The Operator's Diagnosis Task under Abnormal Operating Conditions in Industrial Process Plant

Goodstein, L.P.; Pedersen, O.M.; Rasmussen, Jens; Skanborg, P.Z.

Publication date:
1974

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

Risö-M-1729

Risö-M-1729

Danish Atomic Energy Commission

Research Establishment Risö

ELECTRONICS DEPARTMENT

The Operator's Diagnosis Task
under Abnormal Operating Conditions
in Industrial Process Plant

by
L.P. Goodstein
O.M. Pedersen
J. Rasmussen
P.Z. Skanborg

June 1974

R-9-74

Available on request from: Library of the Danish Atomic Energy Commission
(Atomenergikommissionens Bibliotek), Risö, DK-4000 Roskilde, Denmark.
Telephone: (03) 355101, telex: 5072

A. E. K. Risø

Risø - M - 1729

Risø - M - 1729

Title and author(s)

The Operator's Diagnosis Task under Abnormal Operating Conditions in Industrial Process Plant

by

L.P. Goodstein
O.M. Pedersen
J. Rasmussen
P.Z. Skanborg

Date 20.6.1974

Department or group

Electronic

Group's own registration number(s)

pages + tables + illustrations

Abstract

Analysis of serious accidents in connection with the operation of technical installations demonstrate that the diagnosis task which confronts operations personnel under non-normal plant conditions is a critical one. This report presents a preliminary outline of characteristic traits connected with the task of diagnosis for use in discussions of (a) the studies which are necessary in order to formulate the operator's diagnostic procedures and (b) the possibilities which exist for supporting these procedures through appropriate data processing and display in the control system. At the same time, attempts are made to connect ideas for display which currently are under consideration in the department to various phases of the diagnostic task which itself is postulated as being divided up into a sequence of subtasks each with its own typical features.

Copies to

Available on request from the Library of the Danish Atomic Energy Commission (Atomenergikommissionens Bibliotek), Risø, DK-4000 Roskilde, Denmark
Telephone: (03) 35 51 01, ext. 334, telex: 43116

Fi 25-204

Non-normal operating conditions

Interest is concentrated in. this paper on non-normal operating conditions which can develop into accidents with serious consequences for the plant in the form of equipment damage but where the operating personnel have the possibility for taking corrective action.

Typically this implies that

(a) changes in the plant's primary process have occurred due either to technical failures or to improper maneuvers which directly influence the control of large amounts of energy but where there exists sufficient delay between the detection of these changes by the operator and their ultimate consequence because of integration effects in a disturbed energy balance or time lag in a mass or information flow,

or that

(b) plant conditions have been affected, for example, by a disturbance in an auxiliary system without a direct and immediate consequence for the primary process.

In order to give structure to the following discussion, the diagnosis task is Split into the various phases listed below. In any given situation, however, some of these might well be omitted or inter-changed.

(1) detection of a change which in the operator's judgement may develop into an event chain.

(2) identification of both the ultimate level of risk to which the situation can lead as well as the current proximity to that level (in time or in terms of the probable chain of events) - "what can go wrong and when?"; i.e., a prediction of the cause-consequence pattern.

(3) identification of the control parameters) which when adjusted will minimize the level of risk.

(4) correcting adjustments

(5) localisation of the primary cause "where is the failure?".

(6) repair

In general, it will be noted that considerable importance is attached in the discussion to ways & means of maximizing the gain in operator experience from the diagnostic tasks he is confronted with and supporting his utilization of this experience under subsequent diagnosis.

Detection of non-normal conditions

In modern process plant, hazardous changes in operating conditions are-usually detected by the control system's alarming function. The alarm system i,,3 the tool employed to detect those non-normal states which can be defined with reasonable confidence beforehand by the control designer and can be expressed in terms of an alarm limit.

At the same time, there are indications 'that an operator often can detect an abnormal situation before it has developed to the point where one or another alarm limit is exceeded. This pre-alarm detection is important because

(1) it can extend significantly the time available to -the operator for correction.

(2) it can make use of the operator s perception of the specific situation - a situation which the system designer may not have been able to predict and therefore is not covered by the alarm system.

It is possible that pre-alarm detection can' be enhanced by presenting deviations in data - which incidentally do not have to be restricted to measurements of the process' physical variables - from fixed or experience-based normal values. This can be done in a simple way; for example, by resorting to the use of variations in light intensity on a CRT screen, a method which also permits viewing a large amount of data at the same time and which therefore can lead to a reasonable easy detection.

