RISØ-M-2349

A MODEL OF HUMAN DECISION MAKING IN COMPLEX SYSTEMS AND ITS USE FOR DESIGN OF SYSTEM CONTROL STRATEGIES

Jens Rasmussen and Morten Lind

Abstract. The paper describes a model of operators' decision making in complex system control, based on studies of event reports and performance in control rooms. This study shows how operators base their decisions on knowledge of system properties at different levels of abstraction depending on their perception of the system's immediate control requirements. These levels correspond to the abstraction hierarchy including system purpose, functions, and physical details, which is generally used to describe a formal design process. In emergency situations the task of the operator is to design a

INIS Descriptors BEHAVIOR; CONTROL ROOMS; CONTROL SYSTEMS; FLOW MODELS; HUMAN FACTORS; INDUSTRIAL PLANTS; NUCLEAR POWER PLANTS; PERSONNEL; PLANNING; RELIABILITY

UDC 007.51

April 1982
Risø National Laboratory, DK-4000 Roskilde, Denmark

suitable control strategy for systems recovery, and the control systems designer should provide a man-machine interface, supporting the operator in identification of his task and in communication with the system at the level of abstraction corresponding to the immediate control requirement. A formalized representation of system properties in a multilevel flow model is described to provide a basis for an integrated control system design.

To be presented at the American Control Conference,
Arlington, Virginia, U.S.A., June 14-16, 1982.

ISBN 87-550-0854-2
ISSN 0418-6435

Risø repro 1982

TABLE OF CONTENTS

INTRODUCTION

System function depends on a causal structure. Part of the causal structure of an industrial system is related to energy and mass flows in the physical, i.e., mechanical, electrical and chemical, process equipment. Another part of the causal links depends on information flow paths interconnecting the physical equipment which remove degrees of freedom from system states in accordance with the purpose of system operation. The constraints on system states to be introduced by this controlling information network depend on the immediate purpose or operating mode and will serve to maintain a state; to change operating state in a particular system or subsystem, or to coordinate and "synchronize" states in several subsystems to prepare for systems reconfiguration.

The general aims of the associated information processes which are necessary are therefore: to identify system states, to compare these with target states, to consider goals and purposes, and to plan appropriate actions on the system. In modern, automated process plants and other complex systems, the processing of control information is performed by three parties in a complex cooperation, i.e., the systems designer, the system operator, and the automatic control system. The complexity of this cooperation caused by modern information technology and the requirement for extreme reliability of control decisions in large scale installations now calls for a careful overall design of this information network. The traditional approach is to automate the well structured functions and to ask the operator to cope with the badly structured situations by means of information on system goals and state and education in process fundamentals. This approach is clearly inadequate, even when designers make heroic efforts to assist operators by providing detailed operating instructions for the abnormal situations they have identified and analyzed as part of the design. The usual dichotomy between situations which are analyzed and for which automatic control or detailed procedures are designed and those which are left open by the designer

needs to be replaced by a consistent design of the overall control strategy including an attempt to bring structure to the category of unforeseen situations.

The system designer will have to consider and specify the overall control strategy, which he can do at various levels of detail. He may introduce predetermined links between defined states and relevant actions by means of automatic control loops and sequence controllers or he may introduce control strategies at higher levels by means of process computers with adaptive or heuristic programs. Alternatively, he may ask operators to perform control tasks, either in a preinstructed mode or by problem solving and improvization. In modern systems, all these possibilities are used in various com ations depending upon the actual situation. In order to design the overall control strategy in a consistent way, the designer has to use a model of human performance which is compatible with the models used for design of automatic control systems, together with a consistent description of the actual control requirements of the system in the various operating conditions.

MODEL OF HUMAN INFORMATION PROCESSING

The model of human performance we need for this purpose has several distinct characteristics. First of all, to be compatible with control system design, models of human performance in terms of information processing as they are now emerging within cognitive psychology are most relevant. What we need are not, however, detailed models of human information processes in specific situations, but rather models of the possible categories of human decision strategies which operators will use for various generic types of control tasks. These models will then serve to identify the requirements for psychological models representing the human resources for the types of information processes required and the human performance criteria or subjective preferences which control human choice among possible strategies in a given situation.

Another feature of the models we are seeking is that they should not only cover systematic, analytical decision making used during abnormal situations but also the tricks of the trade and the automated habits used by skilled operators during routine situations. This implies that a model should also include the characteristics of sensori-motor performance, and the output of information processes should be modelled in terms of actions. To be able to evaluate the interference from overlearned routines in performance during unfamiliar situations, it is important to include the two extremes of performance in one conceptual framework. In addition, it is, in general, important that this framework is able to represent also the effects of psychological error mechanisms in terms which can be related to features of the man-machine interface.

The first step in the modelling process is to describe the human information processes required to perform a control task. This should be a description in terms of internal human activities rather than system requirements, i.e., a description of the human decision process from the instant when the need for intervention is detected to the resulting actions.

