On Human Error Analysis and Quantification

Rasmussen, Jens

Publication date:
1977

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

ON HUMAN ERROR ANALYSIS AND QUANTIFICATION

Note for CSNI Working Group Meeting, April 1977

Jens Rasmussen, Research Establishment Risø

DEFINITION AND CLASSIFICATION

The term "human error" is loaded and is very ambiguous. Basically, a human error is committed if the effect of human behaviour exceeds a limit of acceptability. Of course, the classification of a specific behaviour as an error depends as much upon the limits of acceptability as it depends upon the behaviour itself. In practise, the limits are often defined after the fact, by someone who can base his judgements on a careful, rational use of a functional model of the system, while the specific behaviour possibly was a quick response in a stressed dynamical situation. Therefore, as it has been argued Rook (1965) and Swain (1969), it is necessary to distinguish clearly between errors induced by inappropriate limits of acceptability; i.e., by the design of the work situation, and errors caused by inappropriate human behaviour. Furthermore, as discussed by Rigby (1969), errors can be classified as random errors, due to random variability of human performance such as precision; systematic errors, which can be caused by personal abnormalities or inappropriate system design; and, finally, sporadic errors, occasional "faux pas" which are infrequent and often unexplainable erroneous actions.

To reduce the number of system failures which are caused by a misfit of man and machine, it is necessary to decrease the influence of random and systematic errors.

Random errors can be eliminated only to the extent to which the limits of acceptability can be arranged to span the range of natural variability of performance of the people selected to the task.

.Systematic errors can be related deterministically to specific properties of the work situation and can be eliminated if the causal relations can be identified and changed. It is a very important category of errors within our context of monitoring and supervisory task in automated systems. Typically, the operators have to respond to changes in system operation by corrective actions, and in a properly designed system there should be a reverse relation between the probability of occurrence of a change and its potential effect in terms of losses and damage. In modern large centralized systems, the consequences of faults can be extremely serious and consequently the effect of human errors in situations of extremely low probability must be considered. In such cases, the potential for systematic errors cannot be identified from experience, but only by a systematic functional analysis of the process plant and of the

operator's actions. In the present general discussion, two types of systematic errors which seem to be important should be considered.

First, human responses to changes in a system will be systematically wrong if task demands exceed the limits of capability. Demands and capability may conflict at several aspects of a task such as time required, availability of state information, background information on system functioning, complexity of data processes, etc. The operator must be able to trade off demands and limitations by choice of a proper strategy. An example would be for the operator to remove time constraints by first bringing the system to a safe, stationary state.

Secondly, systematic human errors may be caused by a kind of procedural traps. During normal work condition human operators are extremely efficient due to a very effective adaptation to convenient, representative signs and signals which on the other hand very probably lead the man into difficulties when the behaviour of the system changes. An operator will only make conscious observations if his attention is alerted by an interrupt from the subconscious processes. In consequence, he will only with reliability detect a change in the environment if the convenient, representative information modelled by his dynamic world model is also defining attributes of the actual state of the environment. Likewise, he cannot be expected to cope with a new unique change or event in the system in the proper problem oriented way of thinking if the interrupt is caused by information, which immediately associates to a familiar task or action. It is very likely that familiar associations based on representative, but insufficient information will prevent the operator from realizing the need to analyse a complex, unique situation. He may more readily accept the improbable coincidence of several familiar faults in the system rather than the need to investigate one new and complex fault of low probability. In this way, the efficiency of man's internal world model allows him to be selective and therefore to cope effectively with complex systems in familiar situations, and, at the same time, may lead him into traps which are easily seen after the fact. Davis concludes from an analysis of traffic accidents:

"It is usual for a person to have expectations, or to hold to what may be called an hypothesis about every situation he meets, even when information is notably incomplete. This hypothesis, which is in some degree the product of his previous experience of similar situations, governs the way in which he perceives the situation and the way in which he organizes the perceptual material available to him. As he receives further information, his hypothesis tends to be modified or amended or abandoned and replaced. Sometimes, however, an hypothesis and the expectations which go with it, appear to be unduly resistant to change."

The failure of human operators to identify abnormal states of a plant or system plays an important role in accidents and incidents in complex systems (Rasmussen 1969, Cornell 1969) . However, even if the state of the system is correctly identified, the operator still may be caught in a procedural trap. A familiar, stereotyped sequence of actions may be initiated from a single conscious decision or association from the system state. If the corresponding procedure takes some time; e.g., it is necessary to move to another place to perform it, the mind may return to other matters, and the subconscious actions will become vulnerable to interference, particularly if part of the sequence is identified to other heavily automated sequences.

Systematic human errors in unfamiliar tasks are typically caused by interference from other more stereotyped situations and, therefore, the potential for systematic errors depends

very much upon the level of the operator's skill. The fact that operators can control a system successfully during a commissioning and test period is no proof that operators will continue to do so during the plant lifetime.