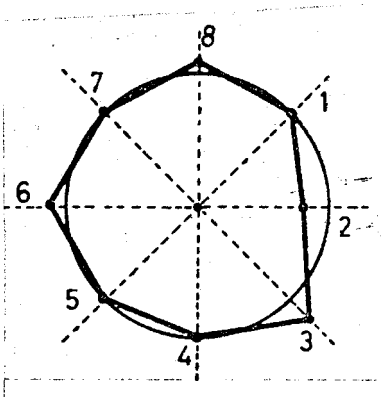
After repair and modification periods it is hot improbable that a process plant will be left in a unrecognized state which is not guarded against by the norm al protective system. Operations personnel should therefore be especially alert after these periods in order to detect such failures and assure that the start-up operation proceeds normally.

Alarm systems usually detect either the deviation of process variables from their full-load values or the exceeding of limits by these variables and therefore can be ineffective during a start-up. The operator can be aided by having these limits automatically altered concurrently with the changes in operating conditions during the start-up. One could also let the alarm system monitor the inter-variable behavior for those parameters directly related to energy and mass balances.

In addition, the operator can be helped in attaining a good overall picture of plant conditions and generating for himself a solid notion of what "normal" is.

Advanced display techniques offer rich possibilities for achieving this objective.

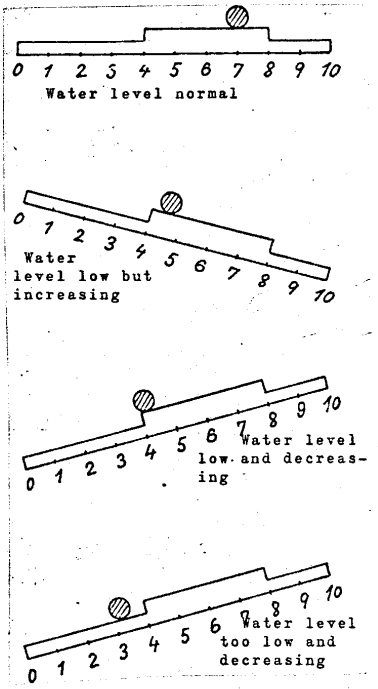
For example, the computer could store information on the past behavior of all signals from which it would be possible the instrumentation system to define an area of experience-based normality. Allowable tolerances would depend on such things as the variations in individual operator behaviour.



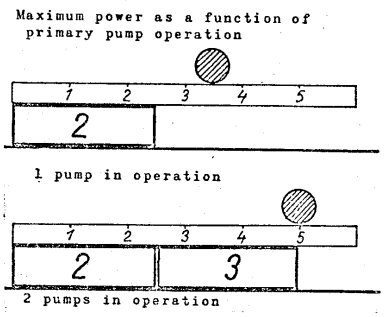
Polar coordinate display with "normal circle"
Coekin 1970

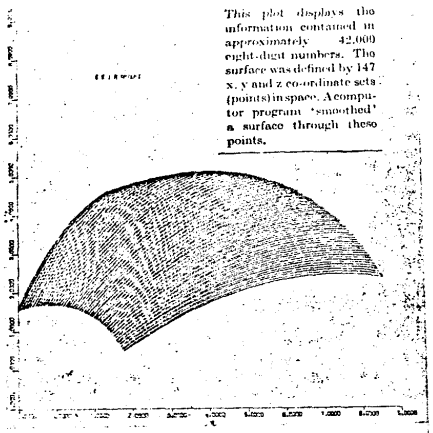
Since pre-alarm detection amounts actually to a kind of "screening" of the entire plant, one could imagine as a supplement to the normal alarm system a form for simultaneous dynamic display of relevant process data formatted so as to facilitate the detection of deviations from normal and, at the same time, enhance the operators use of his pattern-recognition faculties to ai in an identification of the deviation. An illustration from Coekin (1970) gives such an example.

In order to obtain more detailed information, several variables can be shown simultaneously in a way which utilizes the feeling of inherent instability in certain figures from everyday life. See the examples for the display of water level and maximum power. Formats in which changes are easy to recognize because of their graphical form - such as the spiral (phase-plane) representation of a servo-transient (Wohl 1965 for testing Apollo)- also can be employed. Similar ideas led to the survey display for a power plant boiler (see opposite) where the normal profile is "frozen" and subsequent deviations become readily apparent in the form of zero-point shifts. A suggestion by Bowens (1967) illustrates the possibilities for detecting changes in large data sets.

