Some trends in man-machine interface design for industrial process plants

Rasmussen, Jens

Publication date:
1980

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

Risø-M-2228

Risø-M-2228

Some Trends in Man-Machine Interface Design for Industrial Process Plants

Jens Rasmussen

Risø National Laboratory, DK-4000 Roskilde, Denmark
March 1980

Available on request from:
Risø Library,
Risø National Laboratory, P.O. Box 49,
DK-4000 Roskilde, Denmark
Phone (03) 37 12 12, ext. 2262

ISBN 87-550-0662-0
ISSN 0418-6435

RISO-M-2228

SOME TRENDS IN MAN-MACHINE INTERFACE DESIGN FOR INDUSTRIAL PROCESS PLANTS

Jens Rasmussen

Abstract. The demands for an efficient and reliable man-machine interface in industrial process plant are increasing due to the steadily growing size and complexity of installations. At the same time, computerized technology offers the possibility of powerful and effective solutions to designers. In the paper, problems related to interface design, operator training and human reliability are discussed in the light of this technological development, and an integrated approach to system design based on a consistent model or framework describing the man-machine interaction is advocated.

The work presented is part of a Scandinavian research project sponsored by the Board of Nordic Ministers, for the study of control room design and human reliability in nuclear power plants.

UDC 007.51 : 621.039.56

March 1980

Riso National Laboratory, DK4000 Roskilde, Denmark

Preprint

Invited Paper for IFIP-IFAC Symposium ASSOPO'80 Automation for Safety in Shipping and Offshore Petroleum Operations, Trondheim, Norway, June 1980.

ISBN 87-550-0662-0

ISSN 0418-6435

Riso Repro 1980

TABLE OF CONTENTS

INTRODUCTION

The general trend in the technological development of industrial process installations has been towards larger and more complex plants. Very often large plants imply large concentrations of energy or hazardous material, and maloperation can have serious consequences not only for the plant itself and its operating staff, but also for the environment and general public. This situation has forced system designers and safety authorities to take into account the ability of the system to control and counteract potentially risky states of maloperation of very low probability of occurrence.

Since it is impossible to take all possible hazardous combinations of individually low-risk situations into account during system design, the operating staff is generally supposed to cope with such complex, unforeseen situations. In spite of the introduction of complex automatic safety systems industrial accidents do occur. The conclusions of the analyses after the fact typically find important contributions from "operator error", and they point to the need for more effective training while expressing wonder about why the operators did not infer from the indications that a dangerous situation was under way. As it has been discussed elsewhere (Rasmussen 1979), this is not fair to operators, and the technological development, particularly of information processing equipment, raise a number of questions which are important to consider during systems' design.

THE NEED FOR A THEORY

The basic issue is related to the fact that we are now in a period when digital computers are being considered for improvement of the control of industrial systems and for the support of the operating staff in many different ways. The inexpensive and reliable process computer is changing the task allocation between operators and instrumentation; it brings with it new ways of processing and presentation of process variables; it makes possible effective support of operators through disturbance analysis; and it can be used for high fidelity training simulators. Generally, these possibilities are considered separately. However, they are so intimately related that it is difficult to envisage them being graduallly and independently introduced. Introducing new technology in system design is a kind of multidimensional optimization process in a multipeaked landscape in which the different summits represent choices among different basic design concepts. An extensive use of computers in all of the above areas will hopefully create a new tall peak. Unfortunately, however, this cannot be reached in an optimal way by cautious experiments in one dimension at a time, but only by a jump in all dimensions simultaneously. Furthermore, we can only expect to hit the peak within a reasonable vicinity of the top if we know where it is from the outset, i.e., if we have a theory or framework to guide the jump.

