Man-machine communication in the light of accident record

Rasmussen, Jens

Published in:
Proceedings

Publication date:
1969

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

Danish Atomic Energy Commission

Research Establishment Risö

ELECTRONICS DEPARTMENT

MAN-MACHINE COMMUNICATION IN THE LIGHT OF ACCIDENT RECORDS

by

Jens Rasmussen

July 1969

Reprint of paper

S-1-69

IEEE-GMMS, ERS International Symposium on Man-Machine Systems, Cambridge, 1969.

ABSTRACT

In the design of automatic control systems for industrial process plants the designer has to realise that he cannot possibly foresee and analyse all relevant operational conditions of the plant; in certain circumstances he must rely upon an intelligent human operator for the identification and correction of abnormal plant behaviour. He must consider that the operator, for his diagnosis and decision, needs information describing the anatomy and behaviour of the plant that is not needed during normal operation, as well as detailed information on the actual operational state.

In this situation the digital process computer and the related new media for information display offer a great capacity for storing information resulting from plant design considerations as well as a highly efficient means of reduction and conditioning of the information to be displayed to the operator.

In the search for information describing the properties of the intelligent operator to facilitate the design of advanced display systems, published records of accidents and incidents in nuclear plants and of aircraft accidents have been reviewed.

In this review, emphasis is placed not upon cases initiated by human operators, but upon those cases in which the human operator has failed to correct abnormal conditions. The findings are correlated with a simple functional model of the operator which divides his task into detection, identification, decision, and manipulation.

In particular the cases indicating difficulties in the task of identification are discussed as they place special demands on the display coding. In the identification task the operator is faced with a conflict between different goals minimisation of average cost or of immediate risk, and different mental models are available to him. The situation is clearly exemplified by Lalande, who failed to discover Neptune in 1795 - (Jerome S. Bruner, A study of thinking, p. 104).

1 INTRODUCTION

In highly automated plants a variety of tasks must still be allocated to the human operator, as the automation of routine tasks in itself creates the need for supervision and checking. Ideally all tasks should be evaluated and planned in advance by the system designer, and to-day the process computer should be considered as it is an excellent tool for processing and storing of information and procedures to support the operator.

However, in all plants situations arise that cannot be foreseen and evaluated in advance, and during these situations plant safety may depend upon the ability of the human operator to evaluate the circumstances and to improvise the proper correcting actions. In that case the operator has a need for access to a variety of state data from which he can select the proper set to be used in the actual situation.

In conventional control systems the data are presented to the operator by analogue devices (meters, recorders) in a way that has evaluated slowly on the basis of operational experience gained during the simultaneous development of the plants themselves. In these systems the operator has direct access to all data; he may perceive the pattern of several indications simultaneously, or he may choose and read individual data accurately.

The continued development of computer systems will bring about a rapid change in the technology of data display also in industrial plants. As the designer has no explicit formulation of the operator's diagnostic procedures, the best way to ensure proper action by the operator in critical situations appears, even in computer systems, to be that of presenting him with state data in such a way that the tradition from operating experience is maintained, i.e. presentation of measured data and their time history in analogue codes without relying too much on digital data presentation.

To utilize in full the advanced data-conditioning ability of computer systems we need more knowledge of the mental transformation models of the operator in abnormal situations, i.e*' the nature of the system information used by the operator to generate his actions on the basis of the data presented to him.

In this paper some conclusions are drawn from a review of reported accidents in order to isolate critical aspects of the man - machine co-operation. The attention is focussed on the task of identifying abnormal conditions, and a simple model of the operator in a system is presented as a basis for a discussion of the nature of his transformation models and the shift in model and goal needed in abnormal situations. Finally some experiments in trouble shooting tasks are discussed to evaluate the models actually at work in diagnostic tasks, and the categories of mental models with related displays considered in experiments planned for industrial environments are mentioned.

2 REVIEW OF ACCIDENT REPORTS

The human operator has an ability to circumvent deficiencies in the man -machine interface by adaptation to a degree that makes one expect inappropriate display coding to have significant influence only during very complex or stressed periods. It thus appears important to turn

to accident reports to find some indication of the major problems in man - machine communication.

The number of thoroughly reported major incidents or accidents is very low compared with the complexity of the situations and the number of parameters involved. Statistical information on isolated aspects of the human role to be used for 'design purposes cah therefore not be gained from such reports. For this information to be obtained the complex situations have to be broken down to a coincidence of elementary events for which data can be found in isolated experiments or human data banks; Swain (1969), Ablitt (1968).