RELIABILITY AND SAFETY ANALYSIS

There is a trend towards the situation when a plant concept will only be acceptable, if it can be demonstrated by a systematic analysis that the safety and reliability requirements will be met by the operating plant.

To be susceptible to systematic analysis, a plant design is subject to several constraints related to the limitations and assumptions of the accepted methods of analysis.

Guidelines for system design can therefore be derived **by** an analysis of the assumptions and limitations underlying the methods for reliability and safety analysis.

Methods for systematic analysis of reliability and safety of technical systems are today well developed. The basic method behind such analysis is to break-down a complex system into parts or components, to a level at which component properties are recognized from wide-spread use, so that empirical fault data can be collected. At this level then, probabilistic models of system function can be formed and the resulting reliability and safety figures for the total system can be derived.

SYSTEMATIC RELIABILITY ANALYSIS

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).

Classical reliability analysis leads to figures describing the probability that a system will perform the specified function during a given period or at a given time (M.T.B.F., Availability etc.). Reliability analysis is related to the effects caused by absence of specified function. In case of a process plant reliability, figures are used to judge the expected average loss of production; in case of a safety system to judge the expected average loss of protection.

In this way reliability analysis is closely related to the effects of human errors of omission.

However, human elements cause other problems when considering the basic aspects of reliability analysis. Man is an adaptive and learning system element and very probably will respecify a function or task related to certain observations. This is another way to characterize the possibility of systematic errors discussed above.

Consider for example a monitoring task from a power plant. The specified task: "If the frequency meter indicates below 58 CIS, disconnect load to save the generator". If an operator has only met readings below 58 CIS due to poor meter performance, he may very reasonably respecify his task: "If..... then calibrate meter" - and lose a generator (as happened at one stage in the US power black out in 1965). Unless such respecifications are known, reliability prediction will be systematically wrong.

Furthermore, a human operator is a multipurpose element. He may be occupied by another task, and omission of specified function may be due to other events in the system rather than human failure mechanisms.

In the methods of human reliability prediction in practical use (Meister 1971, Swain 1976) the method of technical reliability in which a system is broken down into components to a level where functions are invariate with application has been transferred to analysis of human performance.

The complex and often very system-specific human functions are broken down into typical, recurrent, and elementary functions for which reliability data can be collected. Such elementary functions are in practice only distinguishable by their external effects, and are therefore generally characterized as "subtasks".

This technique, however, must be used with extreme caution. Man is in many respects a holistic data processor responding to total situations rather than to individual events or system states. Complex functions may be performed by skilled operators as one integrated and automated response. In this case fault data can only be obtained by a realistic simulation of the total function (Regulinski 1973). Break-down of complex functions is only acceptable if the performance is paced by the system, i.e., cues from the system serve to initiate elementary skilled subroutines individually and to control their sequence. This is the case in many manual tasks, e.g., mechanical assembly tasks, but can probably also be arranged by more complex mental tasks by properly designed interface systems.

Another basic difficulty arises when human error data are collected and categorized according to the external effects of human functions, i.e., tasks. As it has been discussed in previous sections, the internal function used to perform a specific external task by a man depends strongly upon his training and skill, his prior experiences of system behaviour, his subjective performance criteria etc.

Therefore, failure mechanisms and probability of error related to performance of a subtask may have no relevance, when the same subtask is found in other work conditions. Especially, it will be extremely difficult to obtain data which are relevant to judge failure probabilities in rare work situations.

Finally, the failure properties of a specific internal function depend upon the operating conditions, and for technical components weighting functions are generally used to modify fault data according to load and environmental effects. The great variability of human performance makes a similar weighting of fault data by "performance shaping factors" mandatory (Swainl976 but the application is difficult as "operating conditions", such as motivation, stress, fatigue, etc., are badly defined and difficult to quantify-. "expert judgements" are generally the only method available.

At the present state of the art, therefore, human reliability prediction is only feasible, if "specified function" of human operators is synonymous with a familiar task performed **by** a skill maintained through frequent use or exercise.

In complex task sequences, the elements must be individually cued by the system. The reliability of tasks requiring more complex mental operations, improvisations, etc., can only be quantified if the result of the task is verified by test or inspection based on predictable human

performance. Prediction of test and inspection reliability will give the lower bounds of the reliability of the total task.

SYSTEMATIC SAFETY ANALYSIS

Whereas reliability figures are related to the probability of specified operation, safety considerations are related to the effects of the terminal state into which the system is brought **by** a fault.

. System safety is a measure of the risk - the expected average loss - related to direct effects of the transitions from specified function into a state of accidental maloperation, in terms of human injuries or damage to equipment or environment.

System safety has to be judged from an extensive accident analysis. To identify the course of events following the initiating fault, and to determine the ultimate effect, and its probability, it is necessary to use a detailed functional description of the system including functional properties both within and outside the normal operating r6gimes of the plant.

