Representation of Process State, Structure and Control

Goodstein, L.P.; Rasmussen, Jens

Publication date:
1987

Document Version
Publisher's PDF, also known as Version of record

RISØ

Risø-M-2645

Representation of Process State Structure and Control

L. P. Goodstein and J. Rasmussen

Risø National Laboratory, DK-4000 Roskilde, Denmark
April 1987

RISØ-M-2645

REPRESENTATION OF PROCESS STATE, STRUCTURE AND CONTROL

L.P. Goodstein and J. Rasmussen

Abstract. Supervisory control is essentially a decision-making activity where, among other things, the dm has to maneuver within a complex problem space which reflects key dimensions and attributes of the object system (power plant ...). Of considerable importance therefore is the representation for the dm of this problem space comprising at the one end the target demands, goals, constraints and, at the other, the resources available for meeting the assigned goals - and all of this in pace with the dynamic event-driven environment which characterizes the types of systems of interest.

Previous work has identified the advantages of utilizing the two-dimensional means-ends/part-whole space as a basic ingredient in a system representation. This paper associates more detailed representational requirements at the various levels of the means-ends axis with the activities of state identification and diagnosis. In addition, some examples of display formats which attempt to incorporate the outlined representational principles within the context of a PWR plant are discussed.

April 1987
Risø National Laboratory, DK-4000 Roskilde, Denmark

ISBN 87-550-1320-1
ISSN 0418-6435

Grafisk Service Risø 1987

TABLE OF CONTENTS

INTRODUCTION

Supervisory control can be briefly defined as a decision-making activity concerned with the allocation of resources in a complex many-to-many mapping context characterized in the following way (Lind 1982):

- plant and/or subsystem goals may be multiple and partially conflicting (for example, when considering safety vs. production).

- a plant function can have several alternative physical implementations.

- conversely, a component or subsystem can be used to implement one or more functions and thus contribute to the achieving of one or more goal.

- the functional structure is dependent on the current operating mode.

The situation is complicated by the fact that the plant systems often are highly automated. This is equivalent to saying that there is more than one decision-maker; indeed there could be said to be three - the designer in the form of stored and/or trained rules, decision tables, algorithms, specifications, regulations, the automatic control system and the operating staff.

The automatic system is usually in control during normal daily operations as well as in pre-determined non-normal situations where specified sets of cues (plant data) will lead automatically to specified control actions on the plant which change its physical configuration and hence its functional structure. The criteria for automating vary; economic factors, critical time problems and/or a certain satisfaction derived from replacing the human. In this way, the decision-making problems left for the operating staff can become fragmented but remain nevertheless vital since they relate often to the "leftover" tasks of

coping with unforeseen situations as well as monitoring the automatic control system's performance.

The advent of advanced information technology and, in our view (Rasmussen and Goodstein 1985), the corresponding need for a more systematic approach to implementing the three-way cooperation mentioned above has led to proposals for a more formal and systematic approach to designing and evaluating the operators'/users' work situation - i.e., in the form of a cognitive task analysis (see Rasmussen 1985 & 1986a).

Fig. 1 gives a summarized view of such an analysis as a multilevel mapping process originating with target system demands which give rise to a corresponding set of control tasks. These in turn involve decision making activities which require access to appropriate information. Allocation policies define the allocation of functions among parties while knowledge about information processing strategies and behavioral modes gives a basis for the design of suitable information displays and communication between parties. Thus the analysis leads to a definition and distribution of the functions among the three partners as well as the structure and form of the interaction among them through the system interface.

This paper will deal with the problem of representation of the problem space comprising at the one end the target demands, goals, constraints and, at the other, the resources available for meeting the assigned goals in the dynamic event-driven environment which characterizes a typical process plant.

DECISION MAKING IN THE MEANS-ENDS/PART-WHOLE PROBLEM SPACE

A primary component in mapping between the specified work requirements arising from the object system (e.g. power plant) and the user/operator's ability/resources for coping with the related cognitive tasks is a suitable representation of the problem space defined by the object system.

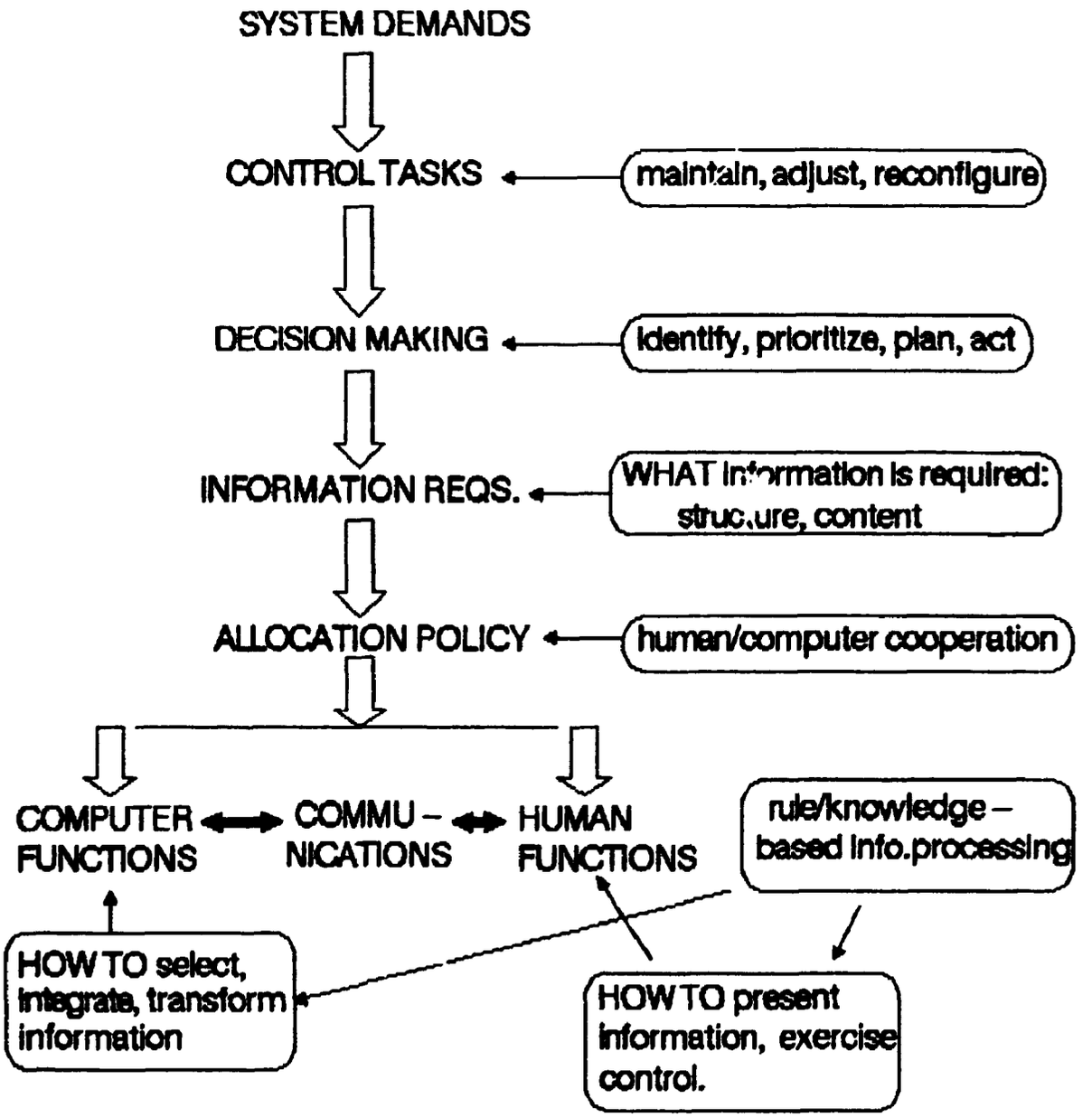


Fig. 1. Overview of the cognitive task analysis.

Previous work (Rasmussen & Lind 1981, Rasmussen 1986b) has described the advantages derived from - indeed the necessity for - utilizing a two-dimensional means-ends/part-whole space within which a decision-making activity can take place. Fig. 2 illustrates the various levels of the means-ends dimension in connection with a technical system. These levels require a variety of representations and relations which become useful in a problem solving situation and thus they will be utilized in connection with the following discussion. Fig. 3 gives examples of corresponding supervisory tasks at the various levels.