With this in mind, accidents reported in the nuclear field have been reviewed. In the present paper reference is made to 29 cases with major consequences to plant or personnel reported by "Nuclear Safety" as "Current Events" during the period 1959 to 1965; the accidents include fifteen at reactor plants, nine at chemical treatment plants for radioactive or fissile material and five major cases which arose during handling of radioactive material in hot-cell plants.

Because of the small number of cases and their complexity, only very general aspects - according-to subjective judgement - can be extracted, but the following considerations are deemed to be relevant in the present discussion: Most of the accidents are initiated during periods with non-routine operations (e.g. initial operation, experiments', maintenance). Only a few (-5) are related to operational conditions that have developed into routine, and they are all initiated by technical failures.

Accidents initiated by human mal-operation amount to roughly three quarters of the total number of reported cases, and only in a few (3) cases do simple accidental operations or manipulations ' seem to be of essential consequence, presumably because such simple maloperations have been foreseen and taken into account during system design. In agreement with this, simple maloperations only contribute to the reported accidents if they coincide with other non-routine conditions.

Only in very few cases have the operators had no possibility of preventing accidents due to fast physical reactions (e.g. explosions.), and, taking both the process and the system knowledge of the operator into consideration, it appears that in nearly all cases the operators would have been able to make an appropriate decision and carry through the action if the actual state of the system had been known to them.

The main conclusion of this review is that a most significant aspect of the human role in the reported accidents has been the difficulty of the operator in non-routine situations to identify the conditions under which to operate.

In spite of the low number of cases it seems reasonable to discuss a few aspects in more detail.

In approximately one third of the cases a significant feature of the development of the accident is that a prescribed procedure has not been followed. This means that it has been realized in advance that infrequent, but dangerous deviations in some state parameters may occur, which would not easily be detected by the operator, and therefore procedures taking such infrequent deviations into account have been devised. As such procedures are not operationally

optimal in normal circumstances, they are very likely to be "improved" by the operator during his normal work at the expense of safety margin.

As the operator's capability of adaptation is one of the very reasons for his presence in the plant, it seems appropriate to try to remedy the drawbacks of his adaptation by supplying him with adequate information before resort is had to "stricter administrative control". This discrepancy between situation and human procedure has been typical of the cases related to handling of radioactive sources e.g. in hot cells.

As regards chemical plants for treatment of radioactive and fissile material(solutions) it leaps to the eye t-hat a typical aspect has been the operator's difficulty in identifying the working situation because of the many parameters in a complex system of valves, tubes and vessels, combined with a non-routine task. Therefore the operator acts inappropriately, and he is not able to detect the consequences of his actions because additional cues for detection are not developed in due time.

Because of the nature of the plants and processes in question the accidents in chemical plants follow immediately upon the inappropriate operator actions, whereas this is not typical of cases related to reactor plants.

It seems to be typical of accidents in reactor plants that the plants have been left in an abnormal or unsafe state after periods of special, non- routine operations, repairs, experiments, calibrations, or the like. In the reported cases these states turn into accidents because the console operator does not detect the abnormal state as insufficient data are displayed, or because he does not interpret the data correctly; it is typical that he does not trust data indicating infrequent, but risky states.

Reactor plants are designed in such a way that maloperations may very likely result in automatic shut-down, and to discover whether human performance has different consequences when such a shut-down feature is not present, a review of some hundred reported accidents within air transport have been made. I.C.A.0. (1959 - 1967)-

Even in such cases with no automatic safety action simple human maloperations plays only a small part in the initiation of accidents, and technical failures play a significant part only in a minority of the cases. The majority of the failures can be attributed to the human operator in complex, non-routine situations when he has to adjust his procedures while taking many parameters into consideration (typical of landing operations in bad weather). In our context it is of value to note in the aviation records a clear indication of the human difficulty in taking many parameters into consideration in a stressed situation, especially if the parameters are not presented in the same way (landing in bad weather with both visual and instrument reference).

Very few cases are reported of aeroplanes left unsafe during "shut-down" periods, presumably because work during such periods has developed into established routine, which is not the case in the nuclear systems considered.

