paper No. 2 in Halden (1980).

Lyman E. G. and Orlady Capt. H. W. (1980) Final draft report on fatigue and associated performance decrements in air transport operations—an aviation safety reporting system study, Batelle Columbus Laboratories, Mountain View, California.

Mallory K. *et al.* (1980) Human engineering guide to control room evaluation, NUREG/CR-1580, U.S. Nuclear Regulatory Commission.

Malone T. *et al.* (1980) Human factors evaluation of control room design and operator performance at Three Mile Island—2, Final Report Prepared for Three Mile Island Special Inquiry Group, NUREG/CR-1270, U.S. Nuclear Regulatory Commission.

McCormick E. (1976) *Human Factors in Engineering and Design,* 4th edn., McGraw-Hill Book Company.

Meijer C. H. (1980) Operational support systems to improve the man–machine interaction in a nuclear power plant, Paper No. 3 in Halden (1980).

Meijer C. H., Frogner B. and Long A. B. (1980) A disturbance analysis system for on-line power plant surveillance and diagnosis, pp. 215–231 of IAEA/NPPCI specialists meeting on Procedures and systems for assisting an operator during normal and anomalous nuclear power plant operation situations, GRS-19, Gesellschaft für Reaktorsicherheit, Cologne, Germany.

Morgenstein M. *et al.* (1981) Guidelines for preparing emergency procedures for nuclear power plants, NUREG/CR-1977, U.S. Nuclear Regulator Commission.

Nadelik A. and Roggenbauer H. (1980) A computerized system for evaluation of the status of a protection system, pp. 351–361 of IAEA/NPPCI specialists meeting on Procedures and systems for assisting an operator during normal and anomalous nuclear power plant operation situations, GRS-19, Gesellschaft für Reaktorsicherheit, Cologne, Germany.

Netland K. (1979) Measurement of operator performance—an experimental setup, Paper presented at IAEA-NPPCI meeting Procedures and systems for assisting an operator during normal and anomalous nuclear power plant operation situations, Munich, 5–7 December 1979.

NKA (1981a) Publications list, NKA/KRU project on operator training, control room design and human reliability, NKA/KRU-(81)14, Nordic coordinating committee for atomic energy, Risø National Laboratory, DK 4000 Roskilde, Denmark.

NKA (1981b) Summary Report, NKA/KRU project on operator training, control room design and human reliability, NKA/KRU-(81)11, Nordic coordinating committee for atomic energy, Risø National Laboratory, DK 4000 Roskilde, Denmark.

NRC (1973) Bypassed and inoperable status indication for nuclear power plant safety systems, Regulatory Guide 1.47, U.S. Nuclear Regulatory Commission.

NRC (1975) Personnel qualification and training, Regulatory Guide 1.8, Revision 1, U.S. Nuclear Regulatory Commission. Proposed revisions were issued for comment in February 1979 and September 1980.

NRC (1975b) Reactor safety study: an assessment of accident risks in U.S. commercial nuclear power plants, WASH-1400, U.S. Nuclear Regulatory Commission.

NRC (1979) TMI-2 lessons learned task force status report and short-term recommendations, NUREG-0578, U.S. Nuclear Regulatory Commission.

NRC (1980a) NRC action plan developed as a result of the TMI-2 accident, NUREG-0660, U.S. Nuclear Regulatory Commission.

NRC (1980b) Clarification of TMI action plan requirements, NUREG-0737, U.S. Nuclear Regulatory Commission.

NRC (1980c) TMI-2 lessons learned task force final report, NUREG-0585, U.S. Nuclear Regulatory Commission.

NRC (1980d) Criteria for preparation and evaluation of radiological emergency response plans and preparedness in support of nuclear power plants, NUREG-065ᶠ Rev. 1, U.S. Nuclear Regulatory Commission and FEMA-REP-1, Federal Emergency Management Agency.

NRC (1980e) Report of the bulletins and orders task force, NUREG-0645, 2 Vol., U.S. Nuclear Regulatory Commission.

NRC (1980f) Second proposed revision 3 to Regulatory Guide 1.?3, Quality assurance program requirements (operation), U.S. Nuclear Regulatory Commission.

NRC (1980g) Instrumentation for light-water-cooled nuclear power plants to assess plant and environs conditions during and following an accident, Regulatory Guide 1.97, U.S. Nuclear Regulatory Commission.

NRC (1981a) Staff supplement to the draft report on human engineering guide to control room evaluation, NUREG-0659, U.S. Nuclear Regulatory Commission.

NRC (1981b) Transcript of commission briefing on action plan implementation, 1 April 1981, U.S. Nuclear Regulatory Commission.