The decision ladder (Fig. 4) (Rasmussen 1976) indicates the main activities connected with decision-making - all of which need informational support. Left branch traversal, consisting of activation, observation and identification, is aimed at establishing "where we are now; what is going on; what could result". Coming up over the top of the ladder involves judgement, prioritization, selection among alternative targets. Right branch traversal includes elements of synthesis in order to plan and carry out the control tasks, using the assigned resources, to correct the immediate situation - a situation which could be routine, unique, unexpected, dangerous, etc.

Thus issues regarding complexity come to life while traversing the ladder; identification of current state and potential consequences, choice of immediate goals, maintaining of critical functions to satisfy these goals, allocation of equipment and materials without deleterious side effects and within the necessary time scale and so forth. Reported problems in the control room reflect operator difficulties in carrying out these tasks (see e.g., Woods et al (1986)).

With regard to **state identification**, in a cooperative decision making system, the computer and the operator each will participate in attempting to continuously identify the state of the plant and ensure that the immediate goals are being satisfied. Since there is an underlying circularity in the iteration of goal->desired state->actual state->goal, steps have to be taken to break this loop in some way.

CONTENT OF MEANS-END REPRESENTATION OF TECHNICAL SYSTEMS

MEANS-END LEVELS	PROPERTIES OF THE SYSTEM SELECTED FOR REPRESENTATION
PURPOSE CONSTRAINTS	Properties necessary and sufficient for relating the performance of the system with the reasons for design, with requirements of environment. Categorization in terms referring to properties of the environment.
ABSTRACT FUNCTION	Properties necessary and sufficient to establish relationships according to design or intention: energy, value, information, truth, etc. Relationship to underlying causal structure and function is depending on convention and design choice. Categorization in abstract terms, referring neither to system nor to the environment.
GENERALIZED FUNCTION	Properties necessary and sufficient to establish "black box" input-output models of functions irrespective of underlying implementation; this level is necessary for coordination of different physical processes to serve joint higher level purpose. Categorization according to recurrent, familiar input-out-put relationships.
PHYSICAL FUNCTION	Properties necessary and sufficient for use of object: for adjustment of object for use, to adjust to limits of use, to predict whether objects will serve particular use to select part to move for control of physical process. Categorization according to underlying physical process.
PHYSICAL FORM	Properties necessary and sufficient for classification and recognition of material objects;

Fig. 2. The content of representations at the various levels of the means-ends hierarchy.

TYPICAL TASKS IN SUPERVISORY PROCESS CONTROL

MEANS-ENDS LEVELS	WHOLE-PART DECOMPOSITION	
	(FUNCTIONAL DECOMPOSITION AT EACH LEVEL INDEPENDENTLY)	
GOALS AND VALUES CONSTRAINTS	PLANT MANAGEMENT:	Maximize Capacity Factor, Maintain Plant availability, Prevent Contamination of Environment, Control Safety and Work Conditions of Employees
FLOW, DISTRIBUTION, AND ACCUMULATION OF MATERIAL, ENERGY, MONETARY VALUES, AND MANPOWER	PLANT CONTROL:	Control Major Flows of Energy and Mass between Sources and Drains. Monitor States of Major Balances Monitor Communication Between Groups and Teams in Plant, Maintenance, Roving Operators, etc.
GENERAL FUNCTIONS AND ACTIVITIES	SYSTEM MANAGEMENT:	Control Reactor Flux, Maintain Core Cooling, Control Pressurizer Level, Maintain Feedwater Flow
SPECIFIC WORK PROCESSES. PHYSICAL PROCESSES OF EQUIPMENT	EQUIPMENT OPERATION:	Start Feedwater Pumps, Check Bearing Temperature, Switch to Stand-by Power Supply
APPEARENCE, LOCATION, AND CONFIGURATION OF MATERIAL RESOURCES	NAVIGATION AND IDENTIFICATION:	Identify Valve 337 for Maintenance Technician Follow Vendor Technician to Emergency Diesel B

The problem space in supervisory process control of the previous figure is here used for illustration of typical control tasks at the various levels. It will be noted that change in level of abstraction and decomposition are rather tightly coupled. Also note, that the tasks are all performed by the same (collective) decision maker, the control room operator(s).

Fig. 3. Typical tasks in supervisory process control.

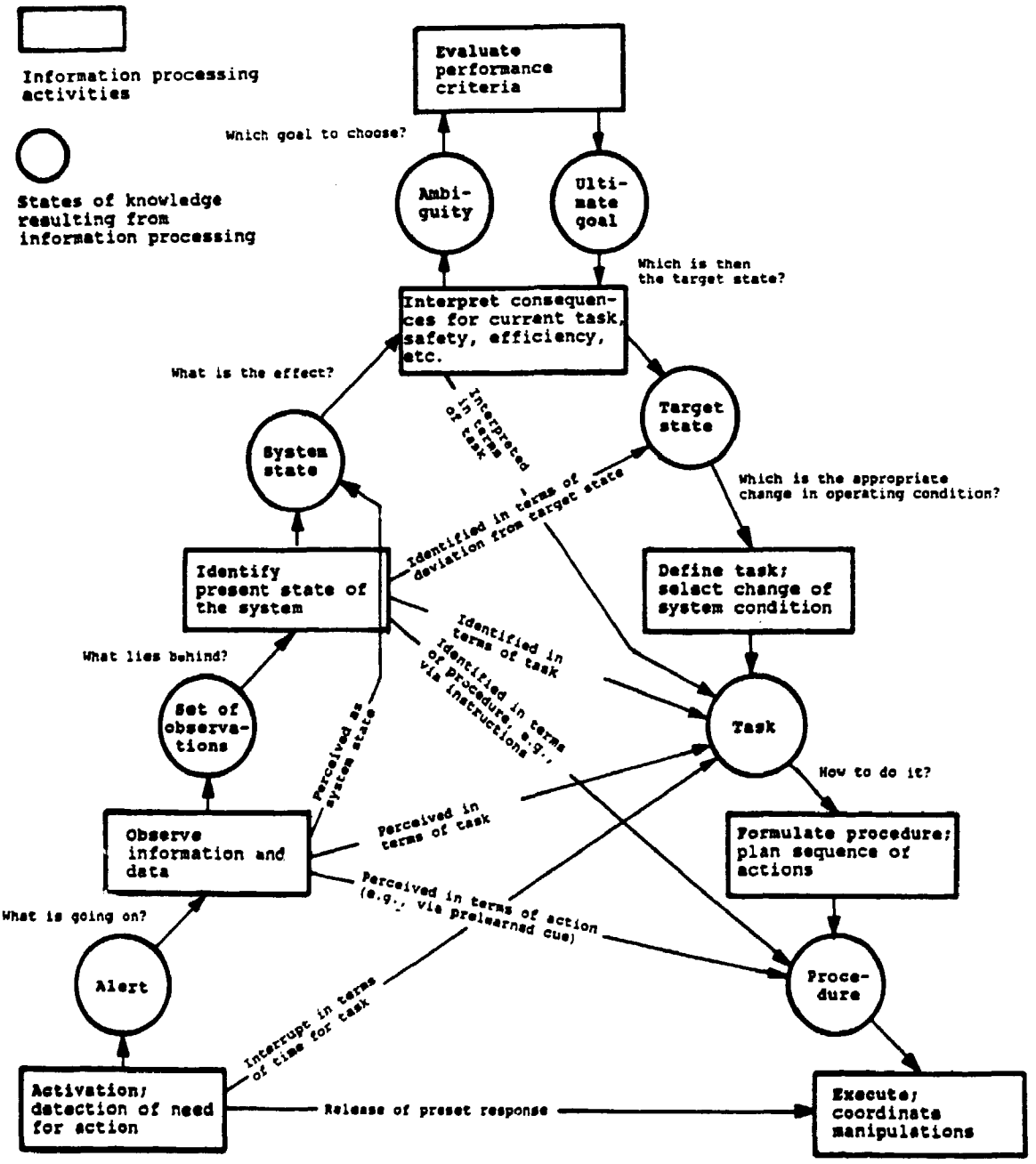


Fig. 4. Decision ladder.

