CONF-830318--3

CONF-830318--3

DE83 009835

COMPUTING AND COGNITION IN FUTURE POWER-PLANT OPERATIONS

R. A. Kisner
Oak Ridge National Laboratory*

T. B. Sheridan
Massachusetts Institute of Technology

Abstract

The intent of this paper is to speculate on the nature of future interactions between people and computers in the operation of power plants. In particular, the authors offer a taxonomy for examining the differing functions of operators in interacting with the plant and its computers, and the differing functions of the computers in interacting with the plant and its operators.

Introduction

The authors believe that speculation and debate about the interaction of people and computers in future plant operations is important at this time in history. Power plant operations are being scrutinized by expert and non-expert as never before. At the same time, computer technology is developing at so rapid a pace that it almost seems to pose its own imperative for adaptation to plant operations. Finally, because of the de facto moratorium on nuclear plant construction in the U.S.A., the operation of existing plants may have to be continued past their 40-year design lifetime, resulting in more concern for and emphasis upon safety.

Several years ago one of the authors sat in on a discussion of plans for the control room of a new nuclear power plant (which, like many others, was cancelled). As with so many such cancelled plants, its control room was planned to be fully computer-based. Several operators of the subject utility were present, and one of them, after enduring several hours of enthusiastic vendor presentation, rose from his seat, strode to the blackboard, and without saying a word wrote in large letters: "Computer programmers are not operators; operators are not computer programmers."

That gentleman was right, of course, at least in terms of what we mean today by operators and computer programmers. But in another sense he was wrong. Looking to the future, operators probably will never have to write programs in anything approaching machine language, but they most certainly will have to learn to instruct computers in specially designed

---

*Prepared by the Oak Ridge National Laboratory, Oak Ridge, TN 37830 operated by Union Carbide Corporation for the U.S. Department of Energy under Contract No. W-7405-eng-26.

MASTER

By acceptance of this article, the publisher or recipient acknowledges the U.S. Government's right to retain a nonexclusive, royalty-free license in and to any copyright covering the article.

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

high-level languages and to understand what computers have to say back to them. In other words, operators will have to get much closer to computers then they customarily are today.

Human factors has become an accepted and useful discipline in the power industry, and human factors reviews have been mandated by the NRC in all nuclear power plants. Yet the explicit analysis of human-computer interaction has hardly begun, in spite of the on-rush of computer systems being marketed to commercial power plants. In our opinion, the power (and perhaps the computer) industry's present understanding of how to engineer computing and cognition is woefully short of the current need.

At the same time the executive summary of a recent two-volume report of recommendations by the Human Factors Society to the NRC[1] states that ". . . there is no solid evidence to suggest an ideal level of automation in the control of complex systems. . . . Nevertheless enough is presently known about human capabilities and limitations to develop a method and criteria for the allocation of functions early in system design to determine an optimal role for the human in a specific system design." (Underline ours.) In the next paragraph the report concludes that for research in this area "the urgency is low." We strongly disagree!

We do not believe that computers will replace operators in the forseeable future. However, we do believe that computers will make profound changes in the ways in which operators think and act. One need only examine the history of operator-computer developments in the control of aircraft and the remote control of robotic manipulators for space, deep-ocean, and manufacturing applications. In these cases the human operator has moved from being a direct in-the-loop controller to being a "supervisory controller." That is, he controls the vehicle or remote manipulator through the intermediary of a computer. The operator intermittently provides high level commands to and receives complex integrated information from a computer in order to establish subgoals and monitor the actions of the computer in implementing them (semi)automatically. The computer executes its instructions by closing the loop through its own external sensors and effectors, returning to its superior when it has accomplished a subgoal (e.g., achieved an altitude or landed the aircraft, or moved the arm to a new location and grasped an object) or when it has run into unexpected trouble and needs help. Supervisory control has been characterized more fully in a recent report.[2]

Interconnections Between Crew, Computer, and Plant Dynamics

In considering the interconnections between the operating crew, computer, and plant dynamics we find symmetry useful both for graphical illustration and to discipline ourselves to examine all causalities. Figure 1 illustrates six component effects amaong the three basic elements: crew system, plant system (plant dvnamics), and computer system.

