# Notes on Human Error Analysis and Prediction

**Rasmussen, Jens**

*Published in:*
Synthesis and Analysis Methods for Safety and Reliability Studies

*Publication date:*
1980

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

# NOTES ON HUMAN ERROR ANALYSIS AND PREDICTION[1]

Jens Rasmussen
Risø National Laboratory

## INTRODUCTION

An increasing effort is being put into the study of human error analysis and quantification. Unfortunately, the need for results has been growing more rapidly than the research needed to supply the basic knowledge on human functions in industrial installations and the related human failure mechanisms. Accordingly, the following review will be as much a review of problems as a survey of possible solutions. However, if the conditions under which present methods are applicable can be stated explicitly, then these conditions can be used as design criteria for systems by serving as "criteria of analyzability". Those criteria can then be modified or released as more efficient methods of analysis and better data become available.

## RISK ANALYSIS, THEORY, AND PRACTICE

When discussing the role of the human element in industrial reliability and safety analysis, it is worthwhile to consider the relation between risk analysis and the actual, real life risk of losses due to accidental events.

The outcome of an analysis of the risk imposed by an industrial plant or system is a theoretical construct which relates empirical data describing functional and failure properties of components and parts of a system to a quantitative or qualitative statement of the over all risk to be expected from the operation of the system. This relation is derived from a definition of the boundaries of the system considered; a model describing the structure of the system and its functional properties in the relevant normal and accidental states; together with a number of assumptions made to facilitate the mathematical modeling. These assumptions, the model, and the source of the empirical data, are equally as important parts of the result of the risk analysis as the statement of risk level found. Therefore, in the overall judgment of the risk potential of the system, it is necessary to consider different categories of risk:

• *Accepted Risks.* These are the risks related to the states of accidental maloperation and to the causes and effects considered in the analysis. It goes without saying that any risk of unacceptable magnitude uncovered

---

[1]In: Synthesis And Analysis Methods For Safety And Reliability Studies. Edited by G. Apostolakis, S. Garribba, and G. Volta. Plenum Publishing Corporation, 1980.

during an analysis will result in a change of the design. The functions of the operating staff in the operation and maintenance of the system will be an important part of this analysis.

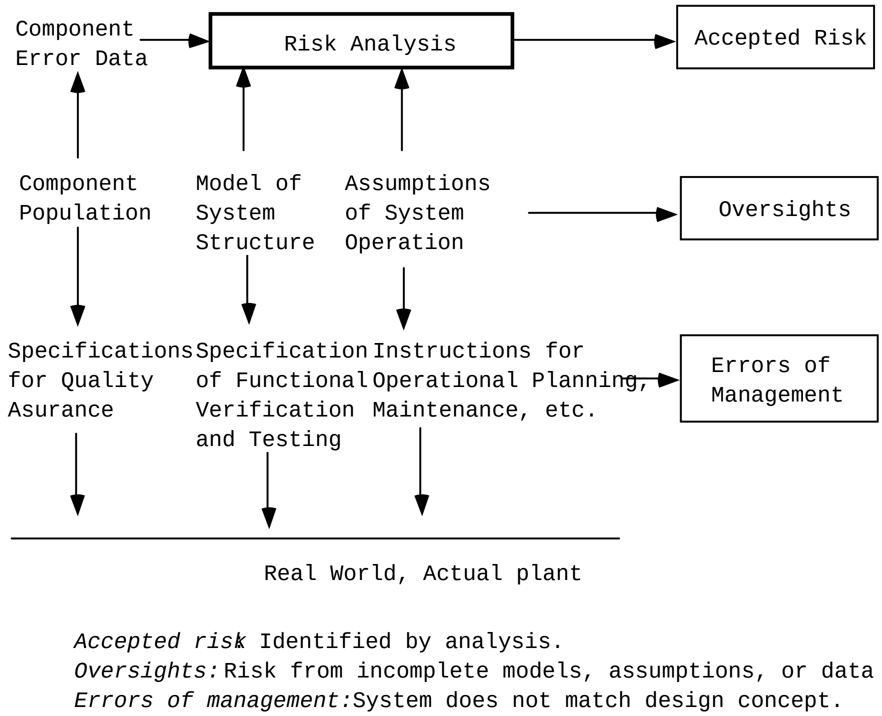


Figure 1. The most important result from a risk analysis is not the accepted risk figure, but the models, data, and assumptions which should serve as instructions for operation.

• *Oversights and Design Errors.* The quality of a risk analysis depends upon the completeness of the analysis. In modern complex industrial installations based on very large production units, an important contribution to the overall risk is due to "major loss" situations of very low probability, often resulting from a complex chain of events including coincidence of errors and from a priori improbable failure modes. Therefore, sources of risk hidden behind an in complete analysis become a major problem. Whether such discrepancies between the analytical model and the actual plant are considered to be design errors or errors of analysis depends upon what is taken for given. The general problem of verifying the completeness of an analysis and thus insuring that a safety-related design target has been met, can very probably lead to the need for criteria related to "design for risk analyzability".

• *Errors of Management.* The value of a risk analysis largely depends upon the degree to which the actual, operating plant will satisfy the conditions and assumptions underlying the analysis. Again, this largely depends upon the managerial organization within the plant. This type of risk is related to such activities as planning of quality control, inspection, and testing which serve to ensure that the components and parts of the plant do match the populations forming the base for the empirical fault data, and that the plant is built according to the design specification and will not be subject to modifications and changes without proper risk evaluations. This relates to the technical equipment as well as to selection, training, and organization of operating staff and to the design of work procedures and operating instructions.

It lies in the nature of oversights and errors of management that they are tied to human errors, but it also lies in the variety and complexity of organizations and design activities that quantitative risk modeling in these areas is practically impossible at present. However, a comprehensive qualitative analysis has been made by Johnson (1973).

The following discussion of the systematic analysis of the human role in system reliability and safety will be concerned with the analysis behind the first category of risk discussed in the previous section (i.e. accepted risks). It follows from the nature of things that over sights are not included. "Errors of management" are violating the basic assumptions of the systematic methods, and they are therefore not considered explicitly in the discussion.

