Decision Support in Supervisory Control of High-Risk Industrial Systems

Rasmussen, Jens; Goodstein, L. P.

Published in:
Automatica

Link to article, DOI:
10.1016/0005-1098(87)90064-1

Publication date:
1987

Document Version
Peer reviewed version

Automatica, Vol. 23, No. 5, pp. 663-671, 1987

Printed in Great Britain 0005-1098/87 $3.00 + 0.00

Pergamon Journals Ltd.

Brief Paper

Decision Support in Supervisory Control of High-risk Industrial Systems*

JENS RASMUSSEN and L. P. GOODSTEIN♣

Key Words-Cognitive systems; computer applications; display systems; decision making; functional

analysis; industrial control; man-machine systems; supervisory control; system failure and recovery.

Abstract. – It is argued that the supervisory control of complex industrial processes having a potential for serious consequences in case of accidents requires careful consideration of the allocation of decision making between the three main agents of control; namely the designer, the operator and the automatic control system. In particular, it is advocated that, instead of continuing their efforts to make their preplanning of responses and countermeasures more and more complete and thus restrict the operators' own initiative, designers should take advantage of modern information technology to make

*Received 11' May 1986; revised 11 February 1987. The original version of this paper was presented at the 2nd IFAC/IFIP/IFORS/IEA Symposium on Analysis, Design and Evaluation of Man-Machine Systems which was held in Varesa, Italy during September 1985. The Published Proceedings of this IFAC Meeting may be ordered from: Pergamon Books Limited, Headington Hill Hall, Oxford OX3 OBW, (J.K. This paper was recommended for publication in revised form by Editor A. P. Sage.

♣ Department of Computer and Information Science, Risø national laboratory, DK 4000, Roskild, Denmark

available to the operators their conceptual models and their processing resources so as to allow the operators to function as their extended arm in coping with the plant. Such an interactive decision-making activity would thus benefit from this simultaneous availability of the design basis, up-to-date knowledge of plant status and accumulated operational experience.

Introduction

THE CONTEXT of this paper is automated industrial processes and the requirements they place for providing adequate and timely support to the operating staff in connection with the tasks commonly associated with the "job" of supervisory control. The operators usually have little or no manual control activities. Thus what traditionally is called "hands-on process feel" cannot play any important role and reliance must therefore be placed on the information and manipulation facilities provided by the display and controls interface to provide what the operators need to know and do in order to ensure that the system operates reliably, economically and safely in the face of deviations from "normal" because of disturbances, technical faults and/or inappropriate human actions.

In truth, the crew is part of a decision-making team which, in accordance with the functional allocations of the designers, plays certain assigned roles in dealing with the process. Use of the word team reflects the fact that the supervisory coritrol of such complex systems is actually a cooperative effort within a group consisting of the designers, the automatic (computer-based) control system and the operating staff. This three-way arrangement arises from the fact that the decisions of the designers are embedded in the automatic system as well as the training of the operators. Thus the prerequisite for a successful cooperation is that the computer and the operators/users have to be able to work together in a positive way by taking advantage of their different and complementary information processing abilities and their different knowledge about the system, the environment, the goals, etc. -,@,'his means that the framework in which this cooperation takes place will/should involve a dynamic allocation of decision functions between the "partners" with appropriate feedback and communication facilities between them.

This paper will treat these issues using previously developed frameworks for structuring the decision making process and for describing the associated decision space and thus to a considerable extent the knowledge required. Some remarks will also be made about the critical problem related to operator *acceptance* of the team role.