To develop a model of the possible decision sequences of human operators in industrial process plants, we have analysed a number of verbal protocols (Rasmussen, 1976). As might be expected, this attempt did not reveal much of the human information processes. However, the analysis identified a number of typical statements of "states of knowledge" in the decision process, which can be arranged in a rational sequence, see figure 1. These states of knowledge divide the decision process into a sequence of more or less standardized subroutines. This structure appears to be very efficient, since a particular decision problem can be dealt with by a sequence composed from standard routines. Formulation of a "state of knowledge" serves to prepare the result of one routine for application in the following routine. In addition, ready-made solutions from previous cases are easily incorporated. However, the structure also invites by-passes and leaps in the basic rational sequence in the form of immediate associations between states and stereotyped, rule-based transformations. This is

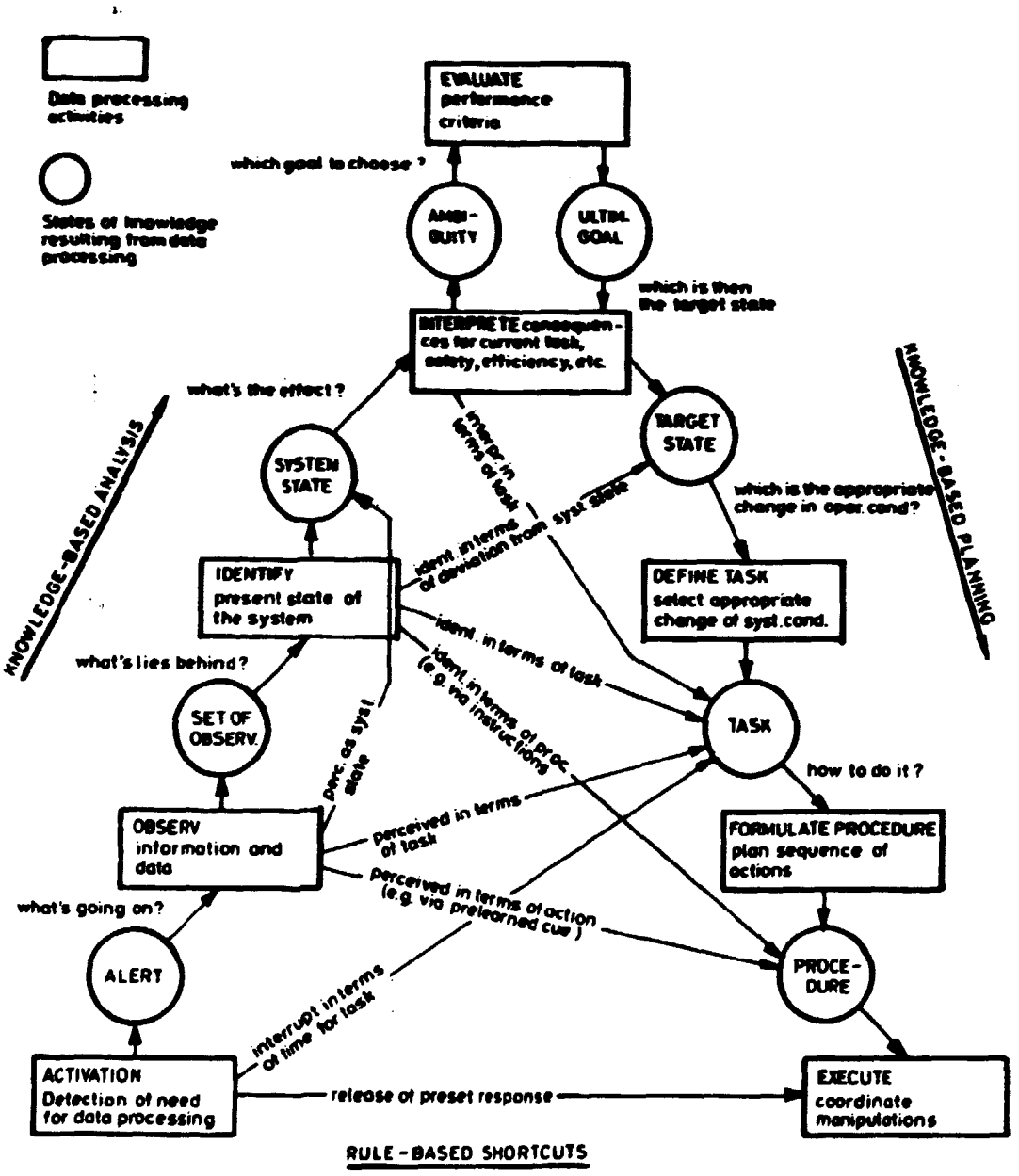

Fig 1. Schematic map of the sequence of mental activities used between initiation of response and the manual action. Rational, causal reasoning connects the "states of knowledge" in the basic sequence. Stereotyped mental processes can bypass intermediate states.

