A TAXONOMY OF THE NUCLEAR PLANT OPERATOR'S ROLE

R. A. Kisner, A. M. Fullerton, and P. R. Frey
Oak Ridge National Laboratory
Oak Ridge, Tennessee 37830, USA

E. M. Dougherty
Technology for Energy Corporation
Knoxville, Tennessee 37922, USA

ABSTRACT

A program is presently under way at the Oak Ridge National Laboratory (ORNL) to define the functional design requirements of operational aids for nuclear power plant operators. A first and important step in defining these requirements is to develop an understanding of the operator's role or function. This paper describes a taxonomy of operator functions that applies during all operational modes and conditions of the plant. Other topics such as the influence of automation, role acceptance, and the operator's role during emergencies are also discussed. This systematic approach has revealed several areas which have potential for improving the operator's ability to perform his role.

I. INTRODUCTION

Twenty years have elapsed since the first reference applying human factors engineering to nuclear power plant control rooms appeared in the literature.[1] By late 1978, several studies emphasizing the anthropometric, environmental, and other physical factors of the control room (e.g. control room and control panel layout, colors/knobs/labels, and illumination) had been completed.[2-9] Since 1979 the volume of research addressing human factors-related problems of nuclear plant operation has increased significantly. This work has been sponsored by most of the worldwide nuclear power community.**

Human factors research in the past two years has resulted in the development of system concepts to improve plant monitoring, diagnostic and corrective actions, and operator/process communication. It has been suggested that operator crew response during upset conditions can be improved by upgrading information quality and reducing information quantity through the application of advanced computer-controlled display and diagnostic systems. Systems that assist plant operators in performing their operational and safety-related roles are referred to as job-performance aids or operational aids.

As a part of this ongoing human factors research, a program is presently underway at the Oak Ridge National Laboratory (ORNL) to define the functional design requirements for operational aids, particularly those that improve the cognitive abilities of operators. A first and important step in defining these requirements is to develop an understanding of the operator's role or function. Initially a top-down approach[10] was employed to describe the operator's role by beginning at the most general level and working downward to the most specific level. It followed the sequence: (1) identify the operator's role, (2) determine the effect of the role on operations (especially safety), (3) identify the factors that influence the role, and (4) determine where changes in the role can improve safety.

The study described in this paper focuses on the operator's role under emergency conditions, and for it we have also employed a bottom-up approach to examine the operator's role as it is inferred from the Emergency Procedures (EP) of a typical pressurized water reactor (PWR).[11,12] Our findings describe (1) the operator's role in terms of the functions and tasks necessary to achieve safety goals, and (2) the factors that influence the operator's responses during emergencies. To complete the picture, however, one must understand the operator's role under both normal and emergency plant conditions, primarily because the operator spends most of his time working under normal conditions and certainly there is a path from the normal to the emergency state. The general framework of the operator's role is the primary topic of this paper. The approach is similar to that of Corcoran et al.,[13,14] who described the operator's role using the safety function concept and employing a hierarchical approach to organize the safety functions. We build on that work by describing the operator's role in functional terms that can be synthesized to form his role under normal or abnormal plant conditions.

*Research sponsored by the U.S. Nuclear Regulatory Commission under Interagency Agreement #DOE 40-550-75 with Union Carbide Corporation under Contract No. W-7405-eng-26 with the U.S. Department of Energy.

**(U.S. Nuclear Regulatory Commission, U.S. Department of Energy, Electric Power Research Institute, Institute for Nuclear Power Operations, Nuclear Safety Analysis Center, Halden Reactor Project, Central Electric Generating Board, TUV Institute for Accident Research, RISO, utilities, and vendors.)

II. FRAMEWORK OF THE OPERATOR'S ROLE

From the earliest reactor projects to the present, the role of the nuclear power plant operating crew has followed an evolutionary path. The changes in operator role in time and from plant to plant are basically a result of changes and advances in control room automation, plant complexity, and accumulated operating experience. The earliest plant designs relied very little on automatic systems because of technology limitations and the prototypical reactor designs. As technological capabilities grew, designs relied on increasingly automated systems. This increased use of automation was further prompted by considerations of system cost, production efficiency, and safety. Differences in degree of automation can also be seen in the appproaches taken by different types of organizations with different objectives. For example, the nuclear operation of the U.S. Navy appears to rely heavily on the human crew and little on automatic systems. In contrast, the designers of the Canadian CANDU reactors have opted for highly automatic computer-driven systems.

Nuclear plant complexity is a function of the physical processes of the reactor design involved. The number of systems and subsystems the operator must oversee essentially determines his role. For example, research reactors are less complex than power reactors because steam generators and electric generator systems are not needed, and research reactors generally are subject to less demanding safety requirements. At the other extreme, LWR and CANDU reactors have multiple cooling loops and support systems that increase plant complexity and greatly expand the quantity of information presented to the operator.

Accumulated operating experience also changes the operator's role. Ideally, as unanticipated system interactions occur and better techniques are thereby developed for plant operation, these improvements are passed along to the utilities. In actual practice, this communication process has been inadequate. Additional operator duties are often mandated by regulatory agencies as a result of such field incidents.

A. The Influence of Automation on the Operator's Role

Automation has become a catchall term. From Melsa and Shultz:[15]

> "The term automatic control system is intended to be somewhat self-explanatory. The word system implies not just one component but a number of components that work together in a systematic fashion to achieve a particular goal. This goal is the control of some physical quantity, and the control is to be achieved in an automatic fashion, often without the aid of human supervision."

A good example is a servo-mechanism, a simple automatic device that maintains a parameter at a set point. It frees the human from a potentially tedious, vigilant, and highly routine task. More complex automatic systems employ multi-parameter control and can switch control schemes as needed to achieve a particular goal. Further, systems employing digital computers can be designed to detect and correct system failures.

Process automation can be discussed in more descriptive terms by scaling it on a continuum in multiple dimensions (see Fig. 1). These dimensions are (1) process control capability, (2) process configuration alterability, and (3) process monitoring and diagnostic capability. The point of origin in this "automation space" represents a fully manual process with no instrumentation or control system implemented. Control is performed by a human operator using his five senses to observe the process and perform all functions manually. Increasing machine functions along any of the axes reflects decreasing human functions and implies increasing machine intelligence. Increasing control capability reflects the machine's responsibility for satisfying ever higher operational goals. Theoretically, autonomous goal selection is ultimately possible. Increasing configuration alterability reflects the increasing capability for deliberate restructuring of a control system or even the process itself, including the modification, addition, or replacement of physical components. Increasing monitoring and diagnostics capability reflects the increasing capability for plant status monitoring and problem solving, including parameter observation and response prediction. In Fig. 2 the planes defined by the base vectors are labeled to illustrate the boundaries of the space. The purpose in defining this space is to illustrate the relationship between the roles of human operators and plant systems. Care must be taken not to carry the analogy beyond its significance. The absolute magnitude of the machine capabilities is not necessarily important.