ORNL-DWG 83-9595

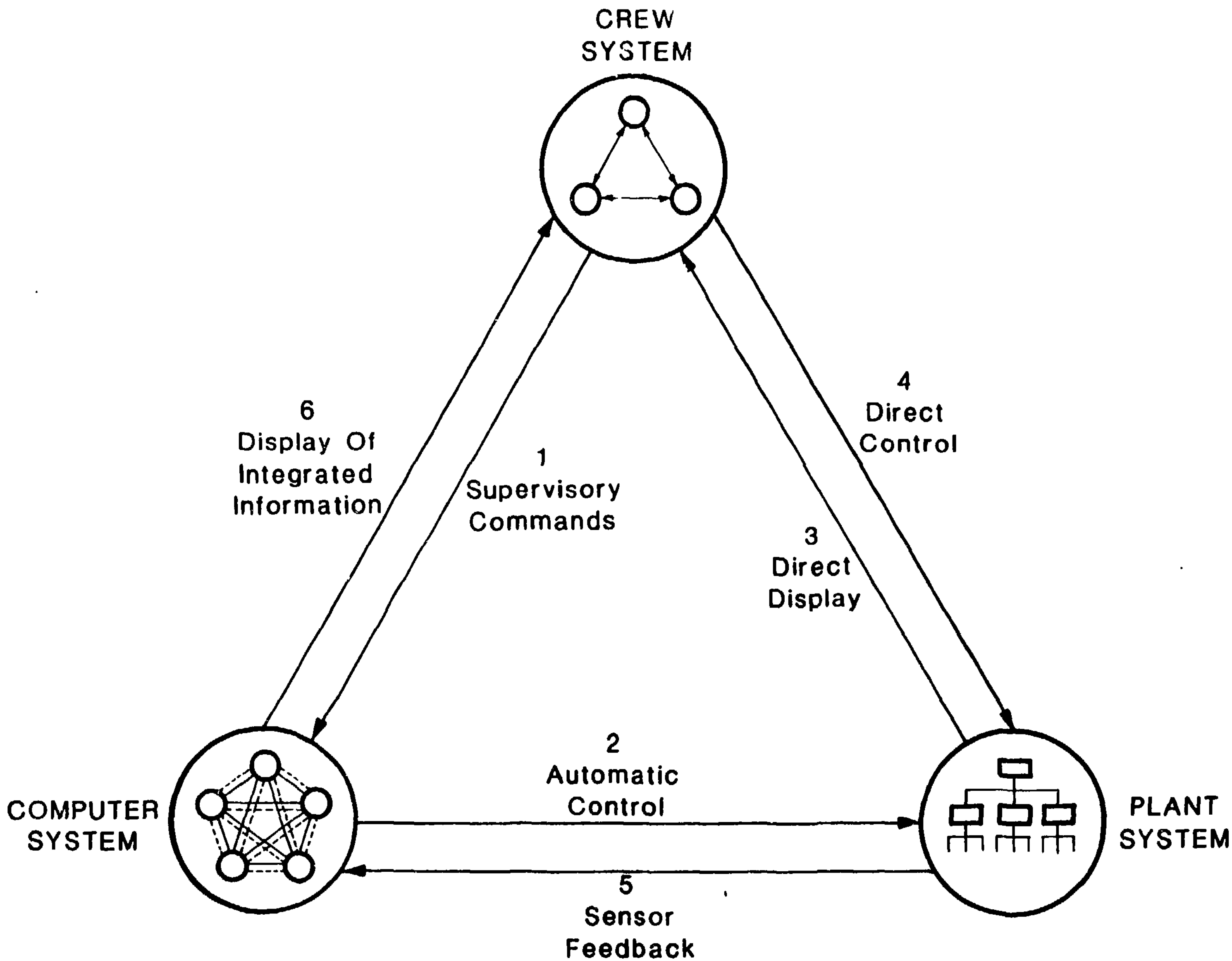

Fig. 1. Interconnections between operators, computers, and plant dynamics.