State identification is the first critical step in the decision process and it can take place at one or several levels of the means-ends hierarchy. Generally speaking, to avoid circularity, state identification follows a "narrowing-in" process where, after an initial coarse classification, the critical state is found through an increasingly focussed attention which, at the same time, implies a top-down movement along the means-ends axis in the problem space.

At each level of the means-ends hierarchy, the functional representation of the process plant will form a causal network in which the type and connection of the individual elements depend on the level of whole/part decomposition chosen. Since the operators' diagnosis in the control room is not usually directed toward the identification of root cause but rather at the identification of appropriate corrective control measures, state identification will be more concerned with a characterization of the state of the elements with reference to acceptable limits - both with regard to the goals set by the next higher level in the hierarchy and the means for implementation reflected in the next lower level.

Decision making about state identification and planning therefore involves iterative considerations of representations of the plant at three consecutive levels along the means-ends axis.

The WHAT TO CONTROL Level

This is a representation of the plant in terms of interacting elements in a causal net which can be selected for control. While this control normally should be exerted on the element encompassing the root cause (e.g. faulty component), other control choices often may have to precede/replace this particular correction because of time constraints, high risk of damage, easier control, etc.

Information at this level should include a functional overview of the plant. The decomposition will depend on the phase in the decision task and can encompass the complete plant or some particular subsystem. The overview should make it possible to

judge the causal interaction among functional elements. This will require a uniform and compatible description. In addition, in order to plan actions, the overview should be structured in terms of elements which can be "utilized", "activated" or "manipulated" in order to produce corrections by means of suitable control actions. Consequently, the elements should be defined in a reasonably "uncoupled" sense as viewed from a control standpoint and appropriate links to control actions should be available.

Thus this implies that the WHAT TO CONTROL overview should utilize the representation and concepts which link directly to the next lower HOW TO CONTROL level. That this probably will tend to enhance the cognitive momentum aspects of the displayed information (Woods 1984) is an inherent advantage.

As an example, consider the possibilities for changing the representation top down through the means-ends hierarchy. Since all major accidents with resulting damages are related to disturbed energy balances, a flow topographic overview at the abstract level should be structured in terms of the major mass and energy balances in the system but represented with respect to related general functions such as heat transfer, cooling, supply of power, etc.

At the next lower level, a representation of the state of the general functions should be in terms of the basic physical processes of the subsystems involved. These, in turn, are described in terms of the major components.

Thus, at each level, the elements used for decomposition will be defined in terms of the concepts commonly used for describing the next lower level in order to aid in the choice of resources for dealing with a fault. In addition, these elements are those for which state information should be available - at the WHAT level in terms of actual state and at the HOW level in terms of possible state to assist in the selection of control means.

Fig. 5 summarizes in diagrammatic form these shifts in the form of the representation at the various levels along the means-ends axis.

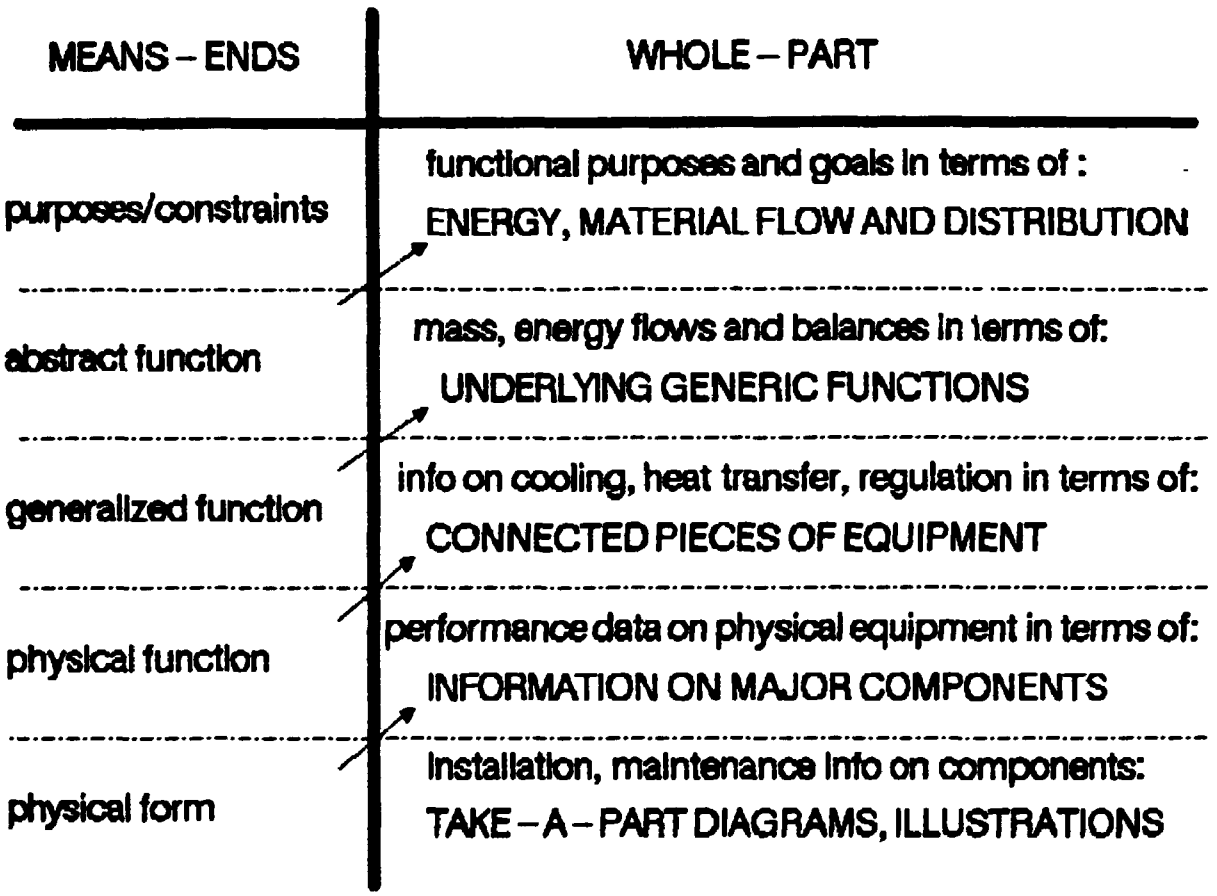


Fig. 5. Representational forms within the means-ends hierarchy.

The HOW TO CONTROL Level

Information at this next lower level has to support the planning of control actions. Therefore information on the internal structure of the elements used to represent the WHAT level is required. Thus the concepts used to describe the various elements may be different. This follows from the fact that the roles of these elements at the higher WHAT level will be different - i.e. supply energy or material, maintain a process parameter at a given critical value, etc. In addition, the well-served principle of diversity in safety-related design will result in various alternate resources being available to satisfy a higher level requirement. These may be based on different process types (e.g. a power supply can be the normal grid, a battery or a diesel generator) and consequently different representations will be necessary.

The WHY Level

The priority judgements and goal evaluations which determine the choice of focus for the selection of control actions depend on information at the WHY level. This level supplies information on the requirements regarding the causal structure and state of the WHAT level with regard to current limits of acceptable operation, consequences of disturbances, operating constraints, etc.

Fig. 6 attempts to illustrate that, dependent on the situation, e.g., the degree of diagnostic narrowing-in, WHY, WHAT and HOW queries can arise at different levels along the means-ends dimension. At the lowest levels, of course, the queries might well come from a maintenance or test technician.