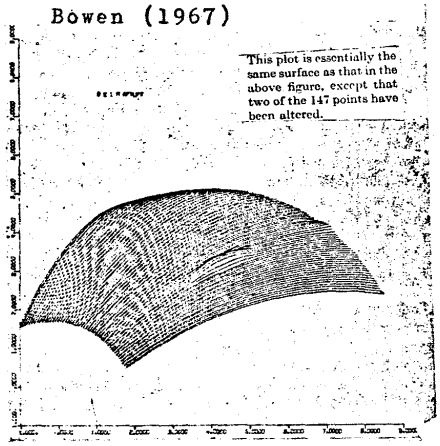


Early detection of a change in a variable and its ultimate effects due to integration build-ups can be aided by a display of the parameter vs. time (trend curve) on a recorder or CRT. The opposite page illustrates possible ways for direct graphic representation of rate-of-change information within the formatting of the parameter itself. This could be used as a supplement for the normal trend displays. A predictive display which extends a recorder curve a little way into the future can have a similar effect.

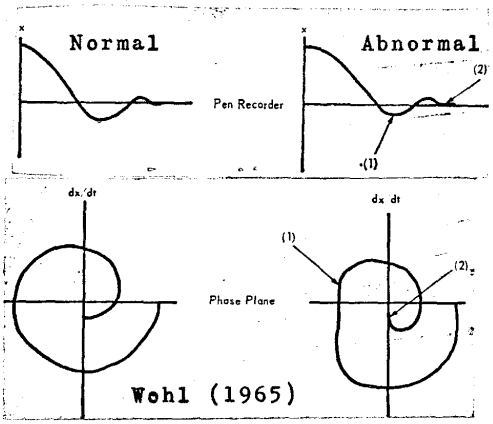




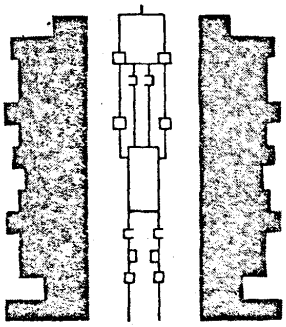
Bowen (1967)



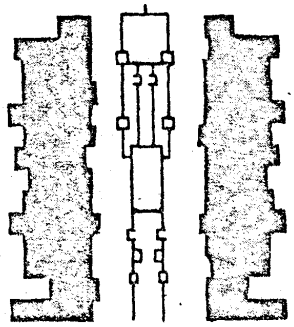
Displaying many coordinates to detect errors.



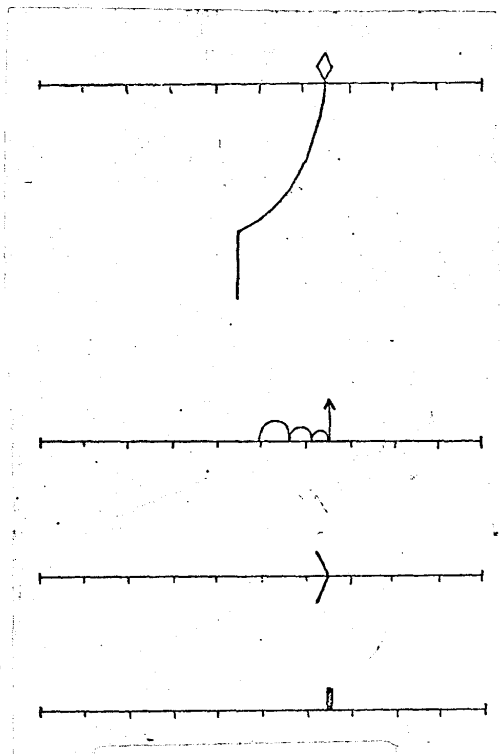
Wohl (1965)