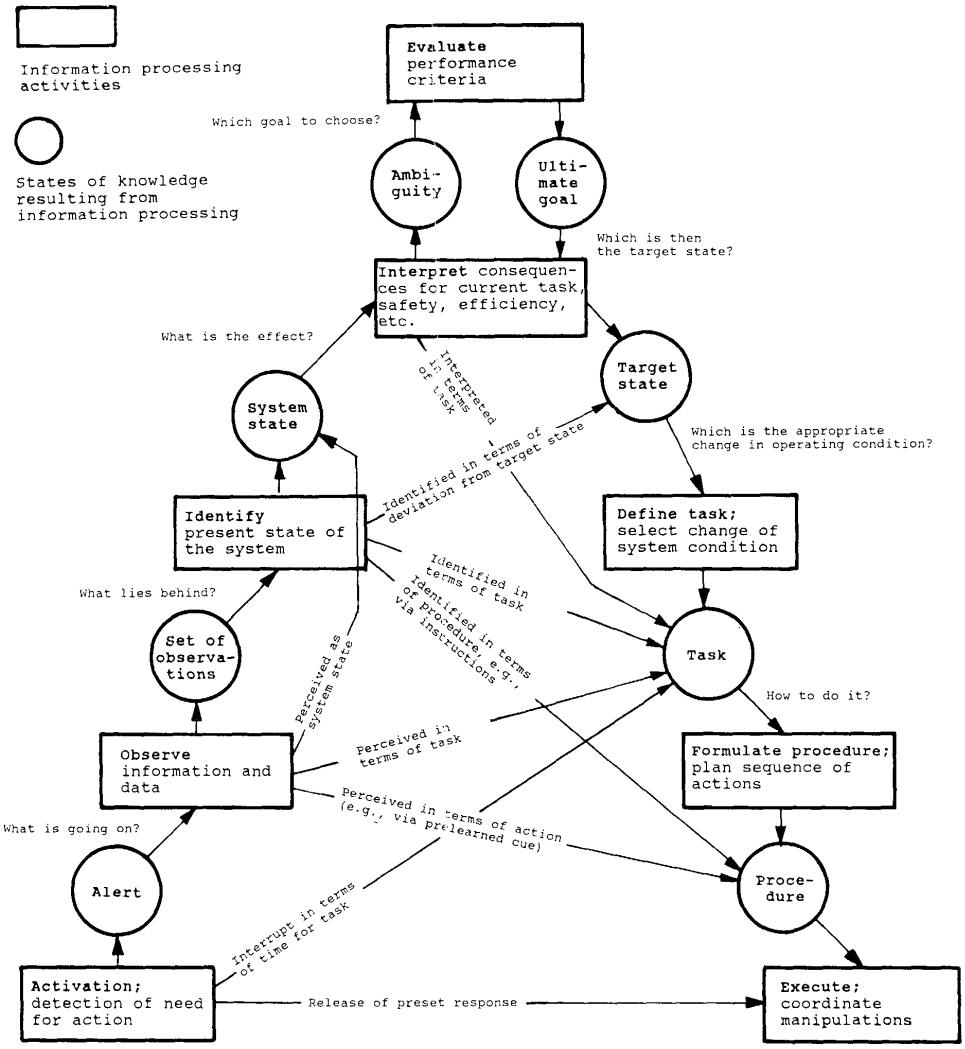

FIG. 1. Schematic map of the sequences of information processes involved in a control decision. Rational, causal reasoning connects the "states of knowledge" in the basic sequence. Stereotyped processes can by-pass intermediate stages. Adopted from Rasmussen, 1976; reprinted with permission from Plenum Press.

Decision making

Figure 1-taken from earlier work (Rasmussen, 1976)describes a framework which encompasses the various types of information processing sequences that characterize a decision maker's (dm = human or computer) activities in dealing with a problem. These include the completely rational approach where the (im "climbs up the ladder" on the left-hand side while *observing,* making an *identification* of state, *interpreting* the implications and *prioritizing goals.* Thereafter the dm "climbs down the ladder" on the right-hand side in connection with *planning and carrying out* the appropriate set of actions in order to achieve or reach the chosen *target* state.

The diagram indicates as well alternate paths from the initiation of a decision making activity to its conclusion. For example, in situations which seem to be familiar to the dm, shortcut paths can exist in the form of a large number of association rules-e.g. IF *xx, 130 yy.* It is these which form the basis for the

veteran or experienced dm's behaviour in dealing with the object system and often comprise the *expert knowledge* which is acquired for building current expert systems.

Thus while in the real world the rational type of decision making behaviour is probably mostly restricted to novices feeling their way, much can be said for forcing experienced users to resort more to this type of response through a suitably designed display and (controls interface. The reason for this is of course that the repertoire of quick and effective responses is not all-inclusive for every possible situation. Thus, in their interaction with the system, operators first have to be made to realize the inherent risk in a hasty response and *thereafter* be supported in more of a knowledge-based decision making sequence in order to solve their current problem,

Cooperative decision making

As stated earlier, decision making in supervisory control is a shared enterprise comprising the designer, the automatic computerized system and the staff of operators/users. Since the designer will not be able to foresee the necessary control responses for all possible disturbances, he needs a representative on site-the opei'ator(s)-who have to be able to take over in a competent way. The operators' supervisory control task is indeed in many respects a completion of the system design for the particular, perhaps infrequent, situation being dealt with. A,,, a consequence, the operator will need information about the problem space underlying the design and the designer will have to communicate this kind of information to the operator. This can take place through the system itself, i.e. by means of the information gathered, processed and stored in the computer-based instrumentation andlor directly through training, manuals and instructions. The cooperative decision making among operator, designer and computer will result in a complex communication depending **on** the extent to which the designer wants his representatives on site to take an active part.

Figures 2a and b illustrate how the basic framework of Fig. 1 can be replicated to reflect how a designer might intend two typical situations to be allocated among the partners. These are discussed in more detail later. At the same time, the diagrams indicate the various classes of communication among them. See also Rasmussen (1984a) and Sheridan (1982, 1986). An identification of such classes can be useful in deciding on appropriate information display support.