To summarize, differences among the three levels are:

- at the WHY level, state identification should be referred to specified or intended states and information should be

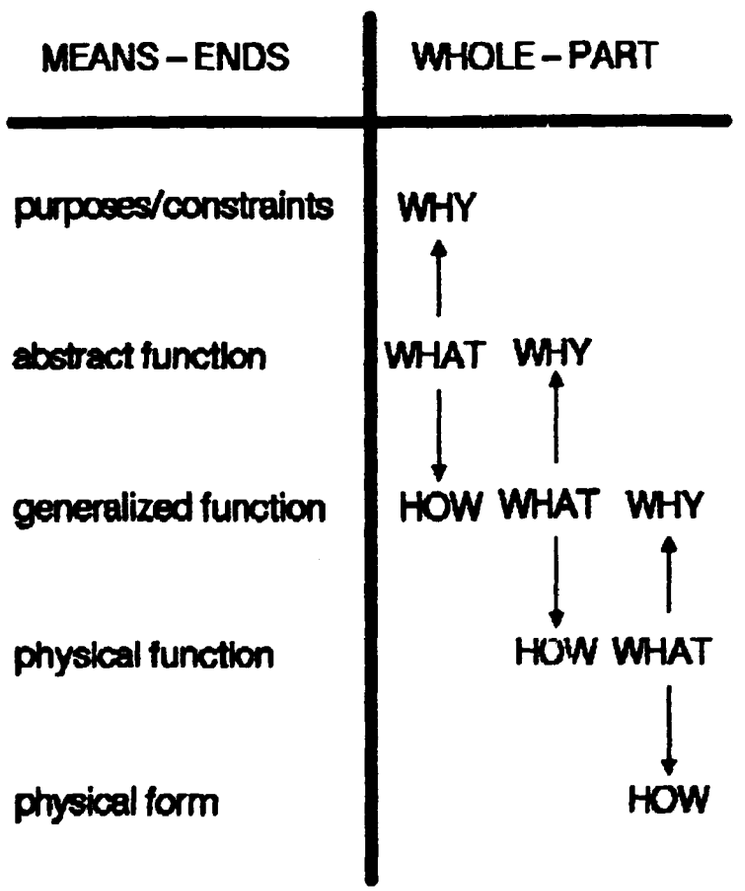


Fig. 6. The three-level interaction.

available for priority judgements (production vs. safety) in case of discrepancies.

- at the WHAT level, state identification should be in terms of actual current state with relations to the interaction of elements which are suitable as control objects.

- at the HOW level, state identification should refer to possible states in terms of margins to limits of capacity, availability for service (potential "success paths" using the terminology of Corcoran et al (1981)) and means for control.

STATE IDENTIFICATION AND RESPONSE

As stated above, the means-ends whole-part space will form the backdrop for decision making - especially when dealing with disturbed operating conditions. In unfamiliar situations, a functional reasoning within the problem space which is based on a conceptual model of the plant and its properties is called for. This should result in an identification of state/cause/response - i.e., a kind of "on-line" diagnosis and planning operation takes place corresponding to what has been called knowledge-based behavior.

Actually more of a rule-based identification will be used in a very large category of situations as the first choice for coping with frequent familiar events as well as when screening for high risk possibilities. Based on the designer's pre-planning and/or the operators' experience, this type of state identification will depend on a heuristic search for a match between the available observations of plant state and the attributes of the members of a task repertoire - i.e., circularity is avoided by direct jumps from identification to action.

As stated in Rasmussen (1986b), the displays of state at the various levels should enable "labels" to be given to operational

situations which in a way "prime" or initialize the operators with regard to their intuitive feel and expectations. It is therefore of primary importance that the displays support a proper adaptation or "focus" on the really relevant features of the situation.

A guiding principle should be that the underlying concepts used for describing and representing the decomposition at a given level should be determined/influenced by the names and labels used by the operating staff themselves. This will assist them in structuring the rule set they acquire with experience. It is important that the rule-based diagnoses on which automatic control actions and communications to the staff are based is compatible with the general professional language employed in the control room so as to promote confidence and trust - even though the underlying automatic data processing is based on different concepts.

APPLICATION TO A NUCLEAR POWER PLANT

Fig. 7 describes an underlying structure for a technical system which directly maps into the various levels along the means-ends axis. Thus the top section (A) expresses in technology-independent terms the purpose and related critical goals of a power plant which relate to production and safety. The lower main part of the figure expands this framework for a given technology (nuclear) and also illustrates the many-to-many mappings which characterize the systems's complexity.

It can be useful to discuss display requirements in terms of certain of the levels along the means-ends axis. In addition, some examples of possible display formats aimed at satisfying the requirements discussed regarding representation will be given to illustrate the ideas.

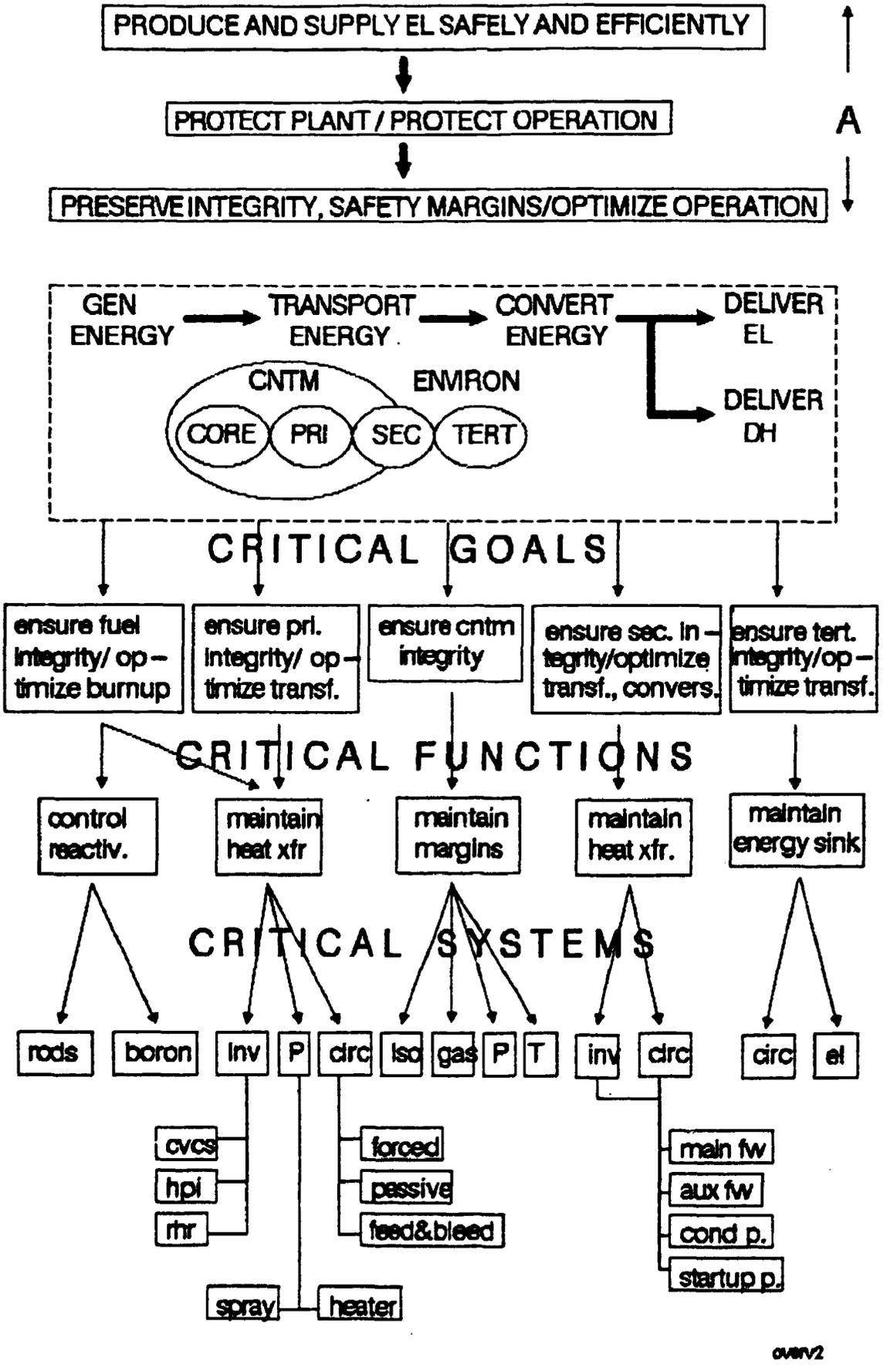


Fig. 7. Multi-level description of a technical system.

Level of Functional Purpose

For the power plant, the decision making at this level has to do with long-range planning regarding plant operations, meeting daily production goals, economic optimizing, coordination with net control, meeting redistribution requirements during transients and major disturbances, observing emission and other conditions with reference to environmental regulations and statutes.