A MODEL OF MAN

An important part of such a theory is a performance model of human plant operators. As long as industrial man-machine interfaces were based on the traditional one sensor - one indicator concept and the size of installations were small enough to allow operators to operate by empirical "tricks of the trade" acquired through apprenticeship, simple models of human operators, like the information channel model used in the Purdue Guideline (Purdue 1975) were sufficient, and knob-and-dial ergonomics can be viewed as a separate discipline. More complex models - like the one shown in the above-mentioned guidelines (p. 27) "merely to indicate the extent to which Human Factors Engineering attempts to study the behaviour of the human operator" - should be taken seriously during systems' design.

Modern large scale industrial systems are drawing upon the whole range of human faculties, as illustrated in fig. 1. In an automated process plant of balanced design, the frequency of events calling for operator attention can be expected to be somehow inversely related to the risk implied in the situations. At the same time, the mode of performance of humans is tightly related to the frequency of occurrence of a task - varying from subconscious routines to knowledge-based problem solving. Even if we do not consider the psychological theories related to the different modes of performance but deal only with basic information processing aspects of the performance in engineering terms, some important distinctions emerge for systems design.

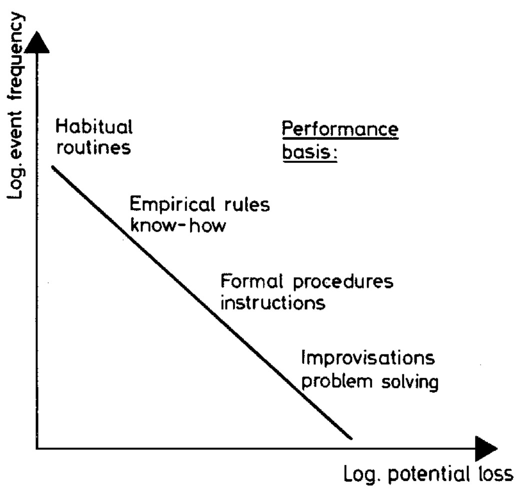

Fig. 1. The basis of human performance depends on the frequency of call for action, and the acceptable frequency of an event will depend upon the potential loss implied.

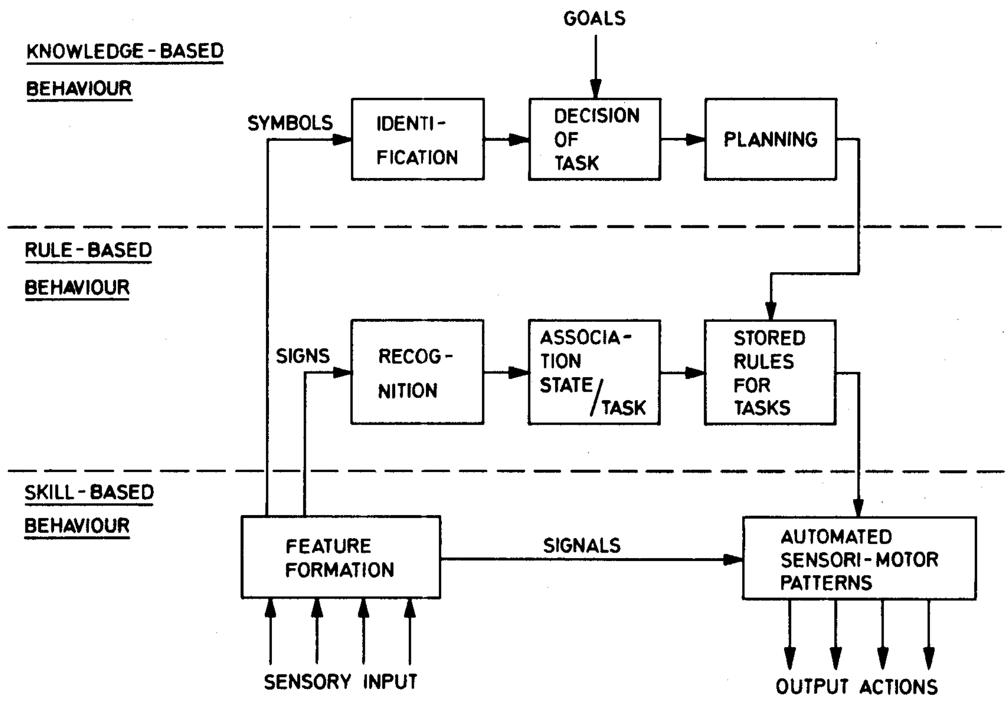

Fig. 2. Schematic illustration of different domains of the control of human performance.