However, what is meant by "systematic analysis" is not always evident and invites some discussion. In the present paper, systematic method will be synonymous to engineering analysis when viewed as the alternative to expert judgment, which is taken to be more akin to the performance of a professional art. In general, engineering analysis is based on quantitative data and invariate relations applied to systems and structure which are accessible to inspection or control. Practically speaking, the opposite is often the case for the behavioral sciences which depend upon personal, professional skills. It is a "well-known fact that the aim of a skillful performance is achieved by the observance of a set of rules which are not known as such to the person following them" (Polanyi 1958). Clearly, great care should be taken when including human behavior in engineering models. In addition, a drastic limitation in the cases which can be handled must be expected, if the analysis is to be based on formalized, systematic methods rather than on expert judgment.

Of course the importance of this aspect depends upon the application of the reliability and safety analysis. If the analysis is used for a relative ranking of different alternative solutions during system design, a number of conditions can be considered equal, and the criteria for analyzability will lead to less tight constraints compared with the situation where the analysis aims at a verification or documentation of the design target in terms of quantitative risk level.

A special problem is caused by current developments of large scale computer codes for overall system reliability and safety analysis. This development is ahead of the formulation of acceptable models of human functions and error mechanisms in the systems under consideration.

Consequently, the only solution for the time being is to include simplistic models of human performance. To be compatible, such models are depending on the mathematical or logical structure of the program rather than on psychological properties. This is acceptable as long as such human error models are used only for sensitivity analysis, to determine the range of uncertainty due to human influences. If quantitative risk figures are de rived, these should be qualified by the assumptions underlying the human error models used, and by a verification of the correspondence of the assumptions to the system which is analyzed.

## "Human Error" - Definition and Classification

The term "human error" is loaded and very ambiguous. Basically, a human error is committed if the effect of human behavior exceeds a limit of acceptability. Of course, the classification of a specific behavior as an error depends as much upon the limits of acceptability as it depends upon the behavior itself. In practice, the limits are sometimes defined after the fact, by someone who can base his judgments on a careful, rational evaluation of the function of the system, while the specific behavior possibly was a quick response in a stressed dynamic situation. Therefore, as it has been argued by 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 behavior. Furthermore, as discussed by Rigby (1969), errors can be classified as *random errors*, due to random variability of human performance such as variations in manual precision or force; differences in timing; simple mistakes; and slips of memory; as *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. From this definition it follows that it is difficult to give general characteristics of sporadic errors.

The influence from *random errors* largely depends upon 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, and the opportunity given the operator to monitor his performance and correct the errors he commits.

*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 the context of monitoring and supervisory task in auto mated systems where the operators typically have to respond to changes in system operation by corrective actions.

In the present general discussion, two types of systematic errors seem to be important and 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, avail ability of state information, background knowledge on system functioning, 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 several kinds of procedural traps. During normal work condition human operators are extremely efficient due to a very effective adaptation to convenient, representative signs and signals. On the other hand, these will very probably lead the man into difficulties when the behavior of the system changes. An operator will only make conscious observations if his attention is alerted by an interrupt from the subconscious processes. This means that he will only deal with the environment consciously when his subconscious, automated, or habitual responses no longer will control the environment adequately. Likewise, he cannot be expected to cope with a new unique change or event in the system in the 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 analyze 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 (Davis, 1958):

> "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 importance of the different categories of errors depends upon the task conditions. In repetitive tasks which are preplanned, errors due to demands exceeding resource limits and errors due to procedural traps, etc., will be of minor importance since when experienced they are readily removed by re-design of the task. Therefore, random errors related to human variability would typically be more prevalent.

On the other hand, systematic errors are significant contributors when operators have to respond to abnormal plant condition during monitoring and supervisory tasks. Reviews indicate that 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 1968). However, even if the state of the system is correctly identified, the operator may still 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 identical 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 life time.

A basic problem when dealing with systematic erroneous responses to unfamiliar situation is the very low probability of such complex situations. In a properly designed system there should be a reverse relation between the probability of occurrence of an abnormal situation and its potential effect in terms of losses and damage. In modern large centralized systems, the consequence of faults can be very 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 realistic scenarios modeling the relevant situations.

Sporadic errors are, by definition, infrequent errors which are not caused by excessive variation in the normal pattern of behavior, but rather are extraneous acts with peculiar effects. They must be considered in risk analysis even though they are insignificant contributors to error rates because they are likely to escape the designer's attention. Therefore, they may not be covered by the automatic protective systems and can cause chains of event with large consequences.

## Reliability and Safety Analysis

In discussing the methodological problems of including the human element of a system in a systematic analysis, it appears to be practical to consider the problems related to reliability analysis and safety analysis separately. The terms, safety and reliability, are not too well defined. In the following discussion, they are used to characterize two different aspects of the sensitivity of a process plant to accidental maloperation.

*Reliability* is a measure of the ability of a system to maintain the specified function. 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.

*System safety* is related to the risk, i.e., the expected average losses, caused directly by the *presence of a state of accidental maloperation*, in terms of human injuries, loss of equipment etc. To judge the safety of a system, it is, therefore, necessary to study the probability of specific courses of events initiated by the primary fault, and to relate the probability to the effects of the maloperation, i.e., judgment of system safety is based upon an extensive accident analysis.

In the following discussion a very clear-cut distinction between the methods used for reliability and safety analyses is drawn, and very simplistic descriptions of the methods are used. This is tolerable since the purpose of the discussion is to reach some general conclusions regarding the conditions which should be met by a system in order to make a systematic risk analysis possible.

## HUMAN FACTORS PROBLEMS IN RELIABILITY ANALYSIS

The definition of the reliability of a system or system component is generally stated in terms of the probability of a specified function versus time, such as: "Reliability is defined as that characteristic of an item expressed by the probability that it will per form 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).

Reliability analysis is concerned with the departure from the specified function of the plant and its parts and components. "Specified function" is rather stable during plant operation and is unambiguous related to the functional design intention. Therefore, the frame of reference of reliability analysis is generally well established. The basic method of reliability analysis is to decompose a complex system into parts or components, to a level at which component properties are recognized from widespread use, so that empirical fault data can be collected. In principle, this break-down must be carried through to a level where component function is invariate with application. This is possible for many standard components, which are designed for a specific function and used according to specifications in system design, e.g., resistors, pumps. In some cases, however, alternative "specified functions" are possible at the level of break down at which data collection can be arranged. For example, in practice relays and valves can serve to close or break a circuit. Fault data must then be classified according to the function performed, as the related probabilities of failure may be very different for different functions.