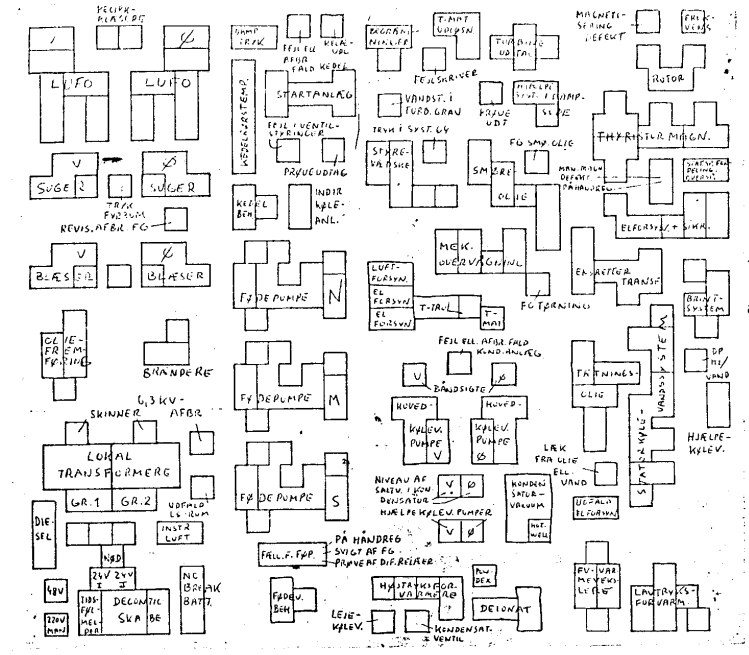
Normal Profile



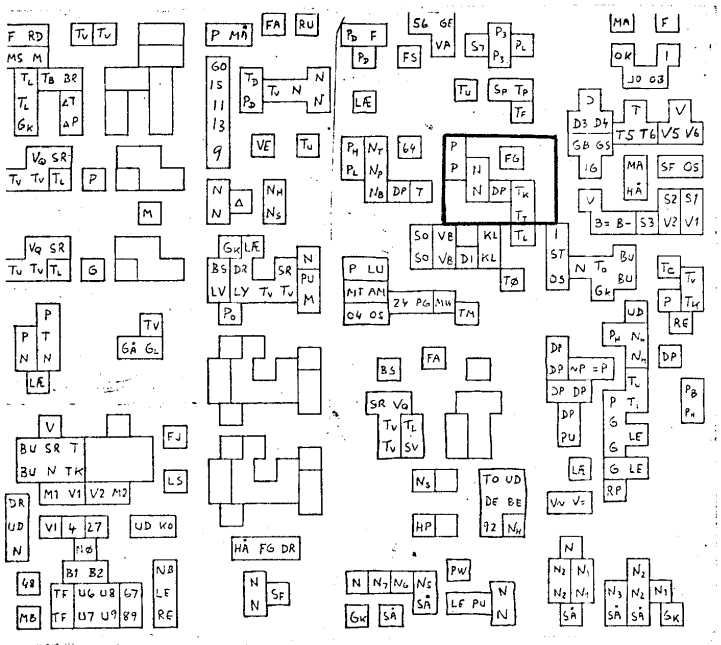
Actual Profile



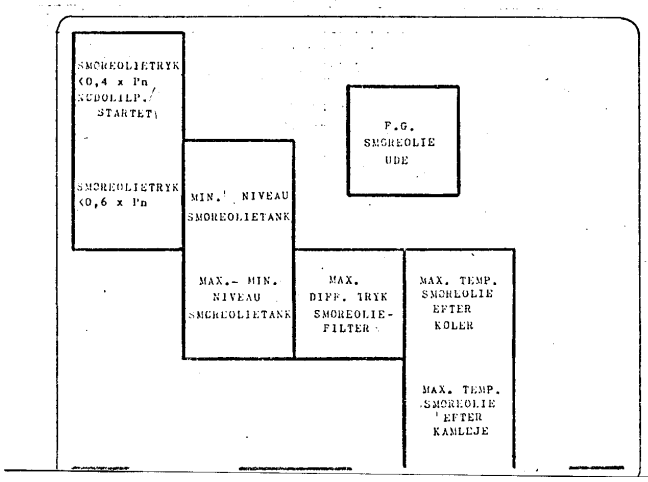
Rate-of-change Information



Alarm display format according to function



Alarm text abbreviations within the functional format together with the window for selecting details