important for reflecting the operators' opportunities for development and use of know-how and skill, but also leads to the potential for "traps" during less familiar situations. In figure 1, different typical by-passes are shown. This model is not a model of human performance but a conceptual framework mapping possible decision sequences which can be used for the same external control task, depending on the know-how of the actual operator. To be useful for interface design, this frame of reference must be supplemented by models of those psychological mechanisms which are used by humans for the subroutines of the decisions process. It is important that these models of psychological mechanisms as they are studied by experimental and cognitive psychology, also represent limiting properties and error mechanisms. As mentioned, the verbal protocols do not in general identify these psychological mechanisms and in well adapted performance they cannot be derived from external performance. Only when adaptation breaks down will properties of the psychological mechanisms reveal themselves and, consequently, we have made an attempt to model the role of internal mechanisms from analyses of human error reports (Rasmussen, 1981) supplemented by findings from verbal reports. The result is shown in figure 2. Three levels of human performance are identified with very distinct features, seen from a control theoretic point of view. The skill-based performance represents the highly automated sensori-motor performance which rolls along without much conscious control. The human performs as a multivariable continuous controller, like a data-driven controller for which input information acts as time-space signals and the functional properties of the systems under control are only represented in the controller as dynamic, spatial patterns. The rule-based performance at the next higher level represents performance based on recognition of situations together with rules for actions from know-how or instructions. Input information acts as stereotype signs labelled in terms of states, events or tasks. The functional properties of the system are at this level implicitly represented by rules relating states and events to actions. The activity at the rule-based level is to coordinate and control a sequence of skilled acts, the size and complexity of which depend on the

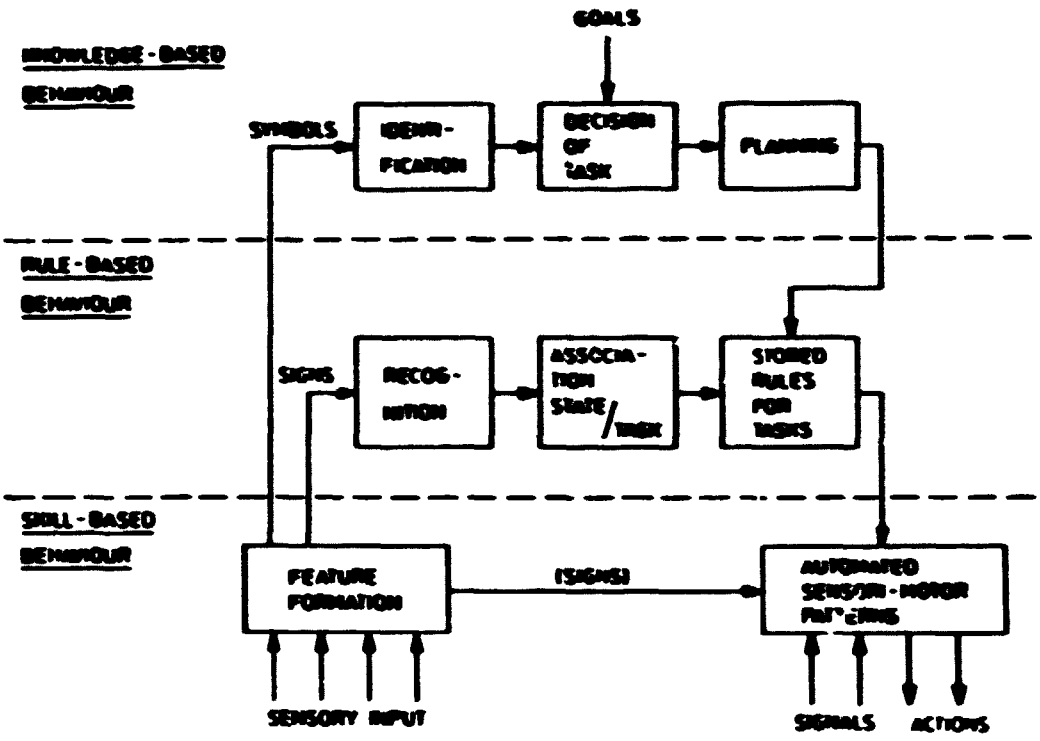

Fig. 2. Simplified illustration of three levels of performance of skilled human operators. Note that the levels are not alternatives, but interact in a way which is only rudimentarily represented in the diagram.

level of skill in a particular situation - one single decision to go home for dinner may be enough for driving you there, if the ride is not disturbed.

When proper rules and familiar signs are not available for a situation, activity at the next level of knowledge-based performance is necessary to generate a new plan for action ad hoc. The main feature here is that information is perceived as symbols which are used for information processing characterized by an explicit representation - mental model - of the functional structure of the system to be controlled as well as the related causal relations. The information process used by a person in a specific unfamiliar situation will depend very much on subjective knowledge and preferences and detailed circumstances for the task. It therefore appears to be unrealistic to model the detail flow of information processes in a decision

sequence. Rather, categories of possible prototypical information processes are described by identifying the overall strategy used to control the decision process, which is tightly connected to a specific type of mental model and the related symbols.