In fig. 2 the distinction is drawn between three different domains of human performance depending upon the underlying control of the behaviour. This model has been described elsewhere (Goodstein and Rasmussen, 1980), in the present context only some important implications for systems design, definition of human errors and operator training will be discussed. The three levels are closely related to the frequency of tasks as indicated on fig. 1. The very frequent daily routines are performed in the domain of <u>skill-based behaviour</u>, the less frequent, but still familiar tasks are performed in the <u>rule-based</u> domain, and finally the tasks which have not been met before and not analysed during design must be performed by <u>knowledge-based behaviour</u>. There are very fundamental differences between the three domains with respect to several aspects of the design problem.

INFORMATION DISPLAYS

The operator's input information - or rather the information sought or taken by him - from the system plays very different roles. In the skill-based domain, when humans in a way perform as multivariable control systems manipulating physical objects (- which can be graphical -Cigures) or navigating through the environment, the sensory information acts as <u>signals;</u>

i.e., analogue representations of spatial variables. When humans are not operating on physical objects directly but by means of displays and keys on a control console, the implication will be that in the skill-based domain the control console itself is operated on instead of the underlying process. In the rule-based domairi7 Performance is based on recognition of states of the system with association to known rules or plans. When operation is performed directly on physical objects, states are perceived very reliably. If however, selected information is available only as individual variables displayed on a control console, reliable state identification will demand conscious inference on the part of the operator, and this cannot be expected from operators during all routine situations. Instead, characteristic indications of the presented information will act as signs representing system states. Signs may be labelled in states, events, tasks or perhaps other names related to the physical states by convention, just as traffic lights are, for example. Finally, for knowledge-based performance observed information from a data display acts as symbols, i.e., representations which can be treated directly by symbolic data processing for problem solving. It is clear from this that the role of presented data varies fundamentally with the task situation and optimal coding presupposes knowledge of the proper domain of performance. Seen the other way, the presentation of properly designed data formats can be used to activate the proper level of cognitive control of behaviour. it seems evident that the same presentation will not be optimal for all three levels and also, with undifferentiated presentation, that indicators which acquire clear significance as signs in familiar situations will have strong bias against playing the role of symbols in rare situations. The data transformations needed to make the same measured information available to operators as signals, signs or symbols is a task which is directly fit for computers.

OPERATOR TRAINING

Another aspect in which the domains differ fundamentally is the mode in which the human learns about system properties. In the skill-based domain, learning is based on behavioural patterns of movements stored during performance of the task under the control of either higher level cognitive functions, or of an external teacher with his "hand on the bicycle saddle". The process computer has led to the development of "high fidelity" dynamic training simulators which generally are considered important for training of aircraft and space-vehicle control during emergency situations, since the task is a time-space multivariable control task. (The empirical evidence is discussed in a recent review by Stammers (1979)). However, it does not appear to be evident that high fidelity dynamic simulators are necessary for training of skill-based behaviour in most process industries. Transfer of "process-feel" seems to be rather effective within time constants and gain characteristics of the same ranges and simple dynamic simulators could serve that purpose. Training within the rule-based domain typically depends on rehersal of the cues and rules of the game. It is important to know the locations of sources of cues and of knobs and switches, but static mock-ups or magnetic board displays have proved efficient (Duncan 1975) for training by exercises or "talk-throughs" (Swain, private communication). Unfortunately, people are mouldable and learning not only during the formal training periods. The plant itself continues their training very effectively and, ultimately, the rule-based behaviour will depend upon interface characteristics rather than formal training. It is therefore important to support rarely used rules and to arrange the interface in a way so that operational optimization of frequently used rules does not violate risky, but latent conditions.