Overall reliability characteristics of the system are derived by means of models representing the relations between component and system failures. The degree of sophistication of the probabilistic system models used to derive reliability figures characterizing the total system depend upon the quality of the component fault data available. If only bulk data on component failure rates are available, as is typically the case for process plant components, simple probabilistic models are used which represent system structure only as far as to specify whether components functionally are connected in series or parallel during specified system function (reliability block diagrams, simple fault trees). If more detailed descriptions of failure mechanisms are available, and if good data are available for failure and repair rates, then much more complete failure modeling becomes worth while.

In the methods of human reliability prediction in practical use (Meister 1971, Swain 1973), this technique has been transferred to human performance. The complex and often very system-specific human functions are broken down into typical, recurrent functions for which re liability 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 must, however, be used with caution, since the human element within a technical system has properties which cause difficulties with respect to the basic aspects of reliability analysis:

Man is an *adaptive and learning system element*, and may very probably re-specify a function or a task. Consider for example a monitoring task from a power plant. The specified task: "If the frequency meter indicates below 58 C/S, disconnect load to save the generator". If an operator has only met readings below 58 C/S due to poor meter performance, he may very reasonably re-specify 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 re-specifications are known, reliability prediction will be systemsystematically 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.

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 per formed by skilled operators as one integrated and auto mated 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.

The failure properties of a specific 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 (Swain 1973), but the application is difficult as "operating conditions", such as motivation, stress, fatigue, etc., are badly defined and difficult to quantify; "expert judgments" are generally the only method available.

New problems arise if *several internal mechanisms* with very different failure probabilities can serve the same external component function. The more flexible a component is, the more difficult will these problems be, especially if the internal organization has autonomous features such as optimization, adaptation, learning. These are the prominent features of the human elements in a system. The internal process used to perform a specific external task by a man depends strongly upon his training and skill, his prior experiences of system behavior, his subjective performance criteria etc. Failure data collected from a system in which an operator meets a specific task frequently and performs it by a sensory-motor response will have no relation to the failure probability in a system where the demand for the task is infrequent, e.g., as part of an emergency action. The response will then probably be performed by a sequence of cognitive functions. The resulting problem can only be solved by classifying fault data according to the internal functions used to perform a task. In this situation, weighting of fault data collected from standard, frequently initiated tasks, by means of "performance shaping factors" is not acceptable. At present, this means that human reliability prediction is only feasible, if "specified function" of human operators is synonymous with a familiar task per formed by a skill maintained through frequent use or exercise.

A human trait having great influence upon the reliability of human performance is the ability of *self monitoring and error correction*. The mechanism of error detection depends upon the task situation and the intention of the operator. If the intention is to perform a given sequence of actions, as will be the case in most familiar and stereotyped tasks, error detection will typically be due to difficulties in the sequence caused by errors in the preceding steps. It is obvious that this kind of error detection has drastic effects on re liability. The probability of selecting the wrong key in your key-ring is high; however, the probability that you should not succeed in entering your house of this reason is nil.

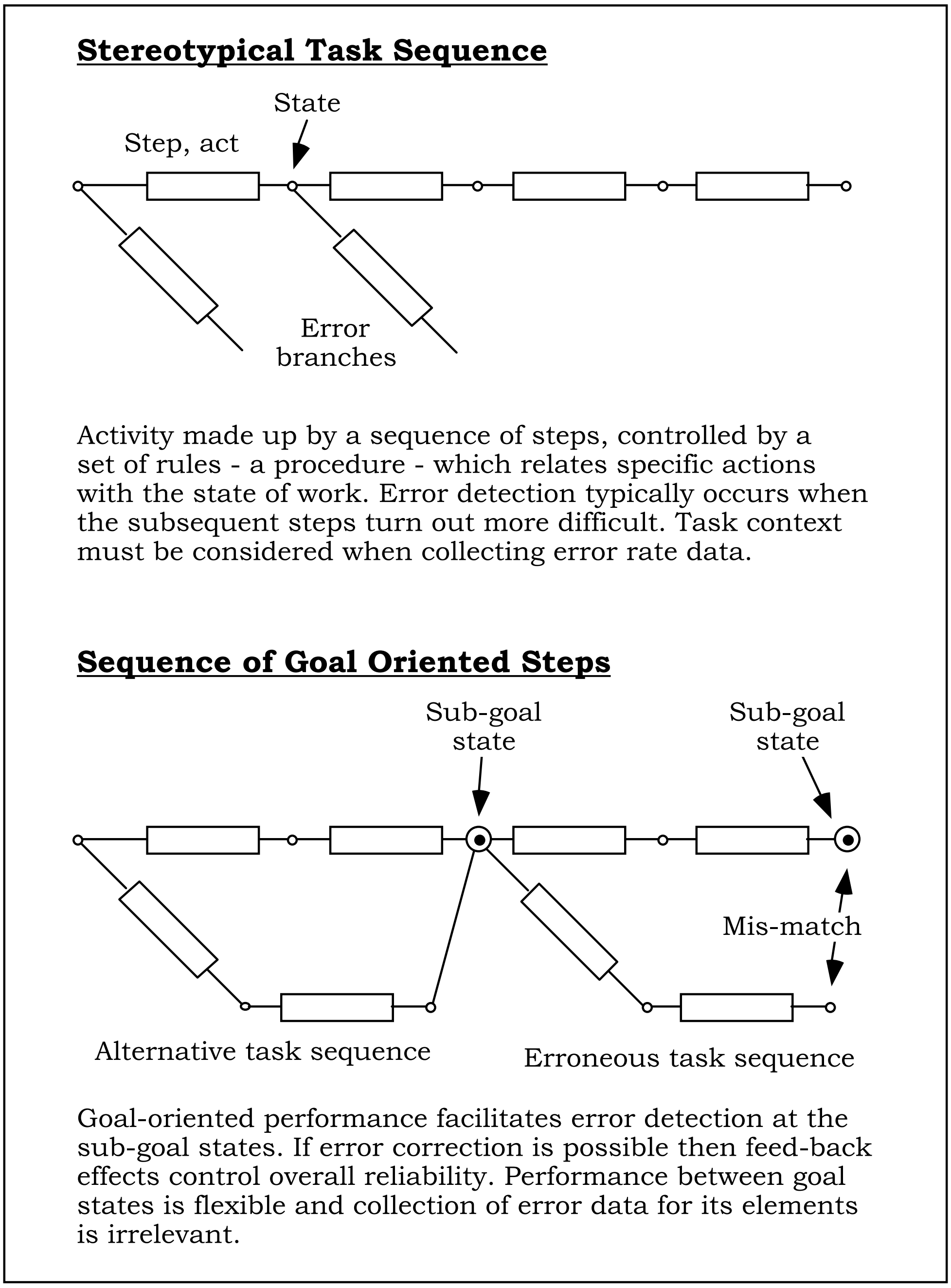


Fig. 2. Simplified illustration of typical task structures.