As depicted in the figure, the crew system comprises a team of communicating operators. Potentially, the crew element could include maintenance as well as operational functions.

The plant system comprises the dynamic portions of the plant under the responsibility of the operating crew. The plant system may be subdivided into the general functional areas of nuclear and related systems, energy transfer, and power generation and plant utilities.[3]

The computer system, interposed between the crew and plant, functions as an extension of the crew. The system may be subdivided into five function areas, which are expanded and discussed below.

Functions of the Operator as a Computer-Supervisor

The operator may be regarded[2] as performing five types of functions: (1) planning, with the help of the computer, what functions the computer should perform; (2) instructing the computer accordingly; (3) monitoring the computer's implementation of instructions; (4) intervening "in the instruction sequence" to provide new instructions, directly modifying plant parameters, or fully taking over from the computer if necessary; and (5) learning from experience so as to plan better the next time. Figure 2 shows these relationships. Three nested feedback loops are closed around these functional elements: an outer loop, from learning to planning, which constitutes a long time constant; an intermediate loop, from intervening to instructing, which constitutes a relatively short time constant; and an inner loop, within which monitoring is more or less continuous.

Functions of the Computer as an Operator Aid

The potential functions of the computer may be considered in five categories (Fig. 3): (1) aggregation of data from the plant, (2) simulation of plant operations, (3) control of the actual plant, (4) display of integrated information to the operator, and (5) diagnosis of abnormalities.

We observe that there are 20 possible interconnecitons between these 5 computational functions. These correspond to:

1. long-term data on which to base a model of the plant logic and dynamics

2. short-term data on which to base real-time plant control

3. display of long-term and short-term trends and conditions

4. use of analytic transformations (i.e., an "observer") to estimate some variables

ORNL-DWG 83-9594

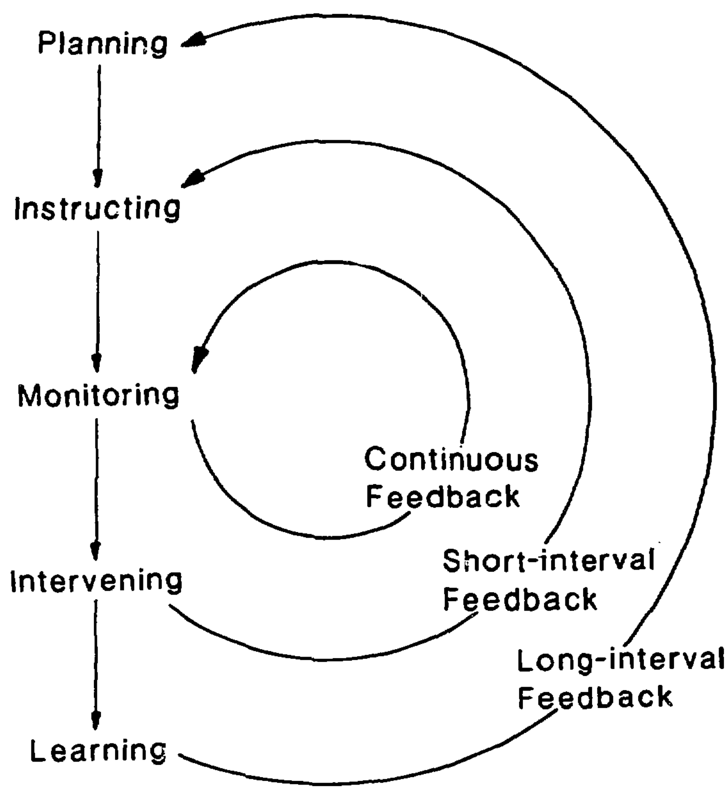

Fig. 2. Functions of the operator as a computer-supervisor.

