The role of the man-machine interface in systems reliability

Rasmussen, Jens

Publication date:
1973

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

Risö-M-1673

Risö-M-1673

Danish Atomic Energy Commission

Research Establishment Risö

ELECTRONICS DEPARTMENT

THE ROLE OF THE MAN-MACHINE INTERFACE IN SYSTEMS RELIABILITY

by

Jens Rasmussen

November 1973

R-10-73

Reprinted from
NATO Conference on Generic
Techniques in Systems
Reliability Assessment.
Liverpool, July 1973

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 - 1673

Risø - M - 1673

Title and author(s)

The Role of the Man-machine Interface in Systems Reliability

By

Jens Rasmussen

Date November 1973

Department or group

Electronic

Group's own registration number(s)

pages + tables + illustrations

Abstract

The use of probabilistic reliability evaluation of industrial process plants is discussed. In this application low probability events leading to severe consequences have to be identified and included in the analysis. Human malfunctions in abnormal tasks are an important factor in such events, but human behaviour in higher level mental tasks cannot yet be predicted. It is therefore important to verify the limits of use of existing methods of reliability prediction.

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

THE ROLE OF THE MAN-MACHINE INTERFACE IN SYSTEM RELIABILITY[1]

Jens Rasmussen

Abstract: The use of probabilistic reliability evaluation of industrial process plants is discussed. In this application low probability events leading to severe consequences have to be identified and included in the analysis. Human malfunctions in abnormal tasks are an important factor in such events, but human behaviour in higher level mental tasks cannot yet be predicted. It is therefore important to verify the limits of use of existing methods of reliability prediction.

INTRODUCTION

The definition of the reliability of a system or system component is generally stated in terms of the probability of specified function versus time, such as: "Reliability is defined as that characteristic of an item expressed by the probability that it will perform its required function in the desired manner under all relevant conditions and on the occasion or during the time intervals when it is required so to perform" (Green and Bourne 1972).

This definition has its root in the vast efforts of the last two decades to develop means and methods to analyse and predict the behaviour of complex electronic systems, such as military communication and weapons systems. This origin of vital reliability problems and the research work involved have caused the reliability definitions and mathematical models to be tightly mission oriented, as they are mainly dealing with the probability of success.

Probabilistic models of the reliability of electronic systems have long proved very powerful tools in the design and assessment of such systems, and applied mathematicians have been very active developing more and more sophisticated and elaborate models.

The success of the methods in the field of electronic systems has during recent years led to rapidly increasing efforts to use probabilistic methods to evaluate system performance in other technical fields.

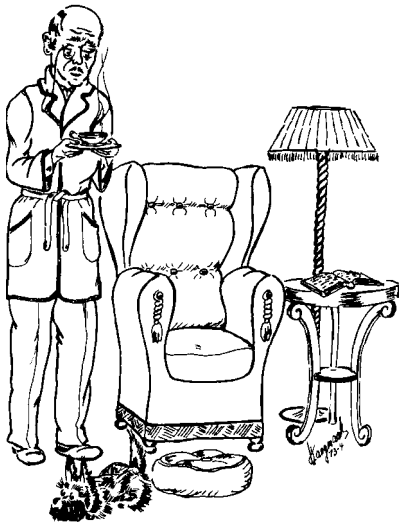
RELIABILITY ANALYSIS OF INDUSTRIAL PROCESS PLANTS

Within the design of industrial process plants, such as power stations and chemical plants, the rapid technological progress is followed by increasing difficulties in using "proven technology" in the traditional sense. Furthermore the rapidly increasing size of production units leads to more drastic

---

[1]Tech Report. Risø-M-1673. Roskilde: Danish Atomic Energy Commission; Research Establischment Risø. Revised edition in: E. J. Henley and J. W. Lynn (Eds.): Generic Techniques in Systems Reliability Assessment. Noordhoff, Leyden, 1976, pp. 315-324.

consequences of faults in terms of production losses and damage to the plant. Consequently there is a great need to prove the technology of a proposed design by a systematic prediction of-system performance. The established probability models and methods may also be powerful tools in the design of electric or mechanical equipment for an industrial plant, but this application generally leads to several complications especially if the reliability or the safely of a total plant are considered.



