Notes on diagnostic strategies in process plant environment

Rasmussen, Jens

Publication date:
1978

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

Risø-M-1983

Risø-M-1983

RISØ NATIONAL LABORATORY

ELECTRONICS DEPARTMENT

Notes on Diagnostic Strategies in Process Plant Environment

Jens Rasmussen

January 1978
R-1-78
NKA/KRU-P2(78)1

Available on request from: Risø Library, Risø National Laboratory, (Risø Bibliotek, Forsøgsanlæg Risø) DK-4000 Roskilde, Denmark.
Telephone: (03) 35 51 01, ext. 334, telex: 43116.

Risø

Risø - M - 1983

Risø - M - 1983

Title and author(s)

Notes on Diagnostic Strategies in Process Plant Environment.

Jens Rasmussen

Date January 1978

Department or group

Electronics

Group's own registration number(s)

R-1-78

NKA/KRU-P2(78)1

pages + tables + illustrations

Abstract

In the report are discussed some aspects of state identification and diagnosis in process plant control which must be considered in connection with automatic disturbance analysis and man-machine interface systems.

The content of the diagnostic process depends upon the overall goal of the diagnostician - whether it is to protect the plant, to maintain operation or to repair, and it may not necessarily include a determination of the cause itself. Important aspects of diagnosis include critical variables and causal flow paths which are intimately related to the paths along which events and changes propagate through the system, i.e. to the flow of energy, matter and information which together form complex, interacting flow structures.

In the process plant environment, a diagnostic task implies a search to identify a change from a normal or planned plant state. Several elementary strategies can be identified. In the report a distinction is drawn between two main groups - topographic search strategies, performed as search through the system with reference to a model of normal plant state; and symptomatic search strategies, performed as a search through a library of abnormal state models with reference to the actual plant state.

Typical properties of the different strategies are discussed such as processing capacity requirements and dependence upon a priori analysis.

The role of the elementary strategies in the overall diagnostic task is not discussed since this is considered possible only with reference to selected scenarios describing realistic and complex real life situations arising from disturbed plant operations. The aim of the report is to identify and formulate some of the issues which should be taken into account when creating such scenarios based on careful field studies and analysis of incident reports. Based on these scenarios, different overall diagnostic strategies can then be formulated and tested by simulator experiments.

The work is part of the interscandinavian project on control room design and human reliability sponsored by the Council of Nordic Ministers. Report No. NKA/KRU-P2(78)1.

Available on request from Risø Library, Risø National Laboratory (Risø Bibliotek, Forsøgsanlæg Risø), DK-4000 Roskilde, Denmark
Telephone: (03) 35 51 01, ext. 334, telex: 43116

Fi 25-204

Table of Contents Page

Introduction

The purpose of a process plant control system is to maintain the plant in - or transfer it to - a target state related to the overall operational goal. If this function cannot be based on feedback or trial-and-error strategies, it is necessary to identify the internal state of the system in a way which enables the controller to plan its control actions in advance. To identify system state means to label the actual state of the system by a name which refers to one of a category of states or events for which rules exist for determination of the appropriate actions. Quite naturally then, the categories used for identification depend upon the type of the appropriate actions or, more basically, upon the current goal. Typically, labels are used which refer to the related actions (e.g. -"your water is now ready for tea"-), to the state of typical variables (-"the temperature of the kettle is now 100 0 C"-) or components (-"the water is boiling"-) and to different types of event. Several types of identification can typically be distinguished. Sometimes, identification serves to verify whether a known system state is present or not, generally in order to decide whether the system is ready for an intended action. otherwise, identification is used to confirm that an action has brought the system to the proper target state. Another type of identification is needed in case of abnormal, unforeseen changes and faults in the system. In this case, the identification implies a determination of the actual internal anatomy and functioning of the system from the observed behaviour. This task is basically an inductive task. In process plant control it is, however, simplified by the fact that the plant generally will be known to have functioned properly, and therefore the identification can result from a search to locate a change with reference to knowledge of the normal state.

The term diagnosis used for this kind of identification is in some respect misleading. The general meaning of diagnosis is the determination of the cause of some observed symptoms, but this is not necessarily the case in our context. The ultimate purpose of diagnosis in process plant control is to link the observed symptoms to the actions which will serve the current goal properly. This can be done in several different ways, see fig. 1. In some cases this can be done directly; in other cases a sequence of data transformations is used to create the link, but even then it depends upon the conditions of the specific occurrence as to whether determination of the cause is needed. The strategies and data processes used by the controller to perform the task primarily depend upon two conditions: the current goal and the kind of a priori knowledge available to the controller.

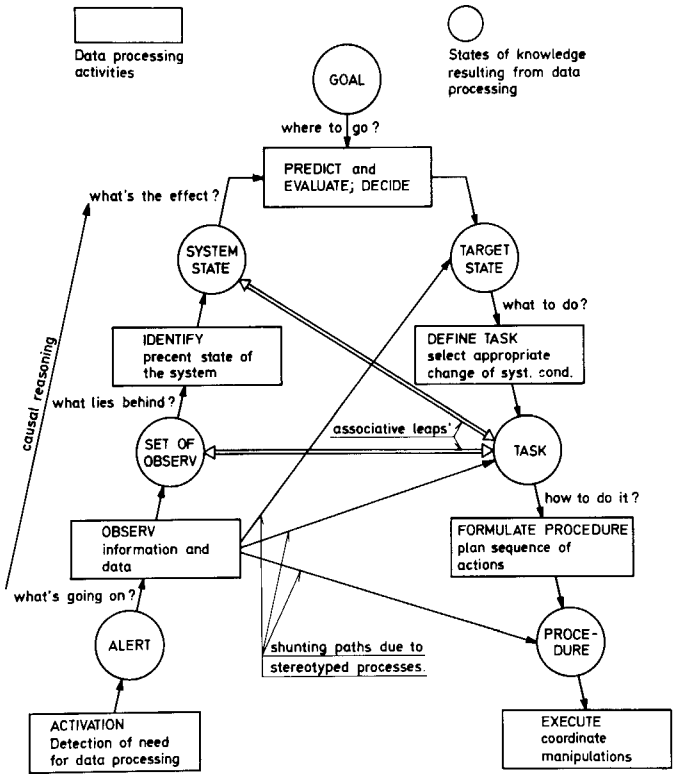


Fig. 1. System state identification diagnosis is an integral part of the sequence of subtasks leading to operator actions. In some cases of rational, causal reasoning, diagnosis is a separate subtask; in other cases of stereotyped responses, a diagnostic task cannot be separated.

The Task Sequence

The dependence of diagnostic strategies upon the current goal and the type of a priori knowledge imply that the diagnostic task cannot be considered in isolation but should be studied as a part of the total task sequence.

The rational sequence of operations in the task to be performed by a controller in response to an accidental change in the operating conditions of a plant is the following:

1. Detect the advent of a change in the system.

2. Identify the actual state of the system in terms of the functional aspects of the change.

3. Interpret the state of the system to predict the operational consequences of the change.

4. Evaluate the current goal and determine the target state into which the system should be transferred in order to comply with the goal.

5. Find the changes in the present operational conditions which will bring the system into the target state.

6. Plan the sequence of actions and locate the proper means of manipulations.

7. Execute.

This rational sequence of operations is necessary in case of new, unfamiliar situations when the control action must be based on causal, functional evaluation of the situation. In absence of specific plant experience, each step is logically necessary.