The control task will be to monitor current operation with respect to current goals and to anticipate the need for future changes by transmitting revised requirements downwards in the means-ends hierarchy when limitations within the present control regime are approached. Heuristics will have been developed for guiding decisions relating changes in operational constraints to utilization of plant resources for the frequently encountered situations.

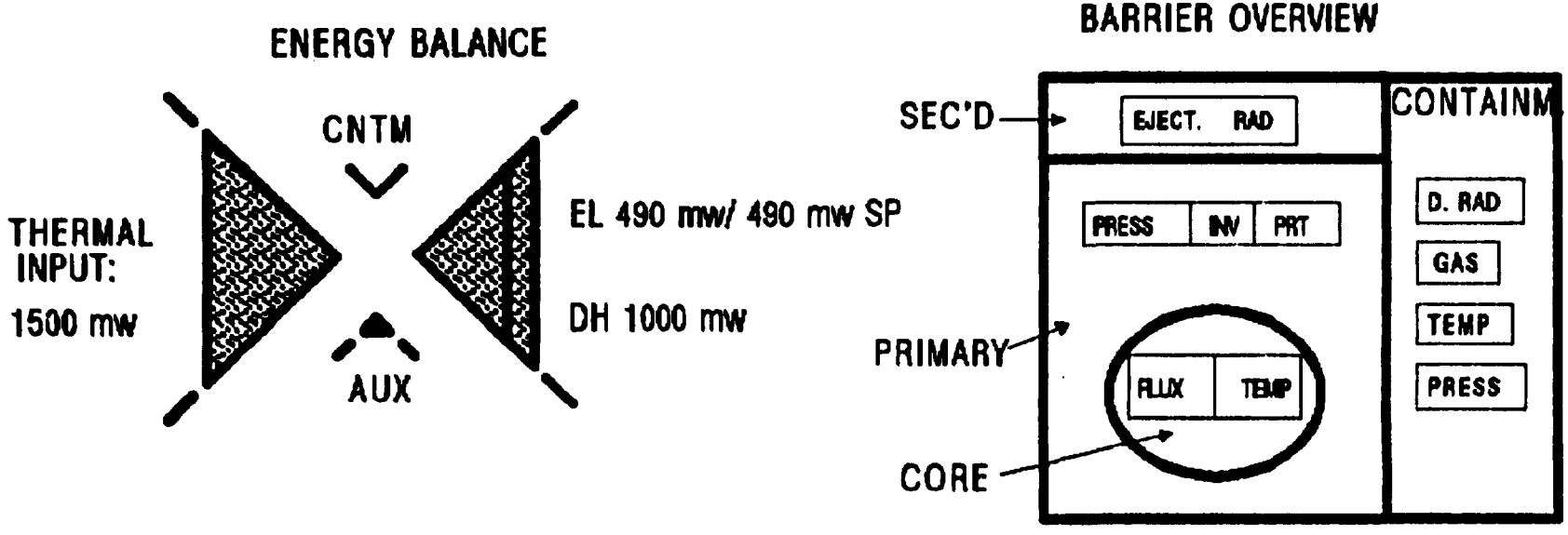
We will follow the ideas expressed previously about structuring the information at one level with reference to the representation describing the next lower level. Thus it is appropriate - for the power plant - to indicate information about functional goals and purpose in terms of energy flow and distribution - these being the primary descriptors at the next lower abstract functional level.

To these production (or availability) data must be added appropriate overviews of safety-related issues - primarily the status of the various barriers to the release of radioactive materials including information on the "nearness to a violation" compared with reference specifications.

Environmental information should also be included as well as messages indicating special conditions in the plant which may restrict the degrees of freedom available for continued operation.

Fig. 8 illustrates a display aimed at fulfilling the above requirements. Thus the production goal state is reflected in

25.JAN.1982 09:24



OPERATING MODE: 100% LOAD

EFFICIENCY: XX%

LOAD FORECAST: RATED BASE LOAD NEXT 12 HRS.

STACK CONDITIONS: XXX

WEATHER FORECAST: THUNDERSHOWERS

WIND SSW 40 M/S

TEMPERATURE: XX

SPECIAL ATTENTION: SAFETY SYSTEM TESTING FROM 8-14 HRS.

overv1 20.2.87

Fig. 8. Overview of production and safety.

the shape of an energy balance icon together with relevant information on current operational state and production. Safety goals have been transposed to a barrier (non-flow) diagram indicating the various lines of defence with appropriate indicators which are sensitive to barrier defects and leaks. The location of barrier breaks can also be shown pictorially. In addition, environmental conditions, radiation levels, load forecasts, notices/reminders about special conditions have been included. The last-named may affect the degrees of freedom available for plant operation and, although not included here, a linking of actual vs prescribed plant state to relevant technical specifications might be feasible (see, e.g. Dworzak, Nedelik and Van Gemst (1982)).

Level of Abstract Function

At this level, interest is in representing the functional structure and state of the current plant configuration in terms which are independent of the specific means for implementation, environmental conditions, etc. Hence there is a need for an high level abstract representation suitable for monitoring and control of a purely functional configuration - the basic causal structure - which is the prerequisite for overall system operation. For the type of plant currently under discussion, a description in terms of a flow topology describing mass, energy and information and having an underlying structure governed by the utilized technology (nuclear, gas, wind ... for power plants) seems to be appropriate.

This level is important because the major risks of the system will be related to disturbances in the major energy and mass balances. There will be no major accident without a release of energy and/or material accumulations. Therefore the diagnostic task should begin here through an identification of the disturbed mass and energy flows. A major balance can often be restored by control actions in several intersecting flow structures. The choice will depend on the consequences predicted, the controllability and time constants of the flow structures involved and the availability of standby resources - i.e., a simultaneous consideration of the plant at three levels

of abstraction. Thus the situation requires an overview of the total situation with respect to normal and acceptable states as well as means for judging the consequences of the disturbance upwards, both in magnitude and time. On the other hand, the flow structure to choose for control actions depends on the accessible means for control, possible cross couplings to other structures and the time constants of response.

For working directly at this level, therefore, it is important to have information presented on the actual operational status of the individual flow structures. This requires therefore the transformation of all relevant "raw" data into indicators of flow magnitudes and accumulated levels in sufficient detail so that the usually very tightly coupled energy flows and energy-bearing mass flows can be separated.

Overview maps representing the major mass and energy flow paths with, for example, an analog representation of flow magnitudes including a reference to normal or specified flow will give an immediate visual identification of the degree of deviation in each flow structure and thereby support priority judgements. Direct visual references to the corresponding conditioning functions will be useful to guide the downwards search for control possibilities. An immediate and straightforward visual access for operator can also support his evaluation of the results of whatever type of automatic computer-based diagnosis is incorporated. See later on.

Thus control decisions at this level are connected with maintaining the overall control of the major energy and mass flows and accumulations. Balances and inventories have to be maintained and coordinated. In addition, margins to acceptable limits of operation have to be monitored for the subsidiary and auxiliary services, functions and conditions which are the "enabling" elements for the main flow paths.

In some cases where disturbances occur, the scenario is known from experience or has been analyzed during design and the control alternatives are reasonably well defined for the available resources and the various operational states. These are

the conditions for a rule-based response; i.e., the root cause is less relevant, distinctions between disturbed and disturbing functions are less important than a state identification in terms of underlying "general" functions which can be used as "control objects". These functions belong to functionally decoupled systems, they can be identified by emphasizing certain (overlapping) domains within the flow topology and, finally, their operational state as well as control references and strategies are available. Thus an identification is possible in terms of action alternates - i.e. targets, tasks, actions related to the right leg of the decision ladder of Fig. 4.

The decomposition of the overview to support this type of decision will depend somewhat on the number of available alternatives for control action which actually exist. The level to choose should serve to identify the aggregates which can be isolated and "decoupled" and therefore controlled individually. As stated, these should be based on the general functions which characterize the given technology (although not its details).

Often these "functions" will be those which are established separately - i.e. during startup - and aligned before being interconnected with others. However, in general, they can be classified as follows:

- they supply energy or material to the main flow path
- they support directly energy transport or storage
- they maintain a parameter or variable at a level which is necessary for maintaining the main process.

It will be possible to identify variables and critical parameters which define these functions' operational status with respect to the support they are intended to furnish as well as the limitations in the resources which implement them. In addition, prioritization support in utilizing these functions may be required.