It is also interesting to compare the results of a review of reported accidents with the figures obtained by means of reporting systems that include elementary technical and human faults during plant operations. Such a system in operation at the Health and Safety Branch, U. K.,

(Ablitt 1969) has shown 10% human failures, which indicates that human failures are more difficult to foresee by system designers than are technical failures, and thus have a higher probability of developing into serious accidents. It is also interesting to note that the ratio of accidental maloperation to in- correct action is 1:5 in the British data, which show that even in cases of simple faults which do not develop any further, the accidental maloperation is of minor importance.

My conclusion is that the critical task of the display system will **be** to support the operator in the identification of his working conditions during abnormal periods such as periods of initial operation, start-up after major repairs or overhaul, or periods of technical failure. At such times the operator has to consider sets of data describing a great number of parameters; he has to judge the internal relations in such data sets to identify the abnormal state of the system, and parameters of no concern to him during normal operations may be of vital importance for this task. To fulfil this requirement, integrated analogue or graphic displays seem to be more appropriate than alpha-numeric displays.

3 OPERATOR MODEL

It is well known from everyday life and from experiments, Miller (1956), that the human data input capacity is greatly limited, but also that information input capacity is very great in cases of appropriate coding i.e. when data are arranged in patterns related to the mental model of the system available to the operator.

To come closer to a formulation of critical aspects of display coding, the functions of the operator in industrial plants have been discussed, Rasmussen (1968), and a simple schematic model of the operator as seen by a system designer has been formulated to show the outlines of the mental transformation model available to the operator in different tasks.

According to this model, shown in fig. 1, the tasks of the operator may be divided into four separate categories:

First. The normal working routine is an automatic - or unconscious matching of sensed data patterns with trained response patterns. This mode is initiated automatically by the appropriate data patterns and is based upon long-term training in pattern recognition and response coordination. The typical tasks will be regulating and tracking tasks and routine sequences. The transformation model of the operator (the system information stored) will be a trained, unconscious plant response model with no relation to physical understanding or knowledge of the process.

In this mode of functioning the operator may come across data patterns that have no corresponding trained response pattern, and these patterns may be perceived - or detected - and cause a conscious pattern identification.

Secondly. When an unusual situation is thus perceived, it will be evaluated more or less thoroughly, additional state data will be searched, and to classify the condition the pattern will be correlated to a mental model of the system and to the actual goal of operation. The situation may be classified as a condition known from the past according to the operator's experience - which in this context stands for a formal behaviour model of the plant based upon

system information extracted from system performance. In this case the situation will be met by an alternative response based upon trained co-ordination.

Thirdly. Where the conditions are not identified as familiar to the operator, he must, on the basis of fundamental education in plant anatomy, dynamic properties and the physical interpretation of the data available, evaluate the situation according to a mental model, taking into account the physical properties of the plant.

Whereas the goal in the trained response has to a ma-or degree been to optimize the average pay-off, the operator, in is choice between different hypotheses about the plant conditions, may aim at different goals: a "scientific" goal to explain the behaviour (especially relevant to repairs and trouble shooting), an operational goal to ensure continuity of production (considering average cost), or a safety goal to protect the plant or staff (considering immediate risk).

The abnormal conditions may be identified as a situation foreseen and evaluated by the system designer, who has formulated appropriate responses in procedure instructions that make up a formal transformation model for the operator, influencing his identification and controlling the co-ordination of his responses.

Fourth. If the conditions are identified as conditions not foreseen and treated by the designer in the instructional system, the operator must carefully evaluate the plant conditions and predict plant response to different possible countermeasures according to a highly detailed physical understanding of the system and a careful appreciation of the relevant goal. His transformation model has to include very detailed physical and technological properties of the plant, which will also be needed to control the co-ordination of his responses.

This model is not intended to be a psychological model of the mental processes of an operator in a basic task, but a functional model to illustrate general aspects of the operator's situation at a higher level as seen by the system designer; yet it has some similiarities to a psychological model (like that suggested by Gagné (1963), in which the shunting effect is similar to the branching of tasks in the present model).

The conclusion here will be that the goal of the operator as well as the nature of the mental transformation model will be fundamentally different in his diverse tasks, varying from a formal model based upon training, experience or instructions in routine, respectively planned tasks, to models related to detailed physical and technological properties of the system and based upon fundamental education in tasks of evaluation and decision.

A computer-controlled graphic display system offers very effective means of presenting plant data to the operator in a variety of codes related to the actual system conditions, and thus makes the best use of his data capacity. Shifting of display coding in accordance with the working conditions may be a way of breaking up improper routines and assisting the operator to aim at the appropriate goal.

