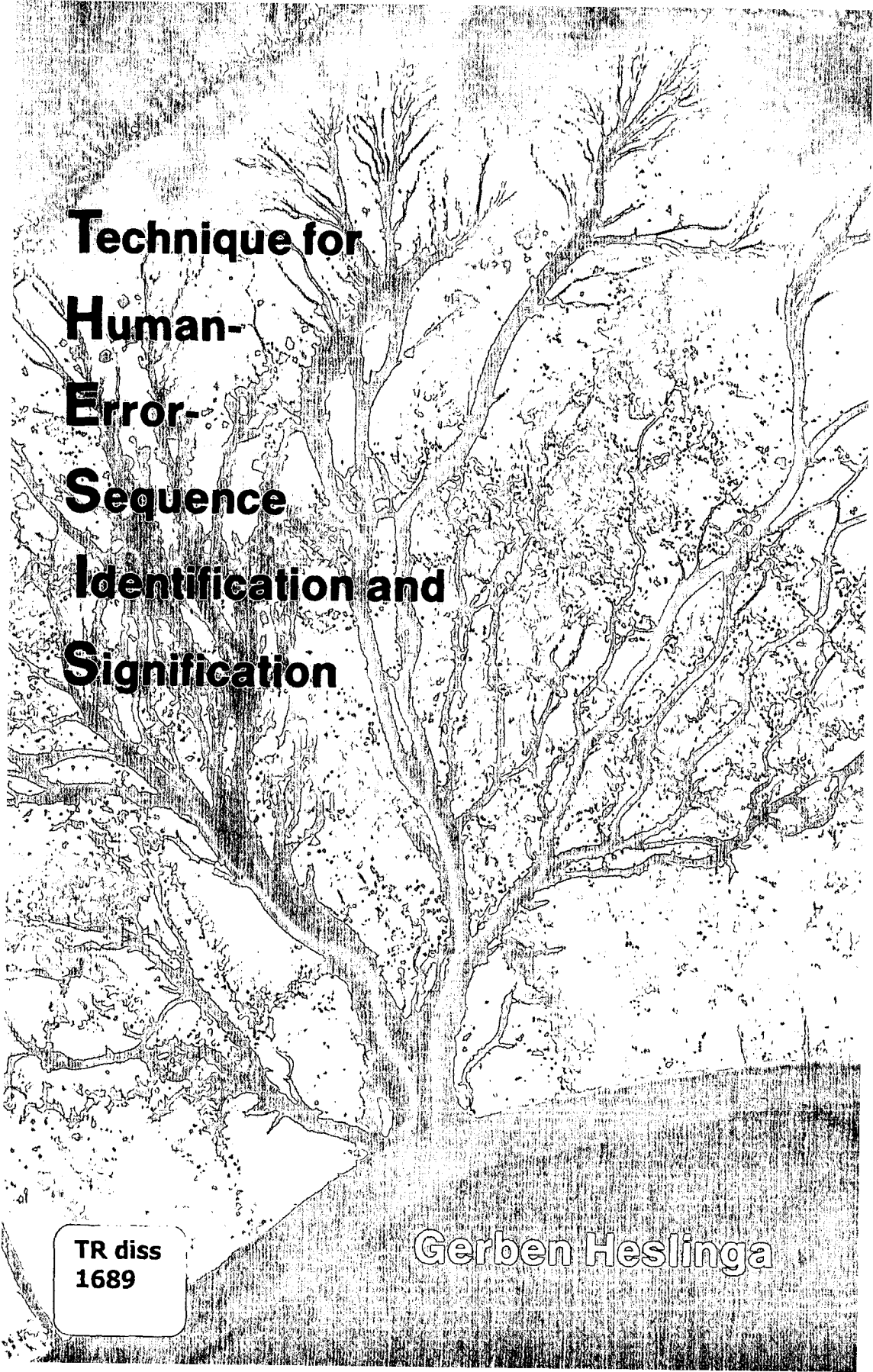
Technique for Human-Error-Sequence Identification and Signification



Gerben Heslinga

TECHNIQUE FOR HUMAN-ERROR-SEQUENCE IDENTIFICATION AND SIGNIFICATION

PROEFSCHRIFT

ter verkrijging van
de graad van doctor aan de Technische Universiteit Delft,
op gezag van de Rector Magnificus,
Prof.Drs. P.A. Schenck,
in het openbaar te verdedigen
ten overstaan van een commissie
aangewezen door het College van Dekanen
op 8 december 1988
te 16.00 uur

door

Gerben Heslinga
geboren te Sneek
werktuigkundig ingenieur

Dit proefschrift is goedgekeurd door de promotoren

Prof.Dr.Ir. H.G. Stassen

en

Prof.Ir. P. Mostert

'To err is human, to forgive divine'

A. Pope (1709)

To Letty

To my parents

Preface

Technical installations have become increasingly more complex during the last decades and the severity of the consequences in the case of malfunction has grown accordingly. This increasing complexity has made it more difficult for governments and for managers to decide about optimally safe installations. Risk analysis is a useful tool for making such decisions since it provides a structured insight into the overall safety of a complex installation. Risk analysis takes both the technical factor and the human factor into account, by means of probability assessments. Knowledge about the influence of the human factor on a risk analysis has, however, developed slowly as compared to knowledge about the technical factor.

The Joint Laboratories and Other Services of the Dutch Electricity Supply Companies, KEMA (N.V. tot Keuring van Elektrotechnische Materialen) at Arnhem therefore started in 1983 to sponsor research in the area of human factors. KEMA was much interested in this subject because of involvement in risk analyses of complex systems. The Man-Machine Systems Group of the Faculty of Mechanical Engineering and Marine Engineering at the Delft University of Technology had experience with human-operator behavior studies in process control. The two institutions therefore set up a cooperative project to gain further insight into the influence of human-operator performance on system safety. The results of Ph.D. research performed by the author as part of this cooperative project are described here.

The author is indebted to KEMA and the Delft University of Technology for support and acknowledges financial support by KEMA. He wishes to express his gratitude for the help of all those involved. Special thanks are due to Ir. R.W. van Otterloo of KEMA for his helpful advice. The author acknowledges the contribution of students, Han Gabriëls, Julien Godding, Aswin Konings, Akkie Okma, Frank Schoof, Bob de Vos, Noël van Weersch and Gert-Jan Wijlhuizen, to this research on the human factor. The author is also indebted for mathematical and statistical advice from Prof. Dr. M.S. Keane, Prof. Dr. P.J.M. Rousseeuw and Dr. R.M. Cooke of the Delft University of Technology.

Thanks are due to Ir. J.W. de Vries of the Nuclear Reactor Institute in Delft (in Dutch known as 'Hoger Onderwijs Reactor' of the 'Interfacultair Reactor Instituut'), who made it possible to study the human actions performed during the start-up procedure. Thanks are also due to the personnel of a power plant who were willing to participate in a psychological experiment so that distributions of human-error probabilities could be collected. The author is indebted to those responsible for the KEMA Experimental Boiler who made it possible to analyze its start-up procedure. The help of

Caeciel Puls who was able to transform my cuneiform handwriting into a readable script and of Drs. A.P.J. van Slingerland, the KEMA corrector, who converted the manuscript into readable English is acknowledged. The author is also indebted for the help by Mr. J.D. Lagerweij and his assistants for drawing most of the figures. Thanks are due to Dr. A.J. van Loon, the KEMA editor, and his assistant Janette Rietbergen who have given the manuscript its final form and who will publish this work in the KEMA journal (KEMA Scientific & Technical Reports).

The study was performed in an area with forces sometimes pulling in different directions. Work at KEMA is oriented towards applied research, while work at the Delft University of Technology is oriented towards fundamental research. The author has experienced this as fertile ground for the study of a topic that hovers on the border between fundamental and applied science. Still, it was not always easy to work in such a setting but fortunately there were also forces providing the necessary moral support. My special and undoubtedly greatest gratitude for this and for support during the years preceding this study, goes to Letty and to my parents.

Contents

Chapter 1

Introduction

Background

The possible influence of human errors on the safety of industrial installations has become a subject of increasing interest in the last few years. The accidents at Three Mile Island, Chernobyl and Bhopal have in particular contributed to the development of this interest. There are several mutually related reasons for the increased interest in the topic of 'human error':

(1) there is a tendency to make installations more and more reliable technically with the result that the operator becomes a relatively weaker link;
(2) the consequences of human errors become more far-reaching due to the larger size of the installations (Rasmussen, 1982a);
(3) the automation of many processes means that an operator has to control the process on a higher level of abstraction, i.e. the cognitive level, so that human errors become less predictable and that fundamental analyses of this cognitive type of behavior will be required (Reason & Embrey, 1985);
(4) certain technical failures are caused by human errors (e.g. technical failures because of bad maintenance by humans) and prevention of these technical failures calls for a closer study of such human errors;
(5) the final, and probably most important, reason is that human error plays some role in nearly every serious accident, as shown by many examples in recent years.

The influence of a human being on the safety of a plant can be twofold. Firstly, persons themselves may initiate an undesired event and thus bring a system from a stable condition to an unstable one. This could be the result, for instance, of failure to follow a procedure correctly. Secondly, a person may not respond properly to a certain undesired condition such as a technical failure (e.g. a tube rupture) initiated by an outside influence. One often speaks of human error in both cases.

The first situation, the occurrence of an undesired event as a result of human errors during the performance of a procedure, is the focus of attention in this study. The interest in this aspect originated from a question concerning the allowable repair time for components of safety systems. If a component or a safety system fails during operation, management has a chance to repair this part within the maximum allowable repair time; if the operator fails to fulfill this condition, operation of the plant must

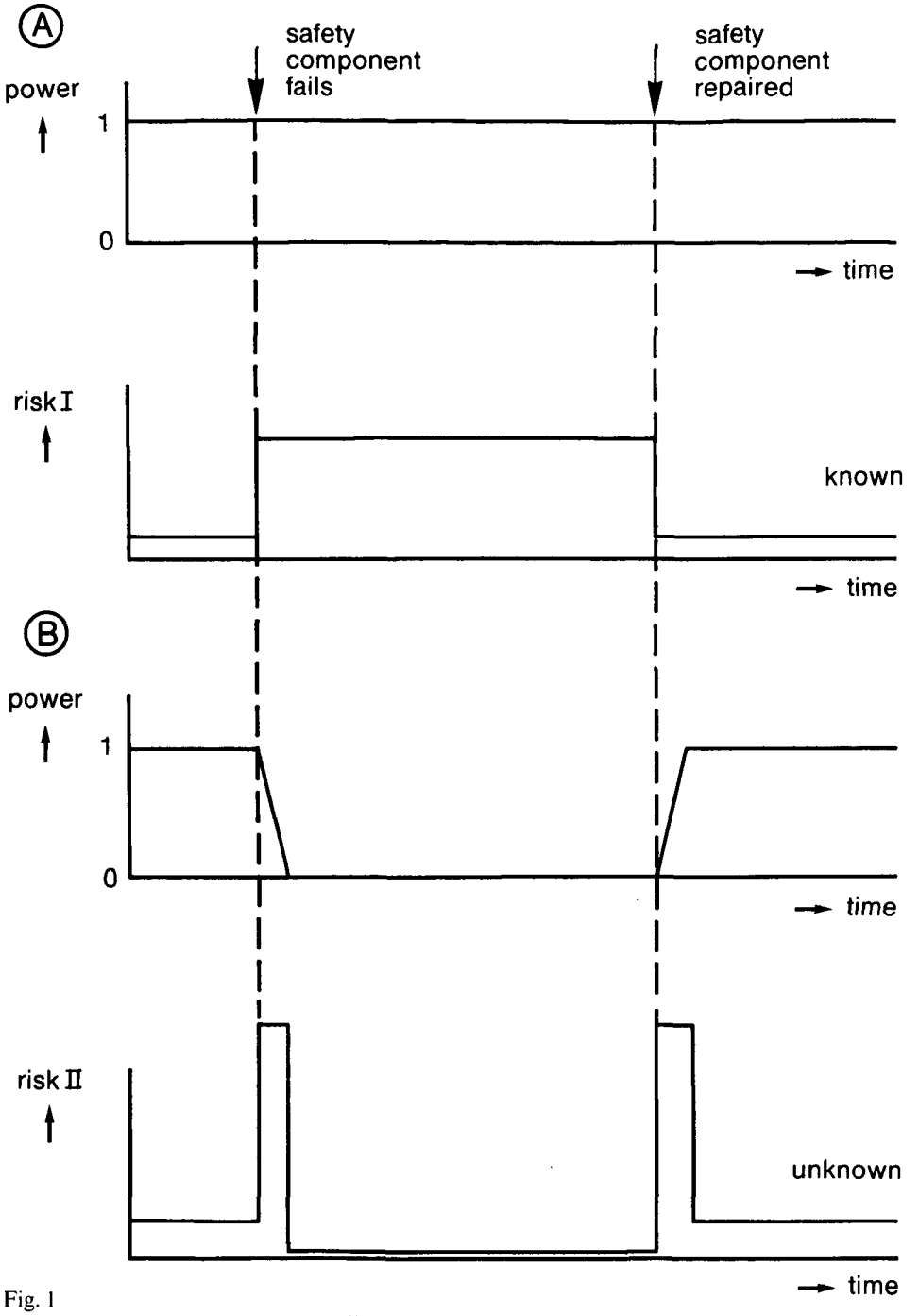


Fig. 1
Simplified scheme of the power supplied and the operational risk of continued operation during repair (1-A), and shut-down and start-up for repair of a safety component (1-B). It is assumed for the sake of simplicity that risk II is the same for shutting down and starting up (from: Heslinga, 1983).

be stopped (GKN, 1978). Such a shut-down, however, might involve a great risk because it implies a change from a stable condition.

Repair times have so far been based on the time necessary to perform effective repair work. The question is whether these repair times can be justified on the basis of risk analysis. Two risks must be compared for the purpose as set out in Figure 1: the top of Figure 1-A shows the electrical power supplied by a nuclear power plant during normal operation. If a component of a safety system fails while the plant is working at full power, operational risk I increases to a higher level and stays at this level until the component has been repaired. The other possibility is to shut the reactor down for repairs (Fig. 1-B). However, there is generally a higher risk II during shutting down and starting up the plant. This is due to the fact that the system changes from one steady state into another; the many human actions which are necessary and which are usually performed in accordance with procedures, have to be accomplished correctly. Allowable repair times can be determined by weighing these risks. If, for instance, the risk of shutting down and starting up the plant is relatively great, it is logical to increase the allowable repair times for safety components and to accept a greater overall operational risk.

Risk I concerns the risk of the technical systems and has been investigated and evaluated in detail, so that it can be described as an accurately known risk. Risk II, however, concerns human performance, a subject about which relatively little is known. A closer study of human performance is needed to determine a justified allowable repair time.

Aim of this study

Some definitions are needed before the aim of this study is described.

General restrictions and definitions – An 'event' is defined as a certain part of an activity, whether technical or human, which has only two possibilities, success or failure, e.g. a reading error YES or NO, or a safety-component failure YES or NO (Fig. 2). An 'outcome' is regarded as the result of an event or combination of events, e.g. turning a switch to an incorrect position following a reading error, or a safety system that fails as a result of a component failure. A 'consequence' is defined as the effect of one or more outcomes on the surroundings, e.g. an explosion as a result of the turning of a switch to an incorrect position in combination with a safety-system failure.

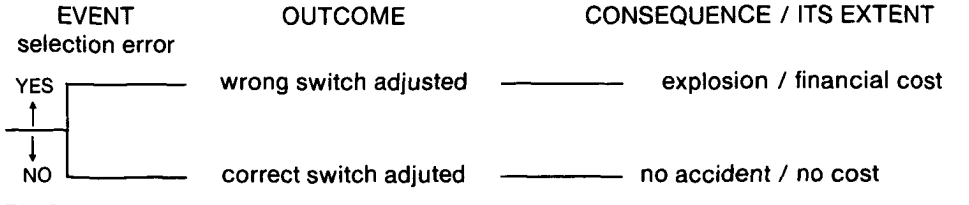


Fig. 2
Graphic presentation of the influence of an event on the extent of a consequence.

The 'probability that a specific event will occur' (P) is defined as the limiting value of the quotient of the number of times (N) that a specific event occurs and the total number of opportunities (n) for that specific event to occur:

$$P = \lim_{n \to \infty} \frac{N}{n}$$

The same definition applies to the probability that an outcome will occur or the probability that a consequence will occur.

'Reliability' is defined as the probability that a desired consequence will occur, e.g. the probability that a procedure is followed correctly by an operator. 'Risk' is the product of the probability that an undesired consequence will occur and the extent of that consequence. 'Safety' is defined as the state in which the sum of all the possible risks has a minimum value. It is noted that the terms 'human reliability', 'human-performance risk' and 'human-performance safety' are used if the items defined are clearly related to human behavior.

The probability that an event, an outcome or a consequence will occur is frequently referred to in the present work as the probability of an event, outcome or consequence or as event probability, outcome probability or consequence probability.

It is common practice that certain procedures are followed during the starting up or shutting down a plant. These procedures may be either explicitly laid down in writing or implicitly present in the mind of an operator. Procedures can be regarded as sequences of specific actions, such as adjusting a set point, pushing a button, etc. A distinction can be made between normal procedures and emergency procedures. Normal procedures are usually performed under low-stress circumstances, such as maintenance and start-up. Emergency procedures are often performed during emergency situations, in which there may be a high level of stress. As this study is performed with the ultimate risk or safety of starting up and shutting down as background, only the performance of operators as they follow normal procedures is considered.

Human reliability versus human-performance safety – A human-reliability analysis (HRA) is focused on the probability that human actions will be performed correctly and the probability that a desired consequence will occur. Only single errors are often considered for this purpose. The types of undesired consequences resulting from human errors are not usually considered. Several techniques are currently available for performing an HRA and have been reviewed by Dhillon (1980, 1986) and Meister (1984).

In a human-performance safety analysis (HPSA), one is not only interested in the probability of actions being performed correctly or incorrectly. One is also interested in the type and the extent of the consequences of incorrect human actions. Two factors must be considered to determine human-performance safety: (1) the probability that a certain combination of events will occur due to human errors and (2) the extent of the undesired consequences resulting from these errors. HPSA is far more difficult to carry out than HRA in so far as the first factor, the probability of a combination of events, must be known. In contrast with HRA, only few techniques are available for HPSA.

Goals – As stated above, this study aims to investigate the risk or safety involved in the performance of a shut-down or start-up procedure. The study is therefore concerned with human-performance safety rather than human reliability itself. This implies determination of the probability that undesired consequences will occur due to human errors.

Two aspects, a qualitative aspect and a quantitative one, can be distinguished in assessing the probability of undesired consequences occurring during the performance of normal procedures. The qualitative aspect is related to the type of error sequences that can be made by humans, so that a particular undesired consequence will occur. The quantitative aspect is related to the probability of following a particular error sequence and the probability of the undesired consequence. Relatively little is known about these aspects. Qualitatively, people may err in many different ways and there may be many error sequences leading to undesired consequences. Quantitatively, little is known about the probability that human errors will be made and how factors of all kinds may influence this probability.

As noted before, only few techniques are available for performing a HPSA. The aim of this work is to develop a technique to analyze (sequences of) human errors for the assessment of human-performance safety when normal procedures have to be followed. Such a technique should satisfy both the qualitative and quantitative aspects and is intended:

(1) to identify human-error sequences leading to a particular set of undesired consequences;
(2) to determine the significance of these sequences in terms of their probability.

Because of these two aspects, this technique is termed the 'Technique for Human-Error-Sequence Identification and Signification', abbreviated to THESIS.

It will be clear that many problems occur in developing such a technique. The multitude of sequences in which human beings can err is only one of these problems. It is thus hoped, in the course of this study, to determine those features that constitute serious problems. This will be done through using THESIS for the assessment of human-performance safety when normal procedures have to be followed. Previous work in this field will be reviewed and the related features will be identified.

Framework of this study

Human error in relation to reliability and risk analyses is a concept fundamental to this study. Chapter 2 will start with a definition and classification of human errors. The way in which human errors can be incorporated in reliability and risk analyses of complete man-machine systems will be presented. This will involve an explanation of the techniques used in these analyses, such as System Event Trees and Fault Trees.

Many techniques are currently available to perform an HRA but only few are available for an HPSA. The existing HRA and HPSA techniques will be described in chapter 3. Their limitations will be analyzed and the extent to which the techniques can be used for an HPSA will be examined.

A presentation of the proposed technique is made in chapter 4. Many problems

occur in the course of developing such a technique. These problems, termed 'man-related features of THESIS', determine the extent to which THESIS can be applied in practice. These man-related features (MRFs), with regard to their possible influence, will be introduced in this chapter.

The rest of the study is concerned with an evaluation of these influences. This is done theoretically, experimentally, and through field research.

How THESIS can be applied for a simple HPSA is shown by the presentation of a case study in chapter 5. This case study will present an analysis of the effect of two common MRFs. The implications of applying an HPSA technique instead of an HRA technique are clarified.

The theoretical evaluation is introduced in chapter 6. The derivation of the analytical model used in this study is presented there. The model is based on THESIS and most of the MRFs will be incorporated in the model by introducing some refinements.

This derivation of the model is followed directly by an evaluation in chapter 7. This evaluation is performed by means of sensitivity analyses using the analytical model. Since there are no data available for most of the MRFs, the sensitivity analyses may show which of these MRFs are irrelevant and need not be further considered in THESIS and thus not in an HPSA either. The analyses are performed analytically and by computer simulation.

Certain MRFs are evaluated in chapter 8 to learn to what extent THESIS can be applied in practical situations. A field study is carried out for the purpose, in which THESIS is applied to a start-up procedure of a process installation.

One of the MRFs is the variation in human performance or, more specifically, in human-error probabilities (HEPs). In the study, the problem is investigated experimentally (chapter 9). An investigation is carried out to discover how HEPs are distributed and in how far HEPs of different types of errors are correlated. The differences between operators and students as experimental subjects are analyzed.