The degrees of freedom remaining in exercising control at this level after the specifications derived explicitly from the functional purpose level have been satisfied must be resolved and reduced through the use of optimizing criteria. Typically these aim at minimizing cost and maximizing availability/safety and can affect the choice of configuration at lower levels and/or parameters for state control.

Fig. 9 attempts to transform the above reasoning into a possible display format. The upper left portion is mass and energy related. The current (dark) and possible (dashed) paths of energy flow are coded within a flow diagram of the main process where energy sources, exchangers, converter and sinks - expressed (succinctly) in operator-friendly terms - are located in rectangular boxes. Flow magnitude is not shown here since, as stated above, Fig.8 includes an energy balance which for all operating modes should give a rough indication of the effect of a disturbance on the overall distribution of energy. However an attempt at including a mass balance window can be seen; this is felt to be an potentially informative support since it should be a sensitive measure of system integrity and, at the same time, can give a strong indication of the type of fault.

In accordance with the requirements stated above, an important feature can be seen in the form of the small circled F's and S's (where F denotes Flow and S denotes support). These serve a twofold purpose. Firstly, they function as high level "alarms" (Goodstein 1985) to indicate at the abstract functional level that a particular flow and/or support function has deviated from normal for the given operating mode. Note that these non-normal indications probably will only be relevant for a restricted set of continuous operating modes (i.e., not transient) where normal can be defined. Secondly they identify possible control "objects" the "manipulation" of which will directly affect the mass/energy relationships. Selection of a particular F, e.g. by means of a mouse, tracker ball, etc., makes it possible to alter the energy flow through the path in the topology associated with the particular F. Upon selection, appropriate guidance appears in the action window including references to relevant checklists, etc.

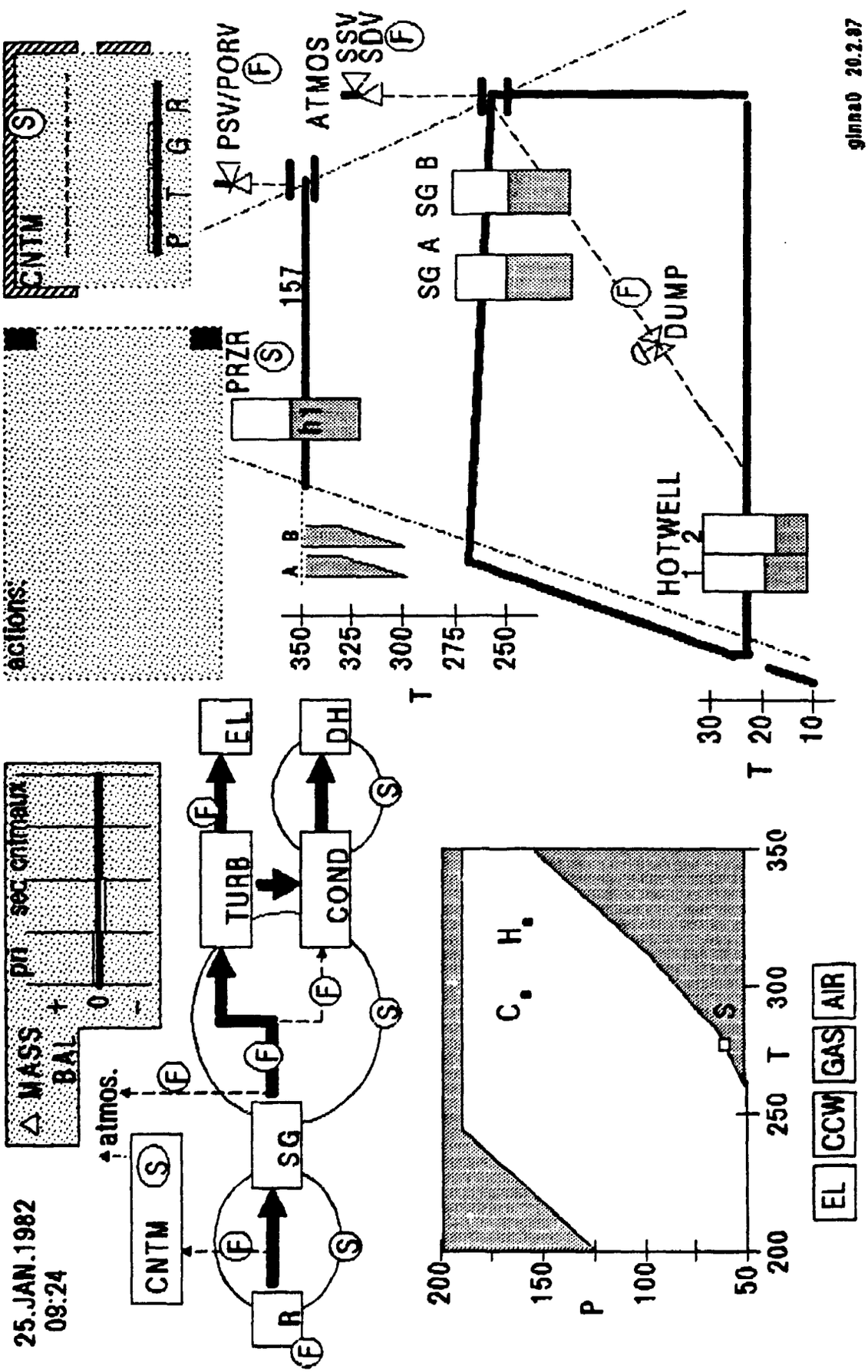


Fig. 9. Abstract and generic level display.

The S's relate to the underlying functions which are necessary in order that the main energy flow can be maintained. As stated earlier, they supply energy or material, they support energy transfer, they maintain a critical parameter and thus need to be established and aligned as a prerequisite for total operation. Selecting an S leads to an associated display with a more physically oriented representation. More on this later.

The remainder of Fig. 9 is intended to support disturbance handling and speculations about energy and mass conditions by including a considerable amount of information which has to do with the generic functioning of the plant - i.e. in this case, the thermodynamics of the process. In fact redundancy is suggested on Fig.9 in the form of a P-T diagram indicating primary and secondary trajectories vs. time (see Broughton and Walsh (1981) for a more thorough discussion of the advantages of this approach) as well as a version of Beltracchi's iconic display based on the Rankine thermodynamic cycle (see e.g. Beltracchi (1984)). The major features of Beltracchi's approach are displays of the state of the energy-bearing medium (liquid water, steam, ..) and the relationships which ensue with regard to temperature, pressure, saturation and, as well, to the related inventories, radiation levels, safety valve positions, etc. Thus equipment-relevant details begin to appear - i.e. two steam generators, two primary loops, etc. In addition, associated control possibilities can be added - e.g., see the circled F symbols which are examples of direct manipulation through the displays themselves. Beltracchi has other examples in his articles.

In essence, then, part of Fig. 9 is intended to support an understanding of the functioning of the main process flow by means of a detailed presentation of the underlying generic functions having to do with thermodynamics, heat generation and transfer, maintaining medium state, etc. Monitoring margins to limits and indicating critical interrelationships is a primary aim as is a linking of state to possible action.

Level of Generic Function

At this level, attention should be paid to the status and structure of the plant described in terms of generic functions (which are also general in that the terminology is commonly found in professional text books and is not connected with a specific plant or installation). Examples are cooling, supply, heat transfer, feedback, etc. To serve the purpose of control planning, the functional performance should be given in relation to the requirements set by the level above. These functions should be "expressed" in terms of overviews of the anatomy of the physical systems currently implementing the function. Again information at three levels.

Information displays at this level will include conventional "mimic diagrams" connecting pieces of equipment together to meet the functional requirements coming from the next level. Integrated state information should be available to indicate whether these requirements are indeed being met. In addition, at this level, detailed information on control means and characteristics as well as links to especially relevant information on critical component requirements and/or performance limitations will be useful.

Of special importance at this level are displays of the status of alternative "back-up" resources to meet the functional requirements. Switching configurations, operational status, priority information would have to be based partly on computerized logs of switching and valving status, maintenance schedules, etc.