ORNL-DWG 83-9596

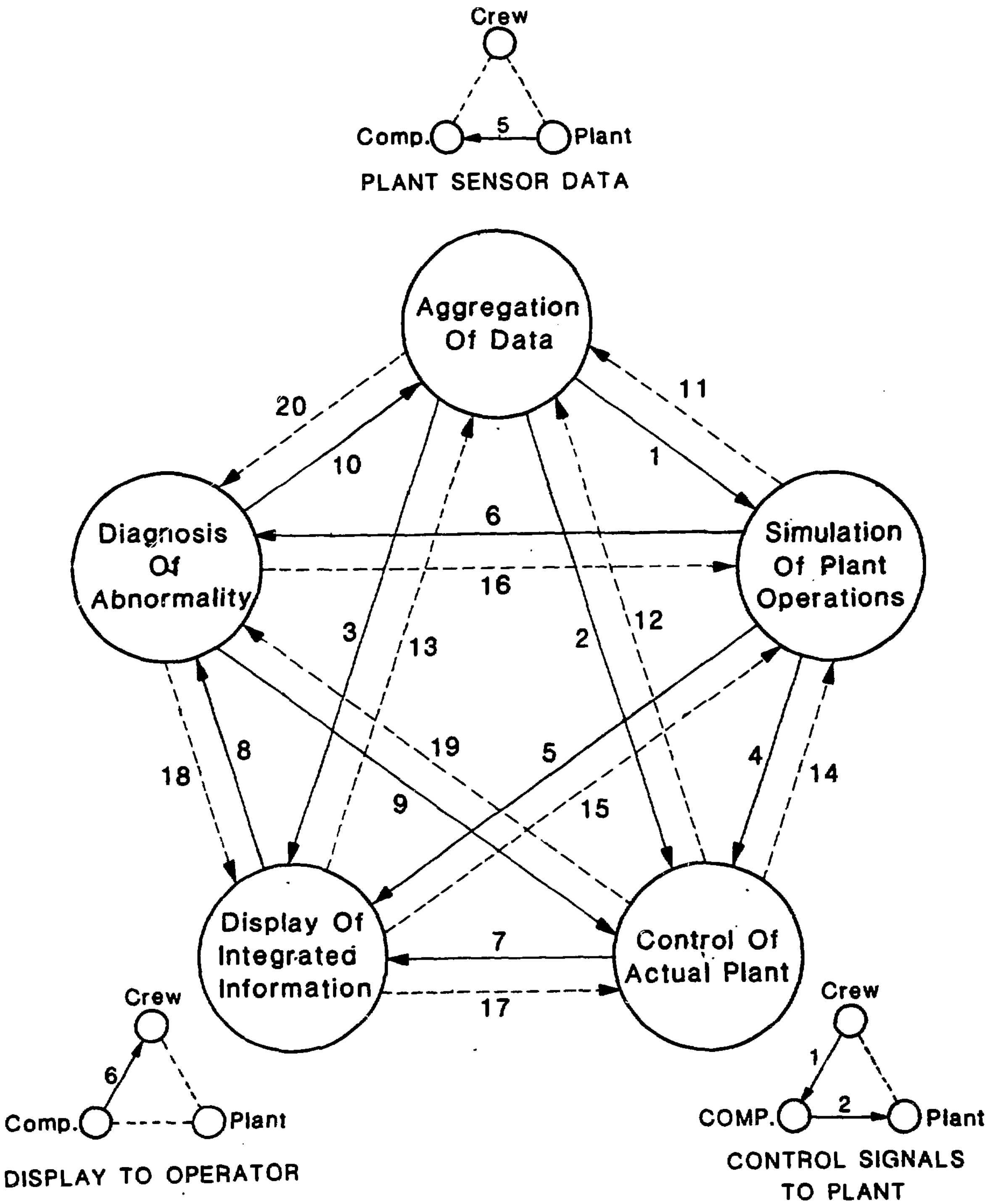

Fig. 3. Functions of the computer as an operator aid. The twenty arrows between functions indicate casual interconnections within computational functions. Small triangles at certain computer nodes indicate computer interconnections 1, 2, 5, and 6 with operator and plant as illustrated by Fig. 1.