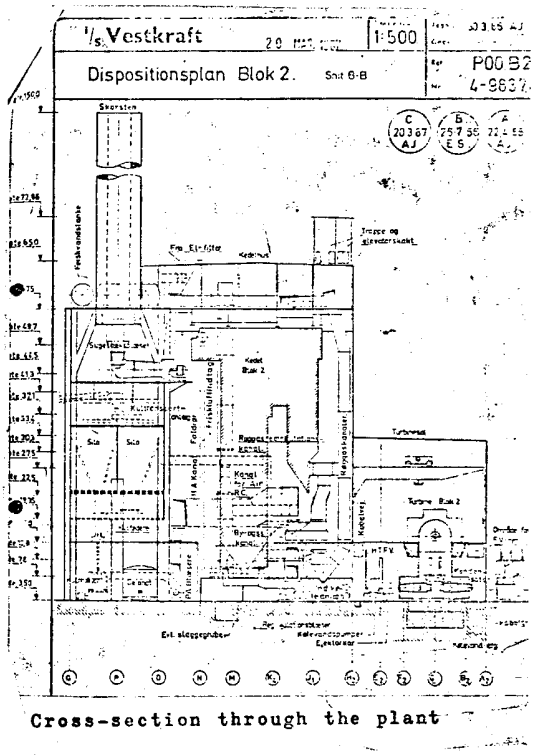


Detail within the window

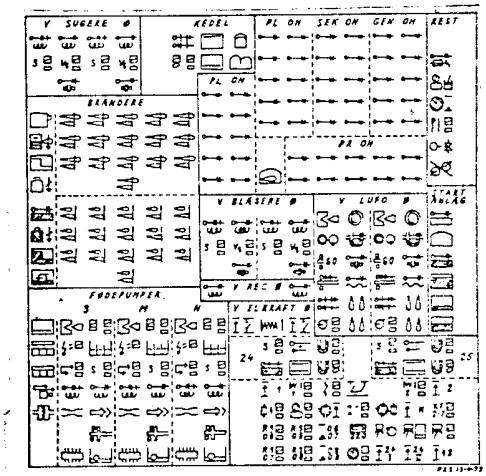
"What can go wrong and when" Identification of ultimate risk level and its imminence

The situation is complicated by the fact that the plant's state is determined both by the plant itself and the automatic control system so that the various control loops can make it difficult for the operator to identify the situation simply by observing plant behaviour.

Possibilities for an operator action will depend on the delay associated with an incident's propagation through the plant or on integration effects from an energy balance disturbance which eventually can result in a dangerous trend in the form of high temperature, pressure, etc. or on the delay associated with a mass or information flow. This phase of the diagnosis is therefore a rough evaluation of both the time available as well as the cause-consequence chain between the incident and possible. consequences with significant energy release, plant damage, etc. In a well-protected plant with many alarm inputs, an overview of the alarm grouping with respect to primary process or auxiliary system will often permit such a quick and direct first diagnosis. This is especially true for the conventional alarm displays where plant state is characterized by a pattern of alarms. On the other hand, a chronological alarm listing in text form tends to worsen this overview by mixing alarms together. As an aid during this initial phase (see opposite) is suggested a graphic presentation which groups alarms according to-the plants functional structure. Similarly, another possibility (see margin) describes a geographic grouping. These two displays are condemned mainly with this first rough evaluation by the operator and therefore concentrate more on the relation between alarms and plant than on an identification of individual alarms. However, this is also possible



Cross-section through the plant



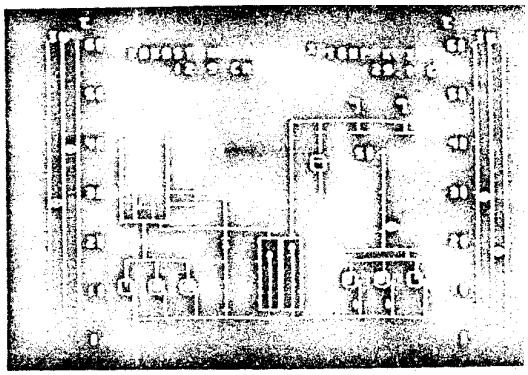
A geographically equivalent display format of all boiler system alarms (approx. 240) together with the symbols used for the individual alarms

through the use, in the one case, of abbreviations and, in the other, of symbols (a la traffic signs).

In the long run, a sorting out of alarms according to their location in the plant could be carried out in the computer by means of an analysis of the alarms and process data. It is considerably simpler to identify the non-normal plant sections than it is to establish primary cause because of the enormous number of 'possibilities for single and combination failures which must be taken into account.

Identification of the control parameter and correction

The next phase is an identification of the control parameter which can be adjusted to avoid possible consequences at high energy levels in the form of damage or a drastic intervention by the automatic protection system. It is still not necessary to identify the primary cause. The task is to delay or stop the incident's propagation, for example, by re-establishing temporarily the disturbed balance so that any integration effects in the form of increasing temperature or pressure caused by the unbalance are restrained before d dangerous level is reached. An increasing temperature can be brought under control by reducing the input energy regardless of whether the increase is due to energy transfer, reduced loading or ineffective cooling. In this connection, there is a need for summary information the flow system in question with a display of the conditions in the input and output lines plus status of the associated controls. Appropriate formats probably are flow diagrams or mimic schema with display of all control organs and their positions. A simple display of this type is illustrated for the DR 2 reactor system discussed in Rasmussen (1974), the process data displayed here should be converted to variables which balance directly - in the



Survey of the reactor primary (left) and secondary (right) cooling system illustrating the combination of two related half pictures.

The primary cooling system shows pertinent quantitative flow and temperature data, combined with a symbolic representation of the reactor core, cooling pumps and heat exchangers. Operational states of the pumps can also be displayed.