The content of the diagnostic task depends upon the specific occasion: if the pressure of a tank or the temperature of a furnace is rapidly rising, the situation typically signals danger, and the immediate goal will be to protect the equipment from damage, presumably by release of some predetermined safety action, e.g. automatic shutdowns In this case, the diagnostic task is a search to locate the change in terms of the state of some critical variables without losing time by searching for the cause of the observed state.

In less dramatic situations the control goal may be to compensate for the effect upon critical variables from the initial change or fault, for instance to avoid drastic automatic safety actions. In this case, the diagnostic task will be to locate the critical variables and to find possible means for counter-actions from the causal or functional flow structure of the system. This can also be done without consideration of the primary cause of the situation. Finally, if the goal of the controller is to restore the normal condition prior to the change, the aim of the diagnosis is to locate the affected component topographically in order to be able to adjust or repair it.

To sum up, the diagnostic task in process plant control will be a search to locate a change in the operating condition of the plant, but - depending upon the circumstances - the target will be related to endangered critical variables, affected causal flow paths, or faulty equipment and components. Apart from this dependence upon the aim of the diagnosis, the strategy used to perform it will depend strongly upon the a priori knowledge of plant properties, i.e. the data processing model, available to the controller.

Critical Variables and Causal Flow Paths in Process Plant

Two typical aspects of diagnosis or identification in industrial process plants are the relations to critical variables and causal flow paths.

In the present context, critical variables are defined as the state variables of the system which are subject to specified constraints or limit values in order to ensure safe or reliable operation. The critical variables must be chosen as targets for causal paths which connect them to control actions in order to counteract the primary change or cause of improper operation. In energy and mass balance systems, the critical variables are basically related to the level of accumulation or "pile up" of the system, representing the stress imposed on the barriers retaining the stored energy or matter. Other critical variables can be related to the actual state or condition of energy containments or barriers (temperature of bearings, stress in tank walls, vibration of structures).

Causal paths are the paths along which events and changes propagate through the structure of the system. A causal path is a chain of directed relations defining the relationships between state variables. Basically, causality is a consequence of the laws of energy and mass conservation, and causal paths can be seen as connected to a flow of matter or energy through the system. In practice, we must also consider causal paths related to the flow of information, e.g. in the control system, which influence the flow conditions of energy and matter flow systems. (Viewing a control system as an energy flow system is unhelpful in most cases related to its function at system level).

Two classes of matter and energy flow systems are important in the present context:

Mass or eneray balance systems in which the input and output flows can be controlled rather independently and which in consequence include a storage facility. In such systems there is a danger of a flow balance being disturbed so that variables related to storage level reach critical limits before intrinsic feedback effects limit input flow. (I.e. the system is fed from a flow - e.g. current - source). Balance systems are typically parts of the main process paths of a plant, and since matter is normally the transport medium for energy, such balance systems overlap and are interconnected in a complex structure, see fig. 2.

In mass and energy transport systems flow is only controlled from the system output terminal, as is the case for supply systems. Intrinsic feedback effects adjust system input flow to match output demand without significant change of level variables (the system is connected to a "flow potential" - e.g. voltage source). Transport systems typically supply necessary operating conditions for the main

processes, and are connected to these and influence them at many nodes in the plant structure.

Information flow systems, typically instrumentation and control systems, interconnect the different causal paths related to flow of energy and matter. Information flow systems introduce feedback paths in the physical processes and change the basic causal structure and relations, often drastically.

Transport systems - supply as well as information systems control the operating conditions of the energy and mass balance systems, and the critical variables in transport systems are those output variables which represent the coupling to the energy flow of the main process. Supply and information systems generally have highly branched structures affecting the causal paths of the main processes of the plant at many points. Changes or faults in supply or control systems therefore obscure the causal structure of the total system considerably.
Energy and mass balance systems have a special significance in process plant diagnosis. First of all, the potential for major hazards is connected to loss of control of major energy or mass (poison) accumulations. However, the laws of conservation of energy and matter provide invariant structures to guide diagnosis which information systems do not have, and the integrating relation between an initial fault affecting a flow and the resulting dangerous level of a balance introduce the time delay which generally makes counteraction to restore equilibrium physically possible.

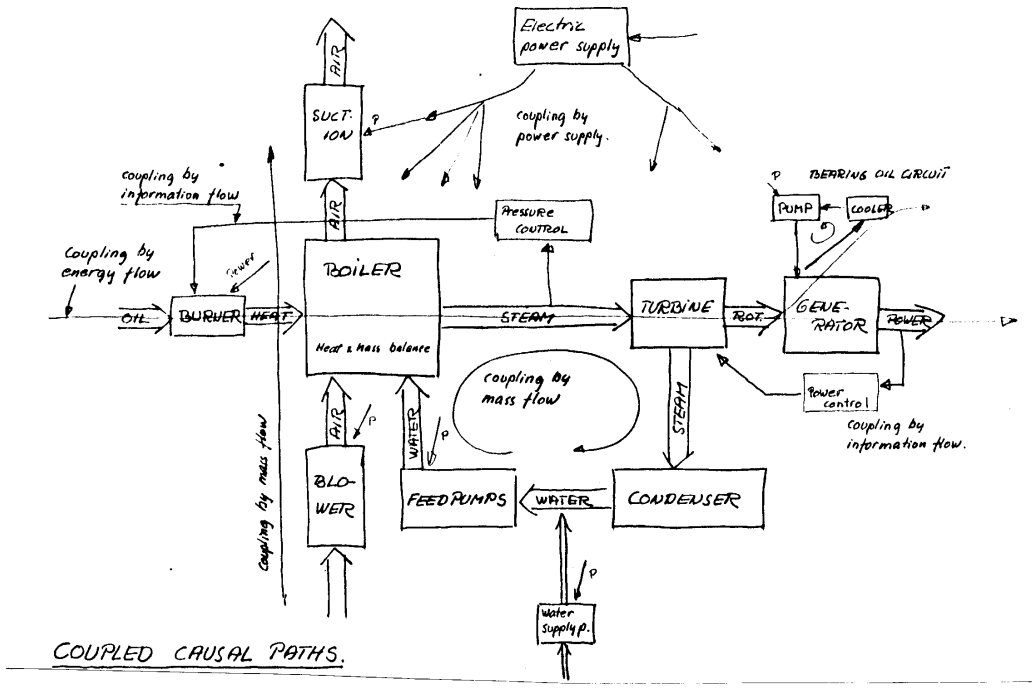


Fig. 2. Map illustrating the complexity of a power plant viewed as a system of overlapping causal flow structures.

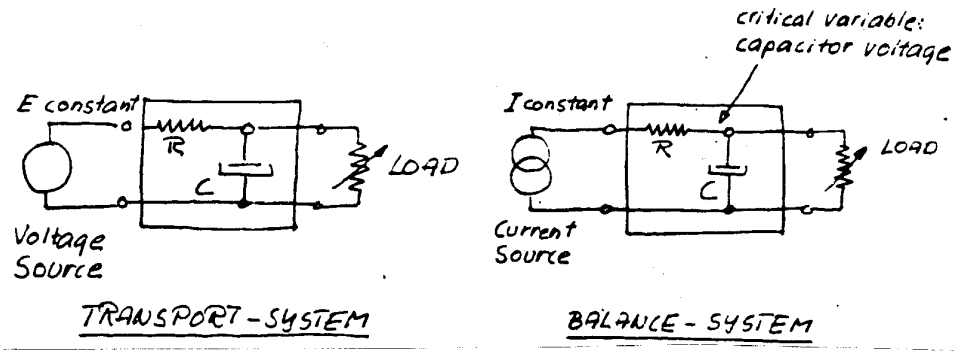


Fig. 3. Transport or balance system? - Depends upon circumstances.