Reliability analysis takes care of the tea -

In the evaluation of such systems, one often feels like acting as the British gentleman carrying a cup of tea so careful that he overlooks the dog on the floor. Or, as Ralph Evans puts it in a recent editorial in IEEE Transactions on Reliability: looking for the purse under the street lamp, not because it was lost there, but because that is where you can see. The aim of the present paper is to support a discussion of identifying areas for which the elaborate probability methods must be extended and modified, and supplemented by systematic look-out for dogs on the floor.

So far, we have found complications in two general aspect in the application of probability methods for industrial process plant equipment,

First, the reliability of process plant equipment cannot be measured simply by the probability of required function. The analysis should be able to relate the probability of different types of faults to their consequences to the system. Secondly, the relevance of the analysis is highly dependent upon a proper coverage of the human functions in the system.

Accident analysis must take care of the environment (Drawings by H. Langmaak)

THE PROBABILITY/SEVERITY RELATIONSHIP

Presumably most researchers advocating the use of probability methods in systems design have been involved in discussions with industrial people and faced with o complicated case story and whether it would be covered by the methods and most probably it would not. The problem is a fundamental one. The general focus of the reliability methods upon figures related to the probability of specified functions allows a rather isolated treatment of subsystems and system parts. The methods are therefore a valuable tool for the designers' judgements of the relative merit of different alternative solutions, and the reliability figures characterising individ-

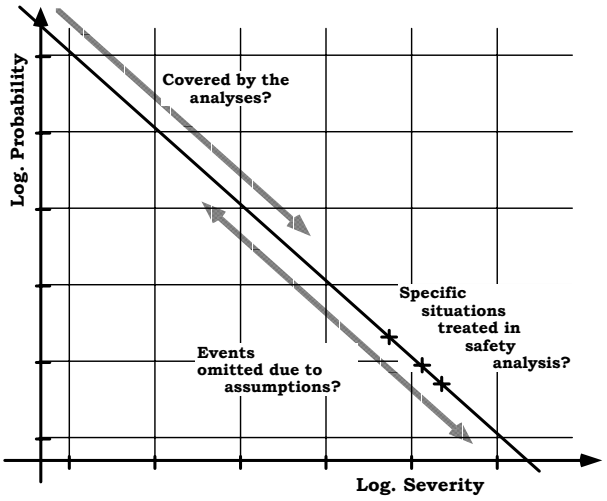
ual system parts can usually be combined to a measure of the total system reliability.

The reliability engineer is usually happy if the result of his analysis can be verified as a successful prediction of the gross reliability figures such as failure rate or availability.

The user of the completed system on the other hand will judge the performance from the total cost resulting from faults in terms of loss of production or damage to plant or injuries to staff. To some extent he may consider the multitude of simple trivial faults as annoying, but nevertheless as the source of part of the normal task of the staff. His attention is focused upon the fault conditions leading to considerable risk of losses.

This complicates the analysis. It is not possible to calculate the reliability of the parts and subsystems individually and afterwards combine the results to find the characteristics of the total system as is done when the probability of required function is calculated, The fault modes and figures to he used for the individual parts have to be identified by a cause-consequence analysis of the total system relating the possible modes of failure of the individual components to the ultimate consequence for the system. Special attention should be paid to the fault mechanisms, which may lead to severe consequences.

In a well balanced design the probability of an abnormal event can be assumed to be inversely proportional to the related consequence to the system operation. This is in agreement with the frequency/severity plot of injuries in American industry shown by Johnson (1972) and is also reflected in the nuclear safety criterion suggested by Farmer (1972). The great importance of low probability events imposing severe risks on the system has to be faced, if reliability prediction should be of any real value in the design and evaluation of industrial plants. In the safety assessment of nuclear plants, for instance, the look-out is for failure probability in the range 10^{-5} to 10^{-7} per year or less.



The probability plot of faults in a reasonably "balanced" plant design. How is the coverage of reliability analysis today?