The secondary cooling system shows flow and temperature information. The cooling tower with its blowers and a representation of the water level are shown. The blowers can indicate off, half-speed or full-speed.

If the two pictures are interchanged, the temperatures are close for comparisons.

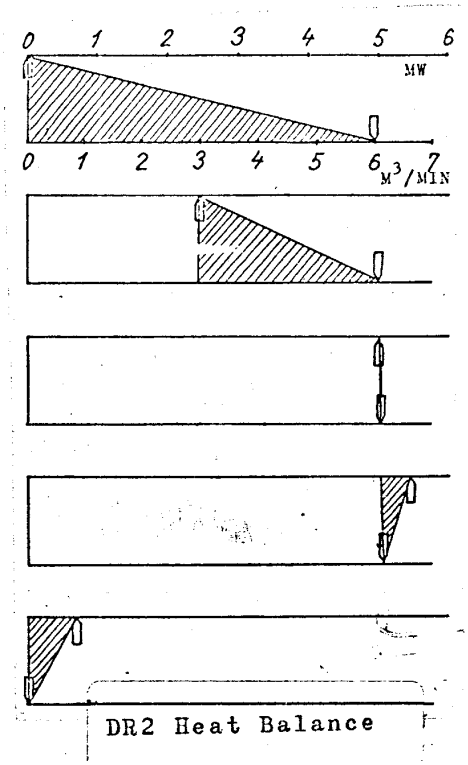
When information is presented by analog devices such as meters and recorders, the visual representations form by themselves a spatial, temporal world, which may be accepted by the subconscious processor; the operator may work "from the expression on the face of the system".

The control surface will be the face of the operator's console, and familiar "face expressions" or data patterns may initiate trained routines, which are repetitious of actions previously found successful.

The closer the temporal, spatial world formed by the visual representations of the information is related to the primary dynamic process, the more capable the man will be to improvise if new, unique situations appear. Every car driver has met critical situations in traffic, which have only been managed due to the improvisations of the subconscious main processor (----whew!).

Rasmussen (1974)

form of indications of both inlet and outlet flow rates as well as the coolant level between this task and continuing his diagnosis.

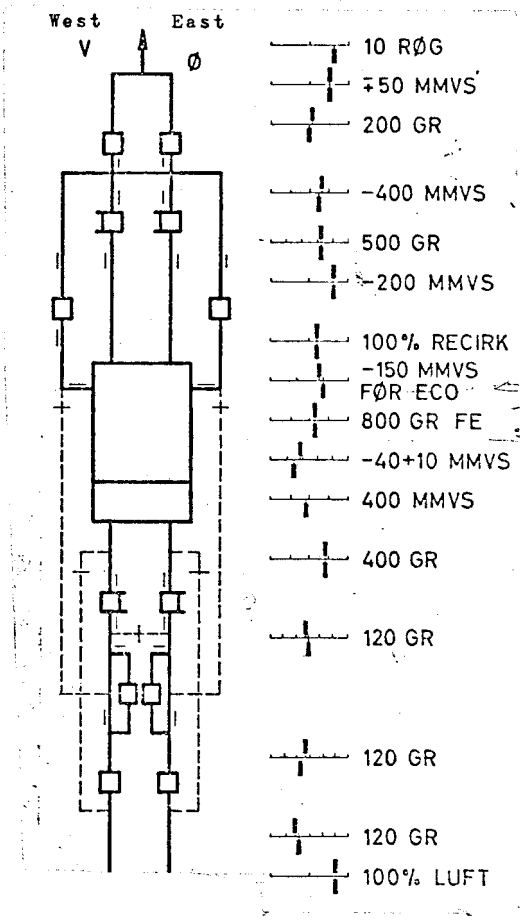


In some cases, support in the form of predictive displays could be considered. These have already been employed, for example, in reactor plants to predict Xenon poisoning.

To monitor any corrective action, a trend display or one of the previously mentioned suggestions for indicating a parameter's rate-of-change can be advantageous in permitting an early evaluation of a transient's final level.

Locating the primary cause

After the plant is brought to a provisional yet safe condition, the primary cause must be located and corrected. In this connection, it is important to remember that the more complicated failure situations often can be a combination of several primary causes including errors committed during repair or inspection tasks. It is therefore doubtful that an extensive automatic analysis will be appropriate. If it is to be more or less complete, its implementation will be expensive and its results often too conservative; if it is not, then the analysis can be misleading or, at best, trivial.



A better basis for assistance would be to support the operator's initiative and use of his own procedures.