Diagnostic Strategies in Supervisory Control

The diagnostic task implied in supervisory control is in general a search to identify a change from normal or planned plant operation in terms which refer the controller to the appropriate actions. The search can be performed in different ways, depending upon the controller's intention or goal which very likely will change during the task. (The controller can in this context be a man and/or a machine).

Following the detection of accidental maloperation for instance by a warning signal, the immediate intention can be to ensure that no major hazard is present. A preselected set of critical variables is scanned to test whether a data pattern related to preplanned safety action e.g. plant shut-down is observed. This sequence can be performed by an operator, but is also in fact the function behind an automatic safety system. If no immediate danger is present, the subsequent intention may be to compensate the effect of the change either to restore normal production or anticipate automatic protective actions. In this case the function can be based on a feedback control loop, or the action must be based on an identification from a search which is performed in cause and effect relationships. Ultimately, the intention will be to judge the need for repair, and a search in terms of parts and components will be needed.

Depending upon the specific situation and the immediate intention of the controller, the search can be performed in two different ways. It can take the form of a search through a library of data sets or state models related to different abnormal system states stored in the controller to find the one that matches the observed data pattern.

On the other hand, the search can be performed by a search in the actual operating system to locate the change in terms of causal relations or parts and com-

ponents, with reference to a model of normal or planned operation which is stored in the controller.

Before the overall search strategies are discussed, the different elementary search routines will be discussed in more detail.

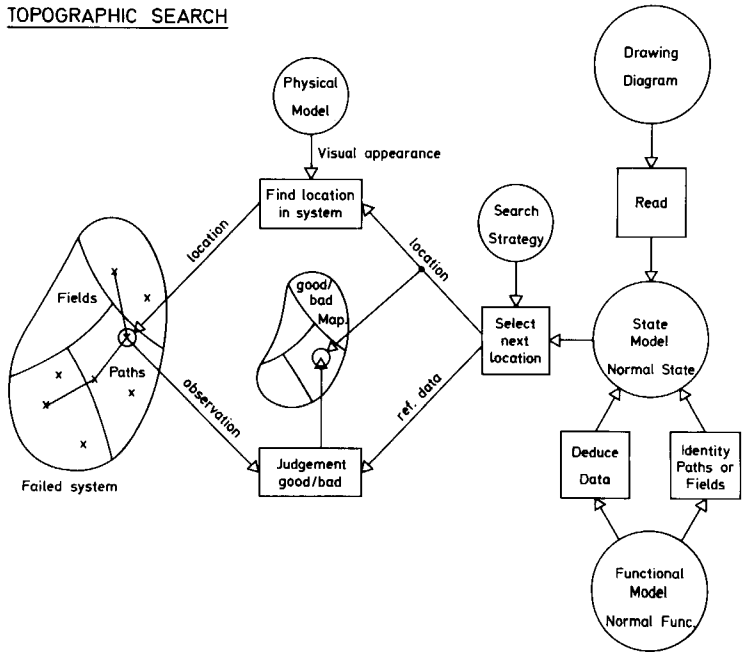


Fig. 4. Schematic information flow graph of topographic strategy.

Elementary Diagnostic Search Routines

Broadly speaking, the two different search routines discussed above can be termed symptomatic and topographic search procedures. Every observation renders information identifying the information source and the content of its message. By symptomatic search, reference to the identity of system state is obtained from the information content of the observations; by topographic search, reference is obtained from the location of the information source, while the results of good/bad judgements of the information content are used to control the strategy.

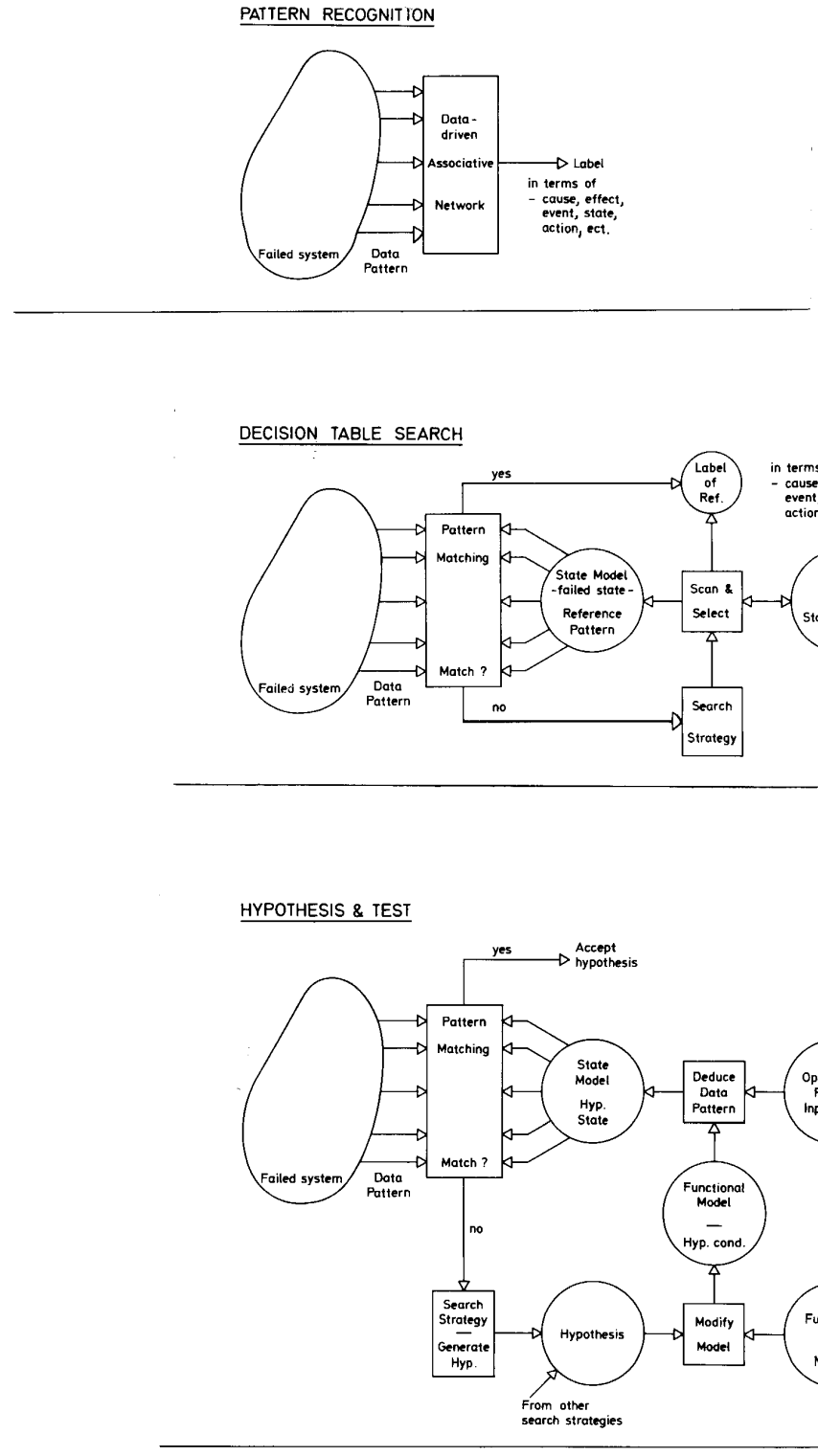


Fig. 5. Schematic information flow graphs of symptomatic strategies.