A major problem in design of man-machine interface systems is to properly support knowledge-based behaviour in supervisory control tasks. One prerequisite for doing this is to present information in a format structured so as to lead operators to develop effective mental models, and to code the information at a symbolic level compatible with these models and with strategies appropriate for the actual decision task. This is what Norman (1981) calls "cognitive engineering". To do this, however, the control task which the operator is supposed to perform, must be formulated - by the control system designer or by the operator himself - at the proper level of detail and abstraction in the control hierarchy and not in terms of individual instrument readings and elementary actions on equipment (Rasmussen and Lind, 1981).

A control task, and the necessary decision strategies with related mental models, for instance, to be used for state identification and diagnosis, can be formulated at several levels of abstraction, see figure 3. These levels range from representation of physical anatomy of the plant through levels of functional descriptions, to a description in terms of design intentions and purpose.

The identification of system state, which is most frequently the critical phase of a supervisory control task, is in general facilitated by the fact that we are not asking for an absolute, isolated identification but rather an identification in terms of deviation from a target state, i.e., a normal, specified or forbidden state. In this way a kind of structure can be imposed on the category of unforeseen events. In the abstraction hierarchy, the discrepancy can be identified at each of the levels and so can, therefore, the control task. Disturbances, i.e., actual states, are propagating bottom-up in the hierarchy whereas target state in terms of topological configuration and

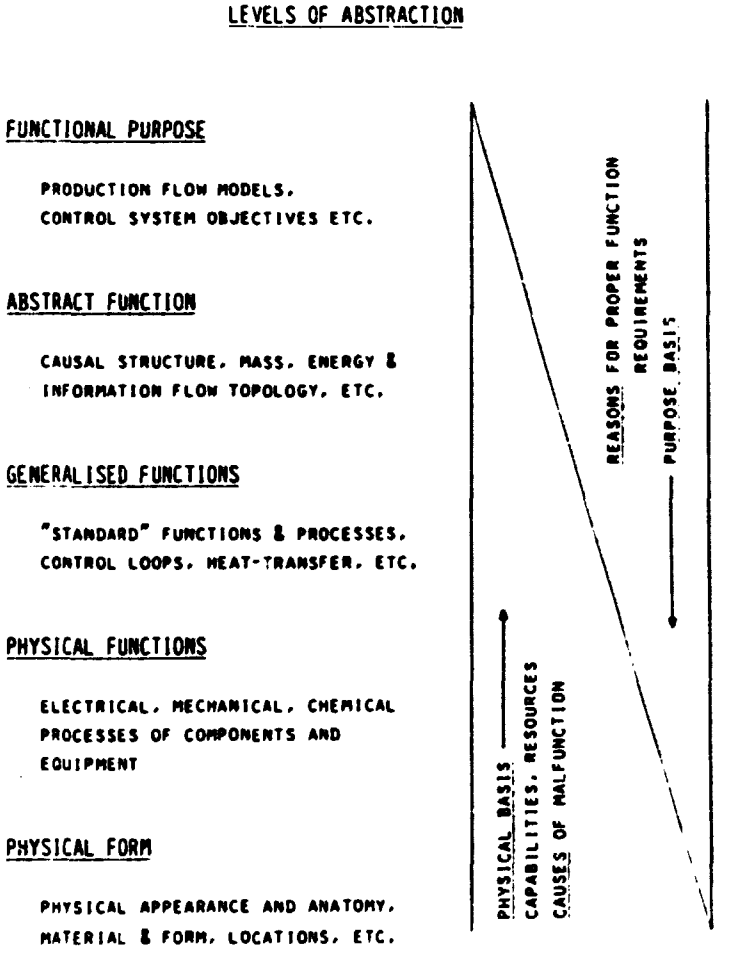

Fig. 3. The abstraction hierarchy used for representation of functional properties of a technical system.

boundaries for allowed and specified states can be developed top-down from consideration of production and safety requirements derived from the purpose of system operation.

The appropriate level of identification depends on the actual circumstances. Identification of disturbances in terms of mass-energy flow topology at a high level of abstraction is appropriate for compensation of production disturbances. In

order to remove the cause of disturbance by repair or replacement, identification in terms of physical anatomy is of course necessary. There is, therefore, a circular relation in the choice of appropriate level of identification which depends on the goal which, in turn, depends on the state to be identified. It is, therefore, necessary to consider a reasonable strategy for search through levels and for prioritizing. Although the functional properties represented at the various levels of abstraction are basically different, it appears to be important to seek a common language in which generic control tasks can be formulated for all levels. For this purpose a representation of causal relations at all levels has been formalized on the basis of energy-, mass-, and information flow topology.