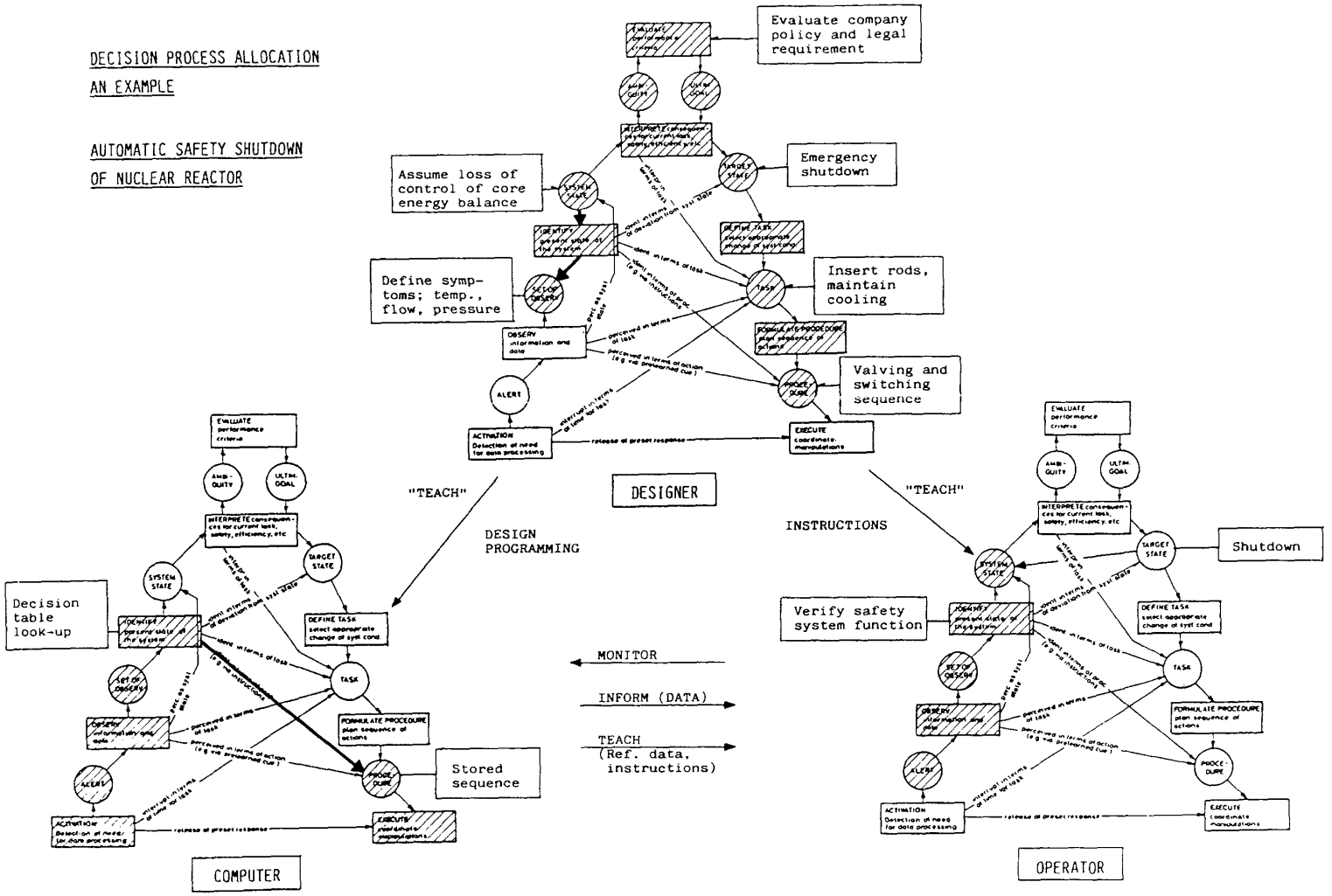

FIG. 2A. The designer, the operator, and the process computer are all parts of a control decision. The figure illustrates their roles (shown hatched) in an automatic safety shut-down, in which they act "in parallel"; each with a diagnositic task based on different strategies.