Given that a level of automation can be selected for a power plant, illustrated as the solid sphere in Fig. 3, the operator would function beyond the level of automation. This would satisfy the goals related to plant control, system diagnostics, and maintenance, which is a combination of diagnostics and configuration alteration. In real applications, the machine functions are inconsistent; that is, not all systems are at the same level of automation. Some systems are purely manual (maintenance block valves) and others employ sophisticated multi-mode control (steam generators).

Human operators are necessary to satisfy functional requirements of the plant that are beyond machine capabilities as well as those at levels where full machine capabilities are not implemented. The technology of process control has far advanced since the first nuclear power plants were designed. For that

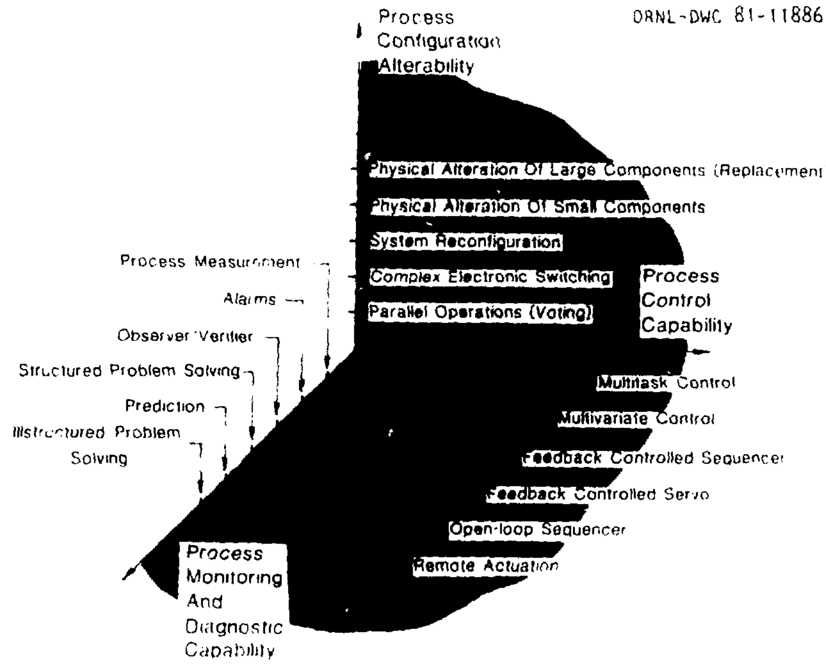

Fig. 1. Three dimensions of possible nuclear plant control automation.

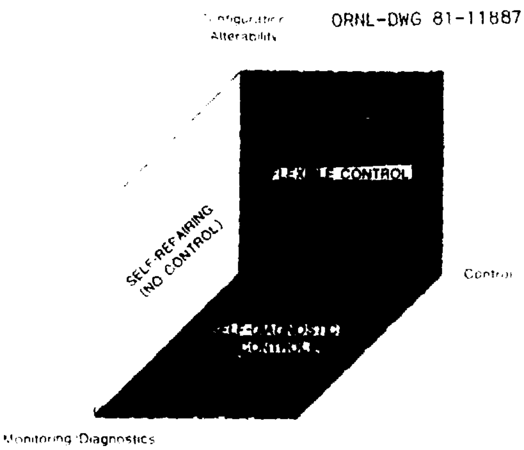

Fig. 2. Function boundaries defined by base planes.

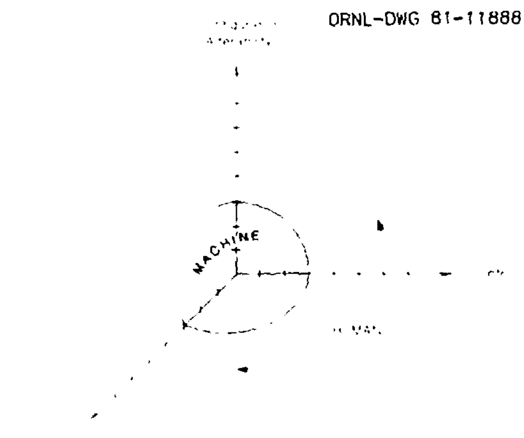

Fig. 3. Representative extent of nuclear plant control automation.

reason, plant systems and subsystems have been automated at widely varying levels; some have been left entirely manual for economic reasons. The technology of automatic monitoring and diagnostics has developed more slowly than that of automatic control, hence the lag in this dimension of plant automation. For example, automatic alarm filtering and fault detection are relatively new to nuclear power plant control rooms. Most operators must still validate information, verify control and safety system performance, predict system performance, and solve problems of various degrees of difficulty. The technology of automated systems for altering the configurations of functional modules and systems and physically relocating components has emerged even more recently. Simple configuration changes can be made electronically by relay devices in hardware or software. However, complex operations such as testing and calibration require human intervention since automatic capability for moving sensors from process to calibration facilities is not usually provided, although techniques for semi-automatic calibration have been used in research reactors. Most likely a highly automated configuration control system would be based on robotics.

The nature and extent of the interaction between man and machine varies with particular types of equipment. Automation is the most crucial factor in this interaction.[16] When functioning as designed, automation simplifies the operator's role while complicating that of the maintainer. In automated systems, the operator's role may be simply to activate a system and monitor those parameters that would enable him to detect and respond if an emergency were to arise. This role is significantly different from operating a system with little automation. Sheridan[17] refers to the supervisory role of a human in a highly automated computer-based system. The operator in this capacity is no longer a communication channel, a continuous one-channel servo-mechanism, or a signal detector; rather he has become a monitor, a planner, and a problem solver. The supervisory function is analogous to an outer feedback loop's control function, with automatic equipment controlling the inner loops. This forms a hierarchy. The further up in the hierarchy one moves, the more intermittent and delayed the system response becomes[18] until control, monitoring and diagnostics, and configuration alterability responses become infrequent.