The results obtained in the study are discussed in chapter 10 in order to conclude to what extent THESIS can be applied for an HPSA. The influence of the MRFs as investigated in this study is therefore considered, and the implications of the findings are discussed. Finally, some suggestions are made for future research.

It will be clear that it is difficult to take all MRFs into account simultaneously. In a first attempt to gain some insight into this relatively unexplored field, a combination of some MRFs will be examined in isolation. Some of the chapters thus have a rather isolated character, and a link with other chapters may not be evident immediately.

Chapter 2

The occurrence of human errors

Introduction

Three main causes of undesirable situations, i.e. the unavailability of a system or the occurrence of an accident, can generally be distinguished: human error, technical malfunction and external disturbances. These causes are not strictly separable; they may occur in combination as the cause of an undesirable situation. Table 1 provides some information from the literature on the contribution of human error in terms of percentages. It is striking that the contribution of human error can vary widely from one author to another. Although some (a.o. Wagenaar, 1983) claim the contribution of human error to be more than 50% regardless of the situation, the table shows that this is not necessarily true. Three reasons can be given for the apparent variation in the numbers.

(1) The consequence that is considered in determining the human contribution. In the case of the 95% contribution of human error to driving, the consequences considered were accidents, whereas the 1% contribution at conventional power plants was related to the loss of electricity supply. The 95% would certainly have been lower if the unavailability of the car, e.g. failure to start, instead of an accident, had been used as a consequence.

(2) The nature of the process involved. If there is little chance of technical malfunction, the percentage of human error will increase. Compared with a nuclear power plant, a car is such a simple system that little can go wrong technically. Hence, about 95% of car accidents are caused by human error (Eid, 1980). A nuclear power plant, however, is of such technical complexity that undesirable situations, such as interruptions of production, are caused by technical malfunction comparatively more often than by human error (Thomas, 1984).

(3) The definition used to determine whether an undesirable situation was caused by human error, technical malfunction or external disturbances. This decision is often a very subjective one. When a car fails to start in humid weather, for instance, one person may blame this on technical malfunction, another on bad maintenance and thus on human error, whereas a third may blame it on the humid weather and thus on an external disturbance. Together with the nature of the process and the sort of consequences considered, this subjectiveness accounts in part for the different percentages found in Table 1.

Table 1
Contribution of human error to causes of undesirable situations, in terms of percentages.

process	percentage of human errors	source
car driving	95%	Eid (1980)
sailing	85%	Ligthart (1979)
aviation	51%	Wittenberg (1978)
industry	40%	Bello & Colombary (1980)
nuclear power plants	23%	Thomas (1984)
conventional power plants	1%	VDEN (1981)

Table 1 shows that the influence of human error on system safety varies widely. As already noted, the definition of human error plays an important role and is therefore considered in more detail in the next two subsections. The manner in which human error is incorporated in a system safety analysis is considered subsequently.

Definition of human error

It is important to start with a definition of the term 'human error'. There are many definitions of human error (Rigby, 1971; Hagen, 1976; Rasmussen, 1982b; Nieuwhof, 1983; Sheridan, 1983; Swain & Guttmann, 1983). In addition to the term 'human error', the terms 'slip' (which is an action other than intended) and 'mistake' (which is an intention that is not appropriate) are often used by some authors (e.g. Norman, 1981; Reason, 1985; Reason & Embrey, 1985).

According to Nieuwhof (1983), some definitions for human error are not entirely correct. It is, however, beyond the scope of this study to discuss these definitions. A new definition will therefore be used here, that reflects as accurately as possible the insights acquired from the authors referred to in this section, namely, 'A human error is the non-performance or incorrect performance of a desired activity, provided that adequate conditions for correct performance are present'. Two terms are essential in this definition of human error. First, what is 'desired activity' and secondly what are 'adequate conditions'.

Desired activities comprise desired actions, such as moving switches to the right position and reading meters correctly, as well as desired cognitive processes, such as making a correct calculation or decision. In addition, a desired activity may mean choosing the right method of analysis or applying the right strategy to achieve a certain goal or to solve a problem. The term 'desired activity' also means dealing correctly with a continuous process. In such a case, for instance, a desired activity may be to keep the temperature of a process within certain limits.

The meaning of the term 'desired activities' can be very subjective. In the case of a car, the desired activity may be keeping its speed within the limit of 100 or 120 $km \cdot h^{-1}$ on the Dutch highways, as set by the government. However, very few will

consider it an error to drive on the highway at a little over this limit for a short period of time. Driving 180 $km \cdot h^{-1}$ for a long time, however, will definitely be regarded as a human error, certainly by law-enforcement officers. The definition of a maximum limit above which one speaks of human errors may therefore be highly individual. Furthermore, the definition is often dependent on the era in which one lives. The era-dependent aspect is present in the changing of rules which may suddenly turn hitherto accepted activities into wrong activities and vice versa.

In determining whether an activity is a human error, the consequences also play an important role. Driving 120 $km \cdot h^{-1}$ need not be looked upon as human error, unless an accident is caused. Allowing the pressure in a process to become too high need not be considered a human error either, provided the operator recovers in time to prevent undesirable consequences. However, opinions may differ as to how far the consequences are to be taken into account, which makes the determination of whether or not a human error has occurred rather subjective.

The other item in the definition of human error is the presence of adequate conditions for correct performance of an activity. These conditions can refer to both the human element and the surroundings. If someone is visually handicapped, for instance, and therefore fails to carry out a prescribed action correctly, this is a human limitation rather than a human error. Similarly, when a control room is on fire so that prescribed actions cannot be carried out, the adequate conditions are not present. Here again, it is evident that the determination of whether adequate conditions are present is subjective and era-dependent.

It may be clear now that the determination of desired activities and adequate conditions can result in lengthy discussions. The occurrence of any specific undesirable consequences plays an important part in this and human error is therefore often determined in retrospect. This, however, does not help us in our efforts to determine the influence of human error on the safety of a system. A system safety analysis implies that what might fail, both the technical and the human factor, can be determined beforehand. In other words, possible human errors should be determined in advance.

Human errors in the carrying out of procedures

Rasmussen (1982a, 1985) has introduced a three-level scheme for a description of the internal control of human behavior (Fig. 3). Human activities at the skill-based level are assumed to be subconscious, activities at the rule-based level are performed according to a certain rule or procedure, whereas activities at the knowledge-based level involve coping with unfamiliar situations for which no procedures exist.

As mentioned in chapter 1, the study is restricted to normal procedures. A procedure can be considered as a sequence of desired activities. In terms of the three-level scheme of Figure 3, the behavior can be regarded as 'rule-based'. A possible classification related to this rule-based human behavior will be discussed in the next subsection.

Classification of human error related to procedural performance – There are many different classifications of human errors in the literature (Comer et al., 1983; Fragola

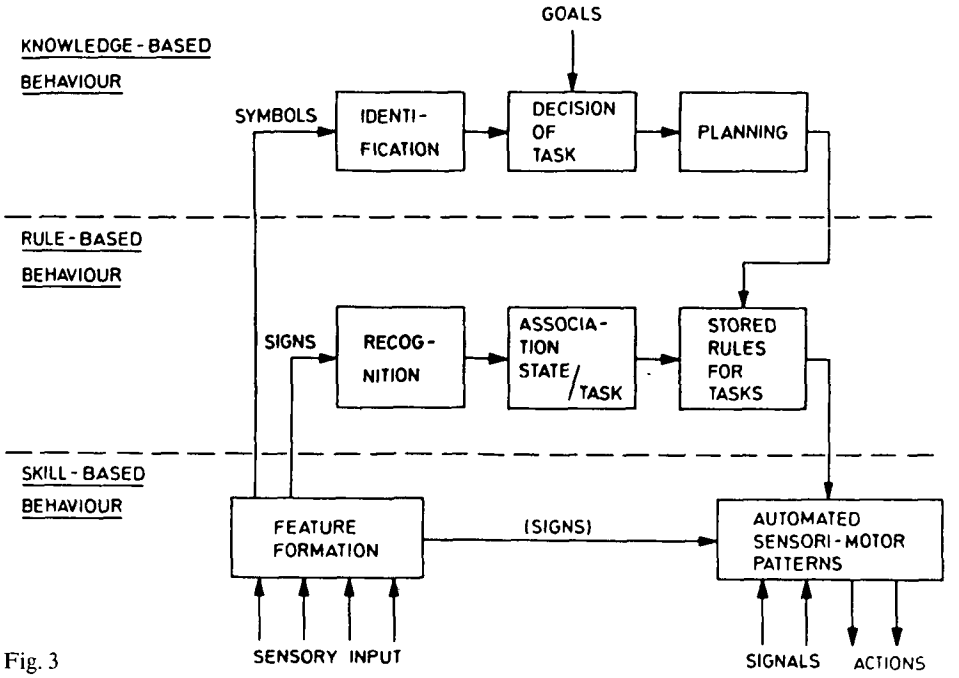


Fig. 3
Three-level description of the internal control of human behavior (from: Rasmussen, 1985).

& Bell, 1983; Mancini & Amendola, 1983; Rouse & Rouse, 1983; Swain & Guttmann, 1983; Beare et al., 1984; Heslinga, 1985a,b; Rasmussen, 1985; Griffon-Fouco & Ghertman, 1987; Reason, 1987a). Some of the classifications only consider the observable external effects of human behavior, such as the incorrect turning of a switch, whereas other classifications also consider the causes of such an error, i.e. incorrect reading of an indication at the switch that is to be adjusted. An example of a classification is given in Figure 4. The observable external effects of human behavior, in particular the observable errors, will be the focus here: what incorrect actions can a person perform that will result in a decrease in system safety during the performance of normal procedures? No mental errors or internal malfunction leading to observable errors are considered. Hence, a diagnostic error, for instance, is not taken into account, but its result, such as the selection of a wrong procedure, is considered. Causes are only important to determine the probability that someone is doing something wrong.

Because this study is done in an attempt to present a technique for identifying human errors and for discovering how significant their probability is, the exact probability for which the causes have to be known is not of primary interest. Consequently, a classification is presented here which is related only to the observable external effects of human behavior. This classification is meant to be a general one, in the sense that it distinguishes between two levels:

(A) the system level, at which systems are considered as a whole and where a certain goal is pursued by applying procedures (for instance: a power plant must supply electric power; a doctor must cure a patient from an illness);

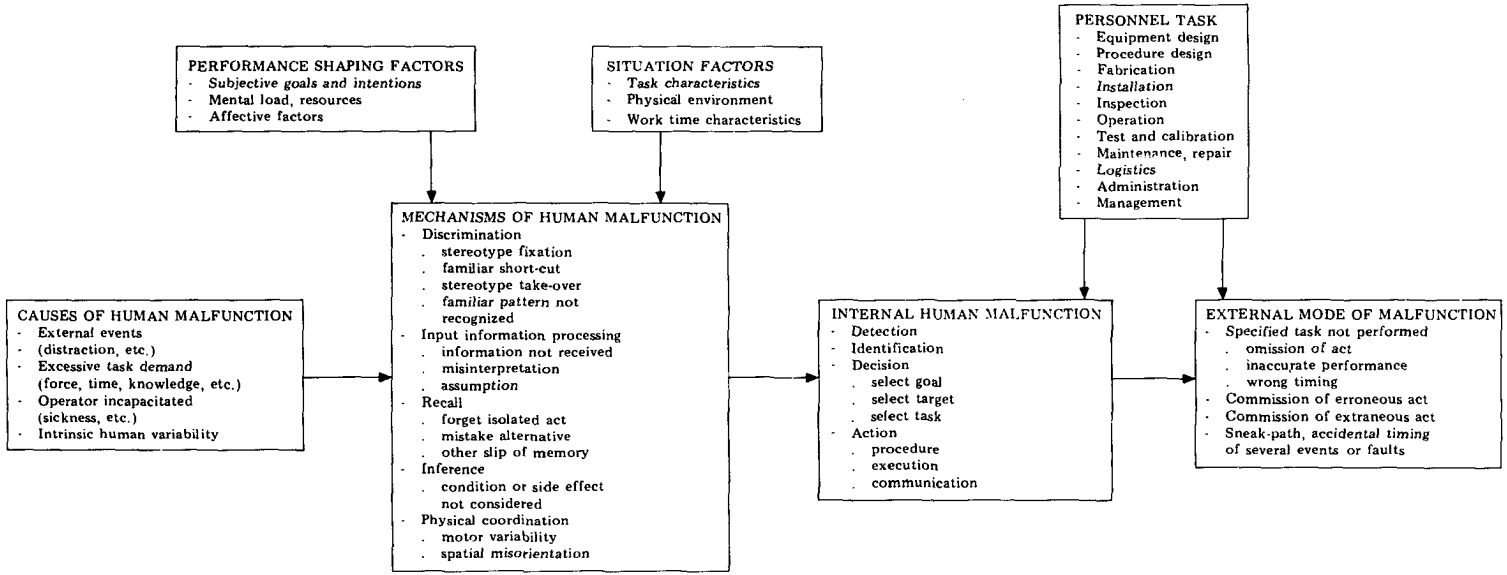


Fig. 4
A taxonomy for the description and the analysis of events involving human malfunction (from: Rasmussen, 1982b).

(B) the component level at which simple components are considered and where simple activities are carried out (for instance: switches and set points must be adjusted, and buttons must be pressed; medicines must be prescribed).

The classification based on this subdivision is as follows:

(1) error of omission: a person fails to carry out the procedure (level A) or desired activity (level B), or fails to do so within the specified time, i.e. does so either too early or too late;
(2) selection error: a person selects the wrong procedure, for instance as a result of selecting the wrong goal (level A), or the wrong component (level B);
(3) handling error: a person makes an error when following the procedure he has selected (level A), or makes an error at the component he has selected (level B);
(4) sequence error: a person carries out the steps in a procedure in the wrong order;
(5) extraneous activity: a person introduces an undesired procedure (level A) or an unforeseeable activity (level B).

The extraneous activity will not be analyzed further in this study.

The need for procedures – If human errors are to be determined for an assessment of system safety, one must be familiar with the procedures involved; this means that the desired activities to be carried out must be known. Only then will it be possible to predict any human errors.

It may be difficult to determine the various procedures to be followed. In normal situations – when activities are carried out as a routine task, such as starting up a power station or curing a patient – the procedures, whether they are described in writing or not, are usually known and available. They have been defined in chapter 1 as normal procedures. It is often different in unknown (emergency) situations when an active and creative reaction is required, since many good strategies or emergency procedures may exist for certain unusual situations which have to be solved by human creativity. Determining these strategies could then become a more and more elaborate process.

The problems mentioned with respect to the determination of the procedure that is followed and to the definition of the errors that may be committed are of minor importance here. In most cases the procedures are known and it is possible to specify the type of human errors that can be made, in particular errors of omission, selections errors, handling errors and sequence errors. The incorporation of these human errors in a system safety analysis will be the next step.

The incorporation of human error in a safety or risk analysis

It is the intention of the safety analysis of a complex system to determine the probability that specific undesired consequences will occur when certain components (technical or human) fail and what the extent of these consequences will be. A simple example is given to explain how the human factor is incorporated in risk or safety analyses.

Assume that there is a process which is guarded against overpressure by two safety devices (the complete system is presented in Fig. 5). The two safety devices form a

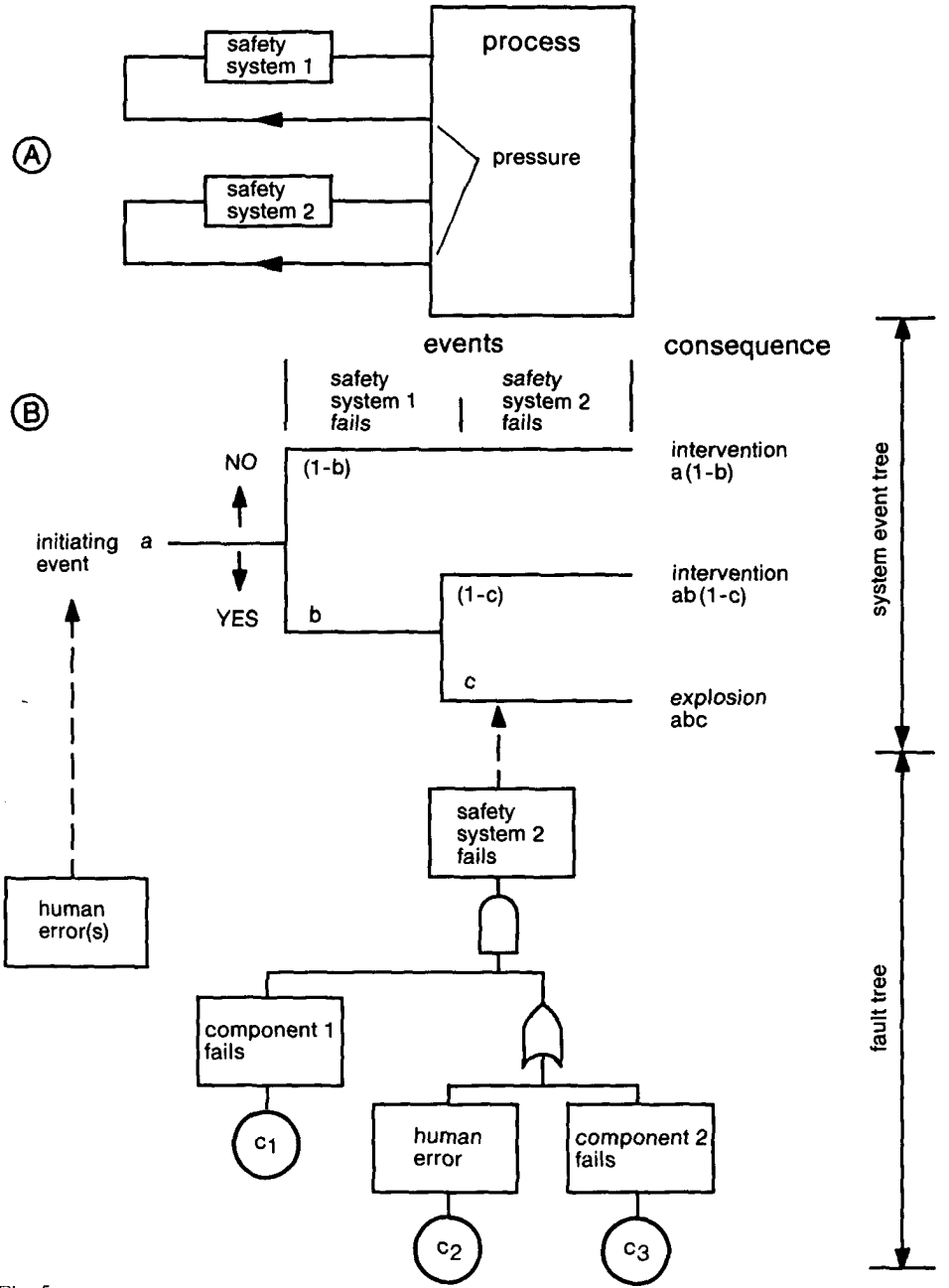


Fig. 5
Scheme of a simple system (top) and the related trees, i.e. the system event tree and the fault tree (bottom). The system is guarded against overpressure by two safety devices; this is expressed in the system event tree by two consecutive events. If overpressure appears as an initiating event, one of the safety systems must intervene. The system event tree shows the consequences that are possible if a safety system fails. The fault tree shows the various causes of the failure of the safety system.

so-called one-out-of-two redundant system. This means that only one device has to function to bring the process to a safe state when overpressure occurs.

A safety analysis usually starts with making a system event tree. The human factor can then be incorporated in two places. This section will start with a description of the system event tree. This will be followed by a presentation of the two places where the human factor is incorporated in the safety analysis of a system.

System event tree – The purpose of the system event tree (also called generic event tree) is to present the possible failure modes of system malfunction that leads to various undesired consequences, and to assess their probability (USNRC, 1975: the so-called Rasmussen report, also known as WASH-1400). The system event tree always starts with an initiating event (Fig. 5), generally representing a change in a process variable: a sudden increase in pressure in the present example. The events related to the intervention of the safety devices then follow. The events always have a 'negative' meaning expressed by 'the safety device fails'. Therefore, if both safety devices fail, the YES-direction is followed in both events; the consequence will be a sudden increase in pressure, e.g. an explosion. If the first device intervenes, however, the NO-direction is followed, and since there is a one-out-of-two redundant system, the second event is not of interest and the consequence is an intervention. This consequence will also occur if the first device fails (YES-direction) and the second device intervenes (NO-direction).

The probability of a certain combination of events can be calculated by assigning probabilities to the branches of the system event tree. The initiating event usually has a probability per unit time, implying that there is a probability that an initiating event will occur during a certain period of time. The events are usually expressed in terms of a failure probability per demand, which means that, in case of a demand to succeed caused by an initiating event, the events will have a probability to fail, i.e. not to intervene. By combining these probabilities, the consequence probabilities can be calculated. This is done in Figure 5, in which it is assumed that there is no dependence between the events.

The human factor as a basic event in fault trees – The first place to incorporate the human factor into system safety analysis is to apply fault trees (USNRC, 1981). The purpose of this technique is to discover the failure modes leading to a particular predefined failure state of a system. This failure state is called 'top event' and the fault tree is a graphic construction containing various combinations of faults leading to the occurrence of the top event. An example of a top event is 'safety system 2 fails' (Fig. 5).

When fault trees are used, the system is decomposed into smaller components which may be either technical components or human actions. The application of 'gates' such as AND and OR gates, allows the failing states of the components, i.e. the events, to be combined in such a way that they cause the top event. If, for some reason, the decomposition is stopped in certain events, the events in which this happens are called basic events'. They are represented by circles in Figure 5. Boolean algebra can

be used to simplify the logical construction of the fault tree.