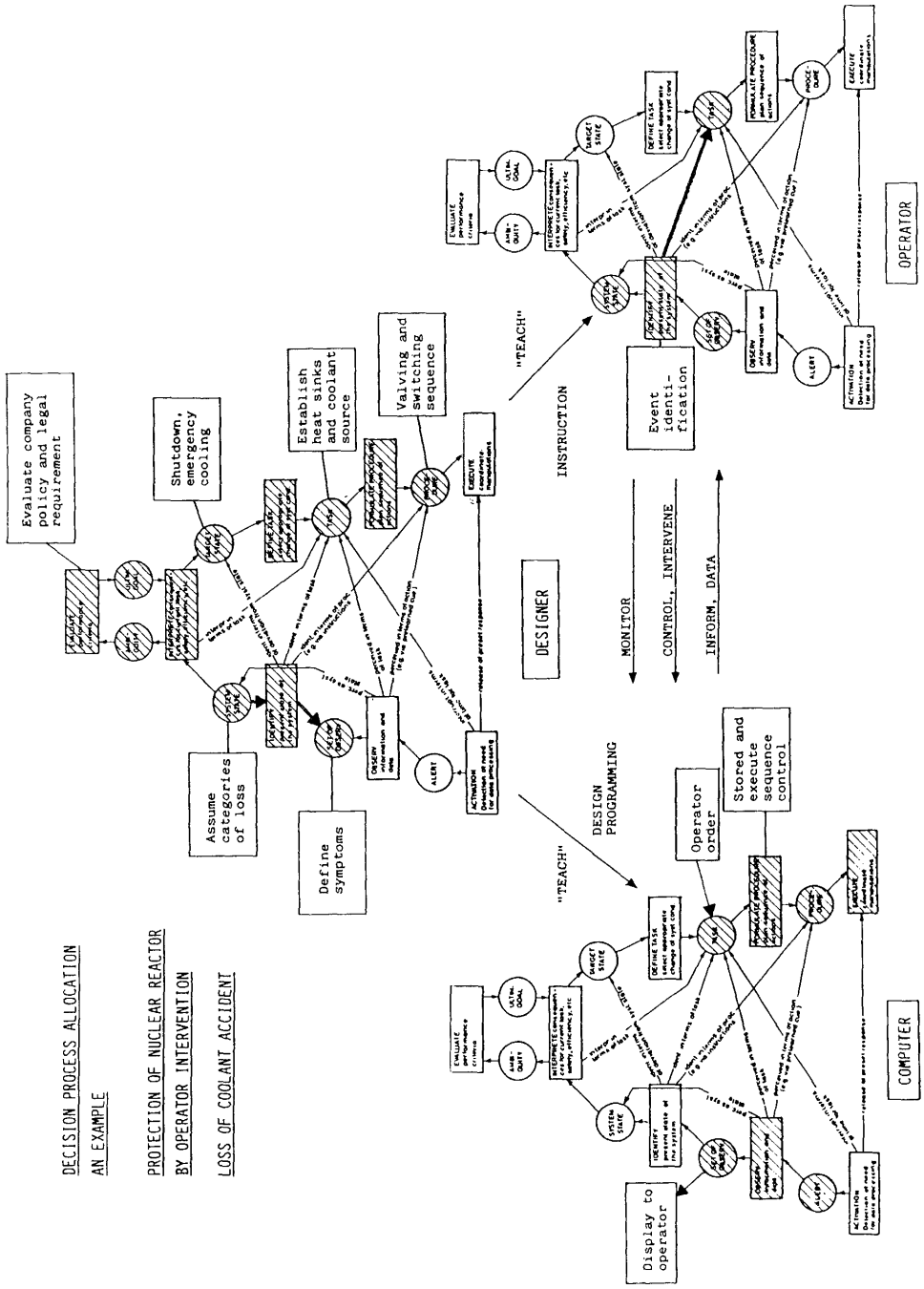

FIG. 2B. The figure illustrates the roles of the designer, the operator and a computer in a control decision which has not been fully automated, i.e. the operator and computer act "in series". The designer has automated a repertoire of protective sequences, but left the diagnosis to an operator. In addition to the decision functions, the designer, operator and computer support each other in different *inform/teach/learn functions*; see Sheridan (1982).

Hierarchical decision space

Another important consideration is the decision context, the representation of the problem space. Rasmussen (1984a) has dealt with this in detail in his description of the different levels of abstraction and decomposition which a human may use to cope with the complexity of a technical system, depending upon the situation and the phase of a decision task.

In the abstraction, or means-end, hierarchy (see Fig. 3), the low levels of abstraction are related to the available set of physical equipment which can be used to serve several different purposes. Models at higher levels of abstraction are closely related to specific purposes, each of which can be served by different physical arrangements. This hierarchy is therefore useful for a systematic representation of the many-to-many mappings in the purpose/function/equipment relationships which represent the context of-and are a necessary precondition for-supervisory decision making. When considering a control task at any level of the hierarchy, information about the proper function, target states, and answers to the question WHY, are obtained from the level above, while information about present limitations and available resources, i.e. answers to the question HOW, can be obtained from the level below (Rasmussen, 1984a).

In the present context, we are in particular interested in those human functions in man-machine systems which are related to corrections of the effects of faults and other disturbances. States can only be defined as disturbances or faults with reference to the planned or intended functions and purposes. Causes of improper functions depend on changes in the physical world. Thus they are propagating and are explainable-bottom-up in the hierarchy. In contrast, reasons for proper functions are derived top-down in the hierarchy; from the functional purpose. During plant operation, the task of the supervisory controller-man and/or machine-will be to ensure by means of proper actions on the system that the actual state of the system matches the target state specified from the intended mode of operation.

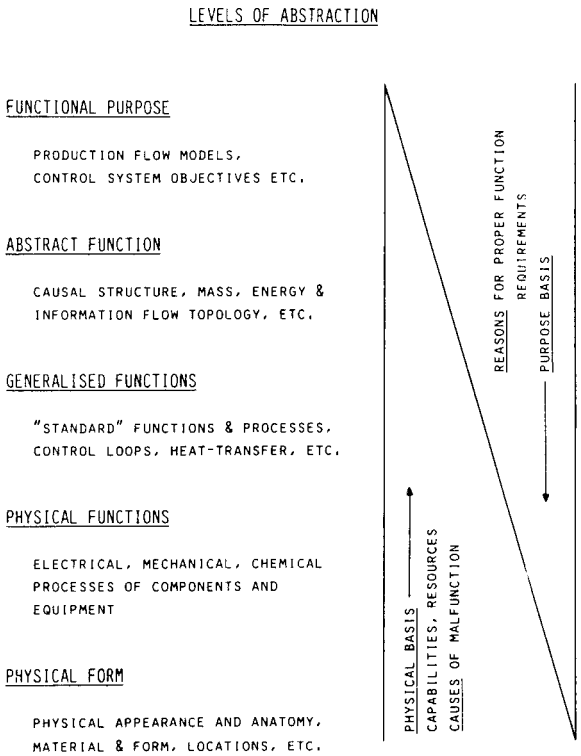

FIG. 3. The system properties considered in man–machine interaction can be described at various levels of abstraction, representing the physical implementation and functional purpose in varying degrees.

This task can be formulated at any level in the means-ends hierarchy. During plant start-up, for instance, the task moves bottom-up through the hierarchy. In order to have an orderly synthesis of the overall plant function during start-up, it is necessary to establish a number of autonomous functional units at one level before they can be connected to one function at the next higher level. This definition of functional units at several levels is

likewise important for establishing orderly separation of functional units for shut-down and for reconfiguration during periods of malfunction.

During emergencies and major disturbances, an important supervisory control decision is the selection of the level of abstraction at which to consider the control task. In general, highest priority will be related to the highest level of abstraction: first consider overall consequences for plant production and safety in order to judge whether the plant mode of operation should be :;witched to a safer state (e.g. stand-by or emergency shut-down). Next, consider whether the situation can be counteracted by reconfiguration of functions and physical resources. This is a judgement at a lower level representing functions and equipment. Finally, the root causes of the disturbance are sought to determine how it should be corrected. This involves the level of physical functioning of parts and components. Generally, this search for the physical disturbance is of lowest priority (not considering the role which knowledge about the physical cause may have for the understanding of the situation).

Thus, when a disturbance has been identified and the control task located at a certain level of abstraction, depending upon the perceived situation, the supervisory control task includes the determination of the target state derived top-down from the operation mode chosen, and an identification of the available functional resources and limits of capabilities, established bottom-up in the hierarchy.

All of this has serious implications for the design itself as well as the determination of the knowledge required by the operators. In practice, system design based on proven technology is largely an updating of previous designs with little specific attention being paid to a thorough task analysis and/or other special operator needs. However, a formal design and/or one based on new technology, such as advanced computer-based techniques, requires a continuous iteration between considerations of purposes, functions and equipment in the means-end hierarchy (Rasmussen and Lind, 1981)-also as the basis for defining the information to be made available to the operators to support their allocated supervisory roles.