In more open and flexible situations, the human intentions will typically be related to attainment of a specific goal, and the reliability in reaching the goal will be related to the persistence in the intention and the care with which a discrepancy is observed or detected, rather than error probability during the striving towards the goal. If you intend to spend a comfortable night reading a good book, the probability of success is not related to the error rate in operating the lamp switch nor to the reliability of the power system, but rather to the probability of having a supply of candles and matches or the proximity of a good restaurant.

Clearly, the error correction features of a task depend upon the structure of the sequence, and not on the individual steps. The potential for error correction influences the reliability of the task drastically and determines which parts of the task should be considered in detail as well as the data needed in an analysis.

Monitoring and error correction act as a feed-back loop around the task performance, and the overall quality of the basic performance itself. In addition to the use of this feed-back feature to improve the reliability of a task design, a proper design of the error detection and correction function can be used as the means for making a reliability analysis of the total task practical, since the lower limit of the overall reliability can be determined independently of the error rate by the re liability of the monitoring function alone together with the frequency of error opportunities. This may be the only way to assess the reliability of poorly structured complex human performance - e.g. in response to unfamiliar situations. It should also be noted that the influence of error correction features of a task will lead to a strong dependence of the error rates collected for human actions upon the context from which they are collected.

To sum up, systematic analysis and quantification of *system reliability* is not feasible unless the design of the system and the work situation of its operators satisfy some general conditions. Necessary conditions for the use of decomposition methods to predict the probability that a specified task is performed satisfactorily by human operators 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 separate subtasks at a level where failure data can be obtained from similar work situations;

*and*

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

*or*

- if these conditions are not satisfied, e.g., because the task is performed as one integrated whole, or it is performed by complex and variable human functions such as higher level cognitive functions, then the effect of the task must be reversible and subject to an error detection and correction function, which in turn satisfies the above-mentioned conditions for predict ability.

In this discussion it has been assumed that empirical data on human error rates in industrial process plants are available. Unfortunately, such data are very scarce. Most of the data discussed in the literature seem to be derived from the original work done at the American Institute of Research (Payne et al. 1962, Munger et al. 1962) or to be very general estimates. Systematic data collection in industrial plants has not been reported apart from the Licensee Event Reports published by US-NRC (see later). Error rates are difficult to derive from these reports because the denominators, the number of error opportunities, are not known. An attempt to estimate the denominators to be used with the Licensee Event Reports has been made by Fullwood et al. 1976.

**HUMAN FACTORS PROBLEMS IN SAFETY ANALYSIS**

System safety is related to the risk, i.e. the expected average loss, in terms of human injuries or dam age to equipment or environment, caused by transitions from specified function into a state of accidental maloperation.

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 regimes of the plant. Different systematic techniques have been developed for this purpose, based on fault tree analysis (Fussel 1973, Powers 1973) and cause -consequence analysis (Nielsen 1971, Taylor 1977).

To evaluate the effects of accidental maloperation, statistical data differentiating the different modes of failure of the components must be available. Furthermore, severe effects are generally results of course of events of extremely low probability, and may be related to component modes of failure which are a priori improbable and insignificant contributors to component bulk data.

In the analysis of accidents, the human element is the imp of the system. The human reliability, i.e., the probability that operators perform the "specified functions" is of course an important factor in system safety, e.g. when operators are assigned special monitoring and protective functions. In safety analysis, however, a more difficult problem is the analysis of the effect of specific, erroneous human acts. The variability and flexibility of human performance together with human inventiveness make it practically impossible to predict the effects of an operator's 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.

These cases indicate that search strategies used to identify accidental chains of events in the technical system will not be adequate to identify the human potential for creating hazardous situations. In general, search strategies related to fault tree analysis and cause-con sequence analysis are sufficient to identify the effects on one part of a system from errors which an operator commits during work on that part due to mistakes etc. How ever, contrary to reliability analysis, a safety analysis cannot solely be based on search strategies which use the specified task as a guide or structure. Effective search strategies have to take into account the fact that operators are multipurpose components moving freely around in the system. Rare, but risky events in one part of the system can be caused by erroneous acts by operators working on quite different parts of the system; such as disconnection of cables to facilitate vacuum cleaning; interference from manipulation of electric welding gear; short circuits from dropped tools. These types of errors must be found by a search guided by a topographical proximity criterion - analysis of all activity close to the part of the system in question. Furthermore, psychological proximity should be considered. It happens that features of an unfamiliar situation demanding a special procedure instead release an automated routine belonging to other task conditions, especially if parts of the two task sequences psychologically speaking are very similar. Examples are given in the case stories in the appendix.

However, a heuristic search based on these criteria may not be sufficient to identify the potential for high consequence, low probability situations which typically are related to complex situations caused by several coincident abnormal conditions and events. A heuristic strategy to identify such situations resembles a design algorithm: First, potential for accidents such as high energy accumulations, toxic material concentrations etc. are identified together with potential targets for accidental release such as people, environment etc. Then possible accidents are designed, i.e., the technical (mal) functions and human actions which are necessary to form the route from source to target are determined. Finally, it is determined how changes in the normal system together with coincident normal and abnormal human activities will meet the designed accident pattern. Such accidents are sometimes due to "sneak paths" which are formed by minor mishaps or malfunctions in simultaneous human activities which only become risky in case of very specific combinations and timing.