In the analysis of accidents, the human element is the imp of the system. His inventiveness makes it impossible to predict the effects of his actions when he makes errors, and it is impossible to predict his reaction in a sequence of accidental events, as he very probably misinterprets an unfamiliar situation. Some illustrating case stories are found in Rasmussen and Taylor 1976.

In practice, human variability makes a quantitative safety analysis unrealistic, unless the system design satisfies a number of conditions.

If a potential for an unacceptable consequence of faults in a system has been identified and the probability of the different chains of events leading to such a consequence is unacceptably high or cannot be determined due e.g. to the possibility of human interference, the design must be changed. This can be done either by inserting barriers or interlocks which will block the course of events or by detecting the advent of risky courses of events at an early phase and releasing protective counteractions. In a way, such monitoring and safety functions solve the variability problem by introducing feed-back paths in the course of events. If this can be realized and the protective function does not in itself introduce potential risks, an upper bound on the probability of a large set of chains of events leading to the effect which is monitored can be derived from a reliability analysis of the barrier or the protective function, which can be automatic or based on human actions.

SUMMARY AND CONCLUSION

To sum up, systematic analysis and quantification of system safety and reliability is not feasible unless the design of the system and the work situation of its operators satisfy several general conditions.

Human reliability:

Necessary conditions for the use of probabilistic methods to predict the probability that a specified task is performed satisfactorily are:

- there is no significant contribution from systematic errors due to redefinition of task, interference from other tasks or activities, etc.;

and

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

and

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

or

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

Probability of unsafe human acts:

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

The probability of specific, abnormal events cannot be quantified unless

- it can be demonstrated that sporadic human acts are not significant contributers to the probability; if necessary by introduction of interlocks or barriers which prevent human interaction;

or

- the effects of human acts are reversible and detectable by a monitoring or safety function which can be performed by operators or automatically.
-

If the reliability of such barriers and safety functions can be quantified then an upper bound of the probability of the event in question can be derived.

Reliability figures and assumptions:

The quantitative results of every analysis describe the reliability of a specific system under certain conditions and assumptions. The result has meaning only to the extent that the system is not changed and the conditions and assumptions are not violated by system operators or managers. The most important part of a reliability and risk analysis probably will be the documentation of conditions and assumptions and a statement of procedures which can protect them from effects of technical and organizational changes (Rasmussen 1973).

As mentioned earlier, the probabilistic method described by Swain (1976) is compatible with the probabilistic methods which are available for quantitative reliability and risk analysis related to technical systems. This method is therefore attractive and promising, but an explicit formulation of the limitations of the method and the criteria to be satisfied by the task conditions to allow its proper use is important. It is also important to formulate specifications for a data and case story collecting scheme which can supply the necessary information and, at the same time, be realistic for practical use.

It seems relevant to test the method by application on a specific system in normal operation. Analysis of human influence upon an automatic protection system like the "Fessenheim" scram system appears to be a realistic test case, because

- the aim is a reliability prediction; i.e., it is related to a normal, specified function;
- the man is not a part of the function itself; i.e., human reliability in stressed situation is not considered;
- the tasks considered will be maintenance, calibration and test which all are preplanned, normal tasks. The task condition can in principle be arranged to fulfil the conditions necessary for reliability prediction;
- since the system is of limited size, analysis to identify potential for effects of both sporadic human actions and systematic errors due to interference from other tasks should be practicable.

REFERENCES

Cornell, C.E. (1968) Minimizing Human Errors Space Aeronavtics 1968, Vol. 49, March, pp. 72-81

Green, A.E. and Bourne, A.J. (1972) Reliability Technology Wiley-Interscience, 1972

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

Rasmussen, J. (1969) Man-Machine Communication in the Light of Accident Records IEEE-GMMS, ERS International Symposium on Man-Machine Systems Cambridge, 1969 IEEE Conf. Records No. 69 (58-MMS. Vol. 3)

Rasmussen, J. (1973) The Role of the Man-Machine Interface in Systems Reliability NATO-Conference, Liverpool 1973 in: Henley, E.J. and Lynn, J.W. (Ed.): Generic Techniques in System Reliability Assessment Noordhoff-Leyden, 1976

Rasmussen, **J.** and Taylor, J.R. Notes on Human Factors Problems in Process Plant Reliability and Safety Prediction Risø-M-1894; RisO Sept. 1976

Regulinski, T.L. (1973) Human Performance Reliability Modelling in Time Continuous Domain NATO-Conference, Liverpool 1973 also in Henley and Lynn (Ed.): Generic Techniques in System Reliability Assessment Noordhoff, 1976

Rigby, L.V. (1969) The Nature of Human Error Sandia Laboratories, SC-DC-69-2062, Oct. 1969
Rook, L.W. (1965) Motivation and Human Error Sandia Laboratories, SC-TM-65-135, Sept. 1965
Swain, A.D. (1969) Human Reliability Assessment in Nuclear Reactor Plants Sandia Laboratories, SC-R-69-1236
Swain, A.D. (1976) Sandia Human Factors Program for Weapon Development Sandia Laboratories SAND 76-0327, June 1976