With the introduction of computers, the allocation of function between humans and machines becomes increasingly complicated. For example, a dynamic approach would allow situation-dependent allocation of function between man and machine. In a study involving aircraft flight management,[19] the use of such an approach improved system performance and attracted user acceptance. However, real-time application of dynamic allocation would require highly complex and sophisticated computer systems.

B. Role Structure

Since under most conditions complete redesign and retrofit of control rooms would not be justifiable on a cost/benefit basis, operator aids seem to offer the most likely means of improving operating crew performance in existing nuclear power plants. Identifying the functions which the nuclear power plant operator needs to perform in order to achieve plant operating goals will permit identification of those schemes and systems that would improve operator performance. Specifically, our interest is focused on operational aids and their relation to plant safety.

The top-down approach outlined earlier was used to analyze the operator's role. This approach begins with the most general systems, goals, and functions and then partitions them into lower levels, forming a hierarchical structure. The lower level functions are those the crew must perform in order to operate the plant. However, to attempt a thorough top-to-bottom approach would be ambitious since this would entail task analysis in reverse at the lowest, most detailed levels. This could be done, and possibly should be, but it is beyond the scope of this study.

A taxonomy--the classifying of hierarchical relationships--could constitute a framework for analyzing the role of the nuclear plant operator. Such a taxonomy should provide a description of function, illustrate the flow of information, and indicate the degree to which a function is well defined. A number of taxonomies have been developed for various specific applications, but no universal taxonomy of the nuclear plant operator's role presently exists. Several taxonomies were constructed for NASA[20] to provide a framework for testing and predicting human performance in manned space missions. The value of a taxonomy lies in what it permits one to do with its results. The taxonomy presented in Table 1 is designed strictly for nuclear power plant operations. It does not describe operations segments (i.e., refuel, cold shutdown, hot shutdown, startup, or power operation), but it does identify general classes of behavior that apply during operation in any plant mode. Of great importance is the crew's function during emergency conditions; this, of course, must be reflected in the taxonomy. These classes of behavior are directly related to system function and can be synthesized or linked together to produce the full spectrum of functions that characterize the operator's role.

Most of the time the operator performs his role under normal circumstances. At such times, the operator's goal is to achieve a particular plant operating mode by following a schedule or plan of operations. Once this goal has been achieved, the operator must next decide whether to hold that goal or choose another one. This is often a management decision based on the power plant's mission: to produce electric power at a profit by operating economically with a minimum of downtime and without endangering the health and safety of plant personnel or the general public.

The utility's goals are also, in a remote sense, the operator's goals. In a practical sense, the goals of the operator are more tangible and are directly related to the immediate situation. These goals often must be transferred to a new operating crew at shift change and, therefore the crew that initiates a change may not see it through to conclusion.

The ultimate goal and reason for the plant's existence is to produce electric power at a profit. For this reason, safety is usually treated as a constraint placed on operation rather than as a separate goal. Only under emergency conditions does safety emerge as an operational goal. Thus to separate operator

Table 1. Outline of taxonomy of nuclear plant operator role

1. Supervision of Plant Operations
    1.1. Planning
    1.2. Monitoring
        1.2.1. Alarm Monitoring
        1.2.2. State Monitoring
        1.2.3. Signal Verification
        1.2.4. System Operation Verification
        1.2.5. Parameter Deviation Detection
    1.3. Controlling Plant Systems
        1.3.1. Manual Tasks
        1.3.2. Mechanized Tasks
        1.3.3. Manual-Automatic Tasks
        1.3.4. Machine-Automatic Tasks
    1.4. Diagnosing Problems
        1.4.1. Problem Anticipation
        1.4.2. Problem Solving
        1.4.3. Reconfiguring
2. Equipment Maintenance
    2.1. Planning
    2.2. Testing
    2.3. Implementation
    2.4. Equipment Improvement
3. Coordination of Support Activities
    3.1. Fire Protection
    3.2. Plant Security
    3.3. Administration
        3.3.1. Recordkeeping/Reporting
        3.3.2. Radiological Emergency Response Coordination
        3.3.3. Communication
        3.3.4. Personnel Supervision

actions distinctly into availability (power production) or safety-related categories, except under extreme conditions, leads to ambiguity and overlap. A better approach would be to classify the operator's function for normal operation in general terms so that the description of his function in off-normal conditions would simply be a rearrangement of these normal functions with redefined goals.

The operator's role can be separated into three functional categories: supervision of plant operation, equipment maintenance, and coordination of support activities. These three categories are valid under all operational conditions and modes of the plant. They are nearly parallel to the three elemental role conventions of men in systems as proposed by Price:[21] basic (operator performance concerned with the requirements of the prime system), complementary (maintaining prime and support system equipment), and support (maintaining human performance capabilities). Following is an itemized discussion of the taxonomy outlined in Table 1.

1. Supervision of Plant Operations

1.1. Planning. The operator sets the objectives for plant operation, with direction from higher level plant management, by deciding whether to continue on the present schedule or to modify it. The global planning function results from setting long-term goals and that may affect plant operation over several shifts. This function pertains mainly to non-safety-related activities; however, in the event of a long-term outage the operator would also perform planning functions where plant safety is of special concern.

According to Rouse,[22] planning includes these six aspects:

Generation of alternative plans
Imagining of consequences
Valuing of consequences
Choosing and initiating a plan
Monitoring plan execution
Debugging and updating plan

The last two aspects apply after the plan has been initiated; they deal with long-term monitoring of progress and subsequent replanning to achieve the goal.

1.2. Monitoring. The operator monitors the operation of the plant by observing the process (primarily through the instrumentation), the equipment, and the control and safety systems. In a highly automated plant, the operator spends a large portion of his time performing this function (up to 36%, according to a study of 381 U.S. reactor operators[23]). The monitoring function can be further divided into subfunctions:

1.2.1. Alarm Monitoring: With automatic systems functioning as planned, job demands tend to drop and response is by exception. Alarms provide a binary indication of subsystem and component status. The process of converting analog parameters to discrete alarms greatly reduces the quantity of information to be monitored.