It should be noted that the fault tree is, in first instance, a qualitative model, although it is often used quantitatively to calculate the probability of the top event. This probability is obtained by combining the probabilities of the basic events as prescribed by the structure of the fault tree. In the case of Figure 5, the probability (c) of the top event, ignoring the higher order terms, is approximately: $c = c_1(c_2 + c_3)$. The human error, e.g. the incorrect resetting of a safety device after maintenance, can thus be incorporated qualitatively and quantitatively into system safety analyses.

The human factor as the cause of an initiating event – The second place of incorporating a human error in a system-safety analysis is more direct: the human error as the cause of an initiating event. This can be the case if an operator follows a procedure incorrectly, e.g. by pushing a wrong button and thus letting the pressure increase too much in the process. This incorporation is presented in Figure 5 as a human error leading to the initiating event via the dotted line. Technical failures that can also cause an initiating event, e.g. a tube rupture, have been omitted from the figure.

Differences in analysis – There are important differences between the two methods of incorporating human errors. When fault trees are used, a model of the system is made and the types of human error that can be made become obvious; these errors are usually indirect, latent failures. The incorrect resetting of a safety device, for instance, can result in an unavailability that may be noticed only if the device must function after an initiating event. Three Mile Island is an example of an accident in which latent human errors played an important role (IEEE-Spectrum, 1979). Human errors as initiating events, however, are usually direct failures. These errors can suddenly change the state variables of a process in an undesired manner. The way in which human errors or sequences of human errors cause an initiating event is most usually not known beforehand. The accident at Chernobyl is an example of the introduction of an initiating event through the ignoring of prescribed procedures (INSAG, 1986; Nuclear News, 1986).

As a result of these different characters, the analyses of human error and the quantification in terms of their probability may differ. The human error in a fault tree, incorporated as the basic event, is always known, i.e. the type of error is defined. The probability can be calculated by determining the success probability that a procedure is followed correctly. The probability of the basic event then becomes the quantity 'one minus this success probability'. The probability of the basic event is, however, assessed directly in most cases. The human error as the cause of an initiating event is usually not known. There may be several human errors or sequences of human errors causing a similar initiating event. This implies that quantification of their probabilities requires identification of the human errors. Several quantification techniques are summarized in the next chapter.

Chapter 3

Human-reliability assessment

Introduction

Determination of the probability that humans will fail or succeed in performing certain activities is usually dealt with in the literature under the collective term 'human-reliability assessment' or 'human-reliability analysis'. The former term will be used in this study. Several techniques are available for performing a human-reliability assessment (HRA) and many of these were reviewed by Vos (1986). Although one should distinguish between human reliability and human-performance safety as defined in the introduction, this distinction is rarely made in the literature: to the best of the author's knowledge, only Rasmussen (1978; 1982a) and Taylor (1979) have distinguished between the two. Nearly all the techniques are presented in the literature under the name of 'human-reliability assessment/analysis', regardless of whether they aim to assess human reliability or human-performance safety.

Some HRA techniques will be reviewed in this chapter in order to investigate to what extent they can be applied to satisfy the aim of dealing with the prediction of human-error sequences. Of the many techniques available, only the most recently developed ones will be considered. It is noted that the rest of this study can be understood without this chapter being read in full.

The techniques can be grouped into four general categories:
- decomposition techniques,
- techniques based on expert judgement,
- simulation techniques,
- advanced techniques.

It should be noted that the classification into these four categories contains a subjective element. Some of the techniques that belong to one category may also belong to another. However, this classification was set up as an attempt to obtain a systematic approach.

An HRA can involve a qualitative part and a quantitative part. The former is concerned with the modeling of the human activities, i.e. an investigation of how the tasks are built up and of the errors that can be made. The latter part is concerned with the assessment of the 'human-error probabilities' (HEPs) of the activities and the quantitative influence of certain factors. Some techniques involve the qualitative part predominantly or even exclusively whereas this is true for the quantitative part in other techniques.

It is sometimes difficult to distinguish between qualitative and quantitative. The qualitative decision of the analyst not to take certain errors into account is in fact a quantitative decision in which the HEP of certain errors is assumed to be so small that they can be ignored.

Decomposition techniques

The decomposition techniques are characterized by the division of a human task into subtasks. Success probabilities are attached to these subtasks and the probability that the task will be performed successfully is calculated by multiplication of these success probabilities. Four techniques are presented in this section.

Technique for human error rate prediction – This HRA technique, abbreviated as THERP, is probably the best known and most widely applied technique to perform an HRA. The technique is extensively described in the 'Handbook' by Swain & Guttmann (1983). THERP is a method for predicting HEPs and evaluating the degradation of a man-machine system likely to be caused by human errors, alone or in connection with relevant system characteristics. The method is a decomposition technique, i.e. it splits the tasks into subtasks, called 'events'. An event represents the possibility that the subtask is not performed correctly.

An HRA event tree is used for making the analysis (Fig. 6). The branches in an HRA event tree represent a binary decision process, i.e. correct or incorrect performance are the only possibilities. At each bifurcation of the branches, the probabilities of the events must total 1. If no errors are made, the success path is followed. Certain events may represent a recovery action, i.e. the possibility of rectifying a human error made earlier. Recovery actions are represented in Figure 6 by the branches with the probabilities c and g. An error made (e.g. passing the branch with probability H), followed by recovery (passing the branch with probability g) implies a return to the success path via the dashed line. The success probability S_T is, according to Figure 6:

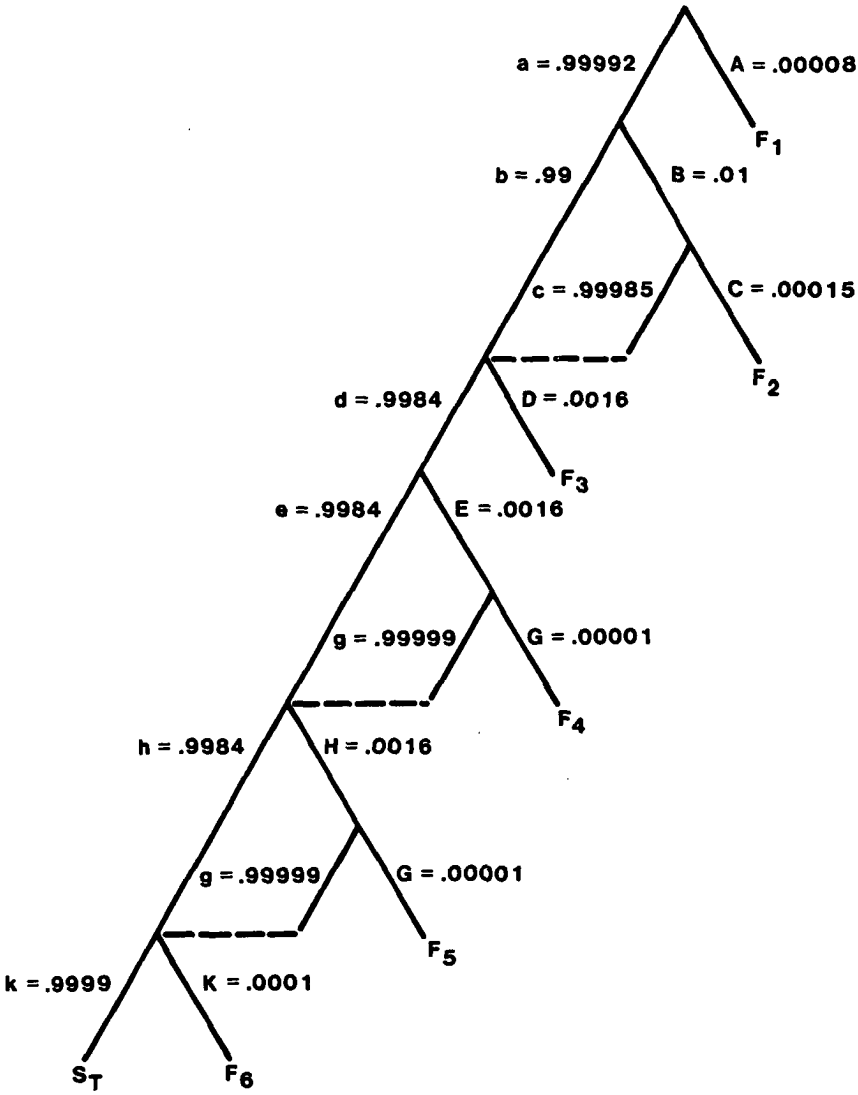
$$S_T = a(b + Bc)d(e + Eg)(h + Hg)k \simeq 0.998.$$

Hence, the failure probability F_T is:

$$F_T = 1 - S_T = 0.002.$$

F_T can be incorporated in the fault tree (Fig. 5) as the probability of a basic event representing human error.

Swain & Guttmann (1983) give a number of values for the HEPs of various events; these values are largely related to the tasks performed in nuclear power plants. Table 2 shows how the HEPs are presented. The first value in the table is the median of a log-normal probability density function, the second value is the error factor (EF). The EF expresses the uncertainty about the real value of the HEP. It is defined as the ratio between the 95% upper bound of the log-normal probability density function and the median (or the ratio between the median and the 5% – lower bound). It should



JHEPs	EVENTS	JOINT HEPs FOR 3 OPERATORS
A	FAIL TO INITIATE ACTION TO ANNs*	.00008
B	MISDIAGNOSIS	.01
C	FAIL TO INITIATE ACTION TO ANN	.00015
D	OMIT STEP 2.4	.0016
E	OMIT STEP 2.5	.0016
G	FAIL TO INITIATE ACTION TO ANN	.00001
H	OMIT STEP 2.6	.0016
K	FAIL TO INITIATE HPI**	.0001

*ANN = ANNUNC:ATOR
**HPI = HIGH-PRESSURE INJECTION

Fig. 6
An example of an HRA event tree (from: Swain & Guttmann, 1983).

Table 2
Human-error probabilities (HEPs) with error factors (EFs) for errors in reading and recording quantitative information from unannunciated displays (modified from Swain & Guttmann, 1983).

Item	Display or Task	HEP	EF
(1)	Analog meter	.003	3
(2)	Digital readout (< 4 digits)	.001	3
(3)	Chart recorder	.006	3
(4)	Printing recorder with large number of parameters	.05	5
(5)	Graphs	.01	3
(6)	Values from indicator lamps that are used as quantitative displays	.001	3
(7)	Recognize that an instrument being read is jammed, if there are no indicators to alert the user	.1	5
	Recording task: Number of digits or letters to be recorded		
(8)	< 3	Negligible	-
(9)	> 3	.001 (per symbol)	3
(10)	Simple arithmetic calculations with or without calculators	.01	3
(11)	Detect out-of-range arithmetic calculations	.05	5

be noted that uncertainty bounds are used instead of confidence limits since the information was not always obtained in a statistical way.

THERP can take various dependencies into account. A dependence implies that the value of an HEP is influenced by the success or failure of a previous event. Swain and Guttmann assume that one event can depend on only one other event. They present formulas and guidelines for calculation of the dependent HEPs.

THERP can also take into account influencing factors, termed 'performance-shaping factors' (PSFs). A list of PSFs is presented in Table 3. Swain and Guttmann approached the influence of the PSFs in several ways. In some tables of the 'Handbook', different values for the HEPs are given e.g. for written or non-written procedures. Furthermore, guidelines are presented for adapting the nominal values, such as for task load and experience. It is noted that the analyst using THERP is left to decide how to adapt the probability given in the 'Handbook', when confronted with certain combinations of PSFs. Since the interaction between certain PSFs is as yet unknown, no guidelines can be given for possible combinations of PSFs.

A shortened version of the 'Handbook' has recently become available (Swain, 1987). It contains a new procedure, called ASEP HRA Procedure for human-reliability assessments (ASEP is the acronym for Accident Sequence Evaluation Program). It can be regarded as a rough method to provide conservative estimates for human-reliability calculations to obtain a first insight. The chief advantage of this procedure over the

Table 3
Some performance-shaping factors in man-machine systems (adapted from Swain & Guttmann, 1983).

EXTERNAL PSFs		STRESSOR PSFs	INTERNAL PSFs
SITUATIONAL CHARACTERISTICS THOSE PSFs GENERAL TO ONE OR MORE JOBS IN A WORK SITUATION	**TASK AND EQUIPMENT CHARACTERISTICS:** THOSE PSFs SPECIFIC TO TASKS IN A JOB	**PSYCHOLOGICAL STRESSORS:** PSFs WHICH DIRECTLY AFFECT MENTAL STRESS	**ORGANISMIC FACTORS:** CHARACTERISTICS OF PEOPLE RESULTING FROM INTERNAL & EXTERNAL INFLUENCES
ARCHITECTURAL FEATURES *QUALITY OF ENVIRONMENT:* TEMPERATURE, HUMIDITY, AIR QUALITY, AND RADIATION LIGHTING NOISE AND VIBRATION DEGREE OF GENERAL CLEANLINESS WORK HOURS/WORK *BREAKS* SHIFT ROTATION AVAILABILITY/ADEQUACY OF SPECIAL EQUIPMENT, TOOLS, AND SUPPLIES MANNING PARAMETERS ORGANIZATIONAL STRUCTURE (e.g., AUTHORITY, RESPONSIBILITY, COMMUNICATION CHANNELS) ACTIONS BY SUPERVISORS, CO-WORKERS, UNION REPRESENTATIVES, AND REGULATORY PERSONNEL REWARDS, RECOGNITION, *BENEFITS*	PERCEPTUAL REQUIREMENTS *MOTOR REQUIREMENTS (SPEED, STRENGTH, PRECISION)* CONTROL-DISPLAY RELATIONSHIPS ANTICIPATORY REQUIREMENTS INTERPRETATION DECISION-MAKING COMPLEXITY (INFORMATION LOAD) NARROWNESS OF TASK FREQUENCY AND *REPETITIVENESS* TASK CRITICALITY LONG- AND SHORT-TERM MEMORY CALCULATIONAL REQUIREMENTS FEEDBACK (KNOWLEDGE OF RESULTS) DYNAMIC *vs.* STEP-BY-STEP ACTIVITIES TEAM STRUCTURE AND COMMUNICATION MAN-MACHINE INTERFACE FACTORS: DESIGN OF PRIME EQUIPMENT, TEST EQUIPMENT, MANUFACTURING EQUIPMENT, JOB AIDS, TOOLS, FIXTURES	SUDDENNESS OF ONSET *DURATION OF STRESS* TASK SPEED TASK LOAD HIGH JEOPARDY RISK THREATS (OF FAILURE, LOSS OF JOB) MONOTONOUS, DEGRADING, OR MEANINGLESS WORK LONG, UNEVENTFUL VIGILANCE PERIODS CONFLICTS OF MOTIVES ABOUT JOB *PERFORMANCE* REINFORCEMENT ABSENT OR NEGATIVE SENSORY DEPRIVATION DISTRACTIONS (NOISE, GLARE, MOVEMENT, FLICKER, COLOR) INCONSISTENT CUEING	PREVIOUS TRAINING/EXPERIENCE *STATE OF CURRENT PRACTICE* OR SKILL PERSONALITY AND INTELLIGENCE VARIABLES MOTIVATION AND ATTITUDES EMOTIONAL STATE STRESS (MENTAL OR BODILY TENSION) KNOWLEDGE OF REQUIRED PERFORMANCE STANDARDS SEX DIFFERENCES PHYSICAL CONDITION ATTITUDES BASED ON INFLUENCE OF FAMILY AND OTHER *OUTSIDE* PERSONS OR AGENCIES GROUP IDENTIFICATIONS
JOB AND TASK INSTRUCTIONS: SINGLE MOST IMPORTANT TOOL FOR MOST TASKS		**PHYSIOLOGICAL STRESSORS:** PSFs WHICH DIRECTLY AFFECT PHYSICAL STRESS	
PROCEDURES REQUIRED (WRITTEN OR NOT WRITTEN) WRITTEN OR ORAL COMMUNICATIONS *CAUTIONS AND WARNINGS* WORK METHODS PLANT POLICIES (SHOP PRACTICES)		DURATION OF STRESS FATIGUE PAIN OR DISCOMFORT HUNGER OR THIRST *TEMPERATURE EXTREMES* RADIATION G-FORCE EXTREMES ATMOSPHERIC PRESSURE EXTREMES OXYGEN INSUFFICIENCY VIBRATION MOVEMENT CONSTRICTION LACK OF PHYSICAL EXERCISE DISRUPTION OF CIRCADIAN RHYTHM	

traditional THERP is that it saves time and money. The ASEP HRA Procedure allows an initial screening to be made which can be followed by an additional, more detailed analysis by means of THERP.

Considering the amount of information in the 'Handbook', THERP can be regarded as the most complete and best documented HRA technique (Meister, 1984) but it is still open to criticism. Baron et al. (1982) and Rasmussen (1987b) claim that THERP can be used only for well-defined procedural actions as these can be decomposed into small units; THERP is less applicable to activities related to decision making and problem solving as these activities are difficult to decompose. Leplat (1987) doubts the value and the validation of the HEPs used. The extent to which THERP could be used to satisfy the aim of the present study will be discussed later.

Tecnica emperica stima errori operatori – This HRA technique, abbreviated as TESEO, was developed in Italy by Bello & Colombari (1980). It describes the probability that an activity is performed incorrectly as a multiplicative function of five parameters:
(1) the type of activity to be carried out,
(2) the time available to carry out this activity,
(3) the human operator's characteristics,
(4) the operator's emotional state, and
(5) the environmental ergonomic characteristics.
The error probability HU equals:

$$HU = K_1K_2K_3K_4K_5$$

where K_1 = activity's typologic factor, K_2 = temporary stress factor, K_3 = operator's typologic factor, K_4 = activity's anxiety factor, K_5 = activity's ergonomic factor.

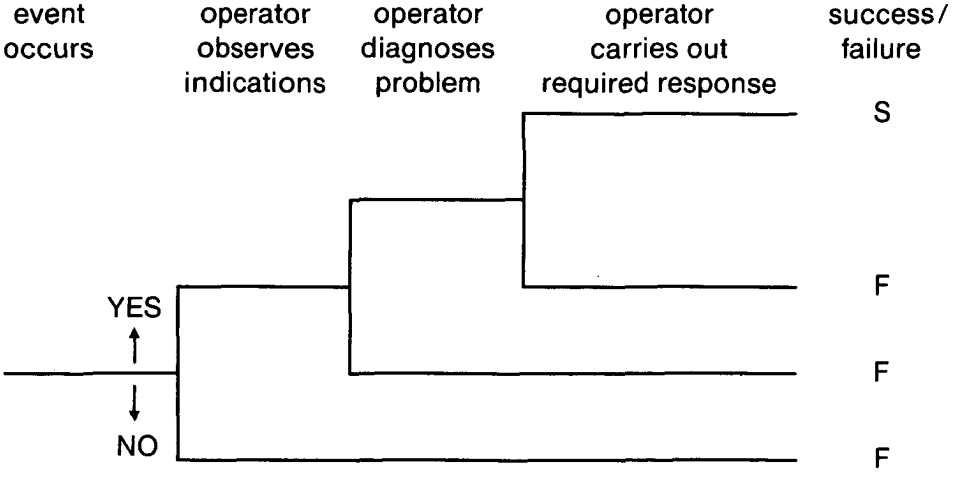


Fig. 7
The basis of an OAT (after: Hall et al., 1982).

Bello & Colombari (1980) gave quantitative values for the K-factors. Most of the K-values were obtained from the English System and Reliability Service.

TESEO is a technique in which a limited number of influencing factors are incorporated via the K-parameters. It is the only technique in which influencing factors are multiplied to obtain the total influence. This may be correct if the value of the influencing factors is adapted to incorporate a possible dependence between certain factors.

Operator action tree — The 'operator action tree' (OAT) is a diagram indicating the errors that can be made in incorrectly responding to a critical state of a system (Hall et al., 1982). The OAT resembles the HRA event tree in its logical structure. The difference is that the errors are more related to the functions an operator must fulfil to obtain a correct response that will bring the system back to a safe state (Fig. 7). The errors are more general, such as 'incorrect diagnosis' and 'operator does not carry out the required response'.

Another difference between OAT and HRA event trees is that, in most cases, the errors are quantified by means of the 'time/reliability correlation' (TRC). A TRC shows how an HEP depends on the time that the operator has available for correct responding to a certain situation. Hence, it is assumed that time is the determining factor for the probability of a correct response. A typical TRC curve is presented in Figure 8. The OAT itself is, in fact, a qualitative method; the TRC is used for the quantification of the OAT.

OATs have been implemented in several studies, e.g. by Hannaman & Spurgin (1984). As opposed to the event trees used in THERP, the OAT focuses on the human errors that can be made in responding to a specific initiating event. It is a qualitative technique (because of the definition of the human errors that can occur) as well as

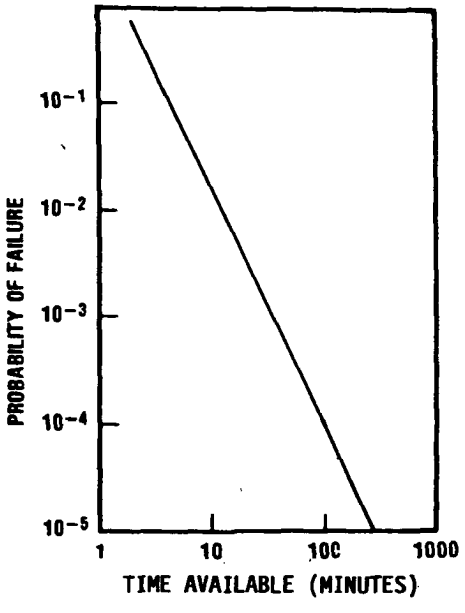


Fig. 8
A curve modeling the time/reliability correlation (from: Hannaman & Spurgin, 1984).

a quantitative technique (because of the application of the TRC). The OAT, however, does not particularly concern itself with the consequences of human errors.

Operator action event tree – As opposed to the OAT presented in the preceding paragraph, the 'operator action event tree' (OAET) focuses on the consequences of human errors. Brown et al. (1982) applied the OAET for describing the human errors that can be made in responding to an initiating event.