In his book "A Study of Thinking" Bruner (1956 p. 104) mentions as an example of the classical human failure Lalande, who failed to discover the planet Neptune in 1795. Quotation:

> The incident in question occurred in 1795, nine years after the discovery of the planet Uranus, and the principal figure involved was the great French as-

> tronomer Lalande. In that year Lalande failed to discover the planet Neptune, although the logic of events should have led him to it. Lalandc was making a map of the heavens. Every night he would observe and record the stars in a small area, and on a following night would repeat the observations. Once, in a second mapping of a partictilar area, he found that the position of one star relative to others in that part of the map had shifted. Lalande was a good astronomer and knew that such a shift was. unreasonable. He crossed out his first observation of the shifting point of light, put a question mark next to his second observation, and let the matter go. And so, not until half a century later did Neptune get added to the list of planets in the solar system. From the aberrant movement, Lalande might have made the inference not that an error had been made but that a new planet of the solar system \%,as present. But he was reasonable. And it was more reasonable to infer that one had made an error in observation than that one had found a new planet.

This example very nicely illustrates the reactions typical of the human operator in a task of identification or diagnosis. In his mental transformation model Lalande did not refer to a physical system, but he recorded data according to a formal routine. His goal was to collect and record numbers, not to study a physical system; and finally he did not even consider the consequence of his data being correct (the immediate risk) to such a degree that it made him repeat the measurement.

The conclusion is that the operator's mental transformation model of the plant varies fundamentally according to his working conditions, and therefore the coding of data sets will have to change in accordance with the nature of the actual task. These changes should be performed not only to ensure a high information input capacity, but also to break the operator's routines and ensure operation based upon a relevant system model and a proper goal.

4 EXPERIMENTS TO EVALUATE IDENTIFICATION PROCEDURES

The problem is now to describe the mental model of the operator under different operating conditions and the use of this model in the operator's search for data to form and test hypotheses during the task of identification.

We have found it very difficult to break down this task into elementary parts which would make it possible to apply data reported from psychological laboratory experiments, and thus we have felt a great need for man - machine experiments in real industrial environments.

A computer-controlled display system to be installed at the research reactor DR-2 is designed to serve this purpose, Goodstein (1969) and, to have some basic information for the design of the experimental displays, a series of experiments are made to evaluate the mental models of electronic technicians and the way they control the search for state information in troubleshooting tasks.

The experiments are made in co-operation with a group of technicians who have a reputation as efficient trouble shooters, and as we are interested in their mental activities, the experiments are based upon tape recordings of the technicians thinking aloud" during the task. Objects in the troubleshooting tasks are electronic instruments that have some similiarity to

industrial plants as they are systems with different co-operating subsystems and have a reasonable variety-in the way they show their response, so that to some extent the fault can be evaluated directly from "display": multichannel analysers, oscilloscopes and TV-receivers. As subjects were selected technicians who had a relation to the particular instrument as qualified users, but not as trouble-shooting specialists.

In the interpretation of the findings from such experiments one of course has to remember that the goal of instrument trouble shooters differ from that of the plant operators.

From thirty cases in the preliminary set-up of the experiments we have found the procedures used more systematic than would have been found from judging the subjects' manipulations alone.

The conclusions drawn from this preliminary work must necessarily be very premature, but some indications are felt to be justified:

Even in cases where the "display" of information on the CRT of the system (instrument) has rather obvious features which after some reasoning would indicate very closely the fault and the appropriate special procedures, and even if these features are mentioned on the recording by the subject, the only thing he will decide on the basis of the display is probably what subsystem he has to turn his attention to.

Turning to the subsystem in question, he will normally carry through a sequence of systematic routines without considering further information from the initial response of the instrument; he will start with procedures related to his general experience (probability considerations such as: replace vacuum tubes) and proceed to locate deviations (test DC voltages or wave forms according to general knowledge or diagrams) by procedures related closely to a model of normal operation of the system; normally reasoning based upon fundamental understanding of the circuitry (a model related to system physics) does not seem to be used to any great extent.

Generally the procedures seem to be a systematic sequence of simple decisions which in some way minimize the information flow rate needed, so that more complicated evaluations are avoided.

This may be a warning to display designers: Technicians with experience as system operators and repairers have normally developed systematic methods, which in most abnormal cases very efficiently lead to an identification of the fault.