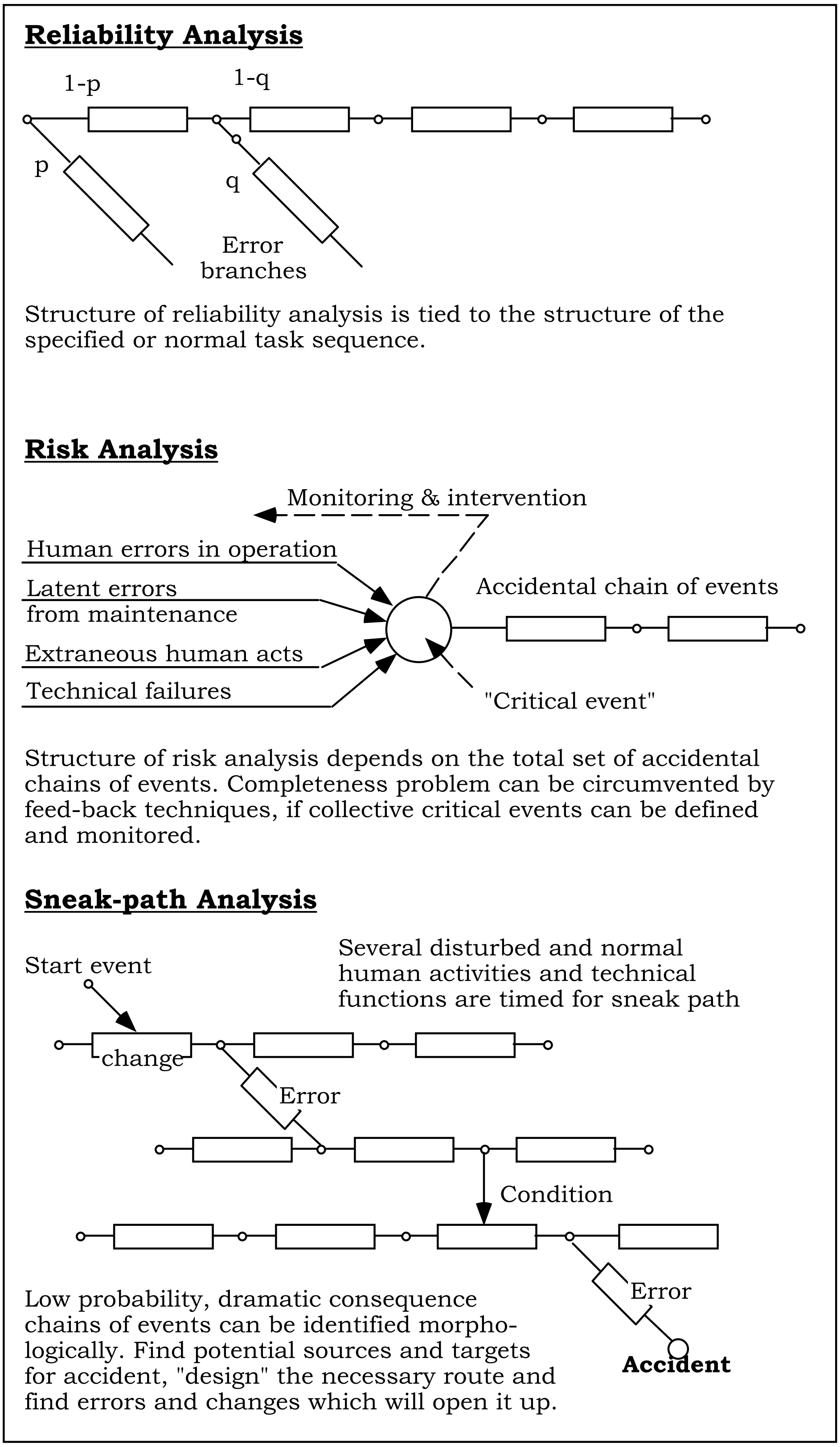


Fig.3. Simplified illustration of typical structures of analysis.

In practice, therefore, human variability makes a quantitative safety analysis unrealistic, unless the system design satisfies a number of conditions. Like other problems in system design caused by component performance the problems in accident analysis can be circumvented if feed-back functions are introduced, i.e., if feed-back links are introduced in accidental courses of events by means of monitoring and correction functions, as it has also been discussed in the previous section. Major losses or human injuries caused by accidental mal operation are typically related to uncontrolled release of stored energy in the system. Apart from accidents caused by spontaneous fractures of energy barriers and explosions, accidents are typically the effects of disturbances of mass or energy balances. There is, therefore, a time delay between the primary cause and the release due to the integrating effect of a disturbed balance. This time delay makes correcting actions possible.

Furthermore, critical variables related to the energy level of the balance can be found which can indicate potentially risky maloperation irrespective of the preceding course of events. If a safe state of the system can be defined, and it can be reached through the action of a monitoring and protection function which does not in it self introduce potential risks, an upper bound of the probability of a large class of event sequences leading to the effect which is monitored can be found by a re liability analysis of the protecting function together with the frequency of error opportunities. Such protective functions can be performed by human operators if the task is designed so as to be accessible to human operator reliability analysis, or can be performed by automatic safety systems.

A properly designed protective function enables the derivation of the probability figures needed in accident analysis by means of a reliability analysis of the protective function. Together with data on the frequency of error opportunities, this analysis leads directly to upper bounds on probability of courses of events leading to the effect which is monitored. It is the extensive use of automatic, protective systems in nuclear power plants that has made it possible to perform a quantitative analysis - including human performance - of the safety level of such installations (Norman Rasmussen et al. 1975).

The difficulty to get the empirical data from real life situations needed to predict the probability of specific erroneous human acts which are possible contributors to rare chains of events leading to accidents, results in the following conditions for quantification of system safety:

The probability of specific consequences of accidental events in a system can only be derived by a decomposition analysis:

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

*or*

- the effects of erroneous 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 from the frequency of error opportunities.

## THE TASK OF CALIBRATION AND TESTING

As a basis of a more specific discussion, the task of calibration and testing has been chosen since it has a great influence upon the reliability of automatic safety systems. The following data are based on a review of "Licensee Event Reports" as they are edited and compiled by "Nuclear Power Experience". The reports reviewed are from the January 1978 state of the collection and include those in the category of operator/technician errors: *calibration, setting and testing.*

In general, reliable statistical information on human error rates related to different types of human errors is difficult to gather from this kind of event reporting. While the denominator problem of obtaining the actual frequency of error opportunities can be solved in principle, the reports do not actually give information on the total frequency of errors committed, but rather the frequency of errors which are not immediately corrected by the operator himself. This means that the frequencies of different categories of errors found in the reports are heavily biased by factors depending upon the specific work situations. Clearly, human errors which lead to latent system faults or to effects which are not reversible by immediately counteraction will typically find their way to the reports.