Operators have no chance for developing empirical rules for infrequent occurrences, and work instructions cannot be preplanned for all possible situations. Furthermore, one of the recent "lessons learned" from TMI has been that it cannot be assumed that an instructional system for major accidents will take care of the less critical situations and thus help operators to cope with these. Consequently, in modern large scale industrial installations, reliable operation to an increasing degree depends upon the operator being able to perform in the knowledge-based domain, i.e., to form the necessary rules ad-hoc in the actual situation. Very little is apparently known about the content and means of training operators for knowledge-based performance; the dynamic and visual verisimilitude of expensive simulators is not related to the necessary knowledge of operators for performance in this domain, and training in the theoretical, physical description of plant function alone is not adequate. Actually, much of the knowledge of internal functions and causes needed can be presented by computer controlled displays in a proper symbolic domain; the difficult information to bring to the operator will be the intentions and reasons which were the designer's basis for the functions chosen and for the operational specifications. Not only is this information difficult to present to the operators, but, generally, the designer's intentions and reasons are not explicitly available to the operating staff, since they simply fade away as soon as the designer has put the schematics on paper. An obvious use of a computer would be as a design aid which could store the information base generated during design and subsequently present it to the operating staff in a suitable form.

THE FEEDBACK DESIGN CONCEPT

To rely on the operator's performance in the knowledge-based domain where the goals and ends are specified, the means are supplied but the operator is left to plan the procedural rules, is, in a way, in accordance with the general system design principle of coping with high intrinsic variability in component performance by the use of feedback correction. One can wonder why the emergence Of large scale, high risk installations has led to an extensive use of detailed formal procedural instruction to control the plants in case of maloperation. This is, in fact, equivalent to choosing a preprogrammed, feedforward function to perform a complex control task; an approach which outside the human function area would not be considered good engineering practise. It is, of course, also possible for the operator in the rule-based domain to detect unsatisfactory outcome of the application of procedural rules and to try to correct this by modifying the rules; but this means that he switches to knowledge-based performance and very likely will end up in the well-known conflict situation - when to "follow the book", and when to "think for yourself". In case of unsuccessful actions, it depends upon the conception by the judging body of the norm as reflected either by the procedure itself or by the goal - as to whether the operator or the procedure/system designer will be made responsible for the error. Moreover, the norm may very likely by perceived differently during the situation and after the fact.

HUMAN ERROR

The definition of human error is related to the deviation from a norm, i.e., some specified or normal performance which itself will be different for the different domains of control of human behaviour. In the skill-based domain, behaviour is controlled by the adaptive patterns stored in the nerve system. Due to the high physiological redundancy of this system, the concept of "human error" becomes meaningless, and inappropriate behaviour can only be explained by changes in the external world leading to a "misfit" with the trained neural patterns in the responding person, or to a variability in the control and coordination of movements exceeding the tolerance of the system. In these cases, the causes cannot reasonably be referred to as "operator error"; they are rather instances of man-machine misfits. In the rule-based domain, the reference norm will generally be the rule, i.e., the right way of doing things, either in the form of general professional know-how or formal work instructions. Errors will often be detected by their effects in terms of terminal state/goal discrepancies but judged against the normative rule. In the knowledge-based domain, however, an error can only be identified from the unsuccessful attainment of the goal, and it can be difficult to judge whether operator error is a proper classification. Since an error can be the outcome of a resource/demand conflict, it is necessary to ensure that the operator had adequate resources during the situation, before we refer the fault to the operator. In conclusion then, two basic design problems are found. One is to create work situations for the operator which lead to a clear discrimination between occurrences where goals are normative and operators are not only allowed to, but also expected to, generate and optimize their own plans, and occurrences where normative rules are effective and mandatory on account of latent, risky conditions. The other problem is that of keeping the operators' knowledge base satisfactorily updated for infrequent needs. This may presuppose changes in present organizational and educational structures. A few weeks refresher course on a training simulator each year is no solution. A solution will imply that tasks demanding knowledge-based performance are integrated in the normal functions allocated the operators. This in turn can mean that operators will perform tasks which are now allocated professional engineers or maintenance specialists, or that such specialists are integrated in the operating staff by either being on hand or on call.