The most likely procedure will be a sequence of simple tests to locate the failing component by judging deviations in state data from a model of normal operation according to experience. In his laboratory work the designer and development engineer will normally not relate his evaluations of system response to simple deviations from a "normal model", but will be forced to use careful reasoning and evaluation of all information available in system response in relation to basic understanding, and he should be careful not to design display coding to his own mental models.

The experiments indicate that it can be very difficult to break routines that the subjects have normally found very efficient. ven in cases specially designed to have obvious short-cut methods, the fault had been found by standard methods.

An important conclusion for our future experiments with computer-generated displays seems to be that the-displays should be in actual operation for a sufficient time to allow the operator to form fixed routines. Not until then will it be possible to judge the efficiency of the displays in identification procedures in case of complex, risky plant conditions during which also causes of low probability have to be considered.

5·EXPERIMENTAL COMPUTER-CONTROLLED DISPLAY SYSTEM

According to this conclusion the computer'-controlled display system mentioned to will be brought into normal operation at the research reactor DR-2, and identification experiments will be carried out only when the use of a particular display coding has turned into routine.

At the present state of the work four typical categories of mental transformation models are considered for the display coding to be used in the experiments in real plant environments:

First. Purely abstract models as generated by the operator from his experience with plant behaviour for which a proper coding will be data in easily recognizable patterns. This type is suitable for monitoring tasks (failure detection), as reference to normal data values can easily be included, and corresponds to the operator's perception of conventional meter indications as patterns (fig. 2).

Secondly. Functional models that represent the physical relation between data in the set describing a situation or a subsystem. These models may be based upon mathematical models of plant response, and the corresponding displays may, as suggested by Wohl (1967) be based upon graphic methods like those normally used in textbooks or graphical design methods to clarify relations between data describing physical processes. This type may be advantageous in the task of identifying the abnormal system, as reference to **nor**mal relations between data can be present (fig- 3).

Thirdly. Models closely related to the technological anatomy of the plant, and which may be supported by display like flow diagrams and "mini" displays, as also used in conventional systems. This type will probably be most suitable for the decision task, where the operator evaluates his countermeasures, during which evaluation he may need support in judging appropriate manipulations.

Fourth. Finally other types of abstract models may come into use when special systematic procedures exist (preplanned procedures or general methods). The display may support logical administration of checks performed by the operator, as the test matrix mentioned by Wohl (1967), or logical reasoning in general, Newmann.(1966).

It is important to bear in mind that the operator has to identify failures in the instruments as well as failures in the plant, and experience from accidents seems to indicate that the operators have a tendency not to trust information from the instrumentation when a very improbable, but perhaps risky condition is indicated, and therefore displays for detection and identification based upon primary measuring data should be at the operator's disposal, leaving him

a possibility of judging the performance of the measuring channels. In such displays the model will be represented by the lay-out of data presented rather than by computer-calculated, derived data.

SUMMARY

A review of accident reports indicates that a critical task of the data display system in an industrial plant is to support the operator in the identification of hi,5,working conditions in abnormal periods. In this task the operator has to consider large sets of data, and Parameters of no con- cern to him during normal operation may be of vital importance.

To fully utilize the data input capacity of the human operator it is important that the coding of data sets presented improperly related to his co mental transformation model. A discussion based upon a simple model of the operator's performance demonstrates how his mental models and his goal have to change according to the actual operating conditions, and it is concluded that the data conditioning capability of a process computer may be an efficient tool for presenting data in a variety of codes to fit his models and to break improper routines.

A great need for information on the nature of the operator's procedures and models is felt, and identification experiments under real plant conditions are planned. Preliminary experiments with electronic trouble-shooting tasks demonstrate the difficulty in breaking a procedure that has turned into routine, and warns the display designer that the diagnostic procedures applied by system operators are different from those of system designers.

ACKNOWLEDGEMENTS

The author gratefully acknowledges the discussions with colleagues in the Electronics Department, especially L. P. Goodstein, who designed the structure of the experimental computer system, and P. Z. Skanborg, who fitted the system to the operational requirements of the reactor.

The interest and co-operation of the electronic maintenance group in the trouble-shooting experiments are greatly appreciated as well as the discussions with Aage Jensen, head of the group, and P. Videriksen from the Institute of Applied Psychology, Directory of Labour.