1.2.2. State Monitoring: While alarm monitoring applies mainly to component (equipment) status, "state" monitoring applies to the overall condition of the plant and its major systems. Often this can be inferred from the observation of equipment alarms. A Safety Parameter Display System (SPDS)[24] under development by several vendors and being evaluated by the Nuclear Safety Analysis Center (NSAC) is designed specifically to assist the operator in his state monitoring function. The SPDS concept would display to the operator a minimum set of key parameters that would provide an overview of the safety status and trend of the power plant.

1.2.3. Signal Verification. The operator must verify that the process signals and alarms are valid indications of the plant status (i.e., whether the signals originating from sensors and activators are giving accurate or defective information). In performing this function, the operator must cross-compare several signals, then decide on the correctness of the signal in question. An outline of signal verification tasks is given in Table 2.

Signal verification as a part of the operator's role is often overlooked as a formal function. Crews do respond to false alarms and to erroneous data, often without verification (see Epler,[25] and Wiener and Curry[26]). Two purposes of signal verification are indication of instrument failure and warning against the use of invalid information in other tasks. Automated signal verification could greatly improve the operator's monitoring capabilities.

1.2.4. System Operation Verification. The operator must verify that the operation of automatic systems is proceeding normally. This is especially important during emergency conditions when the consequences of inadvertent operation or failure to operate are potentially severe. This verification process can range in complexity from a simple go/no-go check, with the quality of the operation left unmonitored, to a quantitative performance evaluation. The operation verification function involves both signal verification and plant status monitoring.

1.2.5. Parameter Deviation Detection. The operator monitors the plant primarily in order to detect impending problems and initiate certain routine preventive maintenance functions. He can detect a problem by observing a deviation from a normal trend or by observing that a command has failed to produce the expected trend or response. In the detection process, the operator must discriminate between normal and abnormal parameter variations and between relevant and irrelevant information. Deviation of a parameter from the expected value leads the operator to the diagnostic process. At the time of detection the operator performs a preliminary severity assessment (prediagnosis). Regularly encountered problems that are not immediately consequential are the least ambiguous and their solutions are well-structured.* Under these conditions the operator will most likely shortcut the complete problem-solving process to make time available for other functions. A model which illustrates this sequence of human problem-solving activities was developed at RISO.[27,28]

1.3. Controlling Plant Systems. The range of human participation in the control of plant systems is on a continuum. Basic design of the process and the control and safety systems determines the level of automation at which the man-machine interface will function.

*See discussion in Section 1.4.2, Problem Solving.

Table 2. Outline of signal verification tasks

Setup
- instrument power on?
- circuit continuity?
- circuit isolation?

Signal variation
- signal time variation normal?
- expected noise present?

Reasonability
- signal within equipment limits?
- signal rate-of-change within normal limits?
- sensor below point of previous damage or stress?
- observed signal comparable to signal estimated from system model?

Instrument agreement
- signals from sensor comparable to signals from other like sensors in same process location?
- signals from sensor comparable to local process parameters calculated from unlike sensors?
- signals from like sensors at different process locations comparable? (Requires system interaction model.)

Instrument environment
- transducer environment (temperature, pressure, moisture, radiation dose, and vibration) within limits of transducer design specification?

Process perturbation
- sensor responds to small variations in process parameters (produced by control rod motion, valve actuation, etc.)?

Input substitution
- intervening instrumentation (transmitter, signal processor, and display) responds to known signal substituted for sensor signal?

The role of the operator as a controller is established when the system designer specifies the role of man in the operation of the plant and allocates functions between operating crew and automatic plant systems. In future systems specification of the operator's role can be carried out in an organized and systematic manner, but for the majority of currently operating nuclear power plants the role of man and machine is not the result of a systematic process. The control room of a nuclear power plant is a collection of instruments from at least five independent major system vendors, with each vendor responsible only for its own equipment. Little effort has been put into integration of plant systems. Man-plant interactions in nuclear power plants range from manual tasks to machine-automatic tasks with no apparent consistent design criteria, except perhaps economic.

The continuum of control functions (see Fig. 1) can be divided into four discrete levels of participation: manual, mechanized, manual-automatic, or machine-automatic (adapted from Price[21]):

1.3.1. Manual Task. The human operator performs the task, generates whatever power, energy, or energy transduction is required, and controls the application of power or directs the energy use. This definition does not preclude the use of tools (e.g. a lever or binoculars), which merely extend man's raw capabilities.

1.3.2. Mechanized Task. The operator performs the task and controls the application of power or directs the energy use, while a machine generates whatever power, energy, or energy transduction is required.* The machine does little more than extend the raw capabilities of man; it may amplify or modify them, e.g. remote activation of circuit breakers, valves, etc. A mechanized task may be of a continuous nature, such as permitting an operator to control a process valve from the control room to maintain a process parameter at a preselected value. The operator becomes a continuous controller under such circumstances--a servo-mechanism. Humans performing this kind of task behave as adaptive and self-optimizing controllers.

1.3.3. Manual-Automatic. A machine performs the task by generating whatever power, energy, or energy transduction is required, but the operator controls, in real time, the application of the power or directs the energy use. Man participates less directly in the manual-automatic task. He may determine what is to be done, and perhaps how. He initiates and terminates the operation of the automatic device, as in the operation of a steam generator level controller or pressure controller. He must monitor the operation to determine whether it meets operational criteria.

1.3.4. Machine-Automatic. A machine performs the task by generating whatever power, energy, or energy transduction is required, and an algorithm controls the application of power or directs the energy use. Man participates in machine-automatic tasks only at remote times and then indirectly. For example, the algorithm may be reprogrammed, but this is not direct or continuous control.

During normal operation, the control of the process proceeds essentially as designed; however, under abnormal conditions (e.g. in cases of equipment failure), automated systems may degrade to lower levels of automation. The operator would be required to accommodate and adapt to such situations, perhaps by substituting his skills for failed or malfunctioning equipment. A certain proficiency must therefore be maintained. This situation is most likely to be encountered during a plant emergency. The automated plant should be modular in nature so that the scope of failures is limited and the operator's manipulative role is not too large to handle.

1.4. Diagnosing Problems. The operator, while performing monitoring functions, is directed to the diagnostic function by the indication of a problem or potential problem. The diagnostic function may be performed at differing levels depending on the anticipated seriousness of the perceived consequence, the cost (in dollars, time, safety implications, etc.) of obtaining additional information, the operator's experience and knowledge of the plant, the time required for action on the primary problem, or the time required for other tasks which may or may not be associated with the primary problem. Diagnosis results in a decision as to whether there is or is not a problem. Operators, on the average, spend 10% of their time diagnosing abnormal performance.[23] One of the justifications for manned systems is the human's capability for solving ambiguous and ill-defined problems. Machines are poor at this, although it is a dimension of automation in which there will certainly be advances in the future. Diagnosis, as it is used in this paper, includes the components of problem solving, problem anticipation, and system reconfiguration.