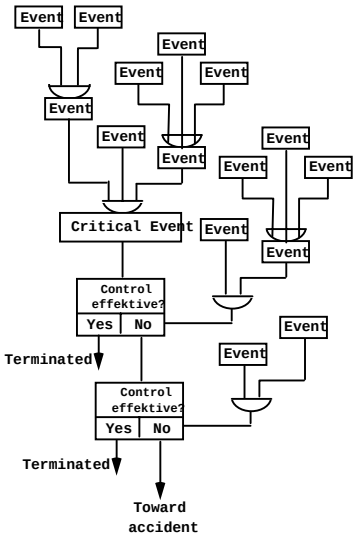
Neither the functional analysis of the system to identify the relevant causes and consequences of faults nor the probability analysis itself can cover all possible events. The analysis must be based upon a number of assumptions and approximations, and there is a danger that important, but low probability, fault modes are excluded from the analysis. It should therefore be realised that a quantitative reliability figure only constitutes a minor

part of the result from the analysis. A very significant part of the result is given implicitly in the assumptions and approximations. as they very often identifies conditions which may be of low probability but vital to the total reliability. Furthermore, they typically involve conditions, which are dealt with by the plant personnel, and it is therefore important that the assumptions and approximations underlying the analysis are interpreted and documented carefully to facilitate their verifications during plant operation.

THE CAUSE /CONSEQUENCE ANALYSIS

The first important step of the analysis of a process system is a cause/consequence evaluation aiming at an identification of the relevant fault traces through the system. A fault tree analysis based upon typical component faults may not identify low probability, but risky fault traces. A vital part of the analysis will be to trace also the possible but improbable faults and combinations of faults, from a postulated set of consequences. This in itself implies an interface problem between the system and the analyst, as it demands a detailed knowledge of the practical layout of the technical system and of the working conditions and behaviour of the plant personnel.

The prime condition to be fulfilled by a reliable analysis is of course that all relevant traces are identified. In a complex system the analysis cannot cover all physically possible faults and their combinations, and it is therefore important to have systematic heuristic methods to identify relevant traces. Such a method should support the creative or inventive powers of the analyst, and we have briefly considered the "morphological" method suggested by Zwicky (1967), which may be a fruitful approach.



The structure of a cause/consequence analysis

Johnson (1972) has recently published a comprehensive work on systematic evaluation of accidents using a similar approach. Johnson traces the possible causes starting from a rather high level of abstraction and controlling the tracing of faults systematically though several levels of detail, such as:

-"an *accident* is

-an unwanted *transfer of energy*,

-because of *lack of barriers* and/or controls,

-producing i*njury* to persons, property or process

-preceded by sequences of *planning and operational errors* which failed to adjust to changes in physical or human factors, and produced unsafe conditions and/or unsafe acts,

-arising out of the *risk* in an activity,

-and interrupting or *degrading the activity*."

We find it very important to develop systematic methods for cause / consequence tracing with tight coupling to appropriate models to facilitate the complete analysis (Nielsen 1971).

A clear systematic approach to the identification of relevant fault traces furthermore facilitates adequate documentation of the analysed mechanisms considerably. This documentation is a vital part of the man-machine interface. A trivial, but important condition of a reliable analysis is of course that it deals with the system actually operating. The system, however, may be subject to changes. Equipment can be modified and improved according to operational experience, as well as working procedures and instructions will be changed-planned or unnoticed. A considerable risk therefore exists that the conditions of plant reliability will be unintentionally violated. To avoid this the analysis must be documented in a systematic form, which can be readily interpreted and used by the operational staff.

THE HUMAN FACTOR IN SYSTEM RELIABILITY

Our attention was directed towards the human element in the system by a review (Rasmussen 68) of reported major incidents and accidents. Its purpose was to enable us to judge whether our methods for reliability evaluation also included such cases and we found they did not.

Among the cases reviewed are 30 cases reported in USAEC Nuclear Safety Bulletin. In 70 80% of these cages, the incidents were initiated from human mal-operation in the system. Furthermore, the mal-operations did not take place during normal tasks, but overwhelmingly during abnormal or special tasks under abnormal plant conditions, such as modifications, repairs or cleaning and calibration operations; typically operations which are difficult to predict and analyse, and therefore normally covered by suitable assumptions in the analysis.