5. display of predictions or "what if" for planning

6. use of real-time model of plant dynamics in failure diagnosis (including detection and location)[4]

7. display to operator the control algorithms that the computer is in the process of exercising

8. blank (see below)

9. switch control into emergency mode

10. record abnormal plant data

11. record simulator data for future use

12. record control settings for future correlation with plant data

13. blank (see below)

14. "innovations" signal to refine plant model to keep it in correspondence with actual plant

15. blank (see below)

16. commands to simulator to switch parameters in order to run in various abnormal modes

17. blank (see below)

18. results of abnormality diagnosis

19. indication to diagnosis logic of control inputs

20. aggregated plant data for diagnosis.

Note that the display is one-way to the operator and does not itself affect the other computer functions. Therefore 8, 13, 15, and 17 are blank in the listing above.

Control Systems That Learn From Their Operators

Our goals of improved availability and reliability for nuclear power operation will require improving the flexibility of the control system to recognize and respond to off-normal conditions, thereby increasing operator acceptance of automated systems, and improving the response of the crew as a team. With the eventual emergence of control facilities that are totally computer-based, intelligent, on-line adaptation and execution of procedures (and even on-line procedure generation) will be possible by machine operation. Surely the computer will participate to a much greater extent than it now does in diagnosing problems in the hardware, software, and process under control.

Programming of the operational system should not be relegated solely to design teams who characteristically do not follow the project through to plant maturity and eventual decommissioning. Some aspects of the programming should come from the operators. To continually refine the control system, as well as to ensure the integration of operator and control system, is to place the operator in the role of instructor to the computer. Provision for this man-to-machine communication necessarily would involve a high-level language which would permit the workings of the control system to be "transparent" i.e., the operator could "see" what he would be changing as well as how both the software and hardware would function together. To accommodate the operator, provision might be made to include a variety of input commands or queries put to the computer (e.g., making use of "fuzzy set" logic under study for control systems,[5] or query languages being developed by the artificial intelligence/computer science community[6]). As part of the human-computer exchange, the operator might be asked by the computer to rank his "utilities" (preferences) for various alternatives. Then, after some limited, self-imposed simulation of plant logic and dynamics, the computer might respond to the operator: "Based on what you've told me, this is what I understand." The preceding discussion, of course, is an expression of what we would like, and is not dissimilar from aspirations for user "friendliness" of computer systems in general.

What the operator would teach the computer can be categorized with respect to the five computer functions presented in Fig. 3:

a. Aggregation of data. Assuming that the collection and storage of certain data would be programmed so that the operator could not interfere with it, he would have the capability to collect and process additional data, up to the capabilities of the available plant sensors, memory, and processors.

b. Simulation of plant operations. The operator could ask for replays of past plant behavior under different control conditions, projections of what the plant would do under present circumstances if he leaves it alone (i.e., rapid-time simulations), or projections of what it would do if he were to alter certain control settings. Also possible would be a mode where the computer, after selecting a control option, itself initiates a rapid-time simulation to demonstrate to the operator what would happen if he allows that control strategy to be implemented. Simulation also would be inherent in control (in the form of "observers" or "Kalman filters") as well as in failure diagnosis.[4]

c. Control of actual plant. The operator could issue commands, in supervisory fashion, for the automatic control system to keep specified plant variables at assigned setpoints (as he does now), to follow certain assigned trajectories, or to achieve certain eventual states without exceeding or contravening assigned limits (most of which he cannot do with his present control system).

d. Display of integrated information. The operator could ask of the aggregated plant data base or of the other three computer functions (simulation, control, diagnosis) for display of information in any format (e.g., words, trends, diagrams, symbols, etc.). He would also have available certain standard formats which he could not change (i.e., those which every operator would know to be in a fixed format).

e. Diagnosis of abnormality. The operator would instruct the system where to look, what kinds of tests to do, what kinds of tolerances to use in declaring trouble, and what kinds of "failures" to ignore (equipment purposely shut off for maintenance, for example). There would be fixed algorithms for abnormality detection, alarm, location, and back-up diagnosis and display that would be off limits for reprogramming by the operator and would have priority on computational resources. We believe that both logical (fault tree, cause-consequence) and dynamic simulation[4] algorithms would be part of the package.