The method starts with construction of the system event tree. This tree is then transformed into an OAET by the addition of operator actions to the system event tree. The result is a model which displays the role of the operator logically throughout the progress of an accident. Figure 9 shows an example of an OAET.

Quantification of the human errors is not the goal of an OAET; the OAET is a qualitative tool for providing information upon which an analysis of operator performance under accident conditions can be based. It can be concluded that the OAET is more divergent in its approach than the previous techniques; it considers the consequences of both human errors and system failures.

Application to this study – Various decomposition techniques have been presented. THERP was treated extensively because it contains a great deal of qualitative and quantitative information. THERP and most of the other decomposition techniques, viz. TESEO and the OAT, consider single human errors only and not their consequences. These techniques can therefore not be regarded as HPSA techniques and do not have the potential to satisfy the aim of this study concerning the prediction of human-error sequences.

The OAET was also regarded as a decomposition technique. It greatly resembles the other techniques but unlike them it takes into account the consequences of both human errors and system failures. The OAET is more or less an HPSA technique and will be discussed in the final section of this chapter.

Techniques based on expert judgement

The disadvantage of the preceding techniques is that they need data about HEPs on which little field material is available. Other techniques may therefore be used which are based more on expert or subjective judgement. Although most HRA techniques implicitly use the judgement of experts either qualitatively or quantitatively, the techniques described in this section make use of expert judgement much more explicitly. Expert judgement can be defined as the estimation of HEPs by persons who are very familiar with the task and the influencing factors. These experts can be, for instance, operators or supervisors. Some of the techniques presented in this chapter use absolute judgements about human reliability whereas other techniques use more relative estimations by experts.

Direct/indirect numerical estimation – The simplest technique based on expert judgement is the 'direct numerical estimation' (DNE), in which absolute HEPs are assessed

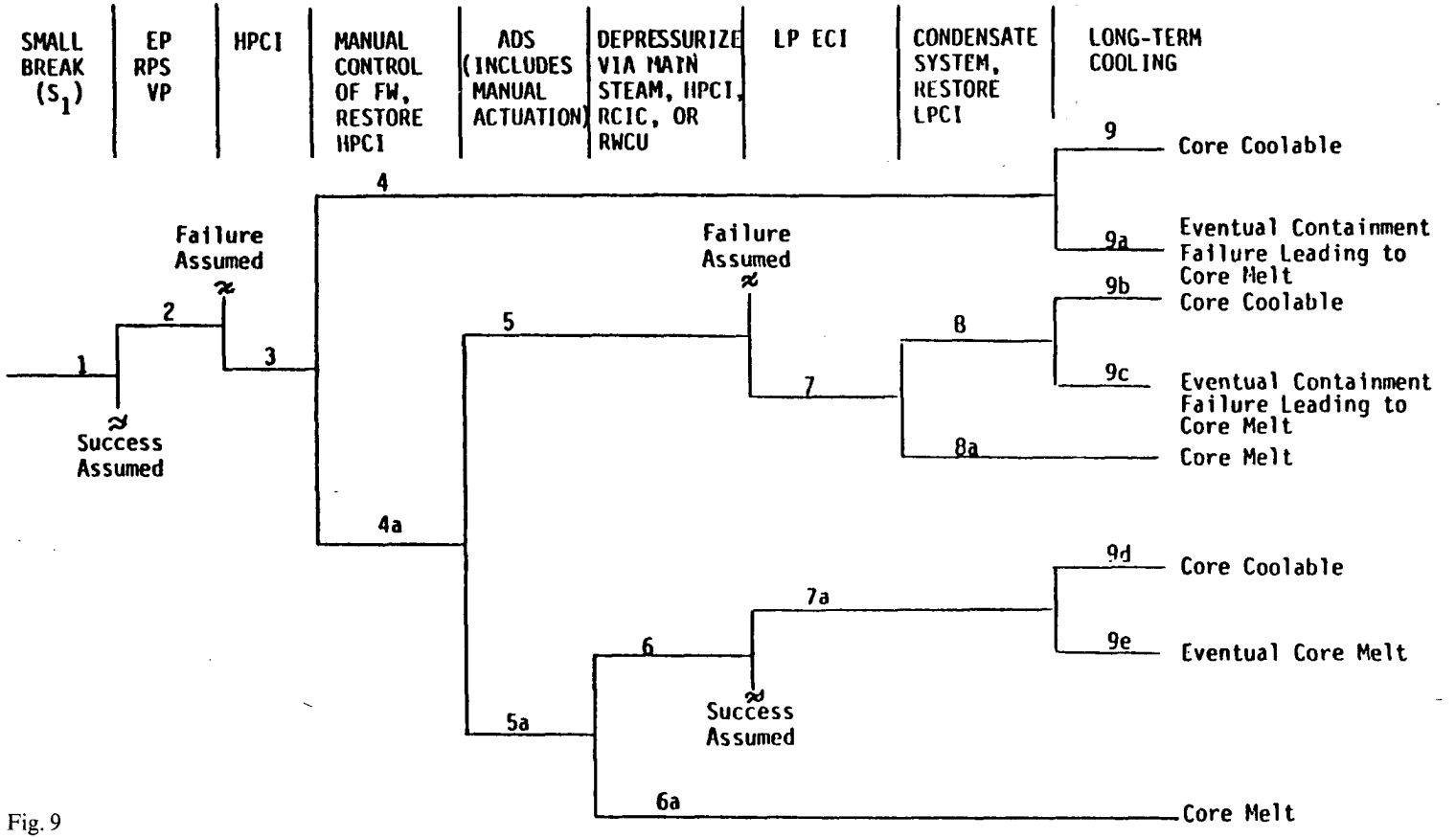


Fig. 9
Example of an OAET. Event 1 is an example of an initiating event: a break in the coolant system of a nuclear power plant that could cause inadequate cooling. Events 2 through 9 describe the successful or unsuccessful intervention of technical components or human actions necessary to mitigate the effects of the initiating event (from: Brown et al., 1982).

directly by experts (Seaver & Stillwell, 1983). A specific logarithmic scale can be used to avoid too many differences between estimations by experts. The estimations are then transformed to HEPs by applying a special formula.

The 'indirect numerical estimation' (INE) involves judging the ratios between certain pairs of tasks, such as 'task A is 10 times more likely than task B' (Seaver & Stillwell, 1983). This is done for several pairs of tasks; assigning a reference HEP for a certain task allows the HEPs of all tasks to be obtained from the ratio judgements. The reference HEP can be obtained from field studies or from the DNE.

Paired comparison procedure – The 'paired comparison procedure' (PCP) is a technique in which a great many pairs of judgements are made within a set of tasks (Seaver & Stillwell, 1983). Instead of ratio scales (Siegel, 1956) as used in the INE, ordinal or ranking scales of the type 'task A is more likely than task B' are used. With this technique, pairs of tasks are selected at random from a set of tasks and judgements are made for each pair. This is repeated by each expert for all possible pairings.

Each task is assigned a scale rank value, S, based on the rankings of the tasks by several experts. This value is then converted to an HEP by means of the formula:

$$\log \text{HEP} = aS + b$$

The constants a and b are obtained by applying this formula to two tasks with known HEPs and with the assessed scale rank values.

The disadvantage of this technique is the large number of judgements required, i.e. n(n-1)/2 in which n is the number of tasks. Seaver & Stillwell (1983) have, however, described procedures for reducing the number of comparisons. Comer et al. (1984) applied the PCP and the DNE to a number of tasks to be carried out in nuclear power plants.

Success likelihood index method – Another scaling technique is the 'success likelihood index method' (SLIM: Embrey et al., 1984). As opposed to the previous techniques based on expert judgement, in which only the tasks themselves are considered, SLIM considers the PSFs influencing the tasks (see Table 3).

When this technique is applied, the first step is to define a set of PSFs. The expert has then to assess the importance of each factor with regard to its relative effect on the task under consideration. Thirdly, an assessment must be made of what the actual state of the PSF is for the task. The second step is called 'weighting' and is expressed by an 'importance weight value'; the third step is called 'rating' and is expressed by a 'scale value'. After normalization, the two values are multiplied for each PSF and the resulting products are summed to give the 'success likelihood index', S. As is the case with the paired comparisons, the formula $\log \text{HEP} = aS + b$ can be used in SLIM to obtain HEPs. Vestrucci (1988) has, however, shown that this equation has theoretical weaknesses and he has presented a more suitable equation to be used in SLIM.

SLIM has been implemented with the computer, together with a program developed earlier, called MAUD. MAUD, which stands for Multi-Attribute Utility Decomposi-

tion, had originally been designed for use in decision-analysis problems. The program elicits information interactively from the expert about the sort of PSFs and the weighting and rating values relevant to the determination of task reliability.

Application to this study – As may be clear from the previous descriptions, the techniques based on expert judgement are explicitly quantitative techniques. The techniques are particularly concerned with the assessment of HEPs and the quantitative influence of PSFs. They can therefore be used as tools to quantify the errors revealed by a qualitative method. The SLIM-MAUD technique in particular has advantages over the other techniques based on expert judgement because it can easily be used to perform a simulation by varying the influence of the PSFs. Decisions on effective changes to be made to achieve low HEPs can thus be arrived at.

The techniques based on expert judgement that were presented here are explicitly HRA techniques; revealing the consequences of the errors is not their prime objective. Hence, they cannot be regarded as techniques applicable to satisfy the aim of the present study.

Computer simulations

The techniques described so far make some use of computers. None, however, makes explicit use of computers for simulation purposes. Techniques will now be presented in which computers are used for simulating operator behavior, with the aim of assessing human reliability and operator strategies.

Maintenance personnel performance simulation – 'Maintenance personnel performance simulation' (MAPPS) is a task-oriented computer model used for simulating maintenance activities in nuclear power plants (Siegel et al., 1984; Kopstein & Wolf, 1985). It was developed to give personnel in nuclear power plants some insight into maintenance processes. The model allows the influences of all kinds of PSFs to be simulated. It can provide maintenance-oriented human-reliability data for probabilistic risk assessment (PRA) purposes.

The computer simulates the subtasks that constitute the maintenance task. A flow chart of the logic of the MAPPS simulation for a subtask is presented in Figure 10. An important function in the model is the comparison between the maintainability level and the subtask requirements. The model establishes the maintainability level by considering extrinsic factors (e.g., temperature); the subtask requirements are assessed in parallel. This is done by considering certain factors such as adequacy of the procedures and the accessibility of equipment. Comparison of these two factors yields the ability difference that serves for the determination of the success probability of the subtask, the time required for subtask completion and the stress level. The determination of the success probability is followed by a comparison of this probability with a certain acceptance level. If the probability is greater than this level, the subtask is assumed to have been performed correctly. Otherwise, a failure is assumed to have occurred. Similar processes of comparisons are made at the error-detection block.

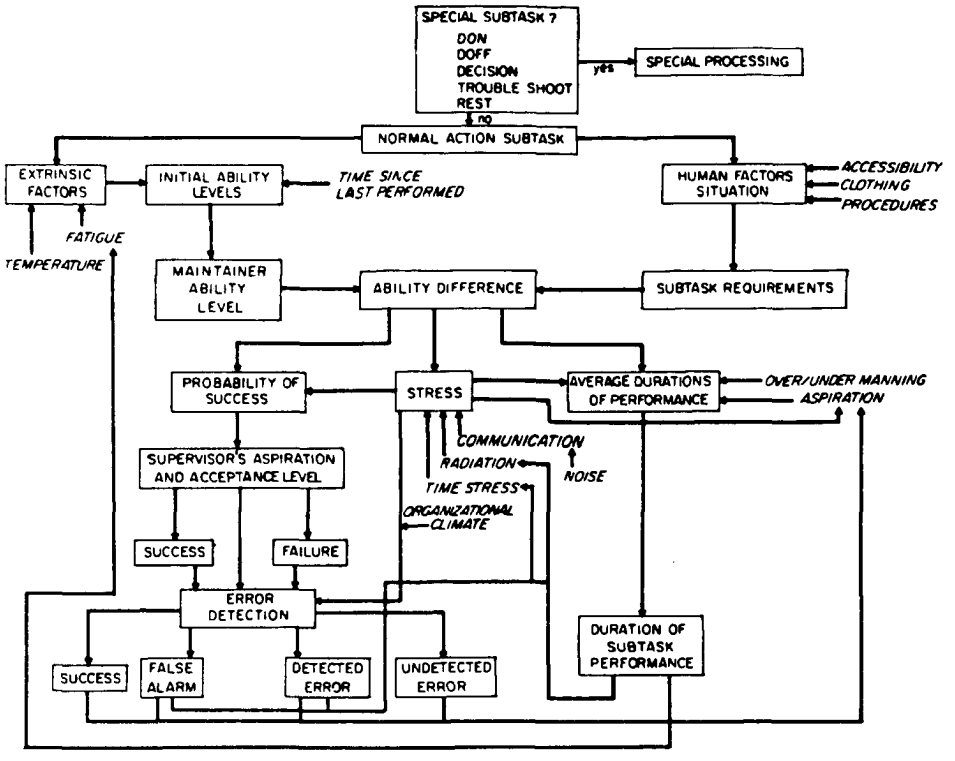


Fig. 10
Flow chart of the MAPPS computer model (from: Siegel et al., 1984).

This procedure continues in series for each subtask. Several output variables such as error likelihood (obtained from the number of failures and the total number of iterations) and the average duration are obtained from this approach. This procedure can be followed for a variety of input variables and for a number of subtasks. Varying the input information permits the requirements for final successful maintenance to be determined.

Dynamic logical analytical methodology – The 'dynamic logical analytical methodology' (DYLAM) is a computer model which is able to simulate system performance as a function of time (Amendola & Reina, 1984; Mancini, 1985). Operator actions and component states are incorporated in the model, either under nominal or under failure conditions. The model can predict undesired consequences resulting from dynamic changes induced by component failures, human errors or both.

The application of DYLAM involves several steps (Nivolianitou et al., 1986). The first step concerns a description of the physical behavior of the system to be analyzed. This description is done with a set of difference equations expressing the relations between the variables in the system. A failure mode and effect analysis is performed next, in which the direct effects of certain technical or human failures are analyzed. On the basis of this information, the difference equations are transformed to para-

metric equations representing the variables under certain failure-mode conditions. The final step is to assign probabilities to the failure modes. DYLAM then generates all the possible event sequences and the probability of these event sequences. The model has certain cut-off features based on a probability limit that retains the dominant sequences with relatively high probabilities.

The advantages of DYLAM over event trees are:

(1) consideration of the dynamic aspects of the system,

(2) automatic and objective generation of the possible event sequences.

DYLAM is not a true HRA technique; it should be regarded as a safety-assessment technique for human errors and system failures. Because of the generation of the event sequences leading to undesired consequences, it can be regarded as a qualitative technique. However, it can also be regarded as a quantitative technique since it calculates the probabilities of these sequences.

Application to the present study – It is obvious from a comparison of the two simulation techniques that the goals of both techniques are different. The outputs of MAPPS are the error likelihood and the average duration of a particular maintenance procedure. The consequences of certain errors are usually not considered. This is different from the DYLAM technique, which considers several errors and sequences of errors and which is capable of generating all kinds of error sequences leading to certain consequences. Hence, MAPPS cannot be used for the prediction of sequences of human errors, which is needed for this study. DYLAM, however, has the capability to do this, which will be discussed more extensively below.

Advanced techniques

Many techniques were presented in the previous sections. Most of these techniques are aimed at quantifying HEPs, sometimes in combination with errors of technical components. Since the analysis of human errors involves many difficulties, however, some authors have chosen more advanced approaches which can be described roughly as going in two directions. The first direction involves the attempt to extend the existing HRA techniques, whereas the approach in the second direction is more in depth, through a more thorough qualitative analysis of human errors. The following subsections deal with some of these techniques.

Systematic human application reliability procedure – The 'systematic human application reliability procedure' (SHARP) follows the first approach (Hannaman & Spurgin, 1984). It is not itself a technique but it is a procedure which combines several of the previously described techniques. SHARP is a framework which helps the user to make a systematic selection from the previous techniques on the basis of the type of human error, in order to determine its probability thoroughly. SHARP consists of seven steps (Fig. 11), according to Hannaman & Spurgin (1984): "...

(1) *definition*: to ensure that all different types of human interactions are adequately considered in the study;

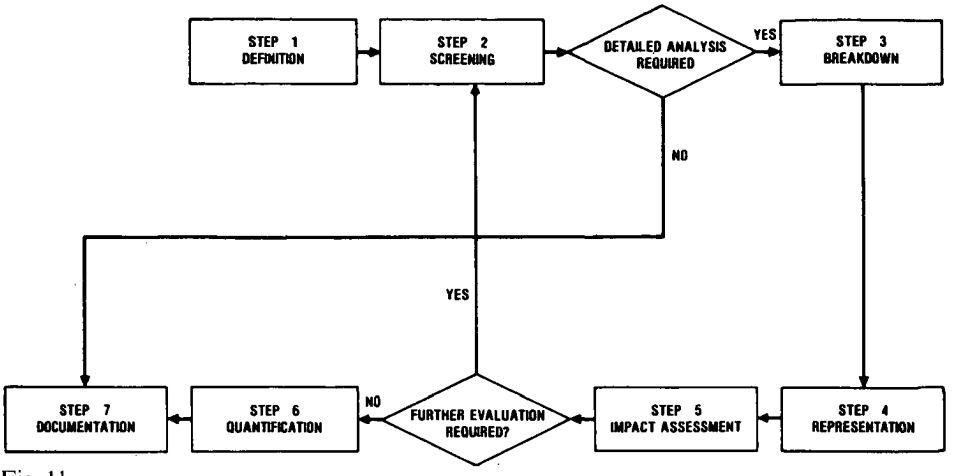


Fig. 11
Links between SHARP steps (from: Hannaman & Spurgin, 1984).

(2) *screening*: to identify the human interactions that are significant to operation and safety of the plant;
(3) *breakdown*: to develop a detailed description of important human interactions by defining the key influence factors necessary to complete the modeling; the human-interaction modeling consists of a representation, impact assessment, and quantification;
(4) *representation*: to select and apply techniques for modeling important human interactions in logic structures; such methods help to identify additional significant human actions that might impact the system logic trees;
(5) *impact assessment*: to explore the impact of significant human actions identified in the preceding step on the system logic trees;
(6) *quantification*: to apply appropriate data or other quantification methods to assign probabilities for the various interactions examined, determine sensitivities and establish uncertainty ranges;
(7) *documentation*: to include all necessary information for the assessment to be traceable, understandable, and reproducible".

Each SHARP step has defined objectives, inputs and outputs, activities, and rules. Hannaman & Spurgin (1984) described the steps in detail. The advantages of SHARP are the systematic approach followed for quantification of human errors and the clear indication of the relation between an HRA and a PRA, the purpose for which SHARP was set up.

Work analysis — 'Work analysis' (WA) follows the second approach of the advanced techniques (Rasmussen & Pedersen, 1982; Pedersen, 1985). The aim of WA is to pre-identify errors in procedural tasks. It can be regarded as a tool for the analysis of immediate consequences of erroneous human behavior in these procedural tasks (e.g. test and calibration procedures). WA consists of four steps (Rasmussen & Pedersen, 1982): "...

(1) analysis of task sequence,
(2) analysis of task reliability,
(3) analysis of immediate risk,
(4) analysis of task disturbances".

WA is mainly a qualitative technique meant to cover two aspects related to human performance. First, it is to be used to improve the design of a certain task; secondly, it is intended to be used for PRA support. It utilizes general formats of which an example is presented in Figure 12.

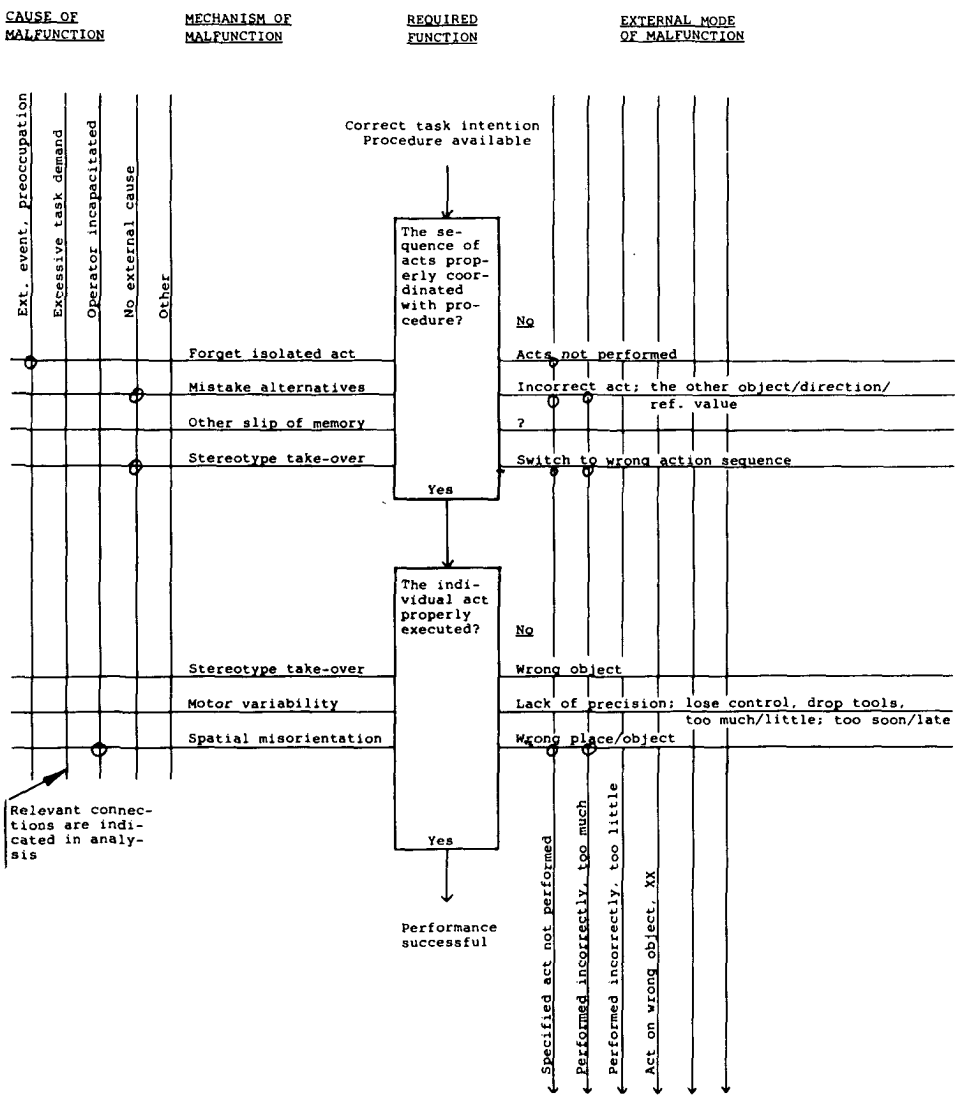


Fig. 12
An example of a format to be used in a WA for discovering potential error causes (from: Rasmussen, 1982b).