The task is to encircle and find the geographical location of the failure; i.e., where the component is physically. Some analogies derived from an earlier investigation of trouble-shooting behaviour in a group repairing electronic instruments (Rasmussen and Jensen (1973) can be relevant here as a starting point.

The first rough localization resembles the

"functional search" with which electronic trouble-shooting begins. The failure is traced to the subsystem with the defective function

Subsequent trouble-shooting can take place in basically different ways. One employs a general search procedure which takes place along the main flow paths through the sub-system. At relevant points along the way simple good/bad -judgements are made to establish whether the status is normal.

This amounts to a topological search an . d requires as support a diagram (road map) of the system with information on normal values. In practice,

the conditions a path are not directly measurable but must be derived from secondary" information in the control room. In a similar manner, a diagram from the "drawing-file" often must be used both as the road map and as a support for deriving actual plant conditions from the available data.

In this search procedure, the variables must be related to details in the process state and component functioning along flow path instead of to the flow balance in the system. Therefore diagrams such as the one suggested in the margin can be useful.

Often the operator will have a hypothesis about -the cause of failure based, perhaps on experience. In these cases, the search procedure can take on another form. A guess is made about the failure, and, using his knowledge of the plant's anatomy and functioning, the operator evaluates the likely consequences of the hypothesized failure including their effects on the displayed information in the control room. Thereafter the hypothesis may be tested by comparison with the actual indications.

Thus it is relevant in this connection to talk about support in the generating and testing of hypotheses.

The operator's formulation of hypotheses can be stimulated by supporting his reasoning with overall functional diagrams showing the connections between systems regardless of whether they relate to air, water, power, instrumentation, etc. Normally these are only available separately This need was recognized in an earlier study which suggested documentation in a flexible form with the assistance of a computer supplied with the information and programs required, for example, to display

- process data under various characteristic situations

- actual connections, for example, geographical, between various plant subsystems, common supplies, common detector locations, common drain systems, etc.

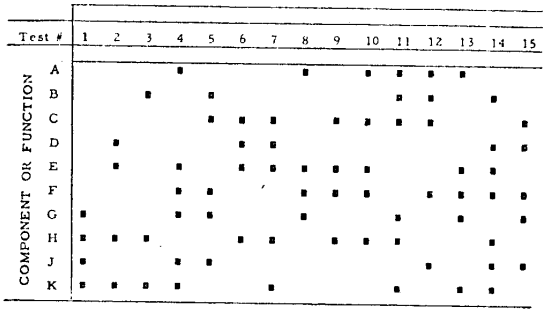


Figure 6. Example of a test matrix display for use in fault isolation. (Cell entries indicate components or functions which must be satisfactory in order for a given test to pass.)

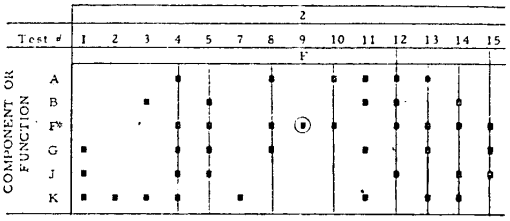


Figure 10. Further reduction of the test matrix following identification of F as a failed component. All tests involving F will fail and therefore can be eliminated from further consideration.

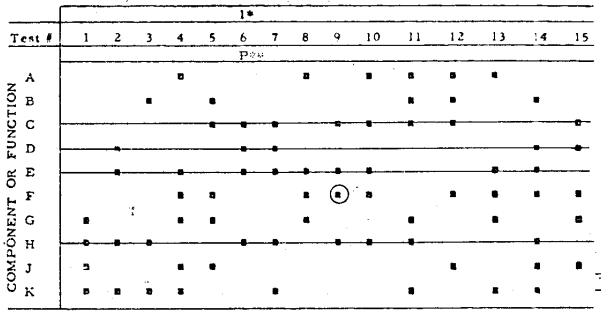


Figure 8. Elimination of matrix rows as a result of completing Test No. 6.

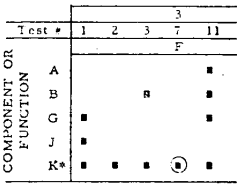


Figure 11. The reduced matrix after all tests involving F are deleted and test number 7 fails.

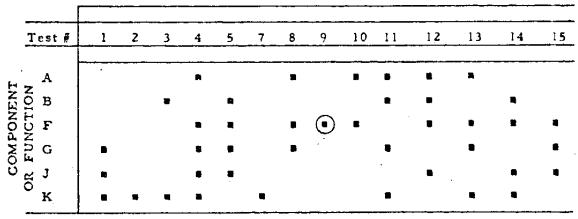


Figure 9. The reduced matrix, showing that Test No. 9 has now been reduced to a single-component test for Component F.