1.4.1. Problem Anticipation. Understanding system and equipment functions and the interactive effects of systems and functions prepares the operator for anticipating problems. The operator must be able to predict the outcome of specific actions or inactions, especially if the result of his actions will affect operations, damage equipment, or release radiation. A warning which occurs before a parameter violates a technical specification or exceeds an alarm limit could provide additional time for the operator to assess the situation and begin the problem-solving process (including implementing corrective actions), thus reducing unnecessary transients and the number of challenges to the protection system. Limited tests of such a concept were performed as a part of the EPRI research project "On-Line Power Plant Alarm and Disturbance Analysis System."[29]

The simulator is a versatile tool for predicting responses and their resulting potential problems. Currently, real-time plant or partial system simulators are not incorporated in the control room. With further advances in computer technology, the possibility for on-line simulation capability comes closer to practicality.

1.4.2. Problem Solving. A problem exists in a nuclear plant when a barrier

*Manual operation, as most use the term, usually refers to a mechanized task.

occurs between the operator and his goal of continued safe plant operation. Typically, a barrier would be a malfunction somewhere in the system. Once a problem has been observed, its solution consists of three steps: definition of the problem, identification and execution of procedures to correct the problem, and evaluation of whether the actions taken have served to remove the barrier(s) to the goal. The problem is considered to be well-structured[30] and therefore relatively simple to solve if all the information necessary to complete this sequence is readily available to the operator, meaning that he not only recognizes the importance of various pieces of information, but also that he can either retrieve them from his own memory or be able to find them easily in the procedures. However, the problem would be defined as ill-structured if the operator lacks information in any or all of the steps. Depending on level of training and experience, a given problem may be well-structured for one operator and ill-structured for another.

The concept of ill-structured versus well-structured problems can be applied to the constituent elements of problems as well as to the problem as a whole. In other words, a problem might be well-structured in terms of task definition and goal, but ill-structured in terms of procedures. Analysis of problems in this way suggests that the development of a taxonomy of problems based on degree of structure would be useful for identifying points in the problem-solving process when information is likely to be unavailable, perhaps due to cognitive processing limitations of the operator.

Using this approach, each problem could be considered to exist in a three-dimensional space, running from well-structured at the origin to ill-structured at the end of the dimension. The dimensions are the three steps noted above: task definition, selection of procedures, and evaluation of results. Each dimension can be further subdivided by the subtasks required in each of the three steps. For example, one subprocess of task identification is to determine the constraints under which the problem must be solved. In a nuclear plant, one constraint would be that an action to keep the plant operating should not have a negative effect on safety and, conversely, that shutting the plant down should not have a negative effect on safety. The subtask would be well-structured if the safety implication of the proposed action was known, and ill-structured if it was not known. As another example, one technique for evaluating complex problems is to divide the problem into subgoals in order to be able to test progress at frequent intervals. Testing is then carried out by pattern-matching, that is, by checking the existing plant status against knowledge of the desired state. Computer aids, by enabling the operator to see the progress being made or not made toward the final goal, would help keep the problem-solving process on track and keep it well-structured.

The problem-solving approach outlined here has two major components. The first is to define as many potential problem classes and subtasks as possible so that training procedures and operator aids can be developed to make these problems well-structured. The second component is to develop a training program to acquaint operators with the tasks and procedures involved in problem solving so that they will be better equipped to deal with ill-structured problems, which will inevitably occur. Although some training in general reasoning methods (e.g. heuristic search procedures) might be valuable for an extremely ill-structured problem, research indicates that problem solvers more often use reasoning skills that are closely related to particular bodies of knowledge.[31] This suggests that identification of and training in reasoning skills which develop along with expanding knowledge (both practical and theoretical) of nuclear plants should be a major research goal. Concomitantly, such research might identify the need for operators with specific cognitive abilities.

The paradigm for a well-structured problem is a closed-form, solvable mathematical equation. Through operator training and the development of aids and procedures, many problems of a nuclear plant could be made well-structured enough to approximate this ideal, and it is probable that many of the more routine problems could be automated. Until such time as computers become capable of the higher-level problem solving required for solution of unexpected ill-structured problems, however, the human operator will be a necessary part of the system.

1.4.3. <u>Reconfiguring</u>. The operator is able to alter the configuration of the plant or any subsystem whenever necessary to ensure economic and safe plant operation. This capability, beyond the realm of system control, allows the operator to change the order of operation or function of systems or equipment, to bypass or alter the flow of the process in effecting a goal (especially a safety goal), or to replace or order the replacement of faulty equipment. This dimension of automation has not yet been implemented in plant systems. A good example of humans performing system reconfiguration under emergency conditions is the rewiring of an electrical panel by an operator during the Brown's Ferry fire of 1975. The operator, working in a hostile environment, bypassed inoperative circuit breakers to energize a set of pumps in order to remove core heat in a novel, unanticipated manner. The reconfiguring function of the operator is part of his role under both normal and emergency conditions, but one would expect more dramatic and unusual system modifications during attempts to subdue unexpected emergency conditions.

2. <u>Maintain Equipment</u>

2.1. <u>Planning</u>. The operator schedules both corrective and preventive maintenance activities for times when they will cause only minimal disruption of plant operations. Highly disruptive maintenance activities are scheduled, if possible, for times when the reactor is down for refueling. Certain maintenance activities may be performed during an unscheduled shutdown. Although the majority of maintenance tasks, especially equipment calibration or replacement, are performed by the maintenance crews, some maintenance tasks associated with the control room or control panels may be performed by the operating crew.

Operators are alerted to the need for maintenance by observing the plant schedule or instrumentation indications (and perhaps the application of a formula). This monitoring activity follows from the monitoring and diagnosing functions performed by the operator as he supervises plant operations.

2.2. Testing. The operator is required to test the operability of plant systems, equipment, and instrumentation. This function may follow from either a schedule or an indicated or perceived need. A part of the testing function is instrumentation calibration.