Topographic search locates a change or fault with reference to a model of normal or planned system performance and is based on good/bad judgements of observations.

Variables measured or observed in the system can be judged individually against stored norm or reference data. In this case the reference model will generally be a flow map of the system supplying reference data related to variables along flow paths. The detailed search decisions will be like this: if observation is judged good, seek down stream; if not, seek up stream. The change is supposed to be between a good and a bad observation. This search is advantageous since search decisions are simple and can be related to observations individually. Low buffer memory capacity is needed, and hierarchical search strategies can easily be implemented (half split search). However, difficulties are often found in practice; the causal direction in a flow path is frequently ambiguous by nature or disturbed by feedback loops. Furthermore, the system must be in an operational state corresponding quantitatively to the state for which reference models are available.
Superior to this simple linear search are strategies which judge relationships in sets of observations. If boundaries can be found around system parts or functions for which the input-output relations are subject to known laws and relations - such as mass and energy balance constraints - reference to location of the change inside or outside the boundaries is obtained by good/bad judgement of data sets related to boundary conditions. This search is advantageous, since it takes feedback properties more readily into account and is more independent of the quantitative level of operation (at least in linear systems). This is because judgements are performed on data relations representing system properties rather than on the magnitude of data representing system states. It demands, however, more complex data processing for judgements and more complex search strategies.

An important feature of topographic search is the dependence upon a model of normal or intended plant operation. This model can be derived from the system designer's a priori information and stored in the controller (by training an operator or programming a computer), or it can be derived by the controller "on-line" if the different intended or normal operational regimes (shut-down, starting up, normal operation, etc.) can be defined and distinguished by the controller. The efficiency of the topographic search may be increased considerably if special operating states and corresponding references are introduced artificially as is the case in preplanned test procedures. Then a sequence of operating states which are especially sensitive to specific faults can be used as test conditions.

Topographic search sequences based on good/bad judgements use the information content of the observations rather inefficiently, and consequently rather long

sequences of judgements may be needed to obtain a precise identification of a fault or change. The ultimate identification will be in terms of the location in a map representing system anatomy which may be structured in terms of system functions or in terms of parts and components.

Symptomatic search procedures obtain the reference to the identity of system state from the information content of the observations. In principle a search is made through a library of data patterns representing abnormal system states which are compared with the observed data pattern until a match is obtained. The reference sets can be generated empirically from system operation or derived by analysis or simulation of the response of the system to postulated faults or changes in operating conditions. Furthermore, the reference pattern can be generated on-line if the controller has a functional model available which can be updated according to the current hypothesis.

When the search is performed in the data domain by a search through a stored library, the reference patterns can be labelled in terms either of the initial cause, of the predicted effect, or of the appropriate action to take by the controller. Depending upon the structure of the controller, the search can be a sequential decision table look up or a recognition by an associative network. The reference sets can be related to specific operational states, but also more general templates can be used to further the search. Specific data patterns can refer to faults in a type of component or function, the patterns being given in terms of their failure properties - e.g. instability, noise characteristics, time constants.

Symptomatic search supported by a ready-made library of reference patterns is a search by pattern recognition.

If the search is based on reference patterns generated on-line by modification of a functional model in correspondence with a postulated fault, the search procedure may be termed "hypothesis and test". The efficiency of this search depends upon the strategy used to generate hypothesis. Typically, hypothesis generation will be guided by topographic identification at a rather general level combined with fuzzy recognition and consideration of the frequency of previously experienced faults.

Symptomatic search is advantageous from the point of view of information economy, and a precise identification can frequently be obtained in a single step or decision, which on the other hand implies a complex data process. One serious limitation is that a reference model of the actual abnormal state of operation must be available. This means that reference sets must be predicted by analysis or recorded by prior occurrences. Or, the reference set must be generated on-line using a model which can be adjusted on occasion to simulate the abnormal operation - which may be outside the normal (linear) operating range.

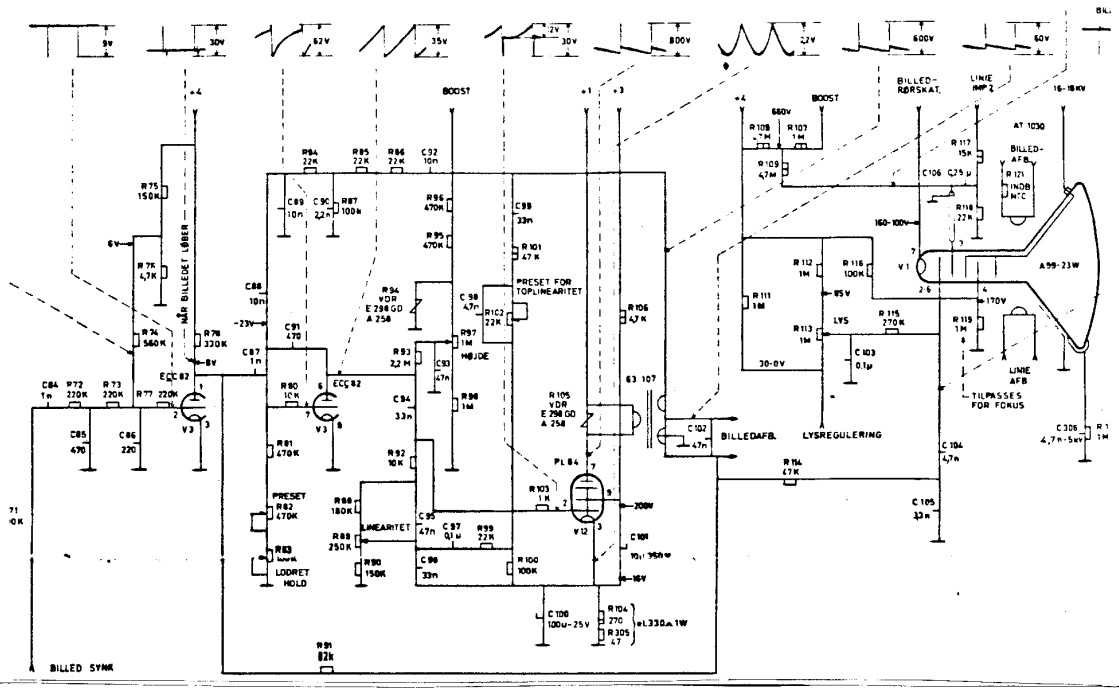
Data Processing Demands from Elementary Strategies

The different elementary diagnostic strategies imply different data processes based on several kinds of data processing models of plant functions or states. Likewise, the demand for data processing and memory capacity vary widely. In the following sections some of these aspects are discussed in more detail.