INTEGRATED CONTROL SYSTEM DESIGN

During design of the process plant itself, the functions of the system and its physical implementation are developed by iteratively considering the plant at various levels of abstraction and in increasing degree of detail, see Figure 4.

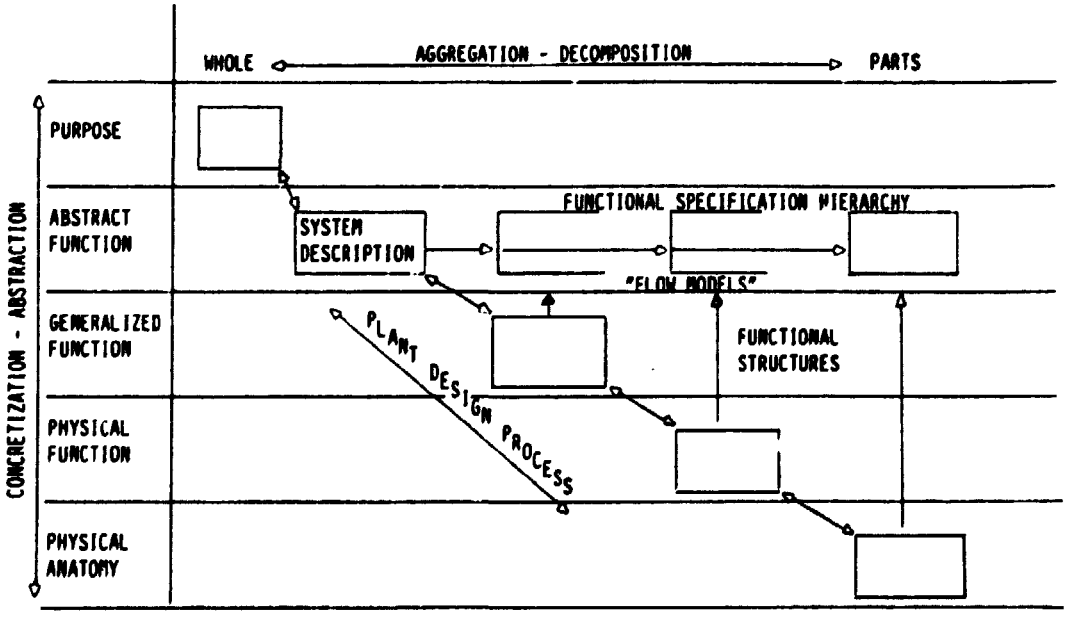

Fig. 4. Derivation of goals and functional specifications during the design process.

During this design process the physical system is identified, i.e., the implementation of those causal structures depending on mass and energy relations. However, as the degree of physical detail increases during the design process, so does the number of degrees of freedom in functional states. Therefore causal links by means of control paths relating desired states with necessary control actions must be introduced to constrain the possible operational states.

In this way, the desired states of functions and equipment will be identified during design at different levels of abstraction, and the necessary information or control constraints will be identified in terms of the conceptual framework related to these levels. In general, a skilled designer will immediately be able to identify suitable and familiar control system concepts. It is, however, the aim of the present paper to demonstrate that a consistent systems design including operator control functions can be performed more systematically by means of the generalised decision model and the flow modelling concept.

The system's control requirements are derived from the necessary relations between the actual states, the desired states or changes of states, and the required actions on the system. This means that planning of control actions involves the rational decision sequence of figure 1, covering state identification, goal evaluation, and prioritizing, in addition to the planning itself. Depending upon the control task allocation, the decision sequence - or parts of it - will be performed by the designer himself, the plant operator or the process computer. The conceptual framework within which decisions are taken, will usually depend on the background of the person, i.e., designer or operator, and upon the immediate context of the decision. However, to have a consistent overall-design and to be able to formalize the decision functions to be performed by the computer, ad-hoc decisions throughout the design process should be replaced, or at least reviewed, by considerations based on a uniform description of the necessary constraints and the related control requirements which are expressed in a suitable language. For this purpose, we consider a transformation of the

desired functional states and the necessary conditions, supplies, and constraints emerging during the various phases of design specification into a uniform description of specified functional states at the level of energy and mass flow structure - the abstract functional level of Figure 4. The result is a consistent hierarchical description of target states and intended functions - i.e., a goal or specification hierarchy as shown in Figure 5 (Lind, 1982).

The importance of dealing with different types of hierarchies in the description of complex systems has been discussed by Mesarvoic and his collaborators (Mesarovic et. al. 1970). In their terminology, our abstraction hierarchy is an example of a stratified system description. The decision making hierarchy introduced in op. cit. is related to our specification hierarchy in the sense that system control requirements specified in the hierarchy are the basis for choices of decision making strategy in control of the system. Mesarovic et. al. do not distinguish clearly between the hierarchies of decision making and of system goals. However, this distinction is essential to the present discussion of control task allocation between the operator and the computer. The allocation strategy leads to the specification of the structure of the decision making processes in control.