REFERENCES

ABLITT **J.F.** (i968) A Quantitative Approach to the Evaluation of the Safety function of Operators on Nuclear Reactors. Private Communication. Safeguards Division, Authority HeaTtE and Safety Branch', U.K.A.E.A., Risley.

ABLITT J.F. (1969) Private communication.

BRUNER J.S., *DOODNOW J.J.,* AUSTIN G.A. (1956) A Study of Thinking John Wiley & Sons, New York.

CURRENT EVENTS (1959 - 1965) Nuclear Safety vol. 1 - 6.

GAGNE R M. (1963) Human Functions in Systems. Psycholgogical Principles in System Development. (New York: Holt, Rinehart and Winston).

GOODSTEIN L.P. (1969) Process Instrumentation for Man - Machine Studies. IEEE-GMMMS ERS Int. Sym)osium on Man - Machine Systems.
Cambridge England, September 1969.

I.C.A.0. Aircraft Accident Digest 1959 - 1967. International Civil Aviation Organization. Montreal Canada.

MILLER G.A. ()956) The Magical Number Seven Plus or Minus Two Psych. Review, 63, p. 81-97.

NEWMAN J.R., ROGERS M. S. (1966) Experiments in Computer Aided Inductive Reasoning. System Development Corp. TM-3227-000-00.

RASMUSSEN J. (1968) On the Co mmuni cation between Operators and Instrumentation in Automatic Process Plants. Riso-M-686 A.E.C Research Establishment, Riso, Denmark.

RASMUSSEN J. (1968) Characteristics of Operator, Automatic Equipment and Designer in Plant Automation. Riso-M-808, A.E.C. Res. Est. *Riso,* Denmark.

SWAIN A.D. (1969) Human Reliability Assessment in Nuclear Reactor Plants. Monograph SC-RV 69-:,@6. Sandia Laboratories, Albuquerque, New Mexico, U.S.A.

WOHL J.G. (1967) Adapting Space Vehicle Checkout Procedures and Philosophy to Near-Future Transport Aircraft. Society of Automotive Engineers National Aeronautic_L22tin& 670337, New York, April 1 967.