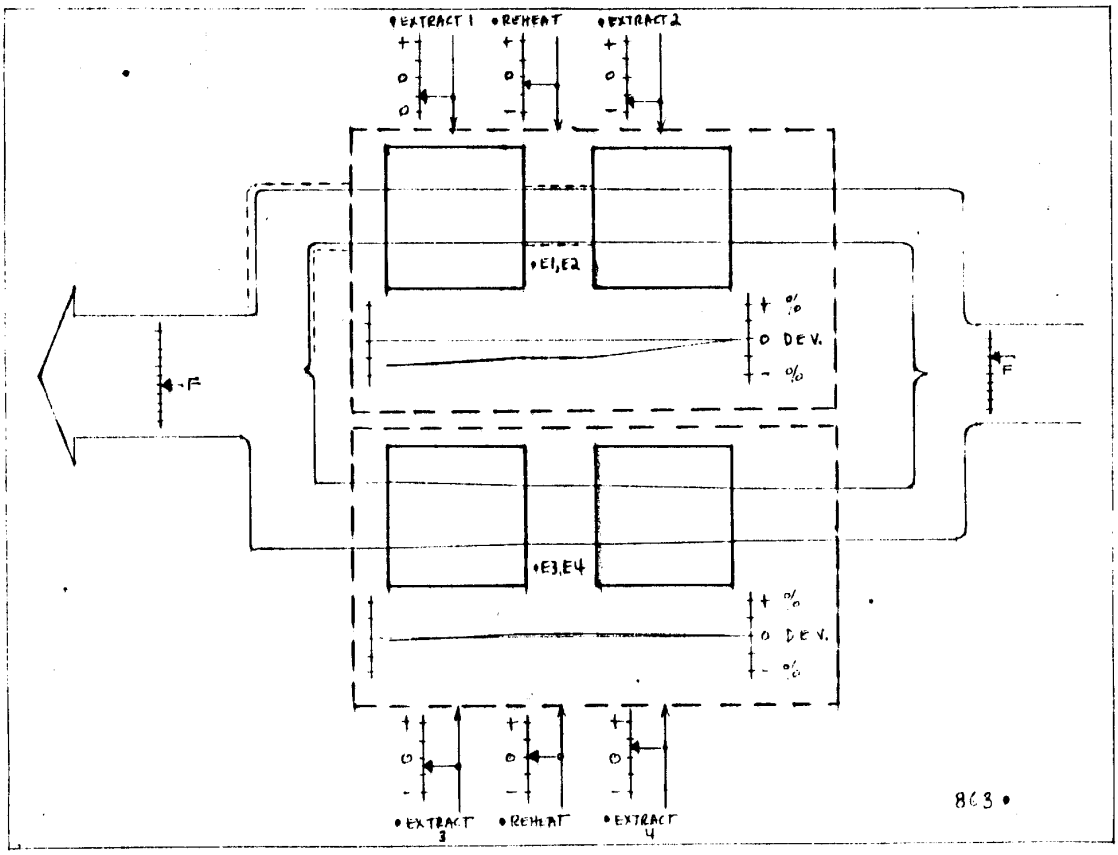
Topographic Search

The characteristics of topographic search along a flow path can be fitted well to the characteristics of human data processing. Observations and instrument readings can be treated individually, and the simple good/bad results of judgements do not create too much memory strain. The precondition is however that a reference model is available with data compatible with observations for immediate judgement and with clear indications of directed flow paths to control the search strategy. If the operator is not presented with external support in the form of the necessary reference model, he will be left with a complex mental task. Unless he remembers the quantitative reference data, he will have to deduce them from a functional model of the system. Functional models at several levels may be involved (Rasmussen 1977). The flow structure model may be deduced from a higher level intentional model of the system, whereas reference data must be deduced from a lower level model of detailed physical processes. Support information can be presented to the operator in the form of graphic flow diagrams or drawings (fig. 6) with reference data. However, the computer offers the possibility of collecting and storing reference data, comparing the actual data, and presenting the deviation from normal state in an integrated display separating the different causal flow systems. Direct visual identification of the location of the change in the flow system can then be performed.

The advantage of topographic search by judgement of component characteristics represented by the relationships in data sets rather than directly of quantitative magnitudes of data has been mentioned. In this kind of search which implies more complex data processing, the computer clearly offers advantages. A sequential narrowing down of the boundaries of the field (i.e. the extension of plant functions) for which input-output relations and balances are examined can lead to an automatic, hierarchical identification of the location of the fault although possibly not to the detail needed. However, the result can then be used for efficient selection of the content and format of displays to support operator judgements. The speed and capacity of low cost computers available now suggest a more careful consideration of dynamic, on-line state identification for advanced good/bad test of functions, e.g. the use of Kalmann filters or "observers" to check energy balances in non-stationary operational states.



Schematic diagram; in trouble shooting used as topographic map with reference data.



Computer generated energy flow map of feed water preheaters. Deviations from normal directly indicated. (From Goodstein, 1977).

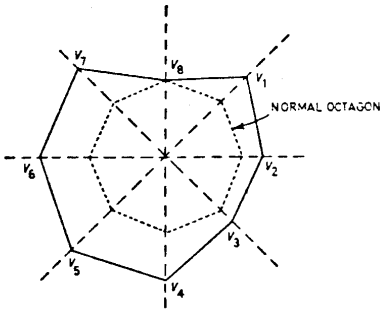
Fig. 6. Examples of flow maps together with reference values.

Search by judgements of relations can be very efficient by computers - human operators are not suited for calculating and testing of relations, unless correctness of relations can be judged visually by special displays which are inherently insensitive to absolute magnitudes or use normalized data (fig. 7).
Topographic search depends on reference models representing intended or normal system operation. Data can be collected on-line by computers, statistically processed and structured into such reference models if the proper operating regimes can be adequately identified.

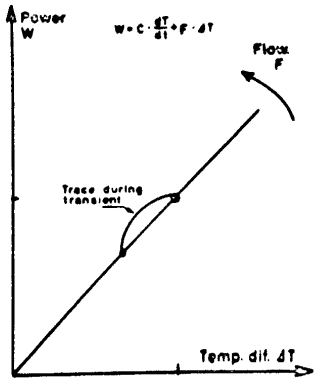
Topographic search can be performed by means of a sequence of tests. Generally, a reference model is chosen which corresponds to a normal operating state of the system. A more efficient search can be obtained, however, if the system can be forced through a sequence of test states which affect different parts of the system in carefully selected combinations and for which reference models can be prepared. Administration and evaluation of such tests depend on logical combinatorial arguments calling for efficient short term memory, and should be automated or the operator should be assisted by an efficient computer book-keeping and display algorithm, as e.g. suggested by Furth et al. (fig. 8).

Topographic search has many elements and subtasks which are eminently suited for computer automation because they are based on causal deductions and logical decisions related to a small set of operating regimes which are chosen by the designer and for which the necessary reference data can be obtained by prior analysis or on-line simulation or data collection.

Traditionally, the information measured in a process plant is supplied to controllers as individual quantities representing physical variables. To support an efficient search in diagnostic tasks, however, the measured information should be combined and transformed to consistent sets of data describing the state in the different causal flow systems. This means that the individual measured data will be used to derive different variables in different overlapping flow structures. Furthermore, computers can readily derive valid reference data for good/bad judgements from statistical processing of measured data.



From Coekin, 1970.