Hierarchical Control and Generic Control Tasks

A multi-level model as depicted in Figure 5 describes mass-and--energy flow topology at different levels of functional decomposition of the plant. It can be used to define plant control requirements on any level in a uniform way (Lind, 1982). Three generic control tasks can be identified using this framework. Two categories of control tasks relate to the constraints in plant variables necessary to remove excess degrees of freedom in order to maintain specified state or to change state within a regime of operation. The third category relates to the changes in variable constraints which are necessary to coordinate the state in two separate flow structures during plant reconfiguration, as, e.g., required during

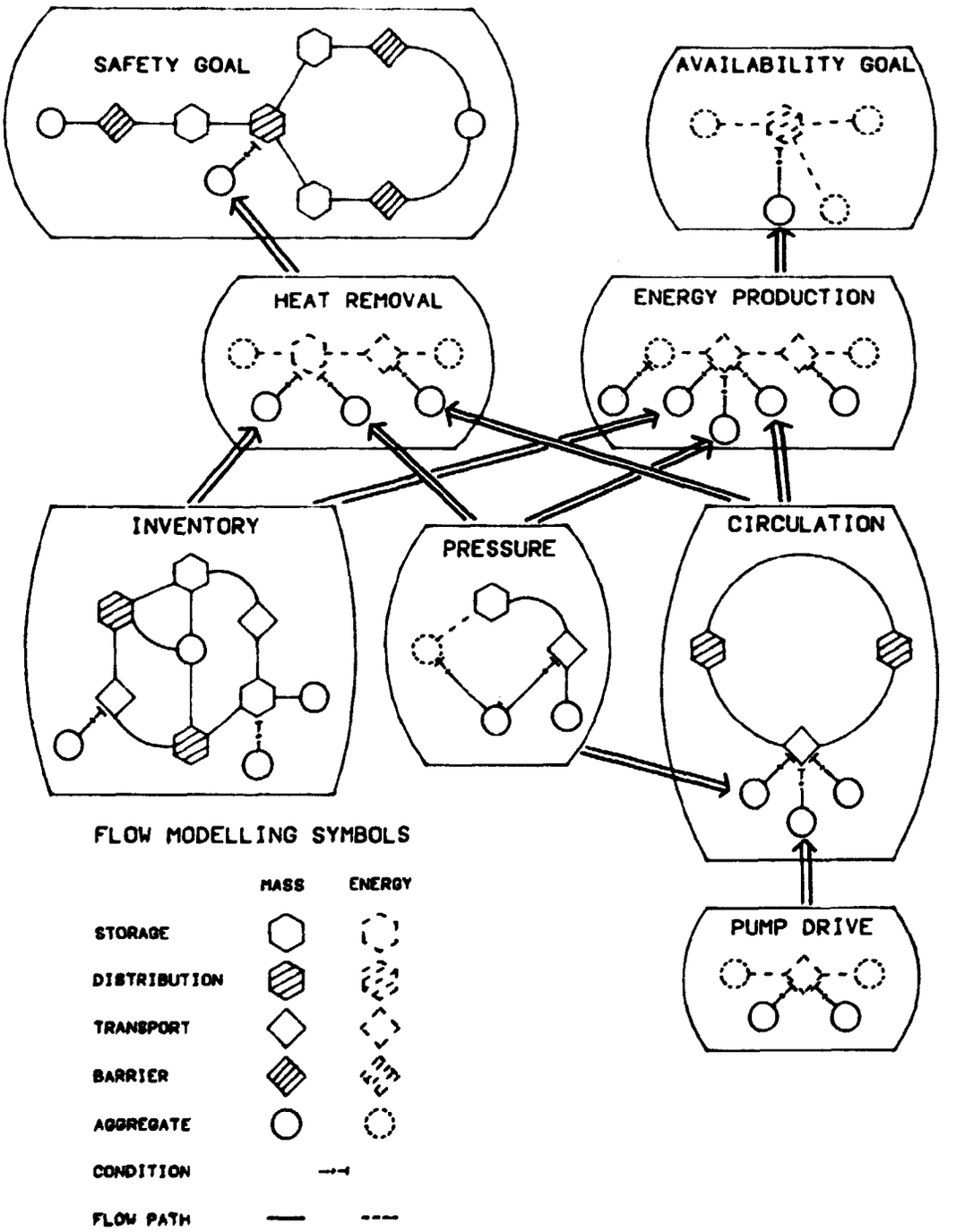

Fig. 5. Multilevel flow model of a nuclear power plant (PWR).

start-up and shut-down (Lind, 1979). The flow modelling framework leads to a systematic identification of plant control tasks at any level of functional decomposition in terms of these generic types and plant control can be systematically planned in generic flow model terms before allocation to operator or automatic equipment is considered.