To judge the effect of error recovery and to relate the errors found in the reports to task content in general, a description of the task in rather general terms is useful. Generally, the task of calibration is a well defined, proceduralized task. The system states, goals and procedures implied in the task are familiar to the operator and subject to formal instruction and training. The errors to be expected are typically omission of steps in the procedure and faults/mistakes related to rather elementary acts. Problems related to conflicts of goals and misinterpretation of system states, which are typical of responses to unfamiliar situations, are of minor importance in the present context.

The task of calibration consists of subtasks of different content, and a preliminary review of the case stories indicates that the following phases should be treated separately:

1. *Establishment of the test circuit.* The component or subsystem to be tested is isolated from the plant and connected to the test equipment.
2. *The calibration act.* The test equipment and/or the sub system to be tested is manipulated or adjusted according to a specified procedure, and the response is compared/judged according to the specified standard in order to obtain agreement.

3. *Restoration of normal operating condition of the system.* The test equipment is removed, and the normal "line-up" of valves and switches in the system is restored.

| | | Task Elements | | |
|---|---|---|---|---|
| | | Test circuit set-up | Adjustment; calibration | Restoration of normal operation |
| Omissions | Functionally isolated acts | 12 | | **50** |
| | Others | 1 | 2 | 1 |
| Errors in task | Improvisation, insufficient knowledge | 2 | | |
| | Secondary conditions not considered | 3 | 3 | 3 |
| | Misinterpretation | 2 | 2 | |
| | Mistakes among alternatives | 4 | **13** | 3 |
| | Manual variability, 'clumsiness' | 1 | 1 | |
| | Topographic misorientation | 3 | | |
| Extraneous acts | 'Clumsiness' | 1 | | |

Table 1. Human error modes in 111 cases from test and calibration in nuclear power plants

The principal observation is the high contribution from omissions of steps in the procedure. It should be noted that nearly all these steps are functionally unrelated to the calibration itself and include such things as return of switches or valves to operating position after test; check of standby channels before disconnecting a channel for test; or purely administrative steps (table 1). It should also be noted that most of the omitted steps are found in the last phase of the task. One explanation of the large contribution from such omissions could be that the effect of these omissions is not directly apparent which therefore prevents any immediate recovery. How ever, this may not be the only cause. The fact that the steps omitted are unrelated to the prime goal of the task - the calibration - may in itself lead to a high probability of omission. In an analogous context, Whorf (1956) in analyzing causes of industrial fires observes that "the name of a situation affects behavior" - which can lead to similar effects. It is also noteworthy that this type of error to some extent is repeated in several redundant channels (see table 2).

| Number of Channels | Number of Cases |
|---|---|

| | |
|---|---|
| 1 | 95 |
| 2 | 11 |
| 3 | 2 |
| 4 | 2 |
| 17 | 1 |

Table 2. Common mode errors in test and calibration

Another significant class of errors are "faults and mistakes" which mainly include two types: One is mistakes such as replacement of sample size with that of another task; use of positive correction factor instead of negative; calibration with increasing pressure instead of decreasing, etc. Another type is the faults concerned with incorrect or inaccurate set points. This class of error is most significant within the calibration act itself, which is the only part of the task subject to quantitative specifications and which may lead to mistakes without immediate detectable functional effects. Broadly speaking, we here have two related kinds of error: Variability and inaccuracy in a quantitatively specified adjustment and mistaken interchange of two or more possibilities.

During the first phase of the task, the establishment of the test circuit, the different types of errors all contribute. This might be expected a priori, since this phase gives the operator most freedom for action, and there will be large differences in task conditions between different types of circuits or components to be tested or calibrated. Again the largest group is omission of functionally isolated - including administrative - acts. Extraneous acts are found only in this phase, and two types are noted - effects on other systems can be caused by in appropriate spatial orientation such as misplacement of jumpers, or by simple "clumsiness".

One type of error affecting all three phases is due to change of procedures in a way that secondary features affect the calibration, i.e. influence of properties of the system which are not effective or obvious when the prescribed procedure is used. They may have the character of procedure "improvements": Adding recorders (which load signal sources); too rapid adjustments (not considering time constants); use of another available size of filter paper (which changes calibration) etc.

The following comments can be made regarding the predictability of the reliability of this specific task:

- Systematic errors play a minor role in the cases considered.
- The task of calibration can be broken down into rather independent subtasks which are frequently performed and for which empirical fault data therefore can be collected. Error rates of the following categories of error are relevant:

- Omission of acts which are functionally isolated from the task sequence.
- Using the wrong alternative of two possible, when the choice has no functional effect upon the subsequent steps.
- Spread in accuracy when adjusting variables to reference values.
- Operational "improvement" of procedures by exclusion of secondary conditions which have no immediate influence upon the task.

There is no indication in the cases reviewed that extraneous acts committed during work on other systems or during other activities play any role in the availability of the systems. In some cases mis-calibration or defeat of system function is explained in the event report by such extraneous, inadvertent acts, but the number is insignificant.

Special problems are found in redundant safety systems in attempting to predict the probability of repetition of errors in subsequent calibration tasks. The cases reviewed indicate that repetition of "omission of functionally isolated acts" in subsequent tasks plays an important role, but, as could be expected, there is also an indication that systematic errors caused by misinterpretations and operational "procedure improvements" play a much more significant role in the overall re liability of redundant systems. Therefore, to make probabilistic prediction meaningful, Strict control of the task sequence and its content by constraints from equipment design is necessary to limit effectively the possibility of improvisation and "improvement". This also places a need for hard constraints upon the *managerial system, which can be the source of changes leading to common mode errors.*

In passing it should be mentioned that the causes behind the dominant types of human errors can very probably be removed through a proper design of equipment and work content. For instance, equipment can be designed so as to link necessary, but functionally isolated acts, tightly to other acts which lead to immediate apparent functional effects if they are omitted. From the present review of event reports it appears that even a simple reliability analysis of the task sequence, based on human reliability data presently available, can support a redesign of the calibration task.

In conclusion, the features of the task of calibration and testing are such that the reliability of the task can be estimated if empirical error rates can be obtained.