Event reports including cases of "human errors" are very important sources of information on human performance and are waiting for serious consideration by researchers and system designers. Information on internal functions and their limitations can only be obtained for adaptive systems from instances when the adaptation proves inefficient. "To the extent that he (man) is effectively adaptive, his behaviour will reflect characteristics largely of the outer environment (in the light of his goals) and will reveal only a few limiting properties of his inner environment - of the physiological machinery that enables his to think". (Simon, 1969, p. 25). It is, therefore, important to analyse event reports and case stories, not only to obtain statistical information on human errors in terms of the effects upon task performance for reliability prediction, but in particular to understand the error mechanisms and to generalize in order to be able to improve interface design.

Thus, several aspects of the instances of human malfunction should be characterized separately. First of all, the analysis must identify the human function that failed its purpose - and the way it failed - in terms referring to the internal human task independent of the external task and system. For this purpose, information processing concepts related to detection, identification, decision, etc., seem to be well suited and compatible with current cognitive psychology as well as control theory. In addition a task analysis is necessary to relate these internal functions to the external task and to identify possible external causes to the malfunction.

CONCLUSION

Major industrial incidents and accidents are generally followed by a "lessons learned" discussion which very often concludes with demands for "more of" all the traditional precautions: operators should be trained better; more instruments should be installed, management should be improved, etc., and the recommendations are typically tailored to counteract the specific situation causing the discussion. The flexibility and capacity of modern inexpensive computer systems practically speaking invite extensive efforts to explore their potential in this context. The present paper is a modest plea for spending a fair amount of efforts and resources in the search for a fundamental framework to guide the design of improved systems. The work presented is part of a Scandinavian research project sponsored by the Board of Nordic Ministers, for the study of control room design and human reliability in nuclear power plants.

REFERENCES

(1) Duncan,' K.D., A simulator and training technique for diagnosing plant failures from control panels, Ergonomics, 1975, vol. 18, no. 6, 627-641.

(2) Goodstein, L.P. and Rasmussen, J., Man-machine system design criteria in computerized control rooms, "ASSOPO 8011, IFIP/IFAC conference, Trondheim, Norway, June 1980.

(3) Purdue, 1975, Guidelines for the design of man-machine interfaces for process **control,** Purdue Laboratory for Applied Industrial Control, Purdue University.

(4) Rasmussen, **J.,** What can be learned from human error reports?, in "Changes in working life", K.D. Duncan, M.M. Gruneberg & D. Wallis (Eds.), John Wiley & Sons, 1980.

(5) Simon, H.A., The sciences of the artificial M.I.T. Press, 1969.

(6) Stammers, R.B., Simulation in training for nuclear power plant operators, report n. 12, Ergonomr'ad, Karlstad, Sweden, 1979.

Risø National Laboratory **Risø - M - 2228**

Risø - M - 2228

Title and author(s)

Some Trends in Man-Machine Interface Design for Industrial Process Plants

Jens Rasmussen

pages + tables + illustrations

Date March 1980

Department or group

Electronics

Group's own registration number(s)

R-3-80

NKA/KRU-P2(80)27

Abstract

The demands for an efficient and reliable man-machine interface in industrial process plant are increasing due to the steadily growing size and complexity of installations. At the same time, computerized technology offers the possibility of powerful and effective solutions to designers. In the paper, problems related to interface design, operator training and human reliability are discussed in the light of this technological development, and an integrated approach to system design based on a consistent model or framework describing the man-machine interaction is advocated.

Copies to

Available on request from Risø Library, Risø National Laboratory (Risø Bibliotek), Forsøgsanlæg Risø), DK-4000 Roskilde, Denmark
Telephone: (03) 37 12 12, ext. 2262. Telex: 43116