Content of designer-operator communication

The content of information to be communicated to the operating staff during a particular abnormal situation depends on the role allocation chosen by the designer for himself, the operator and the computer. It depends as well on the extent to which he is able to foresee the situation and make a detailed analysis, the result of which he wants the operators to consider,

Before such complex examples of cooperative decision making are considered, it is relevant to discuss the information which is needed by the operating staff

if they have to cope with situations which have not been analysed by the designer. This is an important case, since this information will also be needed in other situations for which operating instructions are available, in order to understand the responses of the system to a degree which enables the operators to detect and respond intelligently to the effects of their own--often unforeseen--errors. Studies have shown that the information needed to control execution of pre-established procedures is typically not adequate for error detection and recovery (Rasmussen, 1984b).

The basic content of the information about the design basis which is necessary to enable operators to consider the whole supervisory decision sequence can be identified from the abstraction hierarchy.

An important basis for prediction of responses of the system to control inputs in supervisory control decisions is knowledge about functional relations at each of the levels in the hierarchy. This includes knowledge of plant anatomy and spatial arrangements at the lowest level of physical form. At the level of physical function, important information is the description of the functioning of equipment, for instance, in the form of pressure-flow-rpm charts for pumps, reactivitypower equations for nuclear reactor cores, etc. Possibilities at the level of more generic functions are phase plots for water-steam systems ("steam tables"), heat transfer characteristics of cooling circuits and control strategies for automatic controllers. More general characteristics in terms of power and inventory balances will be typical for more abstract functional requirements. Finally, at the level of functional purpose, the production requirements and the specifications of risk targets and limits for dangerous releases are given.

This kind of information, describing relationships within each level of the hierarchy, can be stated in rather neutral, or objective terms, and will in general be immediately accessible in engineering manuals and system descriptions. Such information as well as descriptions of the functional mapping upwards in the hierarchy is typically related to established and well documented methods for engineering analysis. This is not the case of information describing the downward mapping which, represents the design decisions, i.e. the reasons behind the chosen implementations. This information is typically implicitly found in company or engineering practices or is based on the designer's personal preferences and seldom finds its way to the operators. This may be crucial for control decisions when overruling of a design requirement, e.g. an interlock protection, has to be considered during critical situations. Traditionally, much effort is spent in presenting operators with analytical, bottom-up information about the system. Only little attention has been paid to the need for top-down, intentional information on reasons for the design. To give access to such information, *ad hoc* advice facilities are typically established in the form of technical supervisors on call and-in the nuclear indus-

try-"resident technical advisors" and "technical support centers". This kind of information should be directly available to the operating staff, probably in a kind of "expert system" computer-biased tutoring system.

The lack of information on reasons may not be a problem in systems of moderate size and risk levels. For these, only the rather frequent operational states have to be considered and the reasons for these will be immediately and empirically known to the operating staff, since their effects are frequently met. This is not the case for large systems where safety specifications also have to consider rare events. In such systems, reasons for infrequent yet important functions may be much more obscure to operators and special means may be required to make them understood. The information can be objectively stated, but it may be difficult to collect, once the design has been completed. It is a frequent experience for operating organizations that questions to system suppliers concerning their design bases are hard to have answered; typically, minutes from project meetings have to be retrieved since the man in possession of the knowledge has moved to another position. Information representing reasons for design choices, for production and safety policies in a company, will have the character of heuristic rules which are ver@,,ally stated, and an information base in the form of an "e)cpert system" and an "expert knowledge acquisition" program to collect such information may be a useful tool for alleviating these difficulties.

Communication of what could be called *neutral* information related only to the background for decision making-information which describes functional properties of the system and specifies the intended operating states without trying to guide the decisions of the operators--can be considered as relatively objective and there will in general be no role ambiguity between the communicating partners.

This is not the case when the system designer attempts directly to support the decision process of the operators. In high risk installations, designers will analyse large sets of abnormal events to judge the adequacy of the design and to preplan the necessary supervisory control actions. Some of these may be automated, some left to the operating staff as instructions, and the communication will no longer be the transmission of neutral objective facts to the operators. Communication is now between partners sharing the information processing tasks of the decision ladder, and communication modes may include the total range from neutral messages, to advice, recommendations, and instructions and perhaps to direct orders. The information will not only aim by its content towards a proper control action but also, implicitly via its form, towards allocation of authority and responsibility.

Different communication situations appear depending on the mode of cooperation chosen for the partners. Criteria for the role allocation may be related to reliability requirements, to the resources and conceptual model available to

support the processing by the different agents, or to the actual system state data accessible to them. Thus the designer can choose to automate certain protective functions and thereby take over one of the supervisory iub-goals; he can choose to preanalyse certain phases of the decision sequence through use of his analytical models and issue instructions to the operators; or, finally, a lack of data can lead him to transfer his conceptual tools to the operators in the form of facilities for interactive decision making. These modes of role allocation will be considered in more detail to formulate the communication requirements between designer and operator.

Allocation of different sub.-goals. For large industrial installations, there are some abnormal situations when necessary reaction times are so short or consequences so serious that control cannot be left to the care of humans. The designer then analyses a representative set of scenarios involving events for which a defining set of attributes, e.g. in terms of magnitude of measured variables, can be found, together with a reliable sequence of control actions, such as safety shut-down. This control sequence can be executed automatically, or operators (,an be ordered to follow emergency procedures strictly.