The Licensee Event Reports supply valuable information on human errors in this task, but further in-plant investigations are needed to supply denominator figures or error rates. Furthermore, analysis of operator's opportunities of self-monitoring and error correction in the specific work situations will be needed to facilitate general use of the data.

## CONCLUSION

In principle, a process plant design, which is not based on extensive experience from similar concepts, is only acceptable if performance design targets can be verified by systematic analysis including a quantitative re liability and safety analysis.

A quantitative safety analysis is only possible if the plant design is performed according to guidelines derived from the limitations of the available methods.

The design must be based upon a qualitative accident analysis. Accident potentials cannot be identified by an evaluation of the effects of all possible courses of accidental events. They must be identified directly by a systematic search. Heuristic search strategies related to energy and poisonous matter concentrations have been developed to serve this purpose (Johnson 1973, Powers 1973).

When accident potentials are identified in this way, the sequences of accidental events, which are capable of triggering an accident, must be identified by a systematic, qualitative cause-consequence or fault tree analysis. If a quantitative probabilistic evaluation of the sequences so identified indicates unacceptable risk - or if a quantitative analysis is not possible due to lack of statistical data, monitoring and protection functions must be introduced in the design.

Such functions must be designed so as to be accessible to a quantitative reliability analysis. During the reliability analysis of complex protective systems, it is generally important to keep track of the temporal relations of events, and simple reliability block diagram analysis must be replaced by more sophisticated methods, such as Markov models, renewal theory etc., compatible with an analysis of causal chains of events.

A protective function can be performed by an automatic system or a human operator.

Reliability analysis of human performance is only feasible if the tasks are performed by sequences of skilled subroutines which are separated and initiated by proper cues from the system. The reliability of more complex and free-running tasks cannot be predicted directly; an acceptable prediction of results can only be made in this situation if the effects of the actions are reversible and subject to verification by an operator, following a predictable check procedure, or covered by an automatic protective function.

Automation in this way does not remove man from a system, neither does it force him into the role of a trained robot. Automation serves to replace unexpected tasks at unpredictable moments by tasks which can be planned and trained and which can be based upon qualified decisions, such as supervision, test, and maintenance.

A proper design policy will decrease the influence of unpredictable performance shaping factors, such as stress and motivation. When introducing automatic safety systems, the designer takes responsibility of plant safety and thus relieves the operator from stress. The actions of safety systems are related to rather general criteria concerning the initiating plant states and complex, safe protective systems will decrease plant reliability. The operator thus has a supervisory task to protect the plant from unnecessary automatic safety actions. The responsibility of the operators is related to the reliability of plant operation.

The motivation of plant operators can be maintained in automatic systems if they are allowed to use their abilities and take responsibility in the tasks they are allocated. There is no reason not to permit this as long as the system is designed in a way which allows them to verify the effects of their decisions and actions in a predictable way.

## REFERENCES


Cornell, C. E., 1968. "Minimizing Human Errors". Space Aeronautics 1968, Vol. 49, March, pp. 72-81.

Davis, D. Russel, 1958. "Human Errors and Transport Accidents". Ergonomics 2, pp. 24-33.

Fullwood, R. R., and Gilbert, K.J., 1976. "An Assessment of the Impact of Human Factors on the Operations of the CRBR SCRS". Science Applications Incorporated Report SAI-010-76-PA.

Fussell, J.B., 1973. "Fault Tree Analysis - Concepts and Techniques'. NATO Conference Liverpool 1973. In: Generic Techniques in Systems Reliability Assessment. Edited by E. J. Henley and J. W. Lynn. NATO Advanced Study Institute. (Nordhoff, Leiden, 1976).

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

Johnson, W. G., 1973. "MORT - The Management Oversight and Risk Tree". Prepared for the U. S. Atomic Energy Commission. SAN 821-2. Submitted to AEC. February 12, 1973.

Meister, D., 1971. "Comparative Analysis of Human Reliability Models". AD-734 432, 1°71.

Munger, S. J., Smith, R. W., and Payne, D., 1962. "An Index of Electronic Equipment Operability: Data Store". American Institute for Research Report AIR-C-43-1/62-RPL. Contract DA-36-039-SC-80555.

Nielsen, D. S., 1971. "The Cause-Consequence Diagram Method as a Basis for Quantitative Reliability Analysis". Risø-M-1374. ENEA CREST, May 26-28, 1971.

Nielsen, D. S., 1974. "Use of Cause-Consequence Charts in Practical Systems Analysis". In: Reliability and Fault Tree Analysis. Theoretical and Applied Aspects of Systems Reliability and Safety Assessment. Papers of the Conference on Reliability and Fault Tree Analysis. Berkeley, September 3-7, 1974. Society for Industrial and Applied Mathematics. Philadelphia, 1975, pp. 849-~80.

Nuclear Power Experience. Edited by Nuclear Power Experience Inc., P. O. Box 544, Encino, California.

Payne, D., and Altman, J. W., 1962. "An Index of Electronic Equipment Operability; Report of Development." AIR-C-1/62 FR.

Polanyi, M., 1958. "Personal Knowledge". Routledge and Kegan Paul. London 1958.

Powers, G. J., and Tomkins, I. C., 1973. "Fault Tree Synthesis for Chemical Processes". AICHE Journal Vol. 20 No. 2, pp. 376-387.

Powers, G. J,, and Lapp, S. A., 1977. "The Synthesis of Fault Trees". In: J.B. Fussel and G. R. Burdick (Eds.): Nuclear Systems Reliability Engineering and Risk Assessment. SIAM, Philadelphia, 1977.

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

Rasmussen, N. et al., 1976. "Reactor Safety Study, Appendix 2". WASH-1400.

Regulinski, T. L., 1973. "Human Performance Reliability Modeling in Time Continuous Domain". NATO Conference, Liverpool, 1973. Also in Henley and Lynn (Ed.): Generic Techniques in System Reliability Assessment,

Nordhoff, 1976.

Rigby, L. V., 1969. "The Nature of Human Error". Sandia Laboratories, SC-DC-69-2062, October 1969.

Rook, L. W., 1965. "Motivation and Human Error". Sandia Laboratories, SC-TM-65-135, September 1965.

Swain, A. D., 1973. "Improving Human Performance in Production". Industrial and Commercial Techniques Ltd. 30-32 Fleet Street, London EC4.