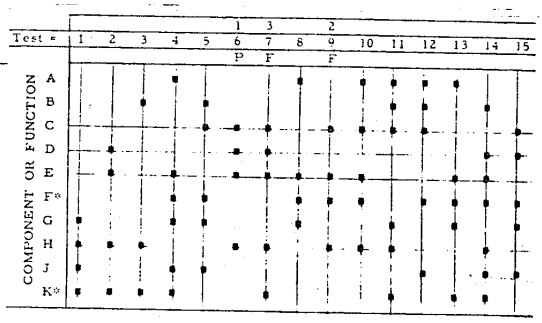


Figure 12. The original matrix, showing all columns and rows eliminated as a result of three tests. Components C, D, E, and H are good; F and K are failed; A, B, G, and J are non-resolvable given the present set of tests and their outcomes.

*Order in which tests are run.

**Test outcome: P = Pass; F = Fail

Wohl (1965)

Instead of supporting hypothesis generation through an automatic diagnosis facility, it would be preferable to provide the operator with more suitable search procedures. Built-in test facilities should be considered together with assistance in the operator's choice of test-strategy; for example, in the form of test-matrices as suggested by Wohl, (1965) for checkout of the Apollo system.

Test of a hypothesis can be supported by ensuring that the operator has access to a collective set of relevant data, structured according to subsystem and function so that he is given direct assistance in remembering the causal relationships within the system.

The operator is likely to consider first the most probable hypotheses which furthermore might be based on just a few typical indications. From a safety point-of-view, it is more desirable of course to investigate first the riskier situations even though their occurrence is much less likely. Instead of forcing this consideration on the operator, for example, through a conservative automatic diagnosis facility, it would be better to help him through a quick t est of these most likely hypotheses and, at the same time, avoid the typical human tendency to "see only what one wishes to see", confirmed by a few typical observations.

These "most likely" hypotheses will be those the operator has experienced earlier. It may become realistic to collect system -based "experience" by giving the operator the possibility for "freezing" abnormal data sets in a store. After a successful diagnosis the corresponding data set can be labeled by writing in the primary cause.,These sets can be used later for quick tests of a hypothesis. Or should there be placed more emphasis on built-in test facilities?

In a discussion of the trouble-shooting procedure, it is important to consider the difficulties which can arise if the plant is shut-down. These difficulties relate to the need for "freezing" process data describing the abnormal pre-shut-down state and possible problems with carrying out realistic functional tests during shut-down.

Conclusions

As stated earlier, these speculations serve only as a rough outline to illustrate different aspects of the diagnostic task ,and to connect an existing set of ideas and suggestions for displays with the various requirements associated with these phases.

However, a more detailed and realistic definition of the various diagnostic phases based on control room studies is necessary as well as a better formulation of the Situations where the operator actually is confronted with a diagnostic task. In parallel with this,, various display ideas can be tested separately by means of simpler laboratory experiments.

Accordingly, the following is a short summary of the current program:

1. Gathering of case stories in order to characterize and evaluate the operator's]ob and work situation.

2. Studies in the control room in order to specify the task phases and procedures employed.

3. Evaluation of appropriate procedures and the possibilities for supporting them through an integrated data processing and display system.

4. Testing of detailed proposals through laboratory experiments.

5. Eventual experiments - preferably with a simulator - using trained operators for testing of the complete system.

In addition, the possibilities for computer collection of process data which can be used to establish "experience-based" normal/abnormal plant conditions will be studied.

List of references

(1) Bowens, H.M. "The Imp. in the System" from "The Human operator in Complex Systems" - Singleton et al (editors) Taylor & Francis Ltd. 1967.

(2) Wohl, J.G. "Man-Machine Relationship in Prelaunch Checkout of Advanced Space Vehicles" Report SSD-65-236 Dunlop & Associates 1965.

(3) Pedersen, O.M. "En analyse af operatorernes behov for kontrolrumsinforma-tion under opstarten af en kraftværkskedel" Riso-M-1693 March 1974.

(4) Rasmussen, J. "Human Dataprocessor as a System Component Bits & Pieces of a model" - In preparation 1974.

(5) Rasmussen'. J. & Jensen, A. "A Study of Mental Procedures in Electronic Trouble Shooting" - Riso-M-1582 - R-3-73, February 1973.

(6) Coekin, J.A. "An Oscilloscope Polar Coordinate Display for Multidimensional Data" - Radio & Electronic Engineer August 1970.

(7) All of the display suggestions without specific references are taken from earlier Risø studies which are described in various unpublished internal reports.