As an example of a display for this purpose, see Fig. 10, which will appear as a result of pointing at/selecting the S on Fig. 9 lying on the primary circle between R and SG. This presentation provides an alarm and selector panel for the relevant critical primary functions - e.g., inventory and chemistry control, pressure control, circulation, etc. In addition composite displays of two critical variables are included. High-level alarms indicating a non-normal state in one or more of the critical functions will be reflected in the status (color, blink) of the

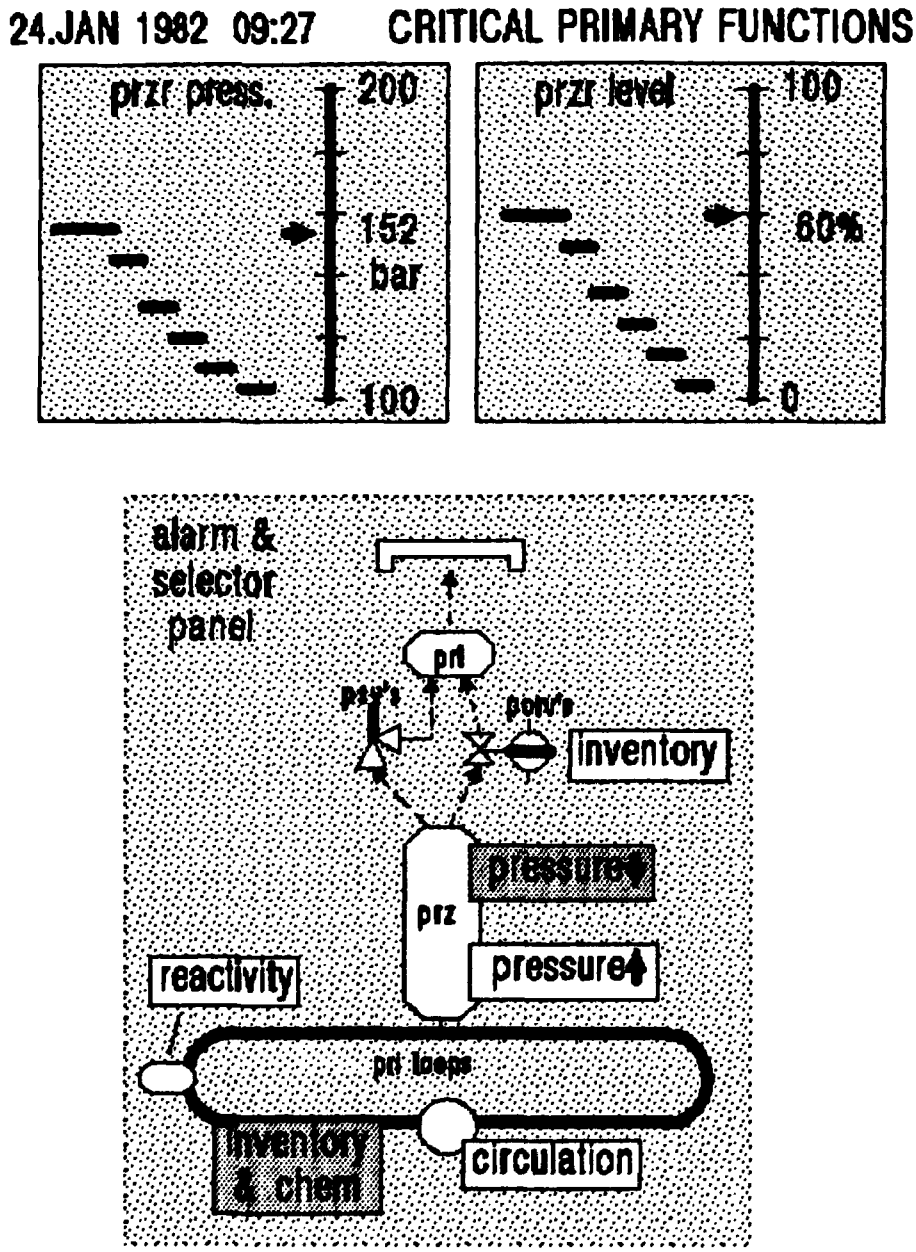


Fig. 10. Physical function "selector" display.

related indicator panel. Pointing at/selecting, for example, inventory and chemistry, will result in Fig. 11 which is a combination of Fig. 10 and an overlay giving more details on the inventory function. Other overlays would result from selecting other critical functions. Thus the right half of Fig. 11 summarizes a considerable amount of information on inventory control - state, other potential resources for controlling inventory, control - and, as well, gives access to lower level displays of valving ("is" vs. "should be"), full mimic diagrams, configuration data, etc.

Level of Physical Function

At this level, we begin to approach the maintenance and trouble shooting task domain. However, a great deal of manipulations are still carried out remotely from the control room and often errors of location and manipulation occur. Thus detailed displays of major components, their state, configuration, handling information, physical location, etc. will be appropriate - especially if this information could be transferred directly to remote displays on location. In addition, switching and valving records would be important. At this level, video disc technology seems especially appropriate here.

An Automatic Knowledge-based Diagnosis Support

As mentioned earlier, in carrying out diagnostic tasks associated with supervisory control, (at least) two basically different approaches or overall strategies are possible - a knowledge-based functional identification of cause and a rule-based diagnosis in terms of action alternatives. At this point, it is relevant to describe how the a knowledge-based approach could be carried out as an aid for the operator.

At the abstract functional level, an analytic context-free method for carrying out a diagnosis can by performed by making inferences about the root cause of the disturbance with respect to a representation based on the flow topology of the system. To do this, the approach to carrying out this identification has to be independent of the actual state of the system and thus