This is quite reasonable from the traditional reliability point of view, as this type of faults normally account for a small fraction of the total number. In a British fault record 8,000 cases from nuclear installations including trivial technical and human faults, the human faults amount to only 10% of the total (Ablitt 1969). But in our context it is most unfortunate that the source of severe incidents is very likely found in a class of faults, which are normally excluded from the analysis by proper assumptions. A few examples will illustrate this point of view.

The reliability of a system very often depends heavily upon an assumption of mutual independence of fault mechanisms Physical sources of common mode faults such as flooding by water, rupture by missiles or trucks, etc., may be identified by a morphological search. But coupling due to people moving around in the plant? If an abnormal condition in the plant, for instance due to a technical fault in a subsystem, calls for manual intervention, there is a probability that an operator misinterprets the situation and manipulates another part of the system. The result is a coincidence of two faults, which are physically independent and as such difficult to predict at an office desk, although it may be likely to happen, judged from the actual working conditions. The problem is that although it may be possible to predict the probability of operator failure to execute the required function, it may be almost impossible to predict what he does instead.

In redundant systems the assumption of independence can lead to extreme reliability figures but the actual figure may likely be controlled by the probability of a faulty repair which is repeated in more units.

Probability modelling of a complex system is often simplified substantially if proper function of equipment is assumed verified at certain intervals and after repair. This assumption is vulnerable and sometimes unrealistic, partly because repair and test in itself can be faulty, but also due to technical difficulties in testing the equipment without putting it into operation. Furthermore, pressure of work during plant shut down can be great to regain plant operation in due time to avoid the operational consequences from process cool down or processes like xenon poison in nuclear plants. Therefore, test and calibration procedures may be postponed to the restart phase. This may be critical, as faults introduced during repair and modification work may leave the plant in an abnormal state, which is not covered by the protection of the normal safety system. Although such periods are normally relatively short, they can in our experience contribute significantly to the total risk of the plant.

In other words, in evaluating the reliability of a system like process plants, the role of the human functions in the system should be considered not only to include primary human functions in the reliability analysis itself, but also to verify the assumptions of the analysis, as the assumptions are ultimately administered by plant personnel.

PREDICTION OF HUMAN RELIABILITY

Several important approaches have been made towards the development of methods for predicting human reliability. Such methods have recently been reviewed by Meister (1972) and are the subject of other lectures of this meeting.

The basic assumptions of these methods are typically:

- The task is well defined and the procedure followed can formulated in detail,
- The procedure can be broken down into a sequence of behavioural units, i.e. subtasks or task elements,
- Data on the reliability of the individual subtasks are available together with the parameters characterising the relevant task situations.

Typically these assumptions do not fit the work procedures found in process plant environments. The work procedures may be known in detail under task conditions, where the physical environment paces the man, and thus forces him to use a known sequence of subtasks, as is the case in e. g. manual assembly processes.

In modern automated process plants, however, the human function is typically higher level mental data processing and decision making, and the human work procedures are constrained by the physical environment to a much lesser degree.

Consequently, the normal practice is to try to control the work procedure in critical tasks by work instructions which take into account the possible deviation from normal working condition that have been identified during system design.

However, in the analysis of accidents it is frequently seen that such safe work procedures have been operationally "improve" to fit the normal work situation in a way that does not take account of the predicted risk.

In reliability assessment this tendency has to be faced in a realistic way. As long as the prime cause to have the people in the plant is the human ability to adapt to the operational needs of the plant and to improvise in all plant conditions not foreseen by the system designer, it is not reasonable to expect them to follow work procedures which are troublesome in the normal work, just for the sake of conditions they possibly never meet.

The concluding remarks in reports investigating accidents, which are due to inappropriate procedures, frequently prescribe "tighter administrative control" of work instructions, A more realistic approach is the situational one, as advocated by Rigby and Swain, who argue that a work situation can only be reliable if properly fitted to normal variability of human behaviour. Human actions due to normal psychological mechanisms should not be classified as operator errors, even if they do lead to system faults. Rather the work situations have not been designed in a way resulting in predictable procedures.

Unfortunately, very few studies have been made to describe the procedures evolving in higher level mental tasks in real life working conditions and to relate them to controlling factors in the work situation. Consequently we have recently initiated such studies. We have examined mental procedures in control room environment and in an electronic work shop, and the

preliminary analysis has identified features which we find illustrating in the present discussion.