Formally, the designer and the operators will have to pursue different subgoals. See Fig. 2A. The designer takes on the task and responsibility to protect the plant by automatic protection, while the operators are typically given an early warning that automatic actions may come up, and are left with the supervisory control task of maintaining operation but within the envelope of the automatic protection. In this case, the designer and operators are cooperating by pursuing separate sub-goals, and responsibility as well as competence are clearly defined. The designer and the operator will be processing in separate decision ladders, and communication of data or results for each other's decision making will not be needed.

In most cases, however, the designer will not be completely confident about his automatic system, and operators will be instructed to monitor that safety actions are executed properly, and to intervene if this is not the case. They are here cooperating intimately with the designer in one single decision task, and will need the whole decision background including reasons for design of the protection system in order to judge properly when to override. (Mistaken overruling of automatic safety actions is one of the major prediction problems in safety assessments.)

In this way, a role allocation which formally and in principle is quite clear and only requires simple designer/operator communication will, at a closer look, require intimate cooperation in practice because the designer will not be confident that the results of his situation analysis which he has stored in the automatic system are reliable.

Allocation of different sub-tasks. See Fig. 2B. A similar situation is found when the designer finds that certain phases of the decision sequence demand conceptual models and processing resources which cannot be assumed to be available to operators during disturbed situations. A typical example is the planning of the reconfiguration of the plant to cope with major faults. The designer will then define a number of typical events, in terms of, for instance, small/large steam tube breaks, or small/large loss-of-coolant accidents. He will analyse the proper countermeasures and issue instructions labelled by the event categories. The diagnostic part of the decision will typically be left to the operating team due to the variability in symptom patterns.

In this case, the designer and operator will be cooperating by sharing a task and will, in turn, take care of different subroutines in the decision process. This switching will take place at the standard key nodes of the sequence and will imply exchange of intermediated results. Operators are in charge of the diagnostic subroutine, while goal priority and plans for action are retrieved from a data base supplied by the designer. The role allocation in this situation is far from clear. If operators are asked to follow the operating instructions strictly, i.e. they are interpreted as orders, the function will be unreliable in practice. Events are much more varied than the stereotype categories the designer can consider, and the resources available for countermeasures depend on maintenance schedules and errors during repair, etc. In effect, then, it should be realized that instruct' ions are to be considered as recommended practice which should only be used by operators as a basis for adaptation to the specifics of the occurrence.

Again, the designer and the operator will have to cooperate within one subroutine of the decision sequence and, in addition to communication of the result of the data processing, the operator will need information about the assumptions and preconditions of the designer's analysis, i.e. not only bottom-up causal data but also top-down specification of reasons, in order to have the necessary reference for judging the adequacy of the existing procedure and the acceptability of his modifications. To consider an operator only as an agent for executing the designer's preplanned actions will be unreliable. Instead, he should be considered to be the designer's representative on site, and the role allocation to consider is that of cooperative decision making.

At present, there seem to be *two* lines of development. One is a continuation of the traditional less resourcedemanding technology which stores the results of the designer's analysis in automated sequential control actions. After Three-Nlile-Island, for instance, there has been a tendency to advocate "symptom-based" procedures instead of "event-based". This means that the diagnostic sequence also has been analysed by the designer and the results stored in the system as a kind of "naturalist field guide" to carry the operators through the diagnosis in a purely rule-based fashion. Similarly, it has been

proposed to use the results of fault tree analyses from probabilistic risk assessments to develop an "alarm analysis" which offers advice to operators during disturbances from stored computer decision tables. Both of these approaches run the risk of giving trivial answers in frequent situations and wrong answers in rare events-and therefore can lead to a loss of operators' confidence.

A fundamental design principle ought to be that consistent on-line engineering analysis is used as far as possible, and that heuristics and hypothetical foresight are only applied to supplement such analysis or to guide the order in which analyses are performed.

The *other* line of development-and that advocated here-is to realize that the modern information technology gives the designer the facilities to place his conceptual models and processing resources at the service of operators, rather than to continue the efforts to make the preplanning of countermeasures more and more complete.

Thus what is advocated here is a kind of interactive decision making where designers and operators are mutually able to bring their own and their partner's advantages into play. The designer will transfer his conceptual models to the operator in terms of an explicitly represented abstraction hierarchy together with his processing models for integrating measured information to match the requirements at the different levels of the problem space. At the same time, the operator will be able to use up-to-date state information and his knowledge about ongoing maintenance work and all the accumulated experience with developing operating practice.

Interactive decision making

The design philosophy where the designer is trying to communicate his conceptual models and processing resources rather than his own analysis of the actual state will be discussed with reference to Fig. 4. The figure reflects the close relationship between the decision process modelled by the decision ladder and the means-end hierarchy. During diagnosis via the analytical leg, of the latter, the task is to identify the state of affairs at the functional level which enables judgements of the operational consequences. In the abstraction hierarchy, this corresponds to a bottom-up determination of the propagation of the disturbance and requires an integration of measured physical data into higher level states. When these actual states have been ' judged with reference to goals, planning of control actions is based on a top-down identification of the functions needed and of the available equipment. The *decision ladder* structures the process into standardized elements which define key nodes in terms of states of knowledge which are suited for communication and transfer of processing between partners. *Tle abstraction (means-ends) hi-*

erarchy is well suited to identify the knowledge needed for the information processing.