Simple lay-out of display referring to internal relation in data set (heat balance).

From Rasmussen, 1969.

Fig. 7. Displays designed to support operators in the task of good/bad judgements of relations between variables.

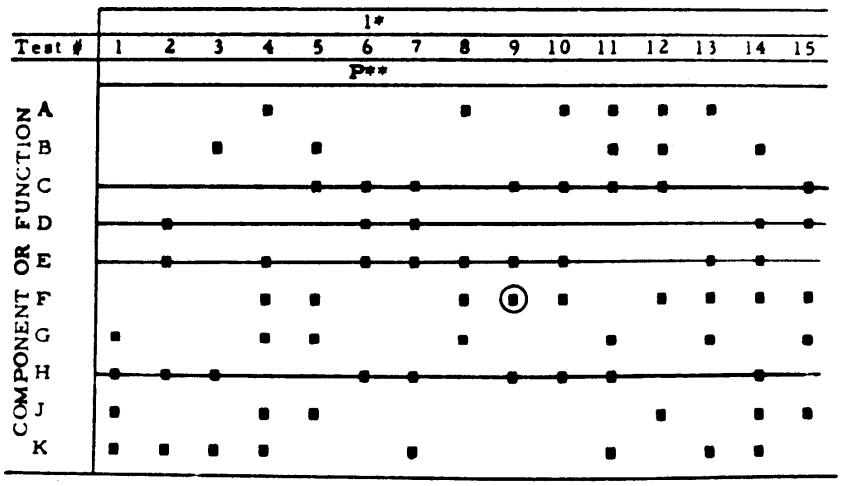


Figure 2a. Elimination of matrix rows as a result of completing Test No. 6.

Fig. 8. Computer generated display designed to assist operators in administration of diagnostic test sequences. Elimination of component or function resulting from a test is indicated by horizontal lines. From Furth et al., 1967.

Automated Topographic Search

Computers are also well suited for storage of information on plant properties in terms of causal flow structures together with rules and relations defining the possible interrelationships between state variables. The computer can deduce reference data and generate normal state models in different domains and configurations and automatically perform a good/bad mapping of the system. As long as effective reference states or operational regimes can be identified and properly defined in a specific abnormal situation, a rather close location of abnormalities can, in principle, be obtained without considering the cause, i.e., whether multiple causes are present etc., and without considering the control intention or the overall goal which is necessary for deciding upon the control action. An appropriate plan for the man-machine cooperation at this stage of the discussion seems to be a scheme where the computer performs a hierarchical and sequential narrowing down of the field of attention in a causal domain to the degree of detail which can be obtained, when only information known to be reliable and valid is used. A graphic presentation of the causal flow structure of the system indicating the state of the disturbed or abnormal flow together with the boundaries within which the source of disturbance has been located, can be a trustworthy support to an operator, who then will have to label the situation in terms of cause, effect, or action to take. The difficult task of structuring and identifying a complex situation which cannot be foreseen by a designer is then left to the man who has the possibility of making an optimal decision. The important aspect in this approach is the fact that the automatic computer analysis can be based on analysis of a set of known and well specified plant operating states and after a sequence of stepwise narrowing of the boundaries around the possible location of the disturbance, the analysis can be terminated when the data or references become uncertain.

The topographic search strategies have the advantage of being universal in many ways. They are related to a general type of plant description, the causal flow map, and are not in their strategic algorithms dependent upon the information describing the actual plant state, only upon result of good/bad judgements. More effort can be justified in development of universal algorithms which are not tied to specific plant types or states.

Symptomatic Search

As we have seen, symptomatic search strategies depend upon reference models representing various specific, abnormal, or unintended plant states. Below we

distinguish the following practical search strategies: Recognition, decision table, hypothesis and test.

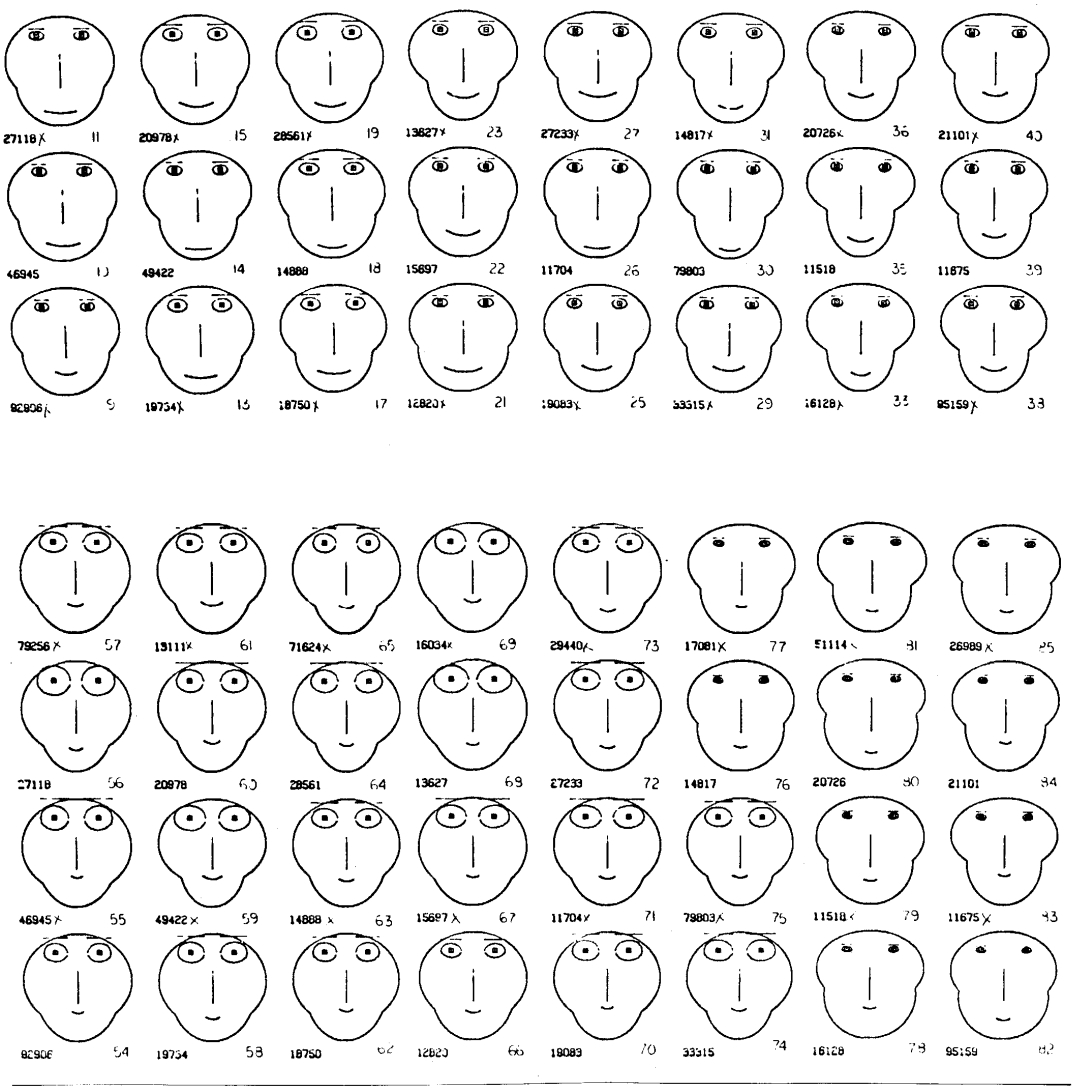


Fig. 9. Display based on the human ability to discriminate face expressions with the purpose of supporting multivariable set classification. From Chernoff, 1971.