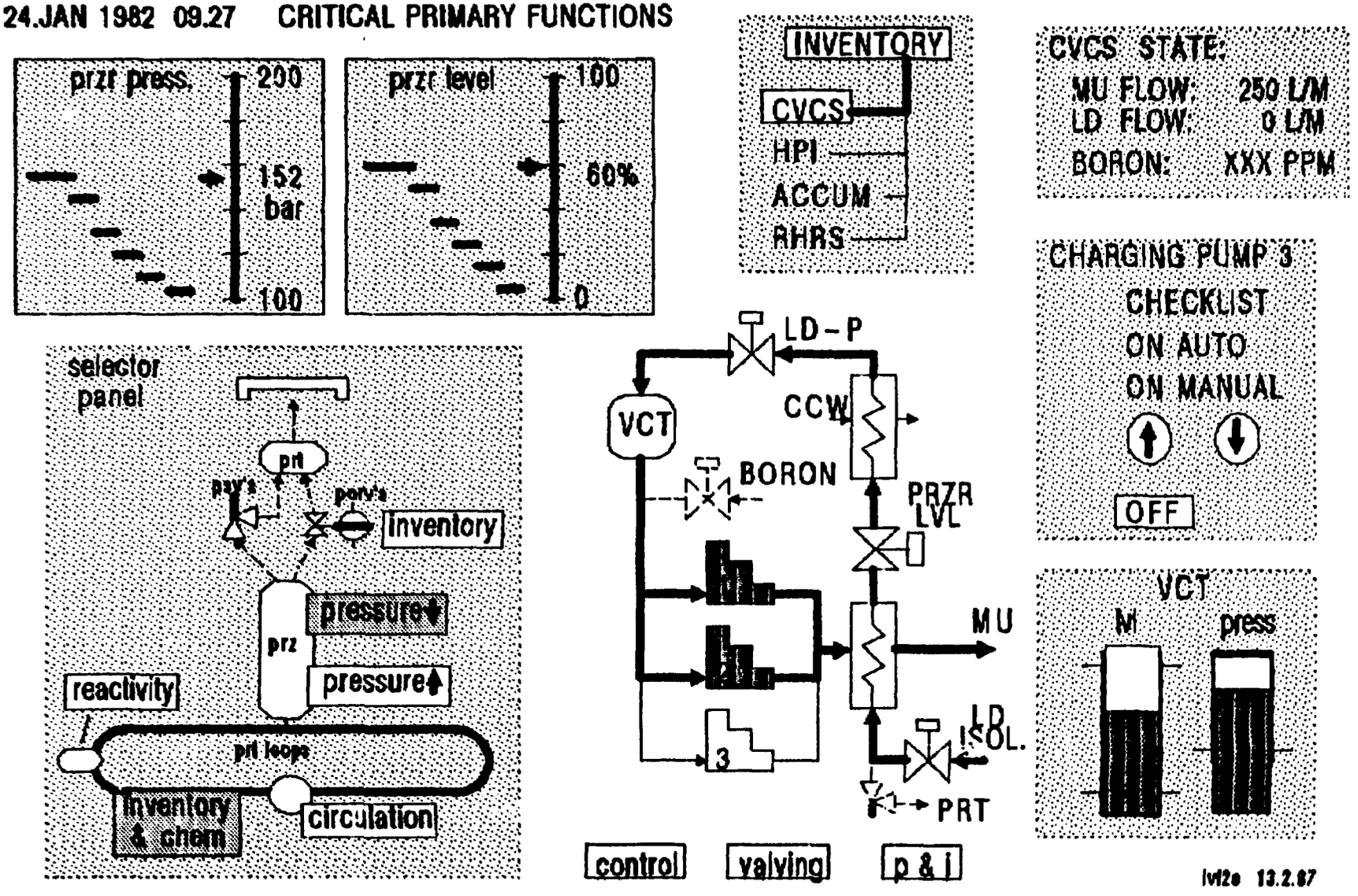


Fig. 11. Fig. 10 with typical overlay.

will be based on "first principles", a synonym for the underlying functional causal relations in the system. The search will use fundamental conservation laws and consist of a topographic search for changes in the mass and energy relations which then can be used to check the actual system. This strategy depends on being able to transform all available process data up to the level of energy and mass flows. In addition, an effective set of inference rules is required for identifying the location of the disturbance in the flow topology. The strategy is inherently powerful in that it gives the possibility for a consistent and verifiable identification which, however, requires considerable resources for memory and inference as well as the availability of suitable reference information concerning "normal" relationships. Such an identification results in a neutral diagnosis in terms of the location of the cause, independent of priorities and procedures.

A systematic identification of the location of the disturbance in the abstract causal structure can, in principle at least, be done through an automatic inference algorithm if the normal or specified state model is available. This approach can be necessary as a back-up diagnostic tool and for dealing with unforeseen and/or multiple faults.

Care should be taken in the communication of such a diagnosis to the operator. Results should preferably be communicated in terms compatible with general or physical functions, component malfunctions and the like. Furthermore, if possible, the diagnostic result should preferably be compatible with the level describing the effective action alternatives and, for example, this will be different for operators and repair staff. A suitable accompanying explanation of the manner in which the automatic diagnosis was arrived at is also a sensitive area if operator acceptance and understanding is to be won.

CONCLUSION

An attempt has been made to structure the information requirements associated with the task of supervisory control of a complex process plant in which decision making takes place within a problem space comprising the two dimensions of means/ends and whole/part. The decomposition of the diagnostic problem which the operator/user will attempt requires support from the information displays to allow questions regarding WHY, WHAT and HOW to be asked (and answered) from any one of several relevant levels of system description. Good linking between display levels and appropriate shifts in representation are needed to support operator "labelling of" or "focusing in on" the distinctive features of a given situation. In addition, compatibility with automatic diagnostic aids is an important problem.

This area of endeavor is fraught with problems regarding evaluation and validation - is it possible to demonstrate/measure convincingly an improvement in performance in the control room with an approach based on the above material when coping with rare and potentially dangerous situations. For a researcher, however, the area is rich in possibilities for doing selective studies of areas within cooperative decision making, cognitive representation, subjective performance criteria, etc.

REFERENCES

BELTRACCHI, L. (1984) A Process/Engineered Safeguards Iconic Display, Symposium on New Technologies in Nuclear Power Plant Instrumentation and Control, Washington, D.C. 28-30 Nov.

BROUGHTON, R.G. and WALSH, P.S. (1981) A Real-time method for analyzing nuclear power transients, Nuclear Technology v.53 May, pp 217-225.

CORCORAN, W.R., FINNICUM, D.J., HUBBARD III,F.R., MUSICK, C.R., WALZER, P.F. (1981) Nuclear Power-Plant Safety Functions, Nuclear Safety v.22 n.2 pp 179-191.

DWORZAK, F., NEDELIK, A. Van GEMST, P.A. (1982) Design and Implementation of a Computerized System for Evaluation of Plant Status with respect to Safety Technical Specifications - in Proceedings of IAEA Symposium on Nuclear Power Plant Control and Instrumentation, Munich 11-15 Oct. pp 151-171.

GOODSTEIN, L.P. (1985) Functional Alarming and Information Retrieval, Risø-M-2511.

LIND, M. (1982) Multilevel Flow Modelling of Process Plants for Diagnosis and Control - International Meeting on Thermal Nuclear Reactor Safety, August, Chicago, Ill.

RASMUSSEN, J. (1976) Outlines of a Hybrid Model of the Process Plant Operator, in Monitoring Behaviour and Supervisory Control, T. Sheridan and G. Johannsen (Eds.), Plenum, New York.

RASMUSSEN, J. (1985) Conceptual Models in Man-Machine Design Varification, presented at the 1985 IEEE Third Conference on Human Factors and Power Plants, Monterey CA, June 23-27, - also Risø-M-2520.

RASMUSSEN, J. (1986a) A Framework for Cognitive Task Analysis, in Hollnagel, E., Mancini, G. and Woods, D. (eds) Intelligent Decision Support Systems in Process Environment, Berlin, Springer-Verlag - also Risø-M-2519.

RASMUSSEN, J. (1986b) A Cognitive Engineering Approach to the Modelling of Decision Making and its Organization - Risø-M-2589.

RASMUSSEN, J. and GOODSTEIN, L.P. (1985) Decision Support in Supervisory Control, in 2nd IFAC/IFIP/IFORS/IEA Conference on Analysis, Design and Evaluation of Man-Machine Systems,

Varesa, Italy, Sept.10-12. - also Risø-M-2525 (to appear in revised form in Automatica).

RASMUSSEN, J. and LIND, M. (1981) Coping with Complexity, in First European Annual Conference on Human Decision Making and Manual Control, Delft, also Risø-M-2293.

WOODS, D.D., O'BRIEN, J., HANES, L.F. (1986) Human Factors Challenges in Process Control: The Case of Nuclear Power Plants, in G.Salvendy (ed) Handbook of Human Factors/Ergonomics, Wiley, New York.

Risø National Laboratory **Risø – M – 2645**

Title and author(s)

Representation of Process State, Structure and Control

L.P. Goodstein and J. Rasmussen

Date April 1987

Department or group Computer and Information Science

Groups own registration number(s) R-3-87

Project/contract no.

Pages 36 **Tables** **Illustrations** 11 **References** 13

ISBN 87-550-1320-1

Abstract (Max. 2000 char.)

Supervisory control is essentially a decision-making activity where, among other things, the dm has to maneuver within a complex problem space which reflects key dimensions and attributes of the object system (power plant ...). Of considerable importance therefore is the representation for the dm of this problem space comprising at the one end the target demands, goals, constraints and, at the other, the resources available for meeting the assigned goals – and all of this in pace with the dynamic event-driven environment which characterizes the types of systems of interest. Previous work has identified the advantages of utilizing the two-dimensional means-ends/part-whole space as a basic ingredient in a system representation. This paper associates more detailed representational requirements at the various levels of the means-ends axis with the activities of state identification and diagnosis. In addition, some examples of display formats which attempt to incorporate the outlined representational principles within the context of a PWR plant are discussed.

Descriptors – INIS

DECISION TREE ANALYSIS; DIAGNOSIS; HUMAN FACTORS; INFORMATION; MAN-MACHINE SYSTEMS; PWR TYPE REACTORS; REACTOR CONTROL SYSTEMS; REACTOR OPERATORS; VERIFICATION

Available on request from Risø Library, Risø National Laboratory, (Risø Bibliotek, Forskningscenter Risø), P.O. Box 49, DK-4000 Roskilde, Denmark.
Telephone 02 37 12 12, ext. 2262. Telex: 43116, Telefax: 02 36 06 09

Available on request from.
Risø Library,
Risø National Laboratory, P.O. Box 49,
DK-4000 Roskilde, Denmark
Phone (02) 37 12 12 ext.2262

ISBN 87-550-1320-1
ISSN 0418-6435