2.3. Maintenance Implementation. In order to repair, replace, check, or calibrate a piece of equipment, the operator must bypass and deenergize the equipment and indicate that a maintenance activity is in progress. The operator dispatches maintenance personnel and coordinates the associated activities of support groups within the plant organization, especially health physics.

2.4. Equipment Modification. One form of maintenance occurs as operators and maintenance personnel modify equipment to improve its function. The most obvious modifications are those to the man-machine interface[3] which attempt to eliminate deficiencies in the original design of control boards and plant maintenance areas. Some modifications act as cues to the operator to prevent accidental activation of controls, while others clarify the meaning or use of a control. Equipment modification can be potentially hazardous, especially if the change produces ambiguous or conflicting information. The practice of equipment modification is discouraged at some plants, encouraged at others. Whether by design or happenstance, equipment modification appears to be a role which the operator assumes.

This study has concentrated on operations- and maintenance-related functions. Support activities, although included in the taxonomy outline for completeness, have not been elaborated. This does not diminish their importance, however, but indicates the need to further examine this aspect of the operator's role.

C. Role Acceptance

Humans are included in systems primarily to provide capabilities which are too difficult or too expensive to automate. Because high reliability (within budget and technological constraints) is a system requirement, the entire man-machine system must be designed to optimize reliability. This not only means reliable equipment but also reliable human performance. The expense and effort put into designing ultra-reliable equipment could be unproductive if a man is inserted in the system with a role unacceptable to him.

There is no lack of literature pertaining to job satisfaction (e.g. Ergonomics Abstracts[32]). The results of a few studies are given here to point out just some of the systems-related factors affecting role acceptance.[33,34] Factors such as remuneration and interpersonal relationships, although important, will not be considered here.

Responsibility/Authority: The levels of responsibility and authority must be defined and balanced above a certain acceptance threshold. This threshold is affected by factors such as education, training, experience, and personal attitudes of the operator. Acceptance is diminished if an individual is assigned a role below his responsibility/authority threshold.

Use and Retention of Skills: Role acceptance will be greater if the individual is able to use and maintain skills which are important to him. This factor is often violated by the selection of overqualified personnel. In addition, the opportunity to learn and develop new skills can increase role acceptance.

Flexibility: The ability to vary the manner of accomplishing his tasks on his own initiative enhances the operator's role acceptance. This flexibility is constrained by management and regulatory requirements. The operator should be made aware of the basis for the constraints.

Allocation of Function: The distribution of function between man and machine affects acceptance. In general, the allocation of frequent, repetitive tasks and continuous servo-control functions to a machine is highly acceptable. However, the automation of high-level decision making tasks is generally not acceptable to operators, particularly when the machine's decision affects the human's load. These are two extremes on a continuum and no ideal dividing line exists. The optimum allocation of function depends on the system performance requirements and the attitudes and abilities of the operator. User participation in the function allocation process will add to acceptance. However, user preference alone is not a reliable basis for improving system performance.

D. Operator's Role During Emergencies

A primary concern in the current study is the nuclear plant operator's role in emergency conditions.* During such conditions, the role of the operator is shifted to that of maintaining vital safety functions, such as adequate core cooling, regardless of whether the cause of the upset has yet been diagnosed. This approach is analogous to the medical doctor who treats an emergency patient's symptoms until the patient's vital signs have stabilized somewhat.

The goal of the emergency procedures (EPs) is to maintain adequate core cooling,[35] which is consistent with the safety-function concept. To support this goal, certain processes are assumed necessary. These processes would ultimately consist of operator tasks--the physical acts that underly the operator's role. This structure represents a hierarchy of goal, processes, and tasks that parallels the hierarchy of behavior categories presented by several analysts at RISO National Laboratory.[27,28] Behavior may be classified on three levels: goal- or knowledge-based, rule- or procedure-based, and skill-based.

The EPs examined fit this general hierarchical pattern, and from them the following role was inferred. Figure 4 illustrates a hierarchy of operator response for the onset of an emergency. The top level is a goal--an interim, safe steady state--which is broader than adequate core cooling alone. Supporting this goal are the processes of (1) observing symptoms, (2) supervising safety functions, and (3) diagnosing for critical events. Each process is then composed of several tasks at the lowest action level. For example, detecting an increase in the average reactor coolant system temperature could be a task supporting the process of observing symptoms. On the other hand, manually switching from main to auxiliary feedwater could be a task supporting safety function supervision.

One perspective of the basis for operator response is that a human operator is basically a generalized problem solver.[36] This conforms with the goal-topped hierarchy developed in the analysis of EPs, since a basic definition for problem solving is:

> "It must be goal-directed, it must involve a sequence of operations, and these operations must have a significant cognitive component."[37]

Thus, to achieve an interim safe steady state[38] the operator must assess the distance

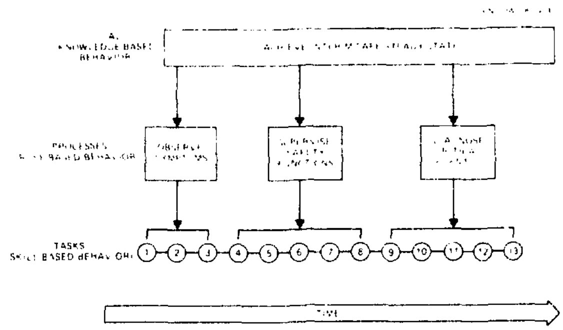

Fig. 4. Operator role hierarchy at onset of emergency.

from the current plant status to the goal-state. The problem then is to close that distance. To solve that problem, the operator must choose a response or set of tasks.

As a problem solver, the operator can be modeled as a sequence of operations (see Fig. 5). Operation (1) is his role as plant diagnostician. Operation (2) requires the operator to know the goals of operations management so that he can define the goal-state appropriate to the assessed plant status. Operation (3) is his role as decision maker, where he chooses the procedure that will carry him from the current plant status to the goal-state. Operation (4) is his role as controller, whether continuous or supervisory. The first three operations are human cognitive processes; thus problem solving, as generalized, can be thought of as the cognitive mechanism that takes the operator from the top (goal) level of the hierarchy in Fig. 4 to the second (procedural) level. This second level is then carried out with an operator aid--the EPs. Recent revisions of the EPs studied include a diagnostic procedure that supports the safety-function approach.

The operator's problem of how to achieve the goal-state is solved only when his response action changes the plant status to match it. The response follows from the procedure selected, with no guarantee that any set of written procedures will be sufficient to solve any unanticipated problem. The diagnostic procedure was developed for that reason.