Swain, A. D., 1969. "Human Reliability Assessment in Nuclear Reactor Plants". Sandia Laboratories. SC-R-69-1236.

Taylor, J. R., and Hollo, E., 1977. "Experience with Algorithms for Automatic Failure Analysis". In: J.B Fussel and G. R. Burdick (Eds.): Nuclear Systems Reliability Engineering and Risk Assessment. SIAM,

Philadelphia, 1977.

Whorf, B. L., 1956. "The Relation of Habitual Thought and Behavior to Language". In: Language, Thought and Reality. Selected Writings of Whorf. Ed. John B. Carroll, MIT Press, 1956.

## APPENDIX

The following case stories illustrate some of the phenomena which make reliability and safety prediction difficult. Unless otherwise indicated, they have been obtained from private communications with process plant operators. In such cases details have been deleted and the information generalized to avoid reference to the source.

### CASE 1

During normal operation of a process plant the power supply to the instrumentation and the control console slowly disappears.

**Investigation**
The manual main circuit breaker in a motor-generator supply is found to be in the off position. The conclusion of an investigation was that a roving operator, inadvertently had switched from a routine check-round to the Friday afternoon shut down check-round and turned off the supply. The routes of the two check-rounds are the same, except that he is supposed to pass by the door of the generator room on the routine check, but to enter and turn off the supply on the shut down check. Something "en route" obviously has conditioned him for shut down check (sunshine and day dreams?). The operator was not aware of his action, but did not reject the explanation.

**Comments**
Human operators move around in the plant, and it can be difficult to predict where in the causal structure of the plant he interferes. His actions may not be initiated by an event in the system or specified by a program, but by subconscious mechanisms, i.e. it is difficult to predict when he interferes and how.

### CASE 2

During start up of a process plant the plant is automatically shut down during manual adjustment of a cooling system.

**Investigation**
During start-up the operator monitored the temperature of a primary cooling system and controlled it by switching off and on a secondary cooling pump to avoid water condensation in the primary system due to the cold cooling water. On this occasion he observed the temperature to reach below the low

limit, signaling a demand to switch off the secondary pump, while he was talking to a co-operator over the phone. He then switched off the primary pumps and the plant immediately shut down automatically. He did not recognize the cause immediately, but had to diagnose the situation from the warning signals.

The control keys for the two sets of pumps are positioned far apart on the console. A special routine exists during which the operator switches the primary pumps on and off to allow an operator in the basement to adjust pump valves after pump overhaul while they communicate by phone. Is the cause of the event subconscious switching of procedures due to the phone call?

**Comment**

The case illustrates some features of operator behavior:

- Change in procedures by secondary, unpredictable events or conditions.
- The operator introduces couplings in the system by coincident omission of one task and performance of an in appropriate action.
- The risk may be related to the inappropriate and unpredictable act rather than to the omission.

### CASE 3

An experimental plant shuts down automatically during normal operation due to inadvertent manual operation of cooling system shut off valve.

**Investigation**

A safety shut-off valve in the cooling system which is routinely closed during post-shut-down check procedures, was closed manually. The valve control switch is placed behind the operating console, and so is the switch of a flood lighting system used for special operations monitored through closed circuit television. The switches are neither similar nor closely positioned The operator has to pass the valve switch on his way to the flood light switch.

In this case the operator went behind the console to switch off the flood light, but operated the shut off valves which caused plant shut down through the interlock system.

**Comments**

Strongly automated and stereotyped action sequences are frequently initiated by a single conscious decision. If the action takes some time, e.g., you have to move to another place to perform the action, the mind may return to other matters, and the sequence is vulnerable to unpredictable conditions, particularly if the sequence in tended in some of the steps overlap other familiar and automated sequences.

### CASE 4

Butadiene explosion at Texas City. (Loss Prevention, Vol. 5, Am. Inst. Chem. Eng. 1971).

#### Investigation

> "Loss of butadiene from the system through the leaking overhead line motor valve resulted in substantial changes in tray composition ...".
>
> ..."The loss of liquid in the base of the column uncovered the calandria tubes, allowing the tube wall temperature to approach the temperature of the heat supply. The increased vinyl acetylene concentration and high tube wall temperature set the stage for the explosion which followed".
>
> ..."The make flow meter showed a continuous flow: however, the operator assumed that the meter was off calibration since the make motor valve was closed and the tracing on the chart was a straight line near the base of the chart. The column base level indicator showed a low level in the base of the column, but ample kettle vapor was being generated".

#### Comment

Wisdom after the event tells that closed valve together with continuous flow signals possible leak, and the risk implied calls for investigation. The skilled operator, however, conforms his observations individually with his expectations and process-feel. If abnormal observation refers to a familiar situation, he sees no problem and does not investigate the matter. You cannot predict his response without knowing his daily experiences. It can be difficult to predict the probability that an operator performs a specified function because he may have re specified his function - sometimes with good reason.

This can happen, even if there is a clear pre warning:

### CASE 6

Melt down of fuel element in nuclear reactor. "Nuclear Safety", September 1962.

#### Investigation

Certain tests required several hundred process cool ant tubes to be blocked by neoprene disks. Seven disks were left in the system after the test, but were located by a test of the gauge system that monitors water pressure on each individual process tube. For some reason the gauge on one tube was overlooked, and it did not appear in a list of abnormal gauge readings prepared during the test  There was an additional opportunity to spot the blocked tube when a later test was performed on the system. This time the pressure for the tube definitely indicated a blocked tube. The shift supervisor failed, how ever, to recognize this indication of trouble. The gauge was adjusted at that time by an instrument mechanic to give a mid-scale reading which for that particular tube was false. This adjustment made it virtually certain that the no flow condition would exist until serious damage resulted.

### CASE 7

Docket 50219-167: Two diesel generators set out of service simultaneously.

**Event Sequence**

8.10 permission to perform surveillance test on containment spray system No. 1 including electrical and mechanical inspection of diesel generator No. 1.

8.20 permission to take diesel No. 2 out of service for oil addition.

Both systems out of service for 45 min. Foreman over looked test of no. 1 system when permitting diesel no. 2 operation.

**Comment**

Coincident unavailability of redundant systems caused by improper timing of routine tasks. Difficult to predict due to dependence on station "software" vulnerable for changes and oversight due to absence of cues from the system supporting attention.