Recognition is typically used in familiar situations by human controllers to identify the state of the control object. Direct recognition by perception and associative labelling is only possible if the relevant information is presented simultaneously in parallel - and formatted in proper patterns or structures. Even then recognition will be biased strongly by expectations and "process-feel", and the pattern should be sensitive to changes in all necessary conditions (defining attributes) of the situation and the format must fit population stereotypes for recognition. The computer has been used to compose visual, graphic displays (Chernoff 1971, Coekin 1969) but also composite computer controlled auditive displays

should be investigated, e.g. to keep the operator's dynamic world model - expectations properly updated.

System states can be perceived directly in terms of functional system condition, in terms of cause, effect, or in terms of the appropriate action - depending upon the immediate intention of the operator. Apart from such specific recognitions, the human operator has a capability for fuzzy recognition referring to more general concepts as types or classes of events or states. Such recognitions can be related to secondary sources of information such as noise, instabilities, non-linearities etc. The possibility of fuzzy recognitions should be considered carefully since they can be an important source of bright ideas in search by hypothesis and test.

If information is not available in parallel as an integrated set or picture, but must be collected from separate sources sequentially, recognition by a human operator is no longer a process depending upon perception, but rather a sequential cognitive process depending upon short term memory capacity and logical reasoning. This process is unreliable due to a tendency to adopt strategies which protect the memory from overload by judging observations individually. Thus complex responses due to one single cause will very likely be ascribed the effect of coincident simple causes. A tendency to base recognitions on characteristic signs or cues rather than on the complete, necessary or defining pattern leads to the same effect.

Search by decision table look-up- depends upon a library of reference models related to specific abnormal plant states. The output from the search can be labelled in functional state, cause, effect, or appropriate action; however, care should be taken in the formulation of the output. If action is required according to the result of the search - which will be the case when the matching set defines a dangerous plant state - such action should be performed automatically by a safety system or the message should be formulated as a direct order to an operator with the system designer taking responsibility for correctness. If the operator is considered responsible, the result of the search should be presented as a hypothesis and labelled in concepts related to the domain for which the operator has facilities to perform a test, e.g. in cause or functional state. Even then, the probability of correctness must be high and not only in trivial cases. Therefore, the search should be hierarchically organized and not pursued to more detail than that for which correctness and completeness can be maintained. The library of,abnormal instances will only cover occurrences which are known from experience and analysis, and major problems in this kind of search strategy can be caused by multiple failure situations.

Digital computers are well suited to perform a plant disturbance analysis by decision table based algorithms, especially if the number and locations of measurements in the plant are carefully chosen to secure high resolution of the search (Bevenblut and Whitehouse 1977).

In search by hypothesis and test the reference model representing a hypothetical abnormal plant state is deduced on demand. A functional model representing normal plant anatomy and function is modified according to the hypothesis, and the corresponding hypothetical plant response pattern is deduced by means of the model and compared with the observed set. This is a complex data process with high demand for processing and memory capacity and will only be possible for operators if they are supported very effectively by external means. If this is not the case, they would very probably chose to test the hypothesis by manipulation of the system - i.e. they would probably modify the system to fit their model rather than vice versa.

Functional Models for Hypothesis Testing

Test of a hypothesis by generating a test data pattern from a model of the specific abnormal system state leads to several important constraints on the functional model used. To discuss such constraints, it is necessary to review the characteristics of different types of functional models, as they have been described elsewhere (Rasmussen 1977).

The functional models represent system properties in terms of rules or laws interrelating the individual state variables. This can refer to different levels of abstraction. The rules can be related to the detailed physical - i.e. mechanical, chemical, or electrical - process and connect physical (measurable) variables. This level of modelling will often be needed to generate or modify state data used as references. At a higher level of abstraction, rules can be related to causal paths describing flow of mass, energy, and information. The rules and variables are more general - system independent - and feasible for describing overall plant relations independent of specific hardware detail. Finally, functional properties may be represented in terms of the effect or purpose in relation to the environment, an intentional representation which relates to states and rules given by the environment.

Apart from these categories, another distinction is important. A functional model can be structured as a network of relations interconnecting variables, and it can be structured as a set of objects or functions which are ascribed properties and potential for action. The latter is typical of human verbal reasoning. In this case system variables are represented by collective data as actions, events, and states; and functional rules as properties of interacting objects or functions. System behaviour is predicted by a linear sequence of complex, qualitative cause-effect ar-

guments. By contrast, a model structured in variables and relations is a network of rules connecting quantitative data, and only a data processor having high memory capacity and speed can use this representation efficiently.

An efficient test of a hypothesis can be obtained if a computer is used to generate a quantitative test pattern from a model structured in variables and relations. To use a computer this way to test hypothesis generated by an operator may lead to interface problems. The change to be introduced in the functional model of the computer will be a readjustment of a set of parameters which probably will not be compatible with the concepts used to express hypothesis by an operator, who thinks in terms of components, events, and intentions. Therefore, a translation between expressions based on objects/events and variables/relations will be needed with the purpose to let the computer accept hypothesis expressed in natural language, and to display its operations and results in a way which allows the operator to judge the conditions and factual content of the performance of the computer.
Translation of hypothesis generated by human operators to changes in a computer model will be simplified if the computer operates from an object based cause-and-effect model. This kind of model has - and for the same reason - been developed for qualitative accident analysis (Nielsen 1974) and has been suggested for on-line disturbance analysis (Dahll 1976, Taylor 1977).

To a great extent, present systems are performing "alarm analysis", i.e. the input information is discretized state information, which is used as signs of more complex states of functions or components. Then, the price of better compatibility to operator's language is simplicity and inaccuracy of the model, which can be critical in complex situations.

Overall Diagnostic Strategies

In the design of an efficient overall diagnostic strategy, several aspects must be considered, which can only be evaluated with reference to detailed descriptions of real life work situations. The following considerations are intended to illustrate the elements of the analysis which are needed before the above elementary diagnostic strategies can be put into the proper context.

The changing goal behind the diagnostic task has been mentioned. The domain in which the result of the diagnostic search should emerge depends upon the goal or intention of the diagnostician. Intention to judge system safety and the need for preplanned safety actions is related to identification in terms of endangered critical variables in the data domain; intention to find counteractions in order to avoid automatic safety actions is related to identification in the functional domain; and intention to remove the cause of abnormality is related to identification

in the domain of physical components. In this way, the intention may be subject to change in the course of events, and the ability to transfer results of diagnostic searches among the different domains of representation is important for an efficient diagnostician, be it a man or a machine.

The complexity of industrial process systems, the effect of which is increased in diagnostic situations by the possibility of multiple faults due to coincident causes or consequent failures, often creates a need to structure the search as a sequential lizooming in" through several levels of detail in the field of attention. The switching of level of detail during diagnosis will often be coupled to a need for a change in descriptive domain, as discussed above. The domain which will be chosen for the search in practical situations will very probably not be guided solely by the domain in which the result is needed. If the result can be easily transferred between the different descriptive domains, the search will typically be performed in the domain for which the most efficient strategy is available.