NRC (1981c) Draft criteria for preparation of emergency operating procedures, NUREG-0799 (for comment), U.S. Nuclear Regulatory Commission.

NRC (1981d) Guidelines for control room design reviews, NUREG-0700, U.S. Nuclear Regulatory Commission.

NRC (1981e) Evaluation criteria for detailed control room design review, NUREG-0801 (for comment), U.S. Nuclear Regulatory Commission.

NRC (1981f) Survey of foreign reactor operator qualification, training and staffing requirements, NUREG-0863, U.S. Nuclear. Regulatory Commission.

NRC (1981g) Papers on operator licensing. Includes: (1) SECY 80-491, Proposed rulemaking-qualification of reactor operators, 4 November 1980; (2) SECY 81-84, Proposed rulemaking qualification of reactor operators, 2 February 1981; (3) SECY 81-84A, Operator qualifications and licensing proposed rule, 27 May 1981; Memo, Commissioner Ahearne, operator qualifications and licensing proposed rule, 9 June 1981; (4) Transcripts of commission meetings, 28 May 1981, and 18 June 1981; U.S. Nuclear Regulatory Commission.

NRC (1981h) Standard review plan for the review of safety analysis reports for nuclear power plants, LWR edition, NUREG-0800; Chapter 13, Conduct of Operations, U.S. Nuclear Regulatory Commission.

NRC (1981i) NRC Licensee assessments, systematic assessment of licensee performance review group (SALP), NUREG-0834, U.S. Nuclear Regulatory Commission.

NRC (1981j) Docketed information on individual U.S. nuclear power plants, available on request from Public Document Room, U.S. Nuclear Regulatory Commission. Inspection of documents is free; there is a fee for copying. Most such references in this paper are to recent NRC staff Safety Evaluation Reports and supplements to them; these are NUREG reports available from U.S. Nuclear Regulatory Commission.

NRC (1981k) Human factors acceptance criteria for the safety parameter display system, NUREG-0835, U.S. Nuclear Regulatory Commission.

NRC (1981l) Functional criteria for emergency response facilities, NUREG-0696, U.S. Nuclear Regulatory Commission.

NRC (1981m) Licensing requirements for pending applications for construction permits and manufacturing license, NUREG-0718, Revision 1, U.S. Nuclear Regulatory Commission. See also *Federal Register* **46**, 18045-49, 23 March 1981.

OECD (1980) Nuclear Safety Research Index, OECD Nuclear Energy Agency, Paris.

Parris H. L. and McConville J. T. (1981) Anthropometric data base for power plant design, Electric Power Research Institute NP-1918-SR.

Pew R. W., Miller D. C. and Feeher C. E. (1981) Evaluation of proposed control room improvements through analysis of critical operator decisions, NP-1982, Electric Power Research Institute.

Podonsky G. *et al.* (1980) Utility management and technical resources, NUREG/CR-1656, U.S. Nuclear Regulatory Commission.

Price H. *et al.* (1980a) Review of staffing requirements for near-term operating license facilities, NUREG/CR-1764, U.S. Nuclear Regulatory Commission.

Price H. *et al.* (1980b) The contribution of human factors in military system development, methodological considerations, Technical Report-476, U.S. Army Institute for the Behavioral and Social Sciences.

Ramos S. (1981) Methodology for evaluation of emergency response facilities, NUREG-0814, U.S. Nuclear Regulatory Commission.

Rasmussen J. (1979) On the structure of knowledge—a morphology of mental models in a man–machine system concept, RISØ-M-2192, Risø National Laboratory, DK 4000, Roskilde, Denmark.

Rasmussen and Lind M. (1981) Coping with complexity, RISØ-M-2993, Risø National Laboratory, DK 4000 Roskilde, Denmark.

Rogovin M. *et al.* (1980) Three Mile Island, a report to the commissioners and to the public, U.S. Nuclear Regulatory Commission.

Sargent T. O. and Blum R. B. (1980) Bimodal theory: understanding human behavior in off-average conditions, Interim Report STRN ORNL/Sub 7960/1, Oak Ridge National Laboratory.

Seminara J., Gonzalez W. and Parsons S. (1977) Human factors review of nuclear power plant control room design, EPRI NP-309, Electric Power Research Institute.

Seminara J. *et al.* (1979a) Human factors methods for nuclear control room design, Vol. 1: Human factors enhancement of existing nuclear control rooms, EPRI NP-1118, Vol. 1, Electric Power Research Institute.

Seminara J. and Parsons S. (1979b) Human factors methods for nuclear control room design, Vol. 2, Human factors survey of control room design practices, EPRI NP-1118, Vol. 2, Electric Power Research Institute.