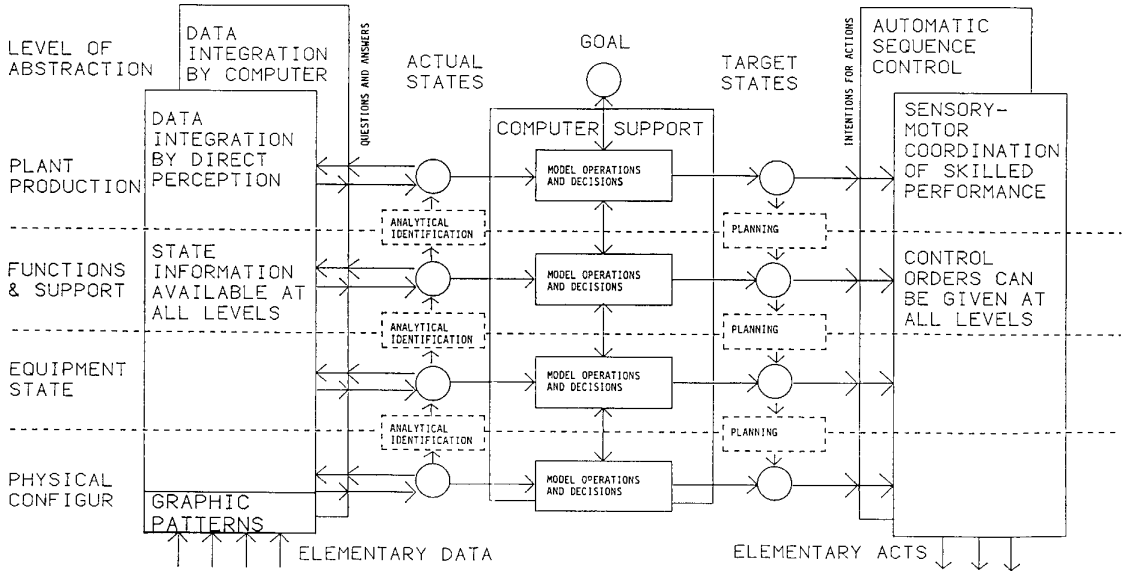

FIG. 4. Schematic representation of computer support for interactive decision making. The decision ladder of Fig. 1 is illustrating a decision sequence which is based on elementary observations. For interactive decision making where information is available directly at the relevant levels of abstraction, the lower stages are only occasionally used. This is illustrated by embedding the ladder in the abstraction hierarchy. Conscious decision making takes place directly at the relevant level which is interfaced to the environment by direct perception and sensori-motor skills and/or computer-based data integration and planning. In addition, computer support of the central decision process may be used. The analytical identification and planning between levels may be optional for cross checks by operators.

Figure 4 illustrates how the computer and the operators cooperate on the (upward) analytical diagnostic leg of the decision ladder as well as on the (downward) planning leg. The basic role allocation is that the operator and designer interact intimately during th(, different phases of the decision sequence. Instead of communicating results of analyses based on hypothetical data, the designer brings his conceptual tools into operation "on site" through the computer. The computer has the capacity and accuracy necessary to test consistency of sensor data, to check correspondence with component characteristics and basic physical relationships (e.g. "steam tables"), and to take account of mass and energy balances. In addition, analyses of the data collected during routine operations can be used for defining "normal states" of the various functional levels for the different operating regimes to serve as reference for locating disturbances in the functional topography. In this way, the computer will be able to interrelate actual states and target states up through the hierarchy. In fact, it thereby performs a diagnosis in terms of lo(@ation of disturbances in the functional topologies without being dependent upon the designer's foresight. The results can be displayed as neutral statements of relationships up through the hierarchy without recommendations of actions or priorities. It will be important to present results from such key nodes in the analysis and to select content and form of displays which

allow operators to make crosschecks with their own judgement, to relate to their empirical symptomatic data and to check hypotheses from such sources. The choice of priorities in goals will be left to operators depending on their perception of policies and available resources. In such a system, the mental load from data integration will be diminished but at the price of the extra task of retrieving ihe proper display or asking the proper question to the data base. Signals calling attention to the functional domain where changes have been identified by the computer (functional alarming, Goodstein, 1985) may be an efficient retrieval support instead of serving as an advice for action, as is the intention for traditional alarm systems.

Judgement of resources is included in the activities in the downward planning leg of the decision sequence. Again, the communication from the designer should be based on a consistent engineering analy@;is of intended functions and on tools for on-line analyses of the available physical resources rather than hypothetical analyses of abnormal states. Frequently, several physically possible solutions may be available, and the choice will be dependent upon economic or maintenance experience. For support of such prioritizing, an "expert system" structure may be useful for the operating staff for recording overall print experience. (Present "expert system" technology probably will be more reliable in a planning task for ranking choices than in the diagnostic task in process control.)

This means that the computer and operators will share the planning function. A basic prerequisite for planning will be information on the operational state and availability of equipment and functions, and computer support will depend on adequate access to actual configuration data, e.g. actual state of the valving and sw@.tching. If this is available, the designer will be able to arrange displays of the possible configurations of equipment for various functions with indications of availability considering the maintenance states-"success-paths" (Corcoran *et al.,* 1981; Long, 1984). Procedural support for establishing higher level functions from choice of a proper success path can be available from a stored library of instructions which will be labelled neutrally by functions, rather than by events. For many such functions, automatic sequence control (:an be incorporated if necessary with input of actual conditioning information based on maintenance states from operators. This leaves the operator free to express the selected target states at different levels of integration, depending on conditions see Fig. 4. Again, information from the computer is in neutral terms representing engineering Lnalysis of defined technical functions and not hypothetical situations.

Operator acceptance issues

It is important to realize that, in any given installation, the cooperation described here has to be carried out over extended periods of time and with shifting human partners. In addition, things are never static; ri,,k management decisions, regulatory edicts, market variations or even ordinary maintenance problems can introduce changes in (sub)goals, recommended /prescribed operating practises, etc.