The performance criterion which can be used to judge the efficiency of a diagnostic strategy depends upon the limitations which constrain the data processing in a given situation. The efficiency depends upon a multidimensional fit between demand and processing capacity which will vary in several aspects.

In general, a data processing system will be a multidimensional demand/resource system. The flexibility of such a system very often makes it possible to solve a demand/resource conflict along one of the dimensions by a change in strategy or type of process.

Some dimensions of the resources in data processing typically are:

- the time allowed for the task;

- the amount of input information available or the cost of observations;

- the a priori information on system structure and function or useful analogies (models);

- the capacity of short term memory;

- the capacity of the data processor;

- the code, level of abstraction, used in processing;

- the repertoire of ready-made-solutions;

- the risk, the cost of mistakes.

Demand/resource conflicts in one dimension can be solved by spare capacity in another: Lack of input information can be compensated by use of a more complex model; capacity problems by recoding and "chunking" information to a higher level of abstraction etc.

When planning diagnostic strategies based on man-computer cooperation, it is important to consider the need for the operator to switch between strategies to cope with demand/resource conflicts in real life situations. This aspect may lead to a need for the operator to be able to order a computer to switch strategy with full transfer of intermediate results to match the immediate limitations of the operator's data processing capacity. In passing, it may be noticed that not only should the operator then have the information necessary for the strategy in current use, but he may also need information to judge the efficiency of alternative strategies.

The influence of attitudinal factors is closely connected to this question of alternative strategies. Studies of operator's accept of computer assistance repeatedly emphasize the importance of the fact that operators must understand the strategies used by the computer and be able to predict its responses in order to gain confidence (Halpin et al. 1973).

Constraints Due to Reliability and Safety

The overall reliability of a diagnostic system is of course of prime importance. In a previously published discussion (Rasmussen and Taylor 1976) of problems related to prediction of human reliability, it has been suggested that analysability for risk must be considered to be a vital design criterion in process systems. In essence, the conclusions of this discussion were the following:
Human reliability: Necessary conditions for the use of probabilistic methods to predict the probability that a specified task is performed satisfactorily are:
- there is no significant contribution from systematic errors due to improper activation of operator's intentions, interference from other tasks or activities, etc.;
and

- the task can be broken down to a sequence of independent subtasks at a level where failure data can be obtained from similar work situations;

and

- the subtasks are cued individually by the system or by other external means, so that modification of procedure does not take place;

or

- if task cannot be broken down to independent subtasks, but is performed as one integrated whole or it is based on higher cognitive functions, then the effect of the task must be reversible and surveyed by a predictable monitoring, testing or inspecting function.

In the present context, these conditions represent aspects, which must be considered when planning an interactive diagnostic system of predictable performance. Important considerations are real life goal structures or intentions; the chance of competing tasks; proper cueing of subroutines, etc. As diagnostic tasks are considered to be complex tasks, improvement of reliability by feed back in terms of facilities for test of the effect of intended actions before execution would be desirable.

The ultimate goal of a diagnostic effort is an action upon the system, typically in abnormal situations and therefore typically in the form of non-routine actions. In this situation, the probability of unsafe human acts is important.

In general, the probability of specific, extraneous human acts caused by sporadic errors cannot be quantified. Such acts, however, can be important contributors to rare chains of events leading to accidents.

Therefore, the probability of specific, abnormal events can only be quantified - i.e. related to empirical data if:

- it can be demonstrated that sporadic human acts are not significant contributers to the probability; if necessary by introduction of interlocks or barriers which prevent human interaction;
or
- the effects of human acts are reversible and detectable by a monitoring or safety function which can be performed by operators or automatically, and for which the reliability can be analysed.

In other words, this means that to be able to analyse and predict risk systematically in high consequence/low probability situations, it is necessary to aim at a design which does not bring operators in irreversible act situations. This criterion leads to a "policy of shared responsibility". The designer takes responsibility for system safety. Protective actions are then either automated or demanded of operators through clear orders based on automatic diagnosis; whereas the operator's responsibility will be to maintain production through timely counter-

action to prevent excessive safety measures and by adequate testing and maintenance.

Redundancy and diversLLZ are important means for improvement of system reliability. In this respect it should be noted that the different diagnostic strategies use different aspects of the information content in observations and depend upon different kinds of models and processes. Therefore, use of the strategies for mutual test and verification can introduce the effects of redundancy in the diagnostic process.

Concluding Remarks

The preceding discussion has touched upon several isolated aspects of the diagnostic task in control room environments. To discuss these aspects in the content of the work situations of real life and to judge the possibility for efficient computer support of operators, a detailed analysis of a number of reference situations is necessary. Such analysis must lead to realistic scenarios which can serve as basis for evaluation of overall strategies and for planning of simulator experiments. Such work is currently in progress as a part of a joint Scandinavian project.

References

Berenblut, B.J. and H.B. Whitehouse (1977): A Method for Monitoring Process Plant Based on a Decision Table Analysis. The Chemical Engineer, March 1977, pp. 175-181.

Chernoff, H. (1971): The Use of Faces to Represent Points in n-Dimensional Space Graphically. Department of Statistics, Stanford University California, Tech. Report No. 71, 1971.

Coekin, J.A. (1970): An Oscilloscope Polar Coordinate Display for Multidimensional Data. The Radio and Electronics Engineer, Vol. 40, No. 2, August 1970, pp. 97-101.

Dahll, G. and R. Grumbach (1976): On-Line Analysis of Abnormal Plant Situations. Presented at OECD Halden Project Meeting, Sanderst6len, Norway, March 1976.

Furth, E., G. Grant and H. Smithline (1967): Data Conditioning and Display for Apollo Prelaunch Checkout. Test Matrix Technique. Dunlapp and Associates; NASA, N-68-12531, 1967.

Goodstein, L.P. (1977): Working Paper on Displays. Private Communication.

Halpin, S.M., E.M. Johnson and J.A. Thornberry (1973): Cognitive Reliability in Manned Systems. IEEE Trans. on Reliability, Vol. R-22, No. 3, August 1973, pp. 165-169.

Nielsen, D.S. (1974): Use of Cause-Consequence Charts in Practical Systems Analysis. (In: Reliability and Fault Tree Analysis. Theoretical and Applied Aspects of Systems Reliability and Safety Assessment. Papers of the Conference on Reliability and Fault Tree Analysis, Berkley, September 3-7, 1974). (Society for Industrial and Applied Mathematics, Philadelphia, 1975), pp. 849-880.

Rasmussen, J. (1969): Man-Machine Communication in the Light of Accident Records. Int. Symp. on M-M Systems, Cambridge. IEE Conf. Records No. 69 (58-MMS, Vol. 3).

Rasmussen, J. and J.R. Taylor (1976): Notes on Human Factors Problems in Process Plant Reliability and Safety Prediction. Riso-M-1894.

Rasmussen, J. (1977): Man as a System Component. In: Smith, H. and Green, Th. (Eds): Man-Computer Research, Academic Press. To be published.

Taylor, J.R. and E. Hollo (1977): Experience with Algorithms for Automatic Failure Analysis. Presented at the International Conference on Nuclear Systems Reliability Engineering and Risk Assessment, Gatlinburg, Tennessee, June 20-24, 1977. To be published by SIAM.