This planning phase of the decision task for known or specified states is, perhaps, the least problematic part. The difficult part will frequently be the analytical state identification part, necessary to cope with disturbances. Since the energy--and-mass flow models represent the causal structure of the physical system in a uniform way, they are well suited to map the propagation of disturbances through the system. This means they can support a systematic state identification in terms of changes or deviations from specified or normal states in the flow topology by means of logic inferences based on measured variables. This is precisely the diagnostic task necessary for systems control. The systematic or consistent structure of diagnosis with reference to specified state and not to known fault patterns is mandatory for automation of the identification of unforeseen disturbances (Lind, 1981). A model based on a description of the mass-and-energy flow structure thus appears to be an efficient tool for an integrated design of the control hierarchy in device-independent terms as well as for a stringent formalization of these analysis and planning processes for computer implementation. The allocation of the decision task to operators or computers will be considered in more detail in the following.

Man-Computer Allocation of Decision Functions

Man-computer allocation of the different parts of the decision sequence is the last stage in a formal control system design process which has several distinct steps.

First, the functional properties of the process plant as identified during the design process at the various levels of abstraction are transformed into a hierarchical description in

terms of mass-and-energy flow structures, i.e., into a functional specification hierarchy for each of the relevant operating regimes. Then the bottom-up propagation in the abstraction hierarchy of disturbances from faults in the system is examined and the measured physical variables necessary to identify the disturbed state and to plan proper control actions, are determined by means of the flow model.

Second, the control or information paths necessary to maintain or change the states in this flow structure are determined together with the decision process necessary to identify the need for and plan execution of control actions in terms of the general decision sequence of figure 1. Furthermore, it is evaluated to what extent stereotype bypasses in the decision sequence can be utilized by the designer to simplify the decision function in the actual operating situation for the foreseen and well specified conditions.

Third, the information processing strategies which can be used during plant operation for the various phases of the decision sequence are identified. In general, strategies with very different structures and resource requirements can be used for a given decision phase. As an example, we can consider the identification of a disturbed state of the plant. This identification or diagnosis can be performed by various search strategies related to different representations or models of system properties (Rasmussen, 1981). An abnormal plant state can be identified by a symptomatic strategy implying search through a set of symptom patterns labelled in names of states or actions. The symptom patterns can be stored in a library of symptoms in the memory of an operator or a decision table of a computer, or they can be generated ad-hoc in a hypothesis--and-test strategy by an operator and/or a computer with access to a proper functional model of the control object. These strategies depend on symptom-patterns or models related to known failed functions, which is not the case for the topographic search strategies. In these strategies, search for the deviation from normal state is done with reference to the normal function, which eases the problem with identifying unforeseen states. In return, labelling in predetermined tasks is not feasible and ad-hoc planning may be necessary.

These strategies have very significant differences with respect to the type of model, the symbolic interpretation of data and the amount of information which is required and with respect to the necessary data processing and memory capacity. Consequently, they match the capabilities of computers and people differently.

Therefore, the fourth step in the systematic design will be to evaluate the match between the requirements of the various possible strategies and the resources available for the decision makers, i.e., designers, operators, and process computers.

To a large extent, this allocation procedure will lead to traditional designs in the clear-cut choices. The control decisions to serve the majority of necessary control links required to maintain specified states in the equipment will be analysed by the designer and implemented by standard control algorithms. Likewise, the control sequences necessary for planned, orderly coordination and reconfiguration for start and stop sequences will be analysed by the designer and the necessary sequences transferred to operators as instructions or to automatic sequence controllers as decision tables. However, in designing for disturbance control the systematic consideration of possible strategies for state identification, prioritizing and planning along the line discussed here will support the search for a consistent overall design.

For more complex emergency situations, a "once-and-for-all" allocation of the decision functions is difficult because demand/resource match will depend on the specific situation and may change several times during the decision processes. A kind of cooperative strategy in which operators and computer in parallel consider the same decision problems may be preferable. It will then be possible to let the role of decision maker and that of monitor and guide shift back and forth between man and computer depending upon the immediate situation. Consider, for example, the use of various diagnostic strategies for system identification. An expert trouble shooter will start using symptomatic search based on recognition of familiar symptoms -

this strategy utilizes all his experience and skill and may rapidly lead to the result. However, the expert is characterized (Rouse, 1981) by his ability to recognize when symptoms are unreliable with the result that he will switch to a careful, topographic search. This requires a high capacity for remembering and inference and can be efficiently supported by a computer. For a computer diagnostician, the reverse will be an appropriate strategy. Thus a consistent, topographic search in the flow topography at several levels with conservative careful inference and data transformation will be more suitable followed, when no more resolution is available, by a seeking of assistance from a human operator for additional knowledge, symptoms, locations of recent repair of the plant etc. In this way, complementary approaches can be used by man and computer, but planning of a successful cooperation depends on an overall structuring of system function, control requirements and decision functions which is device independent.