We have found that the creativity and adaptability of man often result in the evolution of several basically different mental procedures for the same type of task, all capable of ending up with the same result. The procedures may differ in several basic aspects. such as the amount of data or observations which are needed; the complexity of the mental data processing which is implied; the depth of functional knowledge regarding the system anatomy and function which is used; and finally the time spent the task (Rasmussen and Jensen 1973). A fault in an electronic system, for instance, may be located from a minimum number observations if a careful deduction is used, based upon a detail knowledge of system anatomy and internal functioning. However the fault may also be located by a rapid sequence of observations or measurements and simple checks against normal values in a diagram without considering the functioning of the system. In this way different procedures can be available to a human operator for a specific type of task, procedures which fit the different working conditions in which the task is met.

The choice between the different procedures depends upon the performance criteria adopted by the man in the actual working situation. The rapid stream of simple decisions may be valued in some cases, due to the low cognitive strain implied, in other cases the complex reasoning may be chosen due to informational economy. The important point is that the performance criterion of the designer and the real life operator most probable: are different, and the designer very likely will not predict the actual procedures used by trained personnel, unless he is very familiar with the actual task conditions from studies on site.

A further prerequisite to be able to use the classical reliability methods for evaluation of human behaviour is the break down of the procedures used into a sequence of typical and generally used units. This can be done for a task in which the element of the sequence on the work steps are defined and cued by the environment as for manual tasks in production. But again it is not the case for higher level data processing tasks in plant environments.

Newell and Simon (1958) have argued that mental processes underlying human data processing and decision making can be decomposed into a sequence of elementary units, and as such simulated by a digital computer program. But in our experience this is not the whole truth, and Dreyfus (1965) has criticised the assumption and stressed the role of holistic, intuitive processing, which cannot be decomposed into elementary units. Discussing the decisions of chess playing, he argues: playing chess

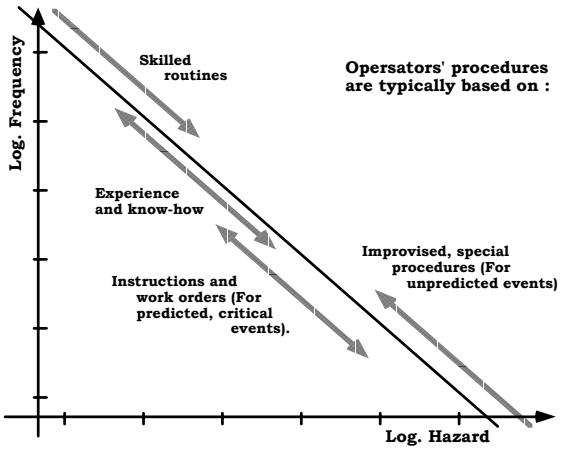
> . . . may involve noticing that 'here something interesting seems to be going on', 'he looks weak over here' etc. Only after the player has zeroed in on an area does he begin to count out, to test, what can be done from there.-

In other words the first, important step in the mental work sequence, the identification of the task situation and the appropriate goal, may be based

upon holistic process, pattern recognition, intuition and "feelings", and based hereupon a sequential processing may take place.

From our reviews of reported accidents we have found the identification of the proper task in abnormal plant conditions to be very critical, and our conclusions from preliminary analysis in control room environments tend to support the view of Dreyfus.

The operator seems to have a "process feeling", some sort of internal dynamic model of the environment, which all the time keeps him prepared for the normal tasks to come. This means .that he may only be prepared to look for very little information the actual time of a task, and it is not possible to predict whether the information actually underlying his decisions is properly updated. Furthermore the source of information chosen may be convenient sources during the normal working condition, such as noise from the system, e. g., relay clicks, rather than information planned by the designer to be task defining and therefore displayed to the operator and considered in a prediction.



Log. frequency/hazard plot of events calling for operators' intervention. The source of operators' procedures depends on the frequency of the event - so does the hazard very likely.