Systematic human error reduction and prediction approach – The overall function of the 'systematic human error reduction and prediction approach' (SHERPA) is the provision of a framework within which human errors can be assessed qualitatively and quantitatively (Embrey, 1986). SHERPA consists of an integrated set of techniques which can be used separately or in its entirety, depending on the resources.

The techniques that are used in SHERPA can be divided roughly into (Fig. 13):

(1) 'hierarchical task analysis', which is a method for identifying the various goals that have to be achieved within a task and the way in which these goals are combined to achieve the overall objectives;
(2) 'human error analysis', which is a method for identifying the human errors that can be made in procedural tasks and for analyzing the immediate consequences of these errors; the method is based largely on the WA method mentioned above;
(3) the quantification of various human-error modes, for which two techniques are used: first, quantification can be done by means of the SLIM-MAUD technique described earlier; secondly, a so-called 'systematic approach for the reliability assessment of humans' (SARAH) can be applied; SARAH is basically a software package for enabling the more rapid and more sophisticated application of SLIM-MAUD;
(4) the last step is to make recommendations for procedures, training and equipment design in order to improve human reliability.

Application to this study – Three techniques were presented in this section that were referred to as 'advanced' because of their more extended or thorough approach. The first technique, SHARP, is meant to be used particularly for the quantification of human reliability. It does not consider the effects of erroneous human behavior in detail and is not meant to predict human-error sequences.

The two other techniques, WA and SHERPA, consider the consequences of human errors. However, only the immediate effects of human errors are considered. The two techniques are not meant to, in the first instance, identify sequences of human errors and analyze their effects. Hence, these two techniques also do not meet the requirements that had been set to satisfy the aim of this study.

Final remarks

Some other techniques that were not covered earlier in this review will now be described. There follow concluding remarks concerning the applicability to this study of the techniques reviewed in this chapter and that consider explicitly the consequences of human errors. Finally, the essential problem of dealing with the shortage of data for HEPs is discussed.

Other techniques – Some techniques were discarded to prevent this chapter from becoming too extensive, as soon as it became clear that they lacked the potential to satisfy the aim of this study. They will only be mentioned briefly here but relevant references are given.

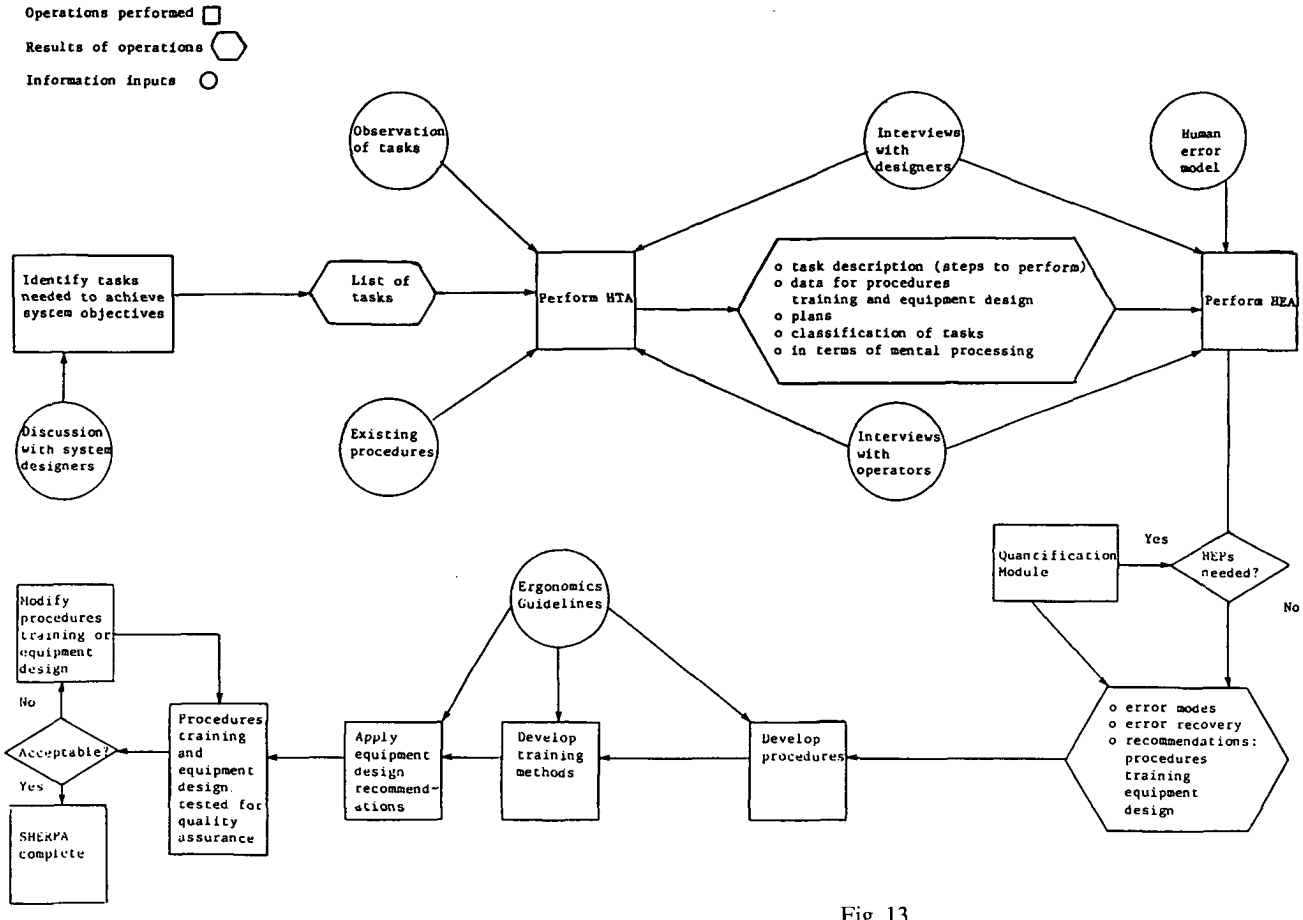


Fig. 13
Flow chart of SHERPA (from: Embrey, 1986).

(1) the 'AIR data store' (Meister, 1984) and the 'technique for establishing personnel performance standards' (Embrey, 1976) which like THERP can be regarded as decomposition techniques concerned only with successful human behavior;
(2) the 'generic error-modelling system' (Reason & Embrey, 1985; Reason, 1987b), which is a cognitive framework intended for analyzing common human errors;
(3) the 'verbal protocol analysis' (Bainbridge, 1979), which is a method for obtaining information directly from operators about tasks they are performing;
(4) the 'critical incident technique' (Flanagan, 1954), which is particularly concerned with near-accidents;
(5) the 'sequential task analysis method' (Drury, 1983), which is a qualitative method for analyzing single human errors when a sequence of actions is performed;
(6) the 'critical decision approach', the 'cause-consequence modelling approach' and the 'socio-technical approach to human reliability' (Embrey, 1984), the first two being methods for analyzing human errors in complex situations and the third a quantitative method for generating HEPs via expert judgement;
(7) the 'management oversight and risk tree' (Johnson, 1980), which can be regarded as a fault tree in a generalized form to trace and manage causal factors leading to a variety of predefined undesired events.

Obviously, there is no lack of HRA techniques. It can, however, not be decided which technique is best; the applicability of the technique depends largely on the purposes of the analyst.

Concluding remarks – The purpose of this chapter was to determine to what extent HRA techniques could be used to predict human-error sequences. Selected HRA techniques were reviewed and divided into decomposition techniques, techniques based on expert judgement, computer simulations and advanced techniques. Most techniques are quantitative and a few qualitative or a combination the two. The present selection of HRA techniques was made in view of the fact that procedural (rule-based) human performance formed the basis of this study.

Only four techniques, viz. the OAET, WA, SHERPA and DYLAM, seem to come near to meeting the demands of the study as they can be regarded as HPSA techniques: all these techniques consider the effects of erroneous human performance. WA and SHERPA, however, look only at the immediate effects of human behavior. DYLAM, on the other hand, considers the effects of sequences of human behavior. However, the primary goal of DYLAM is to determine all possible failure paths leading to a particular pre-defined consequence. Finally, OAET considers sequences of failures (technical and human) but is only concerned with pre-defined critical consequences. It does not indicate how (sequences of) human errors lead to other critical consequences. The four methods mentioned will therefore not be discussed any further. In the next chapter, a technique that has the potential to satisfy the aim of this study will be described.

The databank problem – In marked contrast to the overwhelming number of techniques available, there is a great lack of HEPs (Topmiller et al., 1982). The HEPs

related to knowledge-based errors are particularly difficult to gather. The data of Swain & Guttmann (1983) are probably the most extensive form now available but most contain a number of uncertainties. Knowledge about reliable HEPs is crucial for the application of most of the techniques described so far. It is therefore important to find HEPs and to gather information about the variance of the HEPs. Comer et al. (1983) have set up a proposal for a databank of HEPs related to operations in nuclear power plants. This proposal seems very promising, since it meets most of the requirements for gathering reliable HEPs regarding the influence of the PSFs.

Directly related to the first problem is the aspect of the validation of a certain quantitative technique. Validation involves finding how well predictions correlate with the field data measured. The most important problem related to the acquisition of data, i.e. the low HEPs, implying long measurement times, are particularly applicable to the validation. Only a few such validations are known at the moment. Williams (1985) has investigated the validation of several HRA techniques. It can be concluded from this that too few results have so far been obtained in this area. The issues dealing with the quantification of HEPs in relation to the present study will be discussed more extensively in the last chapter.

Chapter 4

General description of the technique for human-error-sequence identification and signification

Introduction

It was shown in the preceding chapter that, at the moment, there are many HRA techniques and only few HPSA techniques. It was also mentioned that the HRA techniques consider only erroneous human performance; the HPSA techniques consider not only erroneous human performance but also its consequences. It appeared that there is currently no adequate HPSA technique to predict sequences of human errors leading to various undesired consequences, viz. the initiating events of the system event tree. A technique, referred to as 'Technique for Human-Error-Sequence Identification and Signification' (THESIS), which is intended to meet this goal, will now be presented.

Five years ago, when this study was started (Heslinga, 1983), even fewer techniques were available for human-performance safety assessment. The 'Handbook' (with the THERP method: Swain & Guttmann, 1983) became available more or less at this time. As indicated before, THERP is a human-reliability technique that only considers the desired consequence of following a procedure correctly. Since the present study is also interested in the consequences of not following the procedure correctly, THERP was not sufficiently thorough. The idea therefore arose to extend the HRA event tree of THERP by considering combinations of human errors – and the various consequences involved – as in the system event trees used for technical systems. This led to the development of an event tree which shows some features of the HRA event trees and some of the system event trees. It was given the name 'THESIS event tree' and is explained in the next subsection. This is followed by a subsection showing how THESIS is to be used and finally by a discussion of the problems of applying THESIS.

The THESIS event tree

An example of a THESIS event tree related to a particular human activity (a step of a procedure) is given in Figure 14. The human activity concerns the turning of a two-position switch. The panel layout is assumed to be as presented in the same figure. Such a switch is used to close or open a motor-operated valve. It is assumed that switch 2 has to be turned, i.e. valve 2 has to be opened.

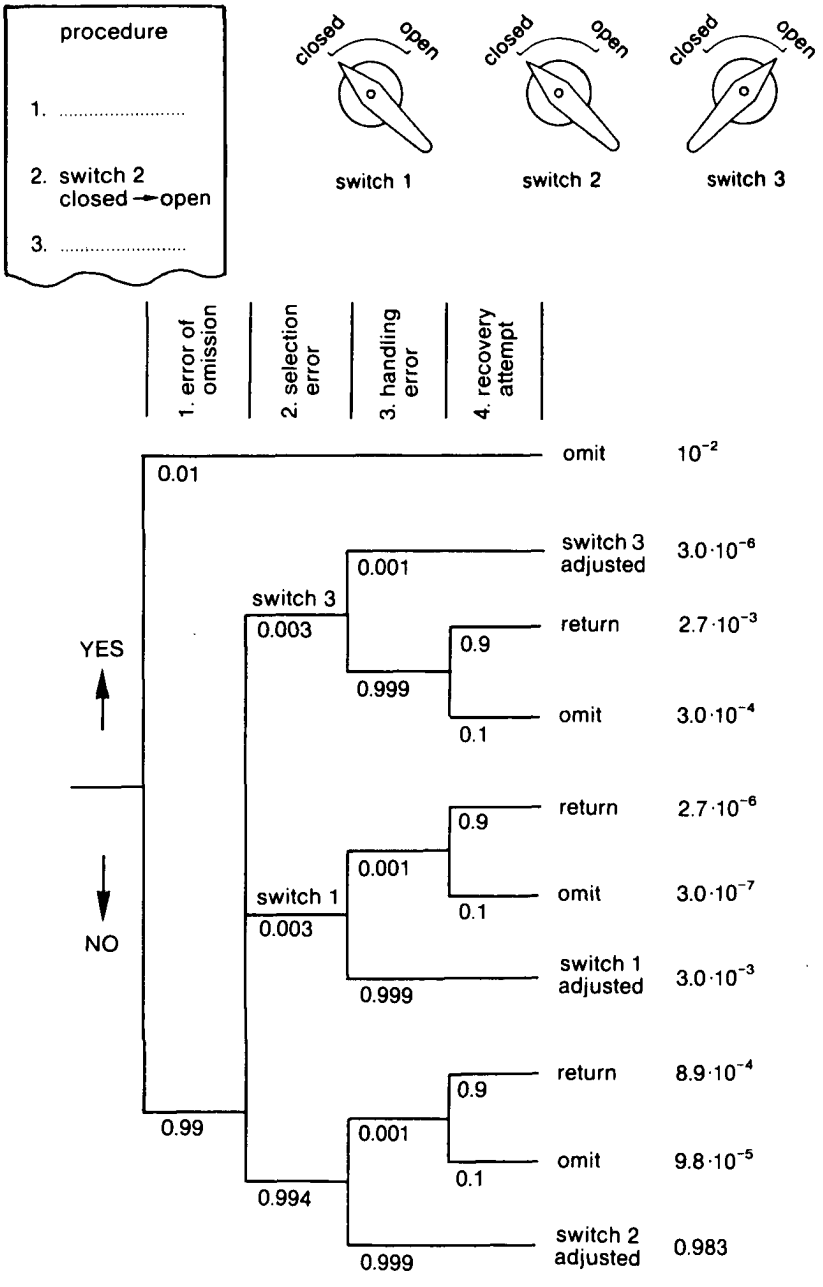


Fig. 14
THESIS event tree (bottom) concerning the adjustment of a two-position switch located on a panel (top). It is presumed that switch 2 has to be turned. The probabilities of making an error or succeeding are presented at the branches. It is assumed that there is no dependence between the events. The outcomes and the outcome probabilities are given at the offshoots of the tree.

A THESIS event tree of a human activity implies breaking down this activity into small elementary steps, called 'events'. Each event carries the possibility of success or failure. Several outcomes are possible, depending on the errors made. If the YES-direction is followed in the first event, an error of omission is made. None of the other events are then applicable and the immediate outcome is 'omit'.

It is noted here that the word 'outcome' is used instead of 'consequence' to be consistent with the literature regarding the word 'consequence' (McCormick, 1981). The word 'consequence' will be used further on in this study to refer to the effect of an outcome (e.g. error of omission) upon the state of a process (e.g. a sudden pressure increase because of the error of omission).

If no error of omission is made, the NO-direction is followed and one reaches the bifurcation of the second event (selection error). If the YES-direction is followed at that point, switch 1 or 3 is selected instead of the desired switch 2. It is further assumed for the explanation that switch 1 is selected. One then reaches the bifurcation of the third event (the handling error). The handling error implies that an error is made at the component selected. This can have several causes, for instance a reading error: 'open' is read instead of 'closed'. If the handling error is made in this way (the YES-direction is followed), the person performing this activity thinks that the valve has already been opened. If no recovery attempt is made, which means that the NO-direction is followed at the fourth event, the outcome will be 'omit' since no switch has been set.

The fourth event in Figure 14, the recovery attempt, indicates an important aspect of human behavior because it is possible that the person involved discovers having done 'something' wrong. As a result, he will make a recovery attempt and the YES-direction is followed at event 4. The person will then reach the 'return' outcome, indicating that he will return to some point in the event tree to repeat the activity. This repetition may be performed partly or completely, dependent on the point returned to. It is assumed in Figure 14, for the sake of convenience, that no recovery attempt will take place if no handling error has been made. A similar explanation accounts for the rest of the tree.

The different types of outcome that are possible on completion of the THESIS event tree are:

(1) the success outcome, if the activity is performed correctly and the NO-direction is followed in each event (in Figure 14: the turning of switch 2);
(2) several failure outcomes, if errors are made in one or more events without any recovery attempts (in Figure 14 these are the turning of switch 1, the turning of switch 3 and omit);
(3) the return outcome, if errors are made in one or more events, followed by a recovery attempt.

The path leading to the success outcome is called 'success path'; all others are called 'failure paths'.

Two essential assumptions are made in this context. The first one is that technical errors are disregarded from the analysis. It implies that the technical system being controlled by an operator is technically perfect. Hence, recovery attempts are not made

to overcome technical errors; they may only occur because of human errors that were made earlier or because of a check in which an operator checks his own or somebody else's performance.

A second assumption is that, when errors have been made and a person makes a recovery attempt, the system is reset. It means that a control device that has been adjusted, is set to its starting position during the recovery attempt. The result of a specific action is then always, whether it is right or wrong, that only one device is adjusted at the most. Because of this assumption, the failure outcomes in Figure 14 only result in 'omit', 'adjust switch 1' or 'adjust switch 3'; a combination of switch adjustments is not possible as an outcome.

Probabilities are shown at each bifurcation in the tree of Figure 14. The probability of someone following the YES-direction is called a 'human-error probability' (HEP) and that of following the NO-direction is called a 'human-success probability' (HSP). Most HEPs are taken from Swain & Guttmann (1983). It is assumed in this example that there is no dependence between the events. This means that the HEP is not influenced by the success or failure of a previous event or activity. The probability that a person will follow a particular path can simply be calculated by multiplication. These probabilities are presented in Figure 14 at the offshoots.

The approach

The aim of this study is to develop a technique for human-error-sequence identification and signification. It may be clear from the previous section that a THESIS event tree of a human activity considers in a qualitative way all possible failure paths (human-error sequences) and the outcomes resulting from the human errors. Assigning probabilities to the branches allows the probabilities that the outcomes will occur to be quantified and significant event sequences leading to the outcomes to be discovered. If the effect of the outcomes on the state of the process is known, the probabilities that certain consequences will occur can be derived from the outcome probabilities. THESIS event trees can thus make it possible to satisfy the aim of this study.

The human activity considered in Figure 14 can be regarded as a specific action. A specific action is defined as a human activity which, if performed correctly, will result in the desired status change of a certain component such as a valve, a switch, etc. Until now a THESIS event tree was made of only one specific action, instead of a complete procedure. When a THESIS event tree of a complete procedure is to be made, it is useful to develop a THESIS event tree for each specific action separately, since a specific action may appear several times in the procedure. Each THESIS event tree of a specific action can be regarded as a THESIS module; an example is the THESIS event tree of Figure 14. By combining the THESIS modules, a complete THESIS event tree of an entire procedure can be obtained.

The general approach followed in THESIS can be described as follows (Fig. 15). First, the procedure is specified which is to be followed in a control room in practice. The procedure is then broken down into specific actions and a THESIS module is made of each specific action. The THESIS modules are then combined to obtain the

THESIS event tree of the procedure. It may be possible in this way to reach the aim of a human-error-sequence analysis of normal procedures. A case study will follow in the next chapter.

Man-related features of THESIS

The method that involves the use of event trees was first applied in the WASH-1400 study by the USNRC (1975) for the probabilistic risk assessments of nuclear power plants in the United States. The method was applied to Dutch nuclear power plants in the same year (SEP, 1975). From that time onwards, event trees were used only to determine the safety of technical systems. More recently, other studies (Bell & Swain, 1983; Swain & Guttmann, 1983; USNRC, 1983) were started that applied event trees for human-reliability analysis.

The present study starts using event trees for human-performance safety analysis. This implies the application of a technique originally and successfully used in technical systems, i.e. the system event tree, to human beings. This will obviously result in a number of additional problems. Since these additional problems are peculiar to humans, these problems are called 'man-related features' of THESIS. A survey of these man-related features (MRFs) is given in the present section. The relation between event trees and decision trees, the two being very similar, will be discussed in chapter 10.