The diagnostic EP is a heuristic* procedure rather than an algorithm, as are the bulk of procedures. Thus Operation (3) in Fig. 5 has been expanded with the realization that not all problems can be solved in advance. The heuristic EP complies with this realization and has some important characteristics: it is goal-directed--its aim is an interim safe

---

*Since TMI-2, reactor manufacturers and utilities have adopted a safety-function approach to procedure writing (see Refs. 13 and 14). This study is based on an examination of the newly revised emergency procedures of one pressurized water reactor (PWR).

*A heuristic procedure is one that has the tendency to achieve its specified goal but does not guarantee it as does an algorithm.

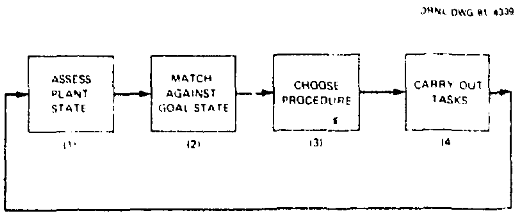

Fig. 5. Operator problem-solving sequence.

steady state; it buys time to allow for diagnosis of the cause of the problem; as a heuristic procedure, it is not guaranteed to succeed but is likely to; and because there is no guarantee of success, it formally requires continual re-evaluation of the plant status.

This last characteristic is crucial to the heuristic procedure, and therefore can best be shown at the process level of the operator hierarchy. Figure 6 shows the relationship of the three processes that support the goal of an interim safe steady state. The first two processes are completed in one pass, while the third is iterative. The first process, observe symptoms, involves recognizing the pattern of some twenty critical plant parameters. At that time a brief assessment of the cause is performed but not necessarily acted upon. The second process, supervise safety functions, involves various checks and alignments necessary to set up the plant system that would be most likely to support the safety functions required. The third process, diagnose critical event, is the heuristic element of the EP. This process involves supervising the implementation of the safety functions, with particular emphasis on adequate core cooling. If the emergency is real (e.g. not an instrument failure), then the third process will lead the operator to transfer from the diagnostic EP to the three critical event EPs: Loss of Primary Coolant, Loss of Secondary Coolant, or Loss of Primary into Secondary by Way of Steam Generator Tube Rupture. These three classes of accidents are called critical because each challenges the success of the safety function--adequate core cooling--through the fundamental thermo-hydraulics of the plant.

Provisions written into the three critical EPs allow the operator to reassess the plant state, measure it against his goal-state, and transfer back to the heuristic EP if necessary. Thus this third process cannot guarantee successful diagnosis of the cause of the upset at any point but provides a feedback loop to allow iterations of the diagnostic process. By directing the operator's attention to safety functions and providing a formal mechanism for iterative diagnosis, the diagnostic EP is intended to give the operator additional time to diagnose the specific cause of the upset, although the possibility exists that he may use up his time with wrong decisions while the accident worsens.

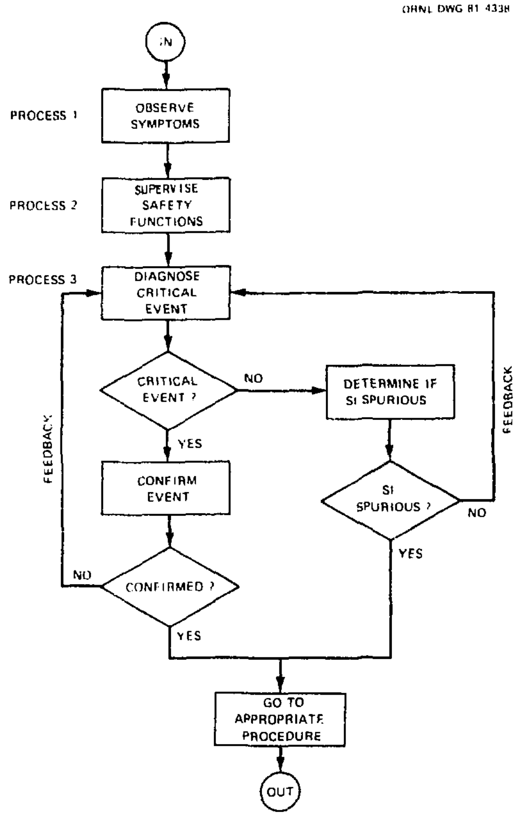

Fig. 6. Operator process model at onset of emergency.

III. CONCLUSIONS

The operating crew's role is continually changing as a result of changes in control room automation, plant complexity, and operating experience. Automation, the most influential factor, can be characterized by three dimensions: process control capability, process monitoring and diagnostic capability, and process configuration alterability. Both operators and plant systems perform these activities to varying degrees, depending upon the designer's allocation of function. The general level of automation can be determined by the degree to which machines are given responsibility in these three dimensions.

In highly automated environments, the operator's role becomes one of a supervisor. However, during malfunctions he must substitute his own capabilities for machine capabilities in order to assure the continuation of necessary functions. The human operator is needed for his ability to solve ill-defined problems and modify equipment configurations, especially during emergency conditions. These abilities are currently beyond the scope of automated systems. For that reason, the operator should be trained and supported by control room equipment to fully use these human characteristics.

This study examined the EPs of a typical PWR using the bottom-up approach, and the results produced a description of the operator's role during emergencies that fitted the top-down approach used in constructing the role taxonomy.

A workable taxonomy can go a long way towards providing a framework for analyzing the role of nuclear power plant operators. No universal taxonomy exists, however, nor would it be feasible to construct one, but a function-oriented role taxonomy does provide a starting point for examining operator training and operational aids. Further refinement of the taxonomy is possible and needed. The authors hope that it can be fused with the results of task analysis efforts to the end that a clear and complete description of the operating crew's role can be realized.

REFERENCES

1. Dickey, D. E., "A Human-Engineered Reactor Control Panel," Nucleonics, 18(12):80-81 (December 1960).

2. Finlayson, F. C., et al., "Human Engineering of Nuclear Power Plant Control Rooms and its Effects on Operator Performance," The Aerospace Corporation, Report No. ATR-77(2815)-1, February 1977.

3. Seminara, J. L., et al., "Human Factors Review of Nuclear Power Plant Control Room Design," EPRI NP-309, November 1976.

4. Proceedings of the Specialists Meeting on Control Room Design, San Francisco, July 22-24, 1975. (In collaboration with the Power Engineering Society, IEEE, 1975 summer meeting.)