Fundamentally this effect of the "process-feeling" links the elements of a task sequence together and they cannot be treated individually. A control room operator typically does not perform isolated actions on well specified bits of information, he is an integrated part of a dynamic situation. This causes difficulties which are hard to predict when abnormal plant conditions suddenly demand the operator to switch to other tasks and performance criteria. The reactions to abnormal plant conditions an only be treated in the light of the normal working conditions prior to the event and setting the process-feeling and thus the expectations of the operator. The reactions can only be treated in isolation, if the man-machine interface can be designed to break the routines of the operator and to set the initial conditions of his data processing in a predictable way at the start of a task.

It is worth noting that the basic aspects of the procedures adopted by man for a task normally will depend upon the frequency of the task. The very frequent tasks are met by procedures based upon pattern recognition and trained, partly subconscious routines; less frequent tasks by procedures based upon plans or instructions whereas the unique, very infrequent task may call for improvisation and complex, deductive reasoning related to understanding plant anatomy and functioning.

Again the frequency/risk relationship intrudes our problem. In a reasonably well designed system an inverse relationship can be expected between the frequency of an event calling for manual intervention and the risk implied in the event, and again the frequent events are easier to predict and analyse, whereas the infrequent, but critical events are of major importance to the system user. As discussed above, the familiar tasks set the stage for the unexpected, new events and consequently the operator tends to approach a new task by the most probable hypothesis, although most safety regulations tend to force the man to consider first the hypothesis covering the most critical cause.

To see how far we can get in planning a man-machine interface that will cause personnel to adopt predictable procedures it is very important to have methods for prediction of human reliability verified by field tests and to have a clear identification of the characteristics of those work procedures and working situations they can be used to analyse, and to have more studies to identify the procedures evolving during process plant operation under different typical working conditions.

CONCLUDING REMARKS

The methods of probabilistic reliability evaluation today are efficient tools internally in the design offices for process plant equipment. To reach the state, where the methods can be used to a quantitative evaluation of the reliability of a complete operating process plant and an assessment of plant safety, it is imperative to create a closer relation to the realities of process plant operation. This implies an interdisciplinary cooperation between the fields of reliability engineering, human factors engineering and plant operation, and a careful verification of the methods including an explicit statement of the limits of their appropriate use.

REFERENCES

Ablitt, J. F., Private Communication. Safeguards Division, Authority Health and Safety Branch, U. K. A . E. A., Risley 1 969.

Dreyfus, H. L., What Computers Can't Do (Harper and Row, New York, 1972) 259 pp.

Evans, R.A., Editorial: Ask a Silly Question. IEEE Trans Reliab R-21 (1972) p. 129.

Farmer, F. R., Reactor Safety and Siting: A Proposed Risk Criterion Nucl. Safety 8 (1967) 539-548.

Green, A.E. and Bourne, A. J., Reliability Technology (Wiley Interscience, London, 1972) 636 pp.

Johnson, W. G., The Management Oversight and Risk Tree-MORT SAN 821-2 (1972) No pagination.

Meister, D., Comparative Analysis of Human Reliability Models. AD-734 432 (1971) 481 pp.

Newell, A., Shaw, I. C. and Simon, H. A. Elements of a Theory of Human Problem Solving. - Psych. Rev. 65 (1958), 151-166.

Newell, A, Simon, H. A., Human Problem Solving (Prentice-Hall; Erslewood Cliffs, N. J., 1 972) 920 pp.

Nielsen, D. S., The Cause / Consequence Diagram Method as a Basis for Quantitative Accident Analysis. Risø-M-1374 (1971) 27 pp.

Rigby, L. V., The Nature of Human Error. SC-DC-69-2062 (1969) 12 pp.

Rasmussen, J., Man-Machine Communication in the Light of Accident Records. International Symposium on Man-Machine Systems, Cambridge, 8-12 September 1969. IEEE Conference Record No. 69 (58-MMS. Vol. 3)

Rasmussen, J. and Jensen, Aa., A Study of Mental Procedures in Electronic Trouble Shooting. Risø-M-1582 (1973) 71 pp,

Swain, A. D., Design Techniques for Improving Human Performance in Production (Industrial and Commercial Techniques Ltd., London, 1973) 140 pp.

Zwicky, F., The Morphological Approach to Discovery, Invention, Research and Construction In New Methods of Thought and Procedure. Edited by F. Zwicky, and A. G. Wilson, (Springer, Berlin, 1967) 314 333 .