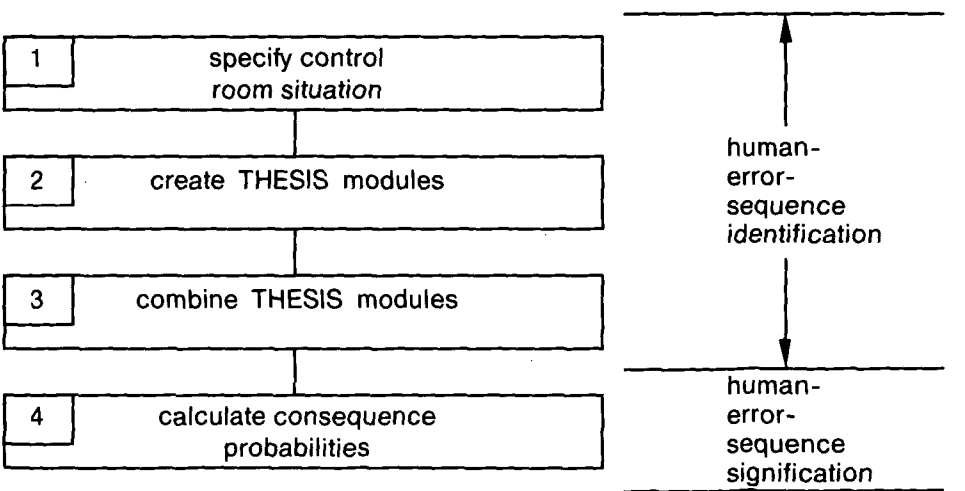


Fig. 15
General scheme of THESIS.

Procedure-selection capability – In practice there may be several procedures for reaching a certain goal. Although there may be a certain prescribed procedure, other procedures may be followed when people deviate from the prescribed ones to achieve the same goal. This procedure-selection capability can have several reasons. For instance, an operator may find it convenient to change the sequence of some steps in the procedure because the relative switches are located on the same panel. Also, the operators may perform parts of the procedure for each other for the sake of convenience, although this is in conflict with the prescribed procedure. Another reason may be that the operator relies on alarm signals before taking action, which may be in conflict with the procedure. It may also happen that certain steps are deliberately omitted because the operator knows from experience that the goal can then also be achieved. This may be true under normal circumstances but may cause severe problems under abnormal circumstances (Rasmussen, 1987a).

An example is the shut-down of a plant because of some abnormal situation. There is the risk of an alternative procedure being used which has been found several times to be more effective than the prescribed procedure used under normal conditions. In the abnormal situation, however, following the alternative procedure may lead to dangerous consequences. Although this problem is worth mentioning, it is beyond the scope of this study: such a procedure, when used under abnormal conditions, can be regarded as an emergency procedure and the study is only concerned with normal procedures.

The procedures set up by the operators may be less safe than the prescribed ones in certain cases, but they may be safer in other cases. This implies that each procedure that is actually followed by an operator in the control room and through which the desired goal is reached, has to be incorporated in the analysis. This means that a THESIS event tree has to be made for each procedure. This can raise an essential problem, certainly if many similar procedures are followed in a control room.

Ergonomics – A second problem lies in the ergonomics of the panel layout. According to the definition of the Netherlands Ergonomics Society (NVvE, 1988), the term 'ergonomics' means: designing products, tools, work surroundings and work methods in such a way that optimal efficiency, safety and comfort are achieved in the control and maintenance of man-machine systems. Ergonomics can have a great influence on the probabilities in the THESIS event tree as well as on its structure. For instance, the HEP for the reading error can be reduced by improvements in the readability of a meter. If the improvement is such that the HEP of an event becomes negligible, the structure of the THESIS event tree can be changed, since a branch can then be removed from the THESIS event tree. This change in structure also accounts for the introduction of extra components on the panel (e.g., as in the case of the example in Fig. 14, where the presence of a fourth similar switch on the panel would lead to an extra possibility of a selection error and, therefore, to extra branches in the THESIS event tree). This implies that, depending on the ergonomics of the panel layout, several THESIS modules of similar actions have to be made and different HEPS have to be applied.

Both the number of components and the number of positions per component have an effect on the structure of the THESIS event tree. In the former case, the effect is on the number of selection errors whereas in the latter case the number of handling errors is affected. The joint effect is multiplicative. If, in the case of Figure 14, the number of components is increased by a factor of two (six components in total) and the number of positions per switch is also increased by a factor of two (four positions per switch in total), there are six times four possible switch adjustments. This implies that there are twenty-four plus one success/failure outcomes (the last one as a result of an error of omission) and that the number of success/failure outcomes is thus increased from seven in Figure 14 to twenty-five! Hence, the THESIS event tree becomes very extensive in complex control rooms with a bad ergonomic panel layout with many similar components. This situation is further aggravated if, in combination with the above, many positions per component need to be distinguished. This blowing-up of the event tree can pose a serious problem for its application.

Continuous actions – Only discrete actions are considered in the event tree. A discrete action is an action in which a limited number of choices exist; the turning of a switch to a certain position is an example. A continuous action is an action in which an unlimited number of choices exists; an example is the adjustment of a set point where theoretically an infinite number of choices regarding the position of the dial can be made. The application of the THESIS event tree to a continuous action implies that the action has to be made discrete; the continuous scale needs to be divided into a limited number of discrete positions. Many discrete positions could possibly have to be distinguished.

The procedural steps are often less clear in the case of continuous actions than with discrete actions. With continuous actions, the procedural steps are less well-defined, e.g. 'increase the temperature of a process by several degrees within a certain period of time by adjusting a set point'. One operator may adjust it many times with a relatively small step size, whereas another will adjust it more roughly in fewer steps. Each adjustment can be regarded as a specific action, for which a THESIS module is to be made. Theoretically this implies that, when an operator adjusts the set point several times, a THESIS module should be made and repetitively combined.

The application of event trees to continuous actions hence implies two extra decisions. First, the analyst has to decide how to divide the action into a number of discrete steps, and second, he has to make a realistic decision of how the procedural step can be regarded as composed of specific actions. It is obvious that the THESIS event tree can become very extensive when many discrete positions are necessary and many specific actions have to be distinguished.

Event dependence – An essential aspect of human-performance safety is the phenomenon 'dependence'. Different types of dependencies can be distinguished. Event dependence is considered in this subsection; the other types will be discussed later. Event dependence implies that the HEP of an event depends on what has happened in a previous event belonging to the same action or to a previous action.

An example of event dependence between two events belonging to different actions could be the adjustment of two valves that are located close together. If adjustment of the first one is omitted, adjustment of the second one will probably also be omitted. The HEP of omitting to adjust the second one, however, is lower if the first one is not omitted, simply because they are together. In this example there is an event dependence between the error of omission in the first action and the error of omission in the second action.

An example of event dependence between two events belonging to the same action can be given from Figure 14. It was assumed for this figure that there is no dependence, which means that the HEP of an event is equal at all branches. Event dependence between a handling error and a selection error would imply that the HEP of the handling error was not equal at each branch. The reason can be that switch 1 has less clear indications than switch 2, thus increasing the probability of a handling error at switch 1.

The outcome probabilities in Figure 14, where no dependence was assumed and all HEPs of an event were equal at each branch, were simply calculated by multiplication. Multiplication is also possible when there is dependence. However, the HEPs have then to be adapted to incorporate dependence. This will be shown in the next chapter.

One event may sometimes depend on several other events. However, it is usually assumed that one event can only depend on one other event as also assumed in, for instance, THERP (Swain & Guttmann, 1983) and in a Markov process (Henley & Kumamoto, 1981). This assumption is justified by the uncertainty in the probabilities of the events, which makes a more thorough calculation of dependent probabilities superfluous. It is, of course, still possible that a third event is explicitly dependent on a second event and implicitly dependent on a first event. This implicit dependence is then caused by the explicit dependence between the first and the second event. In the present study it is also assumed that event dependence can only occur between two events.

Event dependence can be negative or positive. Positive event dependence means that the dependent HEP of making an error, given a previous error, has increased. Negative event dependence implies the opposite. Positive event dependence was present in the example presented above concerning the adjustment of two valves located close together.

Event dependence may have an important influence on the probability that a sequence of events will occur. Unfortunately, little is known about how to assess event dependence between specific actions. Only Swain & Guttmann (1983) give some information on the assessment of the level of dependence between human actions. Dependence can also be present in technical systems, in which case the term 'common mode failures' is often used (Billinton & Allan, 1983). The assessment of the level of dependence for human actions is, however, more difficult.

Recovery attempts – Humans are, contrary to technical systems, capable of recovering errors they have made earlier. This can be explained by means of Figure 16 where

an outline is given of the event tree of Figure 14. Following the YES-direction in the event recovery attempt implies ending at a return outcome, from which the person will return to some point in the THESIS event tree. This is expressed by a few 'return loops', starting at a return outcome.

It is possible that when this action is repeated a person truly recovers the error, i.e. starts following the success path (e.g. in Fig. 16, by following return loop 1). It is, however, also possible that the same or other errors are introduced (e.g. in Fig. 16 by following the return loops 2 and 3). In the latter case someone may again end up at a return outcome and perform a recovery attempt for the second time. The fact that THESIS considers a possible incorrect recovery is where it differs from most human-reliability techniques such as THERP which assume that, if recovery takes place, the success path is followed.

The same explanation applies to a sequence of specific actions, i.e. a procedure. Ending at a return outcome then means a return to some point in the THESIS event tree of the procedure. An essential assumption in the present study is that the same procedure is followed, entirely or in part, during the recovery attempt. This repetition may be performed by the same person or by someone else. The situation in which an entirely different procedure is followed during the recovery attempt, e.g. in order to recover from an unstable process situation, is outside the scope of this study.

Recovery attempts will obviously influence the probability that certain outcomes will occur. The probability of the recovery attempt and the point to which someone returns in the THESIS event tree of the procedure may be important variables. Unfortunately, data about these variables are scant.

Recovery dependence – Directly related to the preceding MRF is the fact that, during the recovery attempt, memory influences are at work. This means that when the ac-

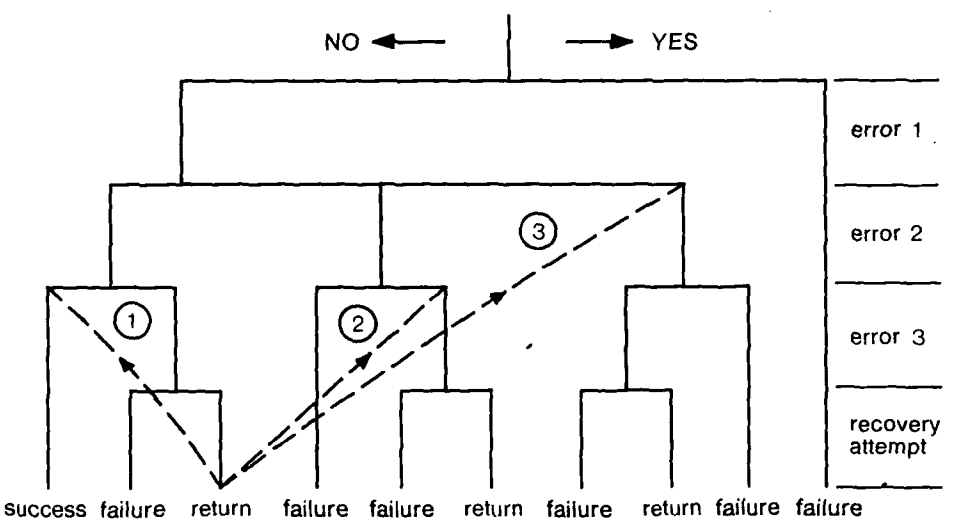


Fig. 16
A formal THESIS event tree with some return loops (dotted).

tion(s) is (are) performed again other HEPs are present for the same errors. The HEPs after the recovery attempt are dependent on what happened in certain events before the recovery attempt. This situation can be regarded as a form of dependence and is called 'recovery dependence'.

An example of recovery dependence is the check of a summation of a few numbers. If someone adds a few numbers and makes an error, it is possible that, not knowing where the error was made, he will again make an error at the same place during the check. This check can be regarded as a recovery attempt and the fact that the same error will probably be made during the recovery attempt can be considered as recovery dependence.

As with event dependence, recovery dependence can be either positive or negative. Positive recovery dependence implies that the conditional probability of making the same error is increased during the recovery attempt. Negative dependence implies the opposite. Positive recovery dependence was assumed in the example given above for the summation of a few numbers. Negative recovery dependence may occur in a control-room situation, in which an alarm shows where a human error was made. This alarm makes it less probable that the same error will be made during the recovery attempt.

In case of recovery dependence, an event will also be taken to depend on one other event only, just as in event dependence. Consequently, a path containing several events can be dependent upon several other events. Hence, the path followed after the recovery attempt can be dependent upon the path followed before the recovery attempt. The result is that the way in which someone performs the action again after ending up at a return outcome will depend on which return outcome was reached.

It is not yet clear whether recovery dependence has much influence on the probability that certain consequences will occur. This aspect therefore needs more study. However, compared to event dependence, even less knowledge exists about recovery dependence.

Performance variability – Another MRF is the variability in human performance. This variability will cause the HEP to differ between persons. This means that there exist distributions instead of point values as in Figure 14. Performance variability is probably the main cause for the uncertainty in HEPs.

Relatively little is known on the shape of these distributions in comparison with technical systems. The so-called log-normal distribution is frequently applied to human-error probabilities. A log-normal distribution is a distribution derived through a logarithmic transformation of the normal distribution. The log-normal distribution has been used by Swain & Guttmann (1983), Heising & Patterson (1984), Apostolakis (1985) and others. The distribution of HEPs, however, has seldom been measured. According to Cooke & Waij (1986), the shape of the HEP distributions can be of importance for the uncertainty in the probability that undesired consequences will occur as a result of several human errors. More knowledge of the shape of the distributions could therefore be of importance when THESIS is to be applied.

Correlation between human-error probabilities – The last MRF to be discussed here is the correlation between HEPs. A correlation shows how the HEP of a person for one task coheres with the HEP of the same person for another task. A high correlation implies that someone who has a high HEP for one task will also have a high HEP for the other task. The correlation is directly related to the previous MRF. A positive correlation between errors can result in a higher mean and variance of the combined errors than the absence of correlation (Apostolakis & Kaplan, 1981).

A correlation can be regarded as another form of dependence. There is, however, an important difference between correlation and event or recovery dependence. In event and recovery dependence, an HEP of an event is dependent upon what happened in a previous event. In a correlation, an HEP of an event is dependent upon a value of the HEP of a previous event. Correlation sometimes occurs in the literature (Cooke & Way, 1986) as 'knowledge dependence' (knowledge about an error probability determines the value of another error probability), whereas the event and recovery dependence is sometimes called 'causal dependence'.

Concluding remarks

A method for human-performance safety analysis, called THESIS, was presented in this chapter. It makes use of event trees and the events in the tree represent human errors and recovery attempts. The method implies the distinction of specific actions in the procedure and suggests that THESIS modules be made of these actions. A THESIS module consists of several errors and ends with a recovery attempt. The THESIS event tree of the procedure can be obtained by combining these modules.

The application of event trees to determine human-performance safety involves more problems than the application of event trees to determine system safety. Eight problems, called 'MRFs', could be distinguished. It is concluded that the MRFs may have an important influence on the assessment of human-performance safety.

Unfortunately, little is known about the quantitative values of most MRFs. Combinations of these MRFs may have important effects, especially because the contributions of separate variables may not be simply additive. This was suggested earlier for certain MRFs (Heslinga, 1983). The influence determines the extent to which THESIS can be applied in human-performance safety analysis. The influences of the MRFs will be examined in the following chapters.

Chapter 5

Application of THESIS
(a case study)

Introduction

THESIS was introduced in the preceding chapter by considering its application to a specific action. As pointed out, THESIS has been designed to be used in making safety analyses of normal procedures. The aim of the present chapter is to show how THESIS will be applied to these procedures and to describe the result of making a human-performance safety analysis rather than a human-reliability analysis.

A case study concerning the control of a boiler, with a procedure consisting of two steps, is presented for the purpose. The effect of only two MRFs of THESIS, viz. 'event dependence' and the 'procedure-selection capability' are taken into consideration, in order to keep the case simple. The effect of other MRFs, such as recovery attempts, are disregarded because they would make the presentation of THESIS too complex to be immediately understandable.

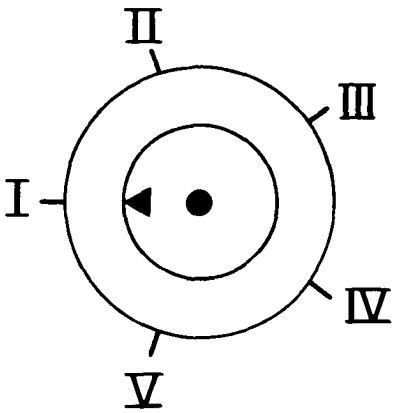
The general scheme of Figure 15 will be followed in this chapter. The human-error-sequence identification of two specific actions for the control of a boiler will be discussed first, followed by human-error-sequence signification, in which the various event sequences are quantified. A discussion of how THESIS can be used as a decision-support tool for the improvement of man-machine system designs concludes the chapter.

Human-error-sequence identification

The first three blocks of Figure 15 will be elaborated on in this section.

Control-room situation — To simplify the case, a panel will be considered which has only one switch with which the set point of the process is adjusted. It is assumed that the set point can be adjusted only to five well-defined positions (Fig. 17). The operator is instructed to change the set point from its starting position (position I) to position IV. If the set point is adjusted, it must be moved as quickly as possible to position IV. However, it must be taken into account that no more than two steps are allowed in ten minutes' time, because otherwise a thermal shock would occur almost immediately. Hence, two procedures are possible, both of which are presented in Figure 18.

Fig. 17
The switch with which the set point is to be adjusted.



PROCEDURE 1

1. adjust set point from position I to position II and wait ten minutes
2. adjust set point from position II to position IV

PROCEDURE 2

1. adjust set point from position I to position III and wait ten minutes
2. adjust set point from position III to position IV

Fig. 18
Two possible procedures for adjusting the set point.

It is assumed that four different consequences are possible when one of the procedures is completed. It is noted that, in practice, so-called 'Hazard and Operability Studies' (DGA, 1982; CISHC, 1977) can be used to retrieve all possible consequences. The consequences are:

(1) success, S, if one of the procedures is completed correctly;
(2) temperature lower than desired, T, if the procedure is completed with the set point in one of the wrong positions I, II or III;

(3) unacceptable strong temperature increase leading to a thermal shock, U, which will occur if the set point is adjusted to position IV within ten minutes;
(4) very high pressure leading to a possible explosion, V, because of the creation of an excessively high temperature; it will be caused by erroneous adjustment of the set point to position V.

THESIS modules – Only one procedure, i.e. procedure 1, will be considered in detail to show how a THESIS event tree of a procedure is made. The THESIS module of each procedural step considers two human errors. The THESIS module of the first step of the procedure 1 is presented in Figure 19. The selection error is not shown because only one set point is considered. The handling error implies the adjustment of the set point to a wrong position that does not correspond with the procedural step. The position of the set point is given above the branch; the HEP, i.e. the probability of following the YES-direction, is given below the branch. The event sequences and outcomes are encoded and the codes are presented at the offshoots of the tree.

The codes are used as follows: The capital in the code denotes the component (since only one set point is used, only the capital A is applied) and the subscript denotes the position of the component. To indicate the difference between the event sequences and outcomes, the former have apostrophes in their symbols. The codes that are used in this chapter stand for:

(1) event sequences
- A'_d – set point A in the desired position
- A'_t – set point A in a tolerable position
- A'_h – set point A in the high position
- A'_e – set point A in the extreme position
- A'_p – set point A in the preceding position
- A'_u – set point A in position under desired.

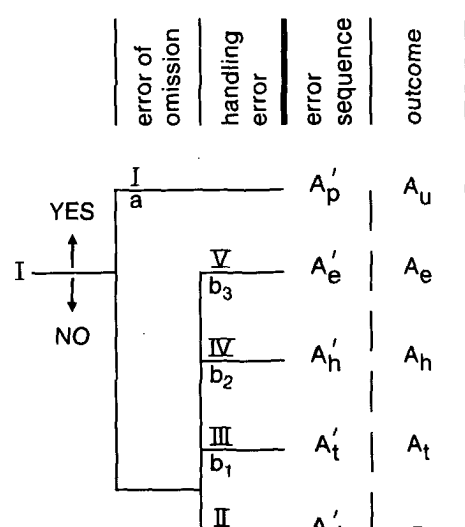


Fig. 19
The THESIS module of the first step of procedure 1, i.e. THESIS module 1. The position of the set point is given above the branch; the HEP is given below the branch. The event sequences and outcomes are given at the offshoots.

(2) outcomes

- – set point A in the desired position
- A_t – set point A in a tolerable position
- A_h – set point A in the high position
- A_e – set point A in the extreme position
- A_u – set point A in position under desired.

Two remarks need to be made in this context. The first concerns the distinction between A_t and –, i.e. turning the set point to position III and to position II, respectively. Although these moves are physically identical, a distinction is made because turning the set point to position III is not allowed according to the procedure that is considered here (procedure 1).

A second remark concerns the difference between event sequence and outcome. An event sequence shows the direct result of some errors of a THESIS module, whereas an outcome shows what the resulting set point position is, taking into account earlier set point positions: the event sequence A'_p, for example, results from an error of omission implying that the set point remains in position I, outcome A_u. As will be shown later, an outcome is an entity that contains the most essential information, regarding previous set point positions, which is needed to predict their influences on the undesired process state, i.e. on the undesired consequences. For this reason, and because interest is particularly focused on incorrect human performance, the outcome contains a dash if the set point is in the desired position.

It is assumed that the activities performed at the set point in the first ten minutes belong to the first procedural step; they are represented by THESIS module 1. The activities performed later belong to the second procedural step. The THESIS module of this step, i.e. THESIS module 2, has the same form as THESIS module 1 in Figure 19.