Even though the overall control structure and task allocation are developed in terms of the abstract flow-topology, the operators may choose to implement their allocated control decisions a conceptual framework at another level of abstraction closer to the physical anatomy level. This may affect the demand/resource match and must be considered when tasks are allocated since, for example, iterations between descriptions at different levels of abstraction may be required. Furthermore, the conceptual framework that operators will tend to prefer as the basis for the actual task will depend on the framework used for the display formats and data conditioning, which therefore should be considered concurrently with the decision task allocation (Goodstein, 1982a & b).

In this way, the abstraction hierarchy is used to design the control system while the specification hierarchy at the abstract function level is used to coordinate the structure of the total control strategy.

ACKNOWLEDGEMENTS

This work is part of the joint Scandinavian NKA/LIT project on Human Reliability supported by the Nordic Council of Ministers. A series of experiments on man-computer cooperation in process plant diagnosis along the lines described in this paper has been planned as part of the project.

REFERENCES

Goodstein, L. P., "Computer-based Operating Aids". Paper to be presented at Design 82, Birmingham UK, September 22-23, 1982a.

Goodstein, L. P., "An Integrated Display Set for Process Operators". Paper to be presented at the IFAC/IFIP/IFORS/ IEA Conference on "Analysis, Design and Evaluation of Man-Machine Systems", Baden-Baden, F. R. Germany, September, 27-29, 1982b.

Lind, M., "The Use of Flow Models for Design of Plant Operating Procedures", paper presented at: IWG/NPPCI Specialists Meeting of Procedures and Systems for Assisting an Operator During Normal and Anomalous Nuclear Power Plant Operation Situations, December 5-7, 1979, Garching FRG.

Lind, M., "The Use of Flow Models for Automated Plant Diagnosis." In Rasmussen, J. and Rouse, W. B., (eds.), "Human Detection and Diagnosis of System Failures". Plenum Press, New York, 1981.

Lind, M., "Multilevel Flow Modelling of Process Plants for Diagnosis and Control." To be published 1982.

Mesarovic, M. D., et al., "Theory of Hierarchical, Multilevel, Systems." Academic Press (1970).

Norman, D. A., "Steps Toward a Cognitive Engineering: Systems Images, System Friendliness, Mental Models", paper presented at Symposium on Models of Human Performance, ONR Contractor's meeting, La Jolla, Ca. (UCSD), June 19, 1981.

Rasmussen, Jens, "Outlines of a Hybrid Model of the Process Plant Operator." In T. B. Sheridan & G. Johannsen (eds.), "Monitoring Behaviour and Supervisory Control." Plenum Press, New York, 1976.

Rasmussen, Jens, "What Can Be Learned From Human Error Reports." In Duncan, K., Gruneberg, M., and Wallis, D., (eds.), "Changes in Working Life." John Wiley & Sons, 1980.

Rasmussen, Jens, "Models of Mental Strategies in Process Plant Diagnosis." In Rasmussen, J. and Rouse, W. B., (eds.), "Human Detection and Diagnosis of System Failures." Plenum Press, New York, 1981.

Rasmussen, J. and M. Lind, "Coping with Complexity", Risø-M-2293, 1982, presented at European Annual Conference on Human Decision and Manual Control, Delft, 1981.

Rasmussen, Jens, "Skills, Rules & Knowledge; Signals, Signs & Symbols and Other Distinctions in Human Performance Models." Risø-N-4-82. To be published, 1982.

Rouse, W. B. and R. M. Hunt, "A Fuzzy Rule-based Model of Human Problem Solving in Fault Diagnosis Tasks." Proceedings of the Eighth Triennial World Congress of the International Federation of Automatic Control, Kyoto, Japan, August 1981.

Risø National Laboratory **Risø-M-** 2349

Risø-M- 2349

Title and author(s)

A Model of Human Decision Making in Complex Systems and Its Use for Design of System Control Strategies

Jens Rasmussen and Morten Lind

Date April 1982

Department or group Electronics

Group's own registration number(s) R-8-82

pages + tables + illustrations

Abstract

The paper describes a model of operators' decision making in complex system control, based on studies of event reports and performance in control rooms. This study shows how operators base their decisions on knowledge of system properties at different levels of abstraction depending on their perception of the system's immediate control requirements. These levels correspond to the abstraction hierarchy including system purpose, functions, and physical details, which is generally used to describe a formal design process. In emergency situations the task of the operator is to design a suitable control strategy for systems recovery, and the control systems designer should provide a man-machine interface, supporting the operator in identification of his task and in communication with the system at the level of abstraction corresponding to the immediate control requirement. A formalized representation of system properties in a multilevel flow model is described to provide a basis for an integrated control system design.

Copies to

Available on request from Risø Library, Risø National Laboratory (Risø Bibliotek), Forsøgsanlæg Risø), DK-4000 Roskilde, Denmark
Telephone: (03) 37 12 12, ext. 2262. Telex: 43116