A recognized issue in connection with the introduction (especially into an existing work situation) ol *new technology* (e.g. advanced decision aids) is the "user acceptance" problem which reflects the degree of (mis)match between the designers' intentions and expectations and the users' actual interpretation of and response to the demands made on them. Early studies by Mecherikoff and Mackie (1970) indicate the strong effect on acceptance of inadequacies in the innovational introduction process with respect to *design factors* (lack of regard for the actual operational environ*ment), cognitive factor*s (concerning the actual operational demands) and *training factors* (degree to which the users felt themselves to be competent).

The success of a cooperative effort between *people* is dependent upon a communication between them that is based on the following factors (e.g. Smith, 1979):

- *predictability,* in terms of a mutual understanding of likely goals and values + cultural and social background;
- *reliability,* underlying social and moral tenets which govern the mutual obligations between parties; *-responsibility,* a definition of each party's accountability (especially if something should go wrong);
- *role status,* the "instantiation" of the above factors in the actual working relationship;
- *confidentiality,* protection of own rights while (hopefully) respecting those of the others;
- *learning,* a continual learning of and adapting to the behaviour of the others.

There is considerable interest in the information flow between the interacting parties in the supervisory control context, i.e. between the operators and the designers' computer intermediary and, in particular, how to reproduce an environment embodying the important I'actors for good human-human communication listed abov,-, again in the interests of promoting operator acceptance of the designers' "knowledgeable artifact".

A sensitive issue pertains to the "pet,-r" relationship between the two parties and, in particular, how advice or even criticism from the intermediary will be received by the operators. Not much consideration seems to have been given to the effect of similar messages sent the other way. However, use of a different classification of information transfer might relieve the situation. As indicated previously, much of what the intermediary sends to the operator can be labelled as *objective/neutral* since it is based on actual top-down or bottom-up derived information about the plant which is validated and checked for consistency by the computer whenever possible before being formatted into suitable information displays.

Alternate identifiers for the information transfer types are available which intuitively seem to provide the potential for a more positive reception by the operators if properly included in their introduction to and training on the system. For example, Sheridan (1982, 1986) uses terms such as PLAN, TEACH, MONITOR, INTERVENE and LEARN. In our context, EXPLAIN and QUERY would also seem to be relevant. In particular, the intermediary's ability to explain its own "deliberations" and "interventions" and "justify" its conclusions is a critical item.

When discussing communication between Human operators and a computer intermediary in the context of supervisory control of industrial processes with a significant risk potential, it should be evident that a key word must be *error-tolerant* (Rasmussen, 1985a, b). This of course is true for other complex systems-administrative, banking, transport. Acceptability will be enhanced because, when carried out in practise, an error-tolerant design will/should define for the operators the scope and bounds of their responsibility. At the extreme, the designer (through his intermediary) could manage operational safety while the operators could function under this umbrella and optimize production.

Conclusion

The approach to computer support of supervisory decision making advocated in this paper -is to consider operators as being capable of taking on the authority and responsibility for the decisions required. Rather than continue a development where designers attempt to preanalyse all abnormal situations and to store their advice in computers, they should instead try to make available to operators their conceptual tools and use the capacity of computers to perform on-line analyses of the available measured data. Supervisory control should be based as far as possible on consistent engineering analysis. Heuristics and hypothetical foresight should be used to supplement such analyses and to guide the priority of choice and not to replace on-site engineering

analyses. However, real life is not black or white; the real systems will have to combine all the approaches.

When an information system contains a mixture of factual information, heuristics and advice based on other people's foresight, credibility may be a problem. For the design of decision support systems, design criteria are necessary for enhancing users' acceptance of advice and establishing the preconditions for user-understanding of explanations and justifications. A basis is needed for establishing and maintaining cooperative attitudes towards a computer intermediary.

References

Corcoran, W. R., J. F. Church, N. J. Porter, M. T. Cross and W. Guinn (1981). The critical safety functions and plant operation. *Nuclear Technology, 55,* 690-712.

Goldstein, L. P. (1985). Fun(@tional alarming and information retrieval. Riso-M-2511.

Long, A. (1984). Computerized operator decision aids. *Nuclear Safety,* **25,** 512-524.

Mecherikoff, M. and R. R. Mackie (1970). Attitudinal factors in the acceptance of innovations in the navy. AD 874789.

Rasmussen, J. (1976). Outlines of a hybrid model of the process plant operator. In Sheridan, T. and G. Johannsen *(Eds), Monitoring Behaviour and Supervisory Control.* Plenum, New York.

Rasmussen, **J.** (1984a). Strategies for state identification and diagnosis. In Rouse, W. B. (Ed.), *Advances in Man-Machine Systems Research, Vol.* 1. J.A.I. Press, Greenwich.

Rasmussen, **J.** (1984b). Human error data. Facts or fiction? *Proc. 4th Nordic Accident Seminar.* VVT. Symp. 55, ESPOO 1985, Finland. Also Ris-M-2499.

Rasmussen, J. (1985a). 'Me role of hierarchical knowledge representation in decision making and system management. *IEEE Transactions on Systems, Man, and Cybernetics,* SMC-15, 234-243.

Rasmussen, J. (1985b). Risk and information processing. Riso-M-2518.

Rasmussen, J. and M. Lind (1981). Coping with complexity. Riso-M-2293.

Sheridan, T. B. (1982). Supervisory control: problems, theory and experiment for application to human-computer interaction in undersea remote systems. *Dept. Mech. Eng. M.L T Tech. Rep.,* March 1982.

Sheridan, T. B. (1986). Supervi@.,ory control. In Salvendy, G. *(Ed.), Handbook of Human FactorslErgonomics.* Wiley, New York.

Smith, H. (1979). A view of people-oriented systems. SIGSOC Bull. 11, 3-4.