Combination of THESIS modules – The THESIS event tree of the complete procedure is obtained by combining the two THESIS modules. The THESIS event tree of procedure 1 is presented in Figure 20. Several branches in THESIS module 2 are combined if they imply similar event sequences. The codes of the event sequences, the outcomes and the consequences are given at the offshoots. The consequences show the effect of the outcomes on the process. As when system event trees (USNRC, 1975, 1983) are used, the consequences are drawn at the offshoots of the complete THESIS event tree of the procedure.

Both a success and a failure outcome can generally be divided into two sorts of outcomes: a temporary outcome and a final one. A temporary outcome can be defined as an outcome after which the analysis is continued; a final outcome is an outcome after which the analysis is stopped. The reason for stopping can be the fact that the last step of the procedure has been analyzed, but it is also possible that an outcome somewhere in the analysis becomes a final outcome, if it results directly in a severe consequence. Since the analysis is stopped after the second procedural step, all outcomes there are final. After the first procedural step, only the adjustment of the set point to position V is a final outcome; all other outcomes are temporary outcomes.

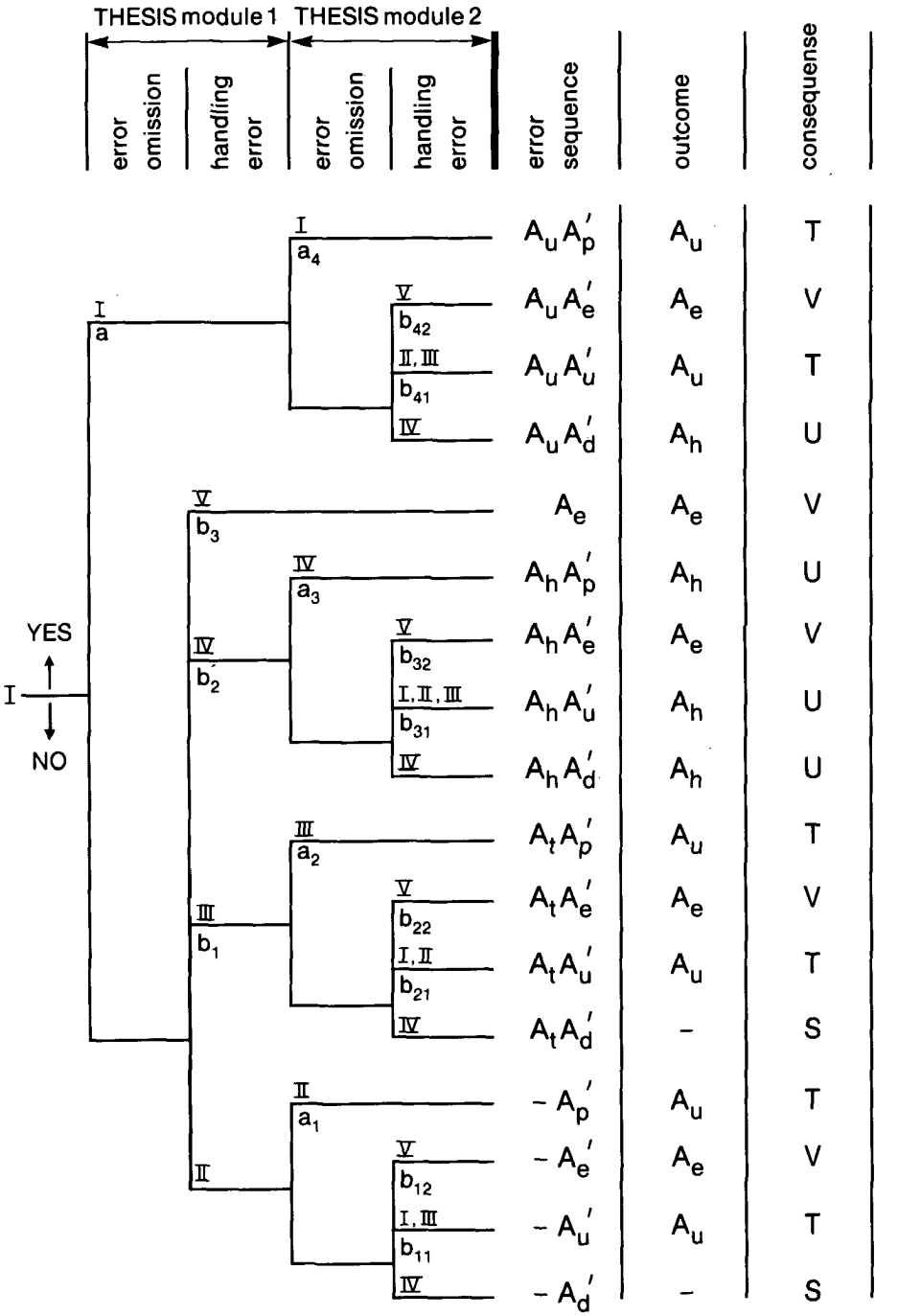


Fig. 20
THESIS event tree of procedure 1. The position of the set point is given above the branch; the HEP is given below the branch. The event sequences, outcomes and consequences are presented at the offshoots.

This is expressed in the THESIS event tree by the coupling of the second procedural step after each branch of the first module, except for the branch resulting in position V, coded A_e.

The THESIS event tree of procedure 2 can be drawn in the same way. This tree is not presented here since it is nearly the same as the one in Figure 20.

All possible event sequences can obviously be identified with the THESIS event tree. Since the THESIS event tree will, however, become rather large simply through combination of THESIS modules, it is reasonable to apply so-called 'combination matrices' instead of event trees. The combination matrix of the THESIS event tree of procedure 1 is given in Table 4. In the column left of the matrix, the temporary outcomes of the first procedural step are presented. In the row above the matrix, the event sequences of the second procedural step (the outcomes are not yet clear) are presented. The cells contain the event sequences and outcomes of the procedure. The combination matrix of the THESIS event tree of procedure 2 is similar to that presented in Table 4.

Human-error-sequence signification

This section treats the last block of Figure 15 in detail.

Consequence probabilities – The following assumptions are made in order to quantify the consequence probabilities Prob(S), Prob(T), Prob(U) and Prob(V).

(1) the HEP of each error of omission is p_1;
(2) the HEP of the handling error of the first procedural step is p_2;
(3) the HEP of the handling error of the second procedural step is also p_2, except for the following cases; these exceptions are made to include event dependence:
   (3.1) the HEP is p_3 if the set point is adjusted with a step size corresponding with the procedure, but with an incorrect result because the set point was adjusted incorrectly in the first procedural step;

step 2 / step 1	A'_d	A'_u	A'_e	A'_p
–	– $-A'_d$	A_u $-A'_u$	A_e $-A'_e$	A_u $-A'_p$
A_t	– $A_tA'_d$	A_u $A_tA'_u$	A_e $A_tA'_e$	A_u $A_tA'_p$
A_h	A_h $A_hA'_d$	A_h $A_hA'_u$	A_e $A_hA'_e$	A_h $A_hA'_p$
A_u	A_h $A_uA'_d$	A_u $A_uA'_u$	A_e $A_uA'_e$	A_u $A_uA'_p$

Table 4
Combination matrix of procedure 1. The left column of the table contains the temporary outcomes of the first procedural step. The top row contains the event sequences of the second step. Each cell contains an outcome (top) and an event sequence (bottom).

Table 5
The branch probabilities of Figure 20 expressed in p_1 through p_4.

$a = p_1$	$a_1 = p_1$	$a_2 = p_1$	$a_3 = p_1$	$a_4 = p_1$
$b_1 = p_2$	$b_{11} = p_2 + p_4$	$b_{21} = 2p_2$	$b_{31} = 3p_2$	$b_{41} = 2p_2$
$b_2 = p_2$				
$b_3 = p_2/2$	$b_{12} = p_2/2$	$b_{22} = \max(p_3 \cdot p_4)/2$	$b_{32} = p_2/2$	$b_{42} = p_2/2$

(3.2) the HEP is p_4 if the step size of the adjustment is the same as in the first procedural step because of memory influences;
(3.3) the HEP is taken to be the larger of p_3 and p_4 if assumptions (3.1) and (3.2) are both applicable; this is indicated as $\max(p_3,p_4)$;
(3.4) the above HEPs are reduced by a factor of two if the set point is adjusted to the dangerous position V, to account for the fact that operators might be aware of the consequence of doing this.

Table 5 shows how the branch probabilities of Figure 20 are expressed in p_1 through p_4. As several branches in Figure 20 were combined, the branch probabilities can be a combination of HEPs (see, for instance, b_{11}). If certain values are assumed for p_1 through p_4, the consequence probabilities Prob(S), Prob(T), Prob(U) and Prob(V) can be calculated.

Although the quantification of the consequence probabilities in this case study is simple, it is obvious that this quantification can become an extensive operation with large THESIS event trees. A computer program called 'PREQUANT' was written in order to facilitate this work. This program serves to calculate the probabilities of the outcomes as given in the cells of the combination matrix, on the basis of the outcome probabilities of the first THESIS module and the event sequence probabilities of the second THESIS module. The outcome probabilities of the first module are regarded as a column vector (n by one) and the event sequence probabilities of the second module are regarded as a row vector (one by m). An n-by-m matrix is calculated from these vectors, in which each element contains the probability of the combination matrix cell. The probabilities of the cells having the same outcomes are summed next. If there is a subsequent procedural step, a new column vector will be created from the outcome probabilities of temporary outcomes, and the program will start again. The outcome probabilities of the final outcomes will be stored. Otherwise the program will stop with the presentation of the final outcome probabilities.

In the case of event dependence, the values of the elements of the row vectors may differ depending on the element of the column vector by which they are multiplied. Each column vector element expresses a certain outcome of the first module; the row

vector expressing the event sequence probabilities of the second module may depend on that outcome. If, because of event dependence, certain elements of the row vector differ from the elements of the row vector with no event dependence, it will be fed into the computer as additional input.

The output of PREQUANT shows, among others, the event sequence probabilities. An example is presented in Table 6. This example concerns a part of the output regarding event sequence probabilities of the combination matrix of Table 4, for certain values of p_1 through p_4. The probabilities of event sequences leading to a particular consequence can be analyzed in this way. Consequently, significant event sequences contributing highly to the probability of a particular consequence can be recognized. The benefit of this technique will be discussed below.

The output of PREQUANT also contains the consequence probabilities. Since two procedures (Fig. 18) are analyzed – only procedure 1 has been considered in detail for explanation purposes – the consequence probabilities have been calculated for both procedures 1 and 2. The results are presented in Table 7. This quantification has been done for several values of p_1 through p_4 to show their sensitivity to both procedures. The HEPs p_3 and p_4 are varied since they are important for the difference in consequence probabilities between the procedures.

Cost functions – Both procedures can be compared at this stage. As pointed out in the introduction, human-error-sequence signification includes both the determination of event sequence probabilities and the extent of the consequences following these event sequences. This signification can be expressed by a cost function in which the event sequence probabilities or consequence probabilities and the extent of the consequences are combined. A selection of the safest procedure can be made by comparing the cost functions.

A linear equation is applied for the cost function of procedures 1 and 2, in analogy with well known methods used in decision theory (Tribus, 1969; Raiffa, 1970; Ang & Tang, 1984; Bunn, 1984). The cost function, K, is obtained here from the following expression: $K = I_1 Prob(T) + I_2 Prob(U) + I_3 Prob(V)$. The quantities I_1, I_2 and I_3

step 2 / step 1	A'_d	A'_u	A'_e	A'_p
–	$9.66 \cdot 10^{-1}$	$1.08 \cdot 10^{-2}$	$4.89 \cdot 10^{-4}$	$9.88 \cdot 10^{-3}$
A_t	$9.29 \cdot 10^{-4}$	$1.96 \cdot 10^{-6}$	$4.90 \cdot 10^{-5}$	$9.90 \cdot 10^{-6}$
A_h	$9.77 \cdot 10^{-4}$	$2.94 \cdot 10^{-6}$	$4.90 \cdot 10^{-7}$	$9.90 \cdot 10^{-6}$
A_u	$9.88 \cdot 10^{-3}$	$1.98 \cdot 10^{-5}$	$4.95 \cdot 10^{-6}$	$1.00 \cdot 10^{-4}$

Table 6
The event sequence probabilities of Table 4 for $p_1 = 0.01$, $p_2 = 0.001$, $p_3 = 0.1$ and $p_4 = 0.01$.

Table 7
The consequence probabilities of procedures 1 and 2 for several probability values p_i through p_4.

p_1	p_2	p_3	p_4	prob(S)	prob(T)	prob(U)	prob(V)	
0.01	0.001	0.1	0.01	0.9673	0.0208	0.0109	0.0010	procedure 1
				0.9717	0.0121	0.0108	0.0054	procedure 2
0.01	0.001	0.05	0.05	0.9282	0.0599	0.0109	0.0010	procedure 1
				0.9522	0.0120	0.0108	0.0250	procedure 2
0.01	0.001	0.01	0.1	0.8794	0.1087	0.0109	0.0010	procedure 1
				0.9276	0.0121	0.0109	0.0494	procedure 2
experimental variables				consequence probabilities				

in this equation are called here the 'weighting factors', expressing the extent of the consequences T, U and V, respectively. A very high pressure leading to a possible explosion, V, may be less desirable in practice than a thermal shock, U, whereas U will be less desirable than state T, a temperature lower than desired. It is therefore assumed that $I_1 \leq I_2 \leq I_3$.

The cost function is presented in Table 8 for the case in which $p_1 = 0.01$, $p_2 = 0.001$, $p_3 = 0.1$ and $p_4 = 0.01$ (the first case in Table 7). Table 8 shows three situations with different weighting factors. It is shown that, for situations 1 and 2, procedure 1 has a lower cost function than procedure 2; the opposite applies for situation 3. Similar results for cost functions are obtained for the other p_i values, as applied in Table 7.

The procedure with the lowest cost function should be preferred for reasons of safety. Table 8 shows that the cost function is lower for procedure 1 in situations 1 and 2 and that the opposite applies for situation 3. It is assumed, in the rest of this chapter,

Table 8
The cost function K of procedure 1 and procedure 2 for several weighting factors I_1, I_2 and I_3, in which $p_1 = 0.01$, $p_2 = 0.001$, $p_3 = 0.1$ and $p_4 = 0.01$.

	I_1	I_2	I_3	K procedure 1	K procedure 2
situation 1	0.05	0.50	2.50	0.0090	0.0195
situation 2	0.5	1.00	1.50	0.0228	0.0250
situation 3	1.00	1.00	1.00	0.0327	0.0283

that the process under consideration is represented by the weighting factors of situation 1. If the weighting factors for situation 1 in Table 8 are considered to be realistic values, the decision must be to recommend procedure 1 instead of procedure 2.

Discussion

Decision support with THESIS – The influence of two MRFs was analyzed in this chapter, viz. event dependence and procedure-selection capability. Therefore, a case study was made in which THESIS was used. Human-error identification resulted in a qualitative analysis of all possible event sequences, whereas human-error signification resulted in a decision about procedure 1 being the safest. It is important to point out that event dependence played an essential role. Had event dependence not been involved, there would have been no difference between the two procedures. This can be understood if it is kept in mind that event dependence is represented here by p_3 and p_4. In the case of no event dependence, implying that $p_3 = p_4 = p_2$, there is no difference between the consequence probabilities in Table 7.

The case study showed that THESIS can be used to support a decision concerning the safest procedure. Two procedures were compared for the purpose. It appeared that the weighting factors can have an important influence on optimization of the cost function and, hence, on decision support in procedure design. It was also found that situation 3 of Table 8, in which $I_1 = I_2 = I_3 = 1$, implied that the consequences were weighted equally. This would lead to an opposite decision concerning the best procedure. Equal weighting happens in human-reliability techniques where the undesired consequences are regarded as identical, since each failure consequence is 'not following the procedure'. This study shows that not following the procedure can lead to failure consequences, some of which might be most undesirable. In that case, equal weighting is not permitted since it may result in opposite decisions on procedure design. It implies that human reliability is not directly applicable to those situations in which some failure consequences are far more undesired than others. In such cases human-performance safety assessment techniques should be applied in which all consequences of human errors are considered. Similar results were obtained by Heslinga (1986) in a study which included recovery attempts.

The statements with regard to the procedures can be generalized to other man-machine system designs. It was already stated in the subsection on PREQUANT that, once the significant event sequences are known, preventive actions can be taken. This can be understood from Tables 5 and 6. It becomes clear, partly on the basis of these tables, that the following event sequences are significant for the undesired consequences T, U and V:

(1) for consequence T, the event sequences $-A_u'$ and $-A_p'$,
(2) for consequence U, the event sequence $A_u A_d'$, and
(3) for consequence V, the event sequences $-A_c'$ and A_c' (the last sequence is not derived from the combination matrix of Table 4 since it is an event sequence of the first action).

Preventive actions to reduce the probabilities of these sequences and, hence, to reduce

the relevant consequence probabilities could be undertaken on the basis of this knowledge. Since the sequence $-A'_p$ is significant, a support measure to reduce the error of omission, such as a check-off provision in the procedure, would be worthwhile. Building an interlock in the set point, so that no more than two set point steps are allowed, reduces both the significant event sequence $A_u A'_d$ for U and the significant event sequence $-A'_e$ for V. This is of greater value than making such an interlock only to inhibit adjustment of the set point to position V, which only reduces the significant event sequence $-A'_e$.

In general, several preventive actions can be performed to increase the safety of a man-machine system. Check-off provisions in procedures and interlocks are two examples. Other preventive actions can be the introduction of alarms (or their reduction, if the analysis shows that too many alarms may confuse the operator(s) significantly), or cutting off the power when the operator commits a certain error that would otherwise lead to severe consequences. An example of this is the Dutch automatic train control ATB (Automatische Trein Beïnvloeding) that stops the train if the train driver does not respond properly to certain signal lights (Berger, 1981). The selection of the safest procedure (if several are possible) should also be included. The case study presented in this chapter is an example of how THESIS can support decisions touching a safer man-machine system design.

Conclusions – The discussion leads to the crucial point of human-performance safety analysis. Preventive actions can be undertaken (such as the safest sequence of procedural steps), but this must be followed by the calculation of the cost functions in which both event sequence or consequence probabilities and the extent of the consequences are combined. Reducing the event sequence probability of a certain consequence might increase the event sequence probability of a more serious consequence. Therefore, reducing significant event sequences should be an iterative process. The conclusion is that a justifiable decision about the best man-machine system design can only be made if the following items are taken into account:

(1) all paths of the THESIS event tree as well as the possible consequences;
(2) the probability that these consequences will occur;
(3) the extent of their occurrence.

Looking ahead – THESIS has the potential to support the enhancement of a man-machine system design. However, it has so far been applied only to a simple procedural design. Various assumptions about certain MRFs were made to simplify the case study. Recovery attempts and recovery dependence, for instance, were disregarded but might have an important influence. These MRFs will therefore be investigated more thoroughly in the following chapter.

Chapter 6

Analytical model to quantify human-performance safety

Introduction

It was shown in the preceding chapter that certain MRFs of THESIS have an explicit effect on the quantification of the consequence probabilities. The MRFs considered were procedure-selection capability and event dependence. Other MRFs were not incorporated to keep the example convenient. There are however other MRFs that might also influence quantification i.e. the recovery attempt and combined with it, the recovery dependence.

The recovery attempt is, if present, the last event of a THESIS module. Following the direction YES at this event implies the return to some point in the THESIS event tree, from which the tree is again passed through. Together with the recovery attempt, the MRF recovery dependence may be present and it involves the presence during the recovery attempt of HEPs different from those before the recovery attempt. Several return loops may be possible in a THESIS event tree that consists of several THESIS modules. These MRFs may obviously present significant difficulties if the probabilities that certain consequences will occur due to human errors are to be quantified.

Quantitative data for the assessment of recovery attempts and recovery dependence are lacking in most cases. There is some knowledge of HEPs valid during the performance of procedural actions. Topmiller et al. (1982), Swain & Guttmann (1983), Comer et al. (1984), and Spettel et al. (1986) show data for practical use and Beare et al. (1984) give data obtained from simulators. Very little is known, however, about the number of recovery attempts and the level of recovery dependence. It would therefore be useful to determine in how far these MRFs affect the quantification.

For that purpose, an analytical model that incorporates the four MRFs mentioned (procedure-selection capability, event dependence, recovery attempts and recovery dependence) could be useful. The application of sensitivity analyses could help to determine which MRFs are really important for the quantification and which are relatively unimportant. The latter type of MRFs might then be disregarded from the HPSA.

The aim of the present chapter is to set up an analytical model, based on the THESIS event tree, which has the above four MRFs as input. Other MRFs that might influence the quantification such as the form of the distributions of HEPs and the correlation between HEPs are not incorporated, as the model would then be too complex to yield adequate insight. The output of the model consists of the probabilities that certain

final outcomes (success or failure) will occur due to human errors. As shown in the previous chapter, these outcome probabilities form the direct basis for the probabilities of certain consequences. The model developed here will be applied for a sensitivity analysis in the next chapter.

A general model founded on the outcome probabilities of the THESIS event tree will be developed first in order to derive the analytical model. This general model will then be refined to derive the proposed analytical model. The refinements involve the determination of the event probabilities that make up the outcome probabilities. Finally, the applicability of the model, its validity and relation to the Markov theory will be considered.

General model

Some assumptions and notations will be dealt with, followed by derivation of the general model.

Assumptions and notations – Four assumptions are made in order to calculate the probability that a certain outcome is achieved taking the recovery attempts into account.

(1) There is a set containing u similar procedures in which only the sequences of specific actions are different; the procedures are indicated by i ($i = 1,2,...,u$). The final outcome that can occur is determined only by the type of human errors that are made, and not by the sequence of the errors. Each procedure i is represented by a THESIS event tree i. The trees 1 through u form a set in which one of the trees is passed through, based on the procedure selected by the operator.

(2) It is assumed that, after a return outcome is reached, there will again be a choice between the procedures of the set. This need not be the same procedure as that passed through before the recovery attempt.