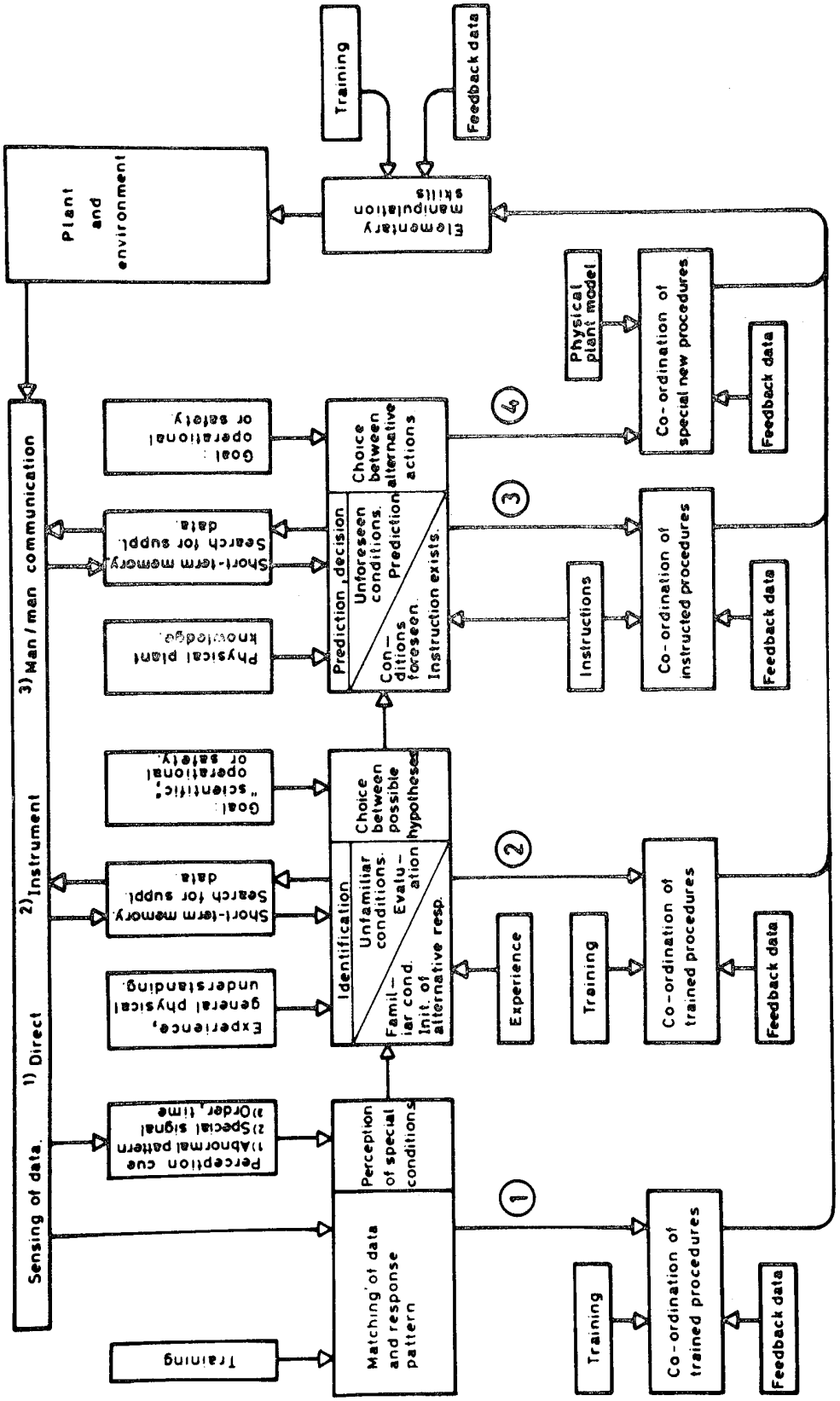

Fig. 1. Schematic diagram of operator performance.

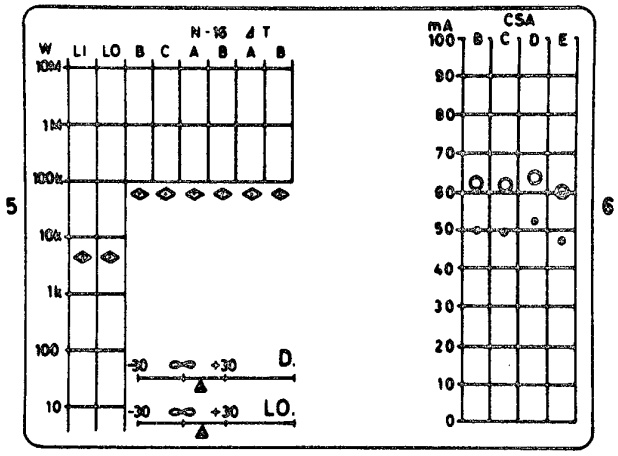

Fig. 2.

Example of analogue display designed to facilitate perception of patterns.

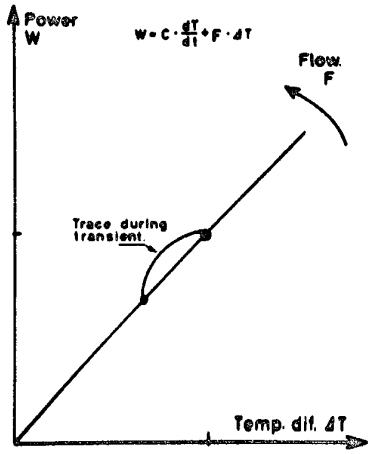

Fig. 3.

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

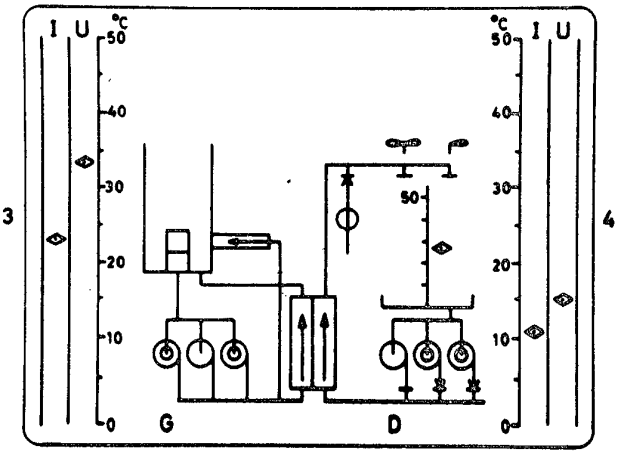

Fig. 4.

Display relating data to anatomy of system (reactor cooling system).
For symbols and other detai see Goodstein (1967).