Seminara J. *et al.* (1980a) Human factors methods for nuclear control rooms, Vol. 3, Human factors methods for conventional control board design, EPRI NP-1118, Vol. 3, Electric Power Research Institute.

Seminara J. and Eckert S. (1980b) Human factors methods for nuclear control room design, Vol. 4: Human factors considerations for advanced control board design, EPRI NP-1118, Vol. 4, Electric Power Research Institute.

Seminara J. L. and Parsons S. O. (1981) Human factors review of power plant maintainability, EPRI NP-1567, Electric Power Research Institute.

Strickert R. J., Schneider M. F. and Kelly R. G. (1981) Progress report by the 12-hour shift task group, Ontario Hydro Corporation; see also *Nucleonics Week*, 20 August 1981.

Swain A. and Guttman H. (1980) Handbook of Human reliability analysis with emphasis on nuclear power plant analysis, Draft report for interim use and comment, NUREG/CR-1278, U.S. Nuclear Regulatory Commission.

Thomassen B. B. and Augustin J. (1980) Alarm generation, a concept based on automatic logical filtering, HPR-260, OECD Halden Reactor Project.

Tuominen L. (1981) Training with simulators, Paper presented at NKA/NRU conference on Control room design, operator training and human reliability, 17–18 June 1981, Fredrikstad, Norway.

TVA (1981) Power Operations Training Center, Tennessee Valley Authority, Chattanooga, TN 37401, U.S.A.

Vik T. J. (Editor) (1978) Reports from workshop on operator-process communication techniques in the light of human factor studies (held at GKSS, Geesthact on 21 April 1978), HP-467, OECD Halden Reactor Project.

Visuri P. and Øwre (1981) A candidate approach to a computer-based alarm handling system (HALO), HWR-23, OECD Halden Reactor Project.

Visuri P. J., Thomassen B. B. and Øwre F. A. (1981) Handling of alarms with logic (HALO) and other operator support systems, HWR-24, OECD Halden Reactor Project.

Volta G. and Misenta R. F. (Editors) (1980) Status report on assistance to operators of nuclear power plants in emergency situations in Europe, 4 Vol., Joint Research Center, Ispra, Italy.

Wahlström B. (1980) Inhibition of alarms during nuclear power plant operation, in Halden (1980).

Wallace P. M., Bauman M. and Smith M. G. (1980a) Review of staffing requirements for near term operating license facilities; Bibliography, BioTechnology, Inc., Falls Church, VA.

WASH-1400 (1975) Reactor safety study—an assessment of accident risks in U.S. commercial nuclear power plants, NUREG 75/014, U.S. Nuclear Regulatory Commission.

Wilson J. T. and Rose K. M. (1978) The twelve-hour shift in the petroleum and chemical industries of the United States and Canada: a study of current experience, Industrial Research Reports, Miscellaneous Series No. 26, The Wharton School, University of Pennsylvania, Philadelphia.

Wirstad J. and Andersson H. (1980) Competency for nuclear power operators, Report No. 16, Swedish Nuclear Power Inspectorate.

Wirstad J. (1981a) Operator role description, Paper presented at NKA/KRU conference on Design, operator training and human reliability, Fredrikstad, Norway 17–18 June 1981.

Wirstad J. (1981b) Operator competence and training: an overview, Paper presented at the NKA/KRU conference on Control room design, operator training and human reliability, 17–18 June 1981, Fredrikstad, Norway.

Yamazaki K. *et al.* (1980) Development of plant operation monitoring system for nuclear power plants, pp. 235–246 in IAEA/NPPCI specialists meeting on Procedures and systems for assisting an operator during normal and anomalous nuclear power plant operation situations, GRS-19, Gesellschaft für Reaktorsicherheit, Cologne, Germany.

PDR

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

CONFERENCE PAPER TRANSMITTAL SHEET

Final

A SPEECH OR PAPER

~~TO BE~~ PRESENTED

~~AT~~/BY

NRC EMPLOYEE: Stephen H. Hanauer

OFFICE: Nuclear Reactor Regulation

~~ASSOCIATION OR~~ JOURNAL: "Progress in Nuclear Energy" Vol. 10, pp. 299-347

TITLE ~~OF CONFERENCE~~: OF ARTICLE The Human Factor in Nuclear Power Plant Safety: Progress Since Three Mile Island

DATE OF CONFERENCE:

LOCATION OF CONFERENCE:

Final Copy
Draft Copy sent to DMB on 2/12/82, please delete draft and replace w/ final.

TRANSMITTAL DATE: 12/6/82
TO DOCUMENT MANAGEMENT BRANCH