(3) It is assumed that each THESIS event tree i contains v paths leading to a final outcome, indicated by q ($q = 1,2,...,v$), plus w_i paths leading to a return outcome, indicated by j ($j = 1,2,...,w_i$). Due to assumption (1), each THESIS event tree i has the same number of final outcomes.

(4) It is assumed that recovery dependence only exists between two consecutive THESIS event trees, i.e. the THESIS event tree passed through immediately before a recovery attempt and the THESIS event tree passed through immediately after this recovery attempt. This recovery dependence is determined by the path that has been passed through to reach a return outcome, and by the THESIS event tree in which this path was completed.

To facilitate notation, a distinction is made between the THESIS event tree passed through for the first time and the THESIS event tree passed through after a recovery attempt. The first one is called 'original tree' and the second one 'recovery tree'. It can be shown that, on the basis of the assumptions just formulated, there is one set of original trees and $\sum_{i=1}^{u} w_i$ sets of recovery trees. The sets differ only quantitatively and do not differ in form.

The following notations are used (Fig. 21 is used for explanation):

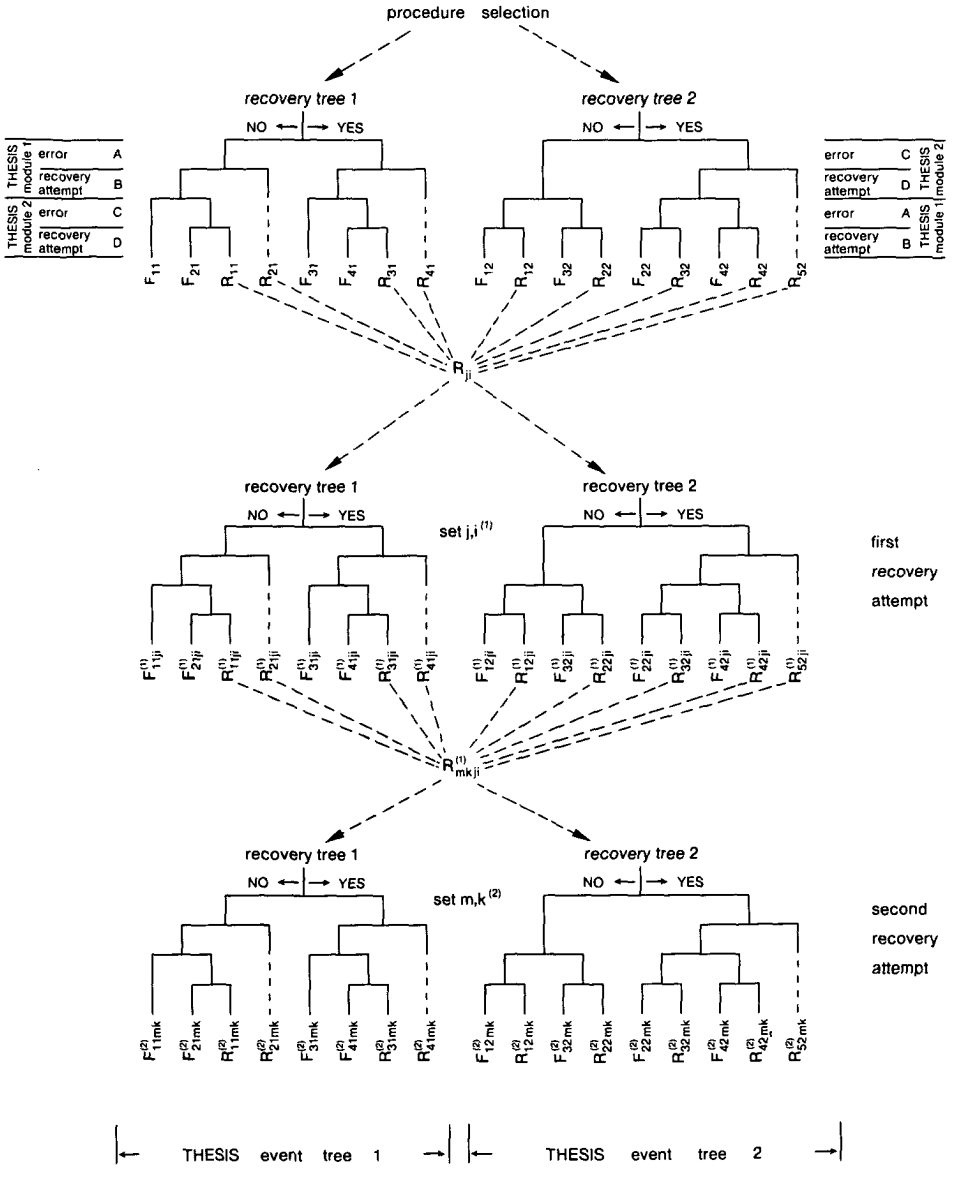


Fig. 21
Two THESIS event trees at various stages of performance (no recovery, first recovery attempt, second recovery attempt). THESIS event tree 1 represents a procedure of two specific actions with event sequence A-B-C-D. THESIS event tree 2 resembles a procedure of the same two specific actions with event sequence C-D-A-B. In the case where THESIS event tree 1 or 2 is passed through for the first time, the tree is termed 'original tree' 1 or 2. The tree is called 'recovery tree' 1 or 2 during the first or second recovery attempt.

(1) The path leading to final outcome q in original tree i is indicated by F_{qi} and its path probability by f_{qi}; the path leading to return outcome j in this tree is indicated by R_{ji} and its path probability by r_{ji} (in Fig. 21: u = 2, v = 4, w_1 = 4, w_2 = 5). These path probabilities are obtained by mutually multiplying the branch probabilities belonging to path j and multiplying this product by the selection probability, i.e. the probability that the THESIS event tree i is selected; the branch probability and the selection probability are considered to be independent.

(2) A set of recovery trees is indicated by set $j,i^{(x)}$, where i denotes the preceding THESIS event tree that was passed through, j the path in that THESIS event tree and x the x^{th} recovery attempt; x varies between 1 and t in which t (t = 0, 1, 2,...) indicates the total number of recovery attempts that were made (in Fig. 21: t = 2).

(3) The path leading to final outcome q in recovery tree k (k = 1,2,...,u) of set $j,i^{(x)}$ is indicated by $F^{(x)}_{qkji}$ and its path probability by $f^{(x)}_{qkji}$; the path leading to return outcome m (m = 1,2,...,w_k) in this tree is indicated by $R^{(x)}_{mkji}$ and its path probability by $r^{(x)}_{mkji}$. These path probabilities are obtained by mutually multiplying the branch probabilities belonging to that path and multiplying this product by the selection probability of recovery tree k being chosen; the branch probability and the selection probability are considered to be independent.

Derivation of the general model – The probability of a final outcome taking into account that t recovery attempts were made, i.e. that a return outcome was reached t times, indicated by $\tau^{(t)}_q$, will be calculated in this subsection. The probability will first be calculated for a simple case (Fig. 22). For q = 1 and t = 2, the probability becomes:

$\tau^{(2)}_1$ = the probability of reaching outcome q via an original tree,
plus the probability of making a return for the first time and then of reaching the outcome q via a recovery tree belonging to the first recovery attempt,
plus the probability of making a return for the second time and then reaching the outcome q via a recovery tree belonging to the second recovery attempt.

This becomes the following formula, in matrix notation:

$$\tau^{(2)}_1 = f_{11} + f_{12} + [f^{(1)}_{1111} + f^{(1)}_{1211},\ f^{(1)}_{1112} + f^{(1)}_{1212},\ f^{(1)}_{1122} + f^{(1)}_{1222}] \begin{bmatrix} r_{11} \\ r_{12} \\ r_{22} \end{bmatrix} +$$

$$+ [f^{(2)}_{1111} + f^{(2)}_{1211},\ f^{(2)}_{1112} + f^{(2)}_{1212},\ f^{(2)}_{1122} + f^{(2)}_{1222}] \begin{bmatrix} r^{(1)}_{1111} & r^{(1)}_{1112} & r^{(1)}_{1122} \\ r^{(1)}_{1211} & r^{(1)}_{1212} & r^{(1)}_{1222} \\ r^{(1)}_{2211} & r^{(1)}_{2212} & r^{(1)}_{2222} \end{bmatrix} \begin{bmatrix} r_{11} \\ r_{12} \\ r_{22} \end{bmatrix}$$

Hence, the probability $\tau^{(t)}_q$ in general becomes:

$$\tau^{(t)}_q = \tau^{(o)}_q + \phi^{(1)}_q \Omega + \phi^{(2)}_q \Psi^{(1)}\Omega + \ldots + \phi^{(t)}_q \Psi^{(t-1)} .. \Psi^{(1)}\Omega \qquad \text{(Eq. 1)}$$

where

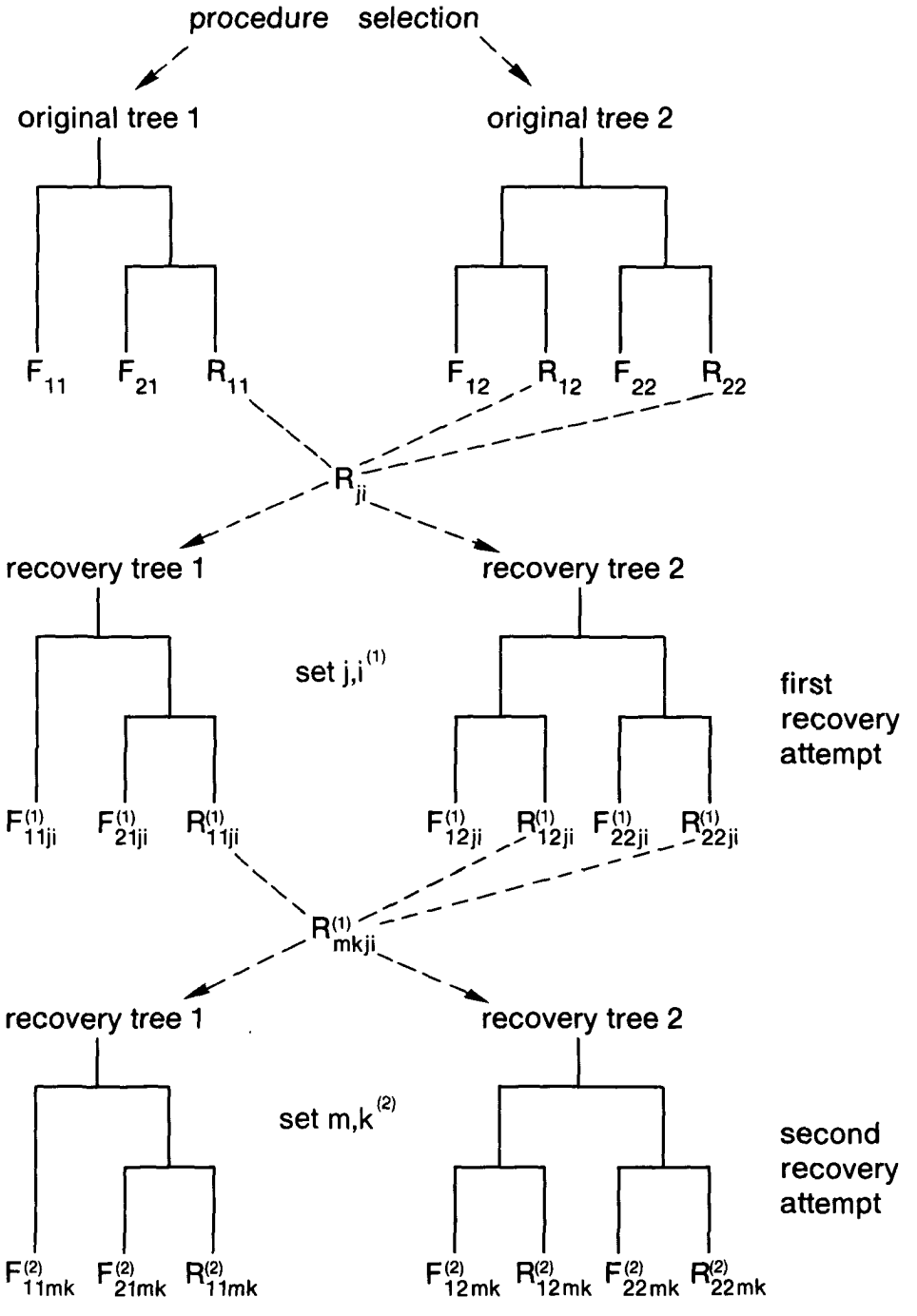


Fig. 22
Two THESIS event trees at three stages of performance (no recovery, first recovery attempt, second recovery attempt).

$$\tau_q^{(o)} = \sum_{i=1}^{u} f_{qi}$$

$$\phi_q^{(x)} = [\varphi_{q1}^{(x)}, \varphi_{q2}^{(x)}, .., \varphi_{qu}^{(x)}] \qquad \text{(Eq. 1–A)}$$

with

$$\varphi_{qi}^{(x)} = \left[\sum_{k=1}^{u} f_{qkli}^{(x)}, \sum_{k=1}^{u} f_{qk2i}^{(x)}, \ldots, \sum_{k=1}^{u} f_{qkw_ji}^{(x)} \right] \qquad \text{(Eq. 1–B)}$$

$(x = 1,2,\ldots,t)$

$$\Omega = \begin{bmatrix} \omega_1 \\ \omega_2 \\ : \\ \omega_u \end{bmatrix} \qquad \text{(Eq. 1–C)}$$

with

$$\omega_i = \begin{bmatrix} r_{1i} \\ r_{2i} \\ : \\ r_{w_ji} \end{bmatrix} \qquad \text{(Eq. 1–D)}$$

and

$$\Psi^{(x)} = \begin{bmatrix} \psi_{11}^{(x)}, \psi_{12}^{(x)}, \ldots, \psi_{1u}^{(x)} \\ \psi_{21}^{(x)} \qquad\qquad : \\ : \qquad\qquad : \\ \psi_{u1}^{(x)}, \psi_{u2}^{(x)}, \ldots, \psi_{uu}^{(x)} \end{bmatrix} \qquad \text{(Eq. 1–E)}$$

with

$$\psi_{ki}^{(x)} = \begin{bmatrix} r_{1kli}^{(x)}, r_{1k2i}^{(x)}, \ldots, r_{1kw_ji}^{(x)} \\ r_{2kli}^{(x)}, r_{2k2i}^{(x)}, \ldots, r_{2kw_ji}^{(x)} \\ : \quad : \qquad\qquad : \\ r_{w_kkli}^{(x)}, r_{w_kk2i}^{(x)}, \ldots, r_{w_kkw_ji}^{(x)} \end{bmatrix} \qquad \text{(Eq. 1–F)}$$

In addition to $\tau_q^{(t)}$, the term τ_q is used and defined as $\tau_q = \lim_{t \to \infty} \tau_q^{(t)}$.

Model refinements

Several MRFs have been taken into account so far in a general way, viz. procedure-selection capability, event dependence, recovery attempts and recovery dependence. In order to calculate the path probabilities as they appear in the matrices Ω, $\phi_q^{(x)}$ and

$\Psi^{(x)}$, model refinements are required next, regarding the branch probabilities (a path probability is obtained by mutually multiplying the branch probabilities and multiplication of this product by the selection probabilities to select a certain procedure).

Variation in the probabilities of the recovery attempts – It is reasonable to assume that the probability that a person will make a recovery attempt depends on the number of errors detected by that person in performing the actions of the procedure. The decrease in self-confidence of the person, caused by errors he has made and resulting in a higher probability of making a recovery attempt, can thus be incorporated in the model. If y is the number of errors made, the probability of the recovery attempt, RAP(y), is given by:

$$\text{RAP}(y) = \eta + (\vartheta - \eta)\frac{y}{\lambda}, \quad \text{for } y < \lambda \qquad \text{(Eq. 2-A)}$$

$$\text{RAP}(y) = \vartheta \quad , \quad \text{for } y \geq \lambda \qquad \text{(Eq. 2-B)}$$

where ϑ is the upper value of the recovery-attempt probability (RAP) reached when λ errors are made and η is the lower value when no errors are made. Figure 23 shows the RAP as a function of the number of errors.

Event dependence – Event dependence implies that the HEP of an event depends on what has happened in a previous event belonging to the same action or to a previous action. The following notation is used for the probability of an event C which is dependent upon an event A:

Prob (error in event C after error in event A) $= c_a$,
Prob (success in event C after error in event A) $= \bar{c}_a$,
Prob (error in event C after no error in event A) $= c_{\bar{a}}$,
Prob (success in event C after no error in event A) $= \bar{c}_{\bar{a}}$.

It is assumed that the influence of event dependence is the same in all four cases. The level of event dependence is given by the parameter α. The event dependence can be positive or negative. In the case of positive event dependence, the notation α_+ is used ($0 \leq \alpha_+ \leq 1$) and the following formulas are applied:

$$c_a = \alpha_+ + (1-\alpha_+)c; \quad \bar{c}_{\bar{a}} = \alpha_+ + (1-\alpha_+)\bar{c} \qquad \text{(Eq. 3)}$$

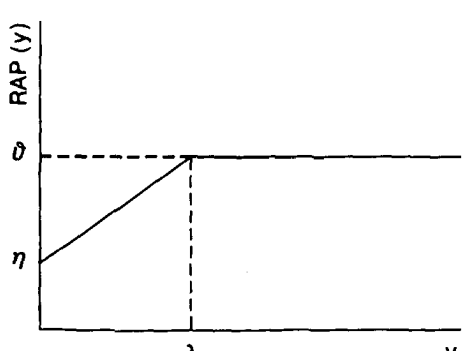


Fig. 23
The recovery attempt probability RAP(y) as a function of the number of errors y.

Since $c_a + \bar{c}_a = 1$ and $c_{\bar{a}} + \bar{c}_{\bar{a}} = 1$, $\bar{c}_a$ and $c_{\bar{a}}$ become:

$$\bar{c}_a = (1-\alpha_+)\bar{c};\ c_{\bar{a}} = (1-\alpha_+)c \qquad \text{(Eq. 4)}$$

In these equations, c_a is independent of the value of a, i.e. the probability of event A. It can be shown that, in the range from no event dependence ($\alpha_+ = 0$) to complete event dependence ($\alpha_+ = 1$), the probabilities satisfy:

$$c \leq c_a \leq 1;\ \bar{c} \leq \bar{c}_{\bar{a}} \leq 1 \qquad \text{(Eq. 5)}$$

and

$$c \geq c_{\bar{a}} \geq 0;\ \bar{c} \geq \bar{c}_a \geq 0 \qquad \text{(Eq. 6)}$$

Equation (3) is the same as that applied by Swain & Guttmann (1983) for positive dependence. These authors use the following equation:

$$c_a = \frac{1+mc}{n};\ \bar{c}_{\bar{a}} = \frac{1+m\bar{c}}{n} \qquad \text{(Eq. 7)}$$

where $m = n-1$. Substitution of n by $1/\alpha$ yields Equation (3).

The notation α_- is used ($0 \leq \alpha_- \leq 1$) in the case of negative dependence and the next formulas are found:

$$c_a = (1-\alpha_-)c;\ \bar{c}_{\bar{a}} = (1-\alpha_-)\bar{c} \qquad \text{(Eq. 8)}$$

from which follows:

$$\bar{c}_a = \alpha_- + (1-\alpha_-)\bar{c};\ c_{\bar{a}} = \alpha_- + (1-\alpha_-)c \qquad \text{(Eq. 9)}$$

It can be shown that, in the range from no dependence ($\alpha_- = 0$) to complete dependence ($\alpha_- = 1$), the probabilities satisfy:

$$c \geq c_a \geq 0;\ \bar{c} \geq \bar{c}_{\bar{a}} \geq 0 \qquad \text{(Eq. 10)}$$

and

$$\bar{c} \leq \bar{c}_a \leq 1;\ c \leq c_{\bar{a}} \leq 1 \qquad \text{(Eq. 11)}$$

In order to prevent the model from becoming more complex than necessary to provide adequate insight, it is assumed that the level of event dependence is not sensitive to the sequence of events. Hence, if event C is dependent upon event A, with a certain value for parameter α, the same value is assumed for the dependence of event A upon event C.

Recovery dependence – Recovery dependence implies that, on returning into the THESIS event tree and performing the action(s) (partly) again, the HEP of an event depends on what happened in that event before the recovery attempt. Two types of recovery dependence are distinguished on the basis of whether the event is a recovery attempt or not.

Recovery dependence for a recovery attempt (e.g. event B in Fig. 21) is modeled by assuming that the operator shows a time-dependent propensity for performing a

recovery attempt. This recovery dependence is considered as the first type of recovery dependence. In probability terms, it is modeled in such a way that, with an increasing number of recovery attempts, the probability of selecting the YES-direction in the event tree at the recovery attempt is reduced. This probability, expressed by $RAP^{(x)}$, is calculated by means of:

$$RAP^{(x)} = \delta^x RAP \qquad \text{(Eq. 12)}$$

where x is the number of recovery attempts, RAP is the original value of the recovery-attempt probability before any recovery attempt is made, and δ is a parameter expressing the level of recovery dependence ($0 \leq \delta \leq 1$). If $\delta = 0$, only one recovery attempt occurs. If $\delta = 1$, there is an infinite number of recovery attempts and there is no decline of $RAP^{(x)}$ with the number of recovery attempts. In this case the model becomes stationary.

The recovery dependence for an event which is not a recovery attempt (e.g. event A in Fig. 21) is modeled next. This recovery dependence is the second type of recovery dependence. The notation $A^{(x)}$ and $A^{(x-1)}$ is used to express event A during the x^{th} and the $(x-1)^{th}$ recovery attempt, respectively. Recovery dependence is modeled for the case that $A^{(x)}$ is assumed to depend only upon $A^{(x-1)}$. The notation for the probabilities is similar to that for event dependence:

Prob (*error in event* $A^{(x)}$ after error in event $A^{(x-1)}$) $= a_a^{(x)}$,
Prob (success in event $A^{(x)}$ after error in event $A^{(x-1)