5. Frogner, B. and Meijer, C. H., "On-Line Power Plant Alarm and Disturbance Analysis System," EPRI NP-613, Interim Report, February 1978.

6. "Electrical Design Guide DG-E18.1.8," Instrumentation and Control, Operator Interface Facilities, Tennessee Valley Authority, Knoxville, Tennessee (final approval date October 18, 1979).

7. Bohr, E., et al., "Human Factors in the Nuclear Power Plant," Volumes I and II, *Technischer Ueberwachungs-Verein Rheinland e.V.*, Cologne, December 1977 (NRC Translation 460).

8. Design of Working Place, Operation, and Environment, Issued by the Association of Authorized Technical Inspection Agencies of Germany, December 1978. (TUVIS Document No. 14-0000-000-01-19,D4; OLS Translation 80-306).

9. IEEE P566/D2, Guide for the Design of Display and Control Facilities for Central Control Rooms of Nuclear Generating Stations, Draft 2, July 1975. (Work presently underway.)

10. Kisner, R. A. and Flanagan, G. F., "A Systems Approach to Defining Operator Roles," IEEE Trans. Nucl. Sci., Vol. NS-28, No. 1, February 1981.

11. Asselin, S. V. and Oh, C. B., "A Characterization of the Nuclear Power Plant Operator's Role During Emergencies," NUREG/CR-1772, ORNL (Draft - to be published).

12. Oh, C. B., et al., "Analysis of the Operator's Role During the Onset of an Emergency," for ORNL, TEC R-81-004 (Draft February 1981, to be published).

13. Corcoran, W. R., et al., "The Operator's Role and Safety Functions," presented at the Workshop on Licensing and Technical Issues -- Post-TMI, Atomic Industrial Forum, Washington, D. C., March 9-12, 1980 (Combustion Engineering Document TIS-6555).

14. Corcoran, W. R., et al., "The Plant Designer's View of the Operator's Role in Nuclear Plant Safety," presented at the Fourth Symposium on Training of Nuclear Facility Personnel, Gatlinburg, Tennessee, April 27-29, 1981 (Combustion Engineering Document TIS-6766).

15. Melsa, J. L. and Shultz, D. G., Linear Control Systems, McGraw-Hill 1969.

16. Meister, D., Human Factors: Theory and Practice, Wiley-Interscience, pp. 11, 1971.

17. Sheridan, T. B., "Theory of Man-Machine Interaction as Related to Computerized Automation," proceedings of the Sixth Annual Advanced Control Conference, Purdue University, April 28-30, 1980.

18. Rouse, W. B., "Human-Computer Interaction in the Central of Dynamic Systems," Computing Surveys, Vol. 12, No. 1, March 1981.

19. Chu, Y. Y. and Rouse, W. B., "Adoptive Allocation of Decision Making Responsibility Between Human and Computer in Multi-Task Situations," IEEE Trans. Systems, Man and Cybernetics, SMC-9, 12, 769-778 (December 1979).

20. Finley, D. L., et al., "Human Performance Prediction in Man-Machine Systems," NASA CR-1614, Vol. 1 (August 1970).

21. Price, H. E. and Tabachrick, B. J., "A Descriptive Model for Determining Optimal Human Performance in Systems," NASA CR-878, Vol. III, March 1968.

22. Rouse, W. B., Systems Engineering Models of Human-Machine Interaction, pp. 124-128, North Holland, NY, 1980.

23. Thompson, J. L., "How Nuclear Reactor Operators Describe Their Job: A Basis for Operator Selection," Center for Nuclear Studies, Memphis State University, Memphis, Tennessee (January 1979).

24. Cain, D., et al., "The Concept and Design of a Safety Parameter Display System," presented at the Conference on Computerized Operator Support Systems, Tampa, Florida, December 16-17, 1980, sponsored by Electric Power Research Institute.

25. Epler, E. P., "Common Mode Failure of Light Water Reactory Systems: What Has Been Learned," Institute for Energy Analysis, Oak Ridge Associated Universities, ORAU/IEA-80-7(M), May 1980.

26. Wiener, E. L. and Curry, R. E., "Flight-Deck Automation: Promises and Problems," NASA Ames Research Center, NASA TM-81206, 1980.

27. Goodstein, L. P. and Pedersen, O. M., "Do Control Room Designers Have Adequate Bases for Computer Displays," proceedings of the Specialists Meeting on Control Room Design, San Francisco, July 22-24, 1975.

28. Rasmussen, J., "The Human As A Systems Component," from Human Interaction with Computers, Smith, H. T. and Green T. R. G. (eds.), Academic Press, 1980.

29. Meijer, C. H. and Frogner, B., "On-Line Power Plant Alarm and Disturbance Analysis System," EPRI-NP-1379, Final Report, April 1980.

30. Simon, H. A., "The Structure of Ill-Structured Problems," Artificial Intelligence, 4, 181-201 (1973).

31. Rumelhart, D. E., "Schemata: The Building Blocks of Cognition," R. J. Spiro, B. C. Bruce, and W. F. Brewer (eds.), Theoretical Issues in Reading Comprehension: Perspectives from Cognitive Psychology, Linguistics, Artificial Intelligence and Education, Hillsdale, NJ, Erlbaum, 1980.

32. Ergonomics Abstracts, Ergonomics Information Analysis Centre, Taylor and Francis, Ltd.

33. Price, H. E., Smith, E. E., Behan, R. A., "Utilization of Acceptance Data in a Descriptive Model for Determining Man's Role in a System," NASA-CR-95, September 1964.

34. Frey, P. R., Kisner, R. A., "Factors Influencing Operator Acceptance of Operational Aids," to be presented at 1981 IEEE Standards Workshop on Human Factors and Nuclear Safety, Myrtle Beach, SC, August 1981.

35. NRC Action Plan Developed as a Result of the TMI-2 Accident, NUREG-0660, Vol. 1, Nuclear Regulatory Commission, Washington, DC, August 1980.

36. Simon, H. A., The Sciences of the Artificial, Massachusetts, The MIT Press, 219 (1981).

37. Anderson, J. R., Cognitive Psychology and Its Implications, San Francisco, W. M. Freeman Company, 1980.

38. Newell, A. and Simon, H. A., Human Problem Solving, New Jersey, Prentice Hall, 1972.

END

DATE FILMED

08/24/81