Fixed Operating Procedures vs New Advice from the Computers

A dilemma now being faced is whether to preplan all operating procedures on a rigid "if plant state is X then do Y" basis, or whether the operator should interpret the information provided by the Safety Parameter Display System and use his own judgment to a greater degree than now. Clearly, were the procedures always correct and the sensors and control system always reliable there would be no need for the operator--the computer could follow the procedures unerringly.

The operator, we realize, is present to be a supervisor and "field commander" of the computer, both to give orders and to back it up in case it cannot implement them as desired. As a field commander, he needs scouts and advisory staff. The computer must give the operator cognitive advice, that is suggestions on how and what to think, as well as its own (the computer's) assessment of how confident it is of that advice.

Research on advice-giving "expert systems" is growing. Thus far enough research has been done to make us realize that for computer advice to be understandable and useful to the operator, the computer's internal model (its framework) must cohere with the operator's mental model (his way of thinking about the plant).[7] This doesn't mean that the computer must always agree with the operator, but at least they must share linguistic and graphical terms, syntax, and a modicum of assumptions about the plant.

In addition, as has been suggested by Rasmussen[8] and others, control room advice-givers might do well to include some background information from the designers of the plant, like the reasons why it was designed as it was and assumptions made at the time of design about how it should be operated. Such information is not usually available to operators, at least not in a form they can use. The particular form in which the background information should be available is not clear, except that it should be linked to queries made or problems which occur in various plant systems, operating modes, or classes of upsets.

The accumulated prevalent wisdom of both maintenance and plant management should be integrated into the advice-giving software on the basis thac "human error" is often design error, maintenance error, or management error.

Where in the computer should the advice-giving function reside (i.e, in which of the five functions)? While the advice necessarily would emerge from the displays, it seems to us that appropriate advice-giving might originate from each of the other four functions in the same way that the operator might instruct each computer functon individually.

Conclusions

The theme of an intelligent, learning computer system is not a new concept neither are the five computer functions discussed in the text. Research in these areas is proceeding somewhat independently; thus innovative thinking is needed to integrate the isolated functions into a synergistic system. The taxonomic classification of these functions and their interconnections, which is by no means exhaustive, is hoped to provide a basis for such integration, to the end that improved control systems will result in improved palnt availability and reliability.

References

1. C. O. Hopkins et al., "Critical Human Factors Issues in Nuclear Power Regulation and a Recommended Comprehensive Human Factors Long-Range Plan," NUREG/CR-2833, Vol. 1 Executive Summary p. 16.

2. T. B. Sheridan, "Supervisory Control: Problems, Theory and Experiment for Application to Human Computer Interaction in Undersea Remote Systems," MIT Man-Machine Systems Laboratory Report, March 1982.

3. R. A. Kisner and P. R. Frey, "Functions and Operations of Nuclear Power Plant Crews," NUREG/CR-2587, Oak Ridge National Laboratory, April 1982.

4. U. Tsach, T. B. Sheridan, and J. Tzelgov, "A New Method for Failure Detection and Location in Coupled Dynamic Systems," Proc. 1982 American Control Conference, June 14-16, Arlington, VA.

5. A. Buharali, "Fuzzy Sets and Other Methods for Telling a Computer How to Decide," MIT Man-Machine Systems Laboratory Report, September 1982.

6. P. H. Winston, Artificial Intelligence, Addison-Wesley, NY, 1977

7. T. B. Sheridan et al., "Workshop on Cognitive Modeling of Nuclear Plant Control Room Operators," NUREG/CR-3114 Proceedings of Workshop at Dedham, MA, August 15-18, 1982.

8. Personal Communication with Jens Rasmussen, Riso National Laboratory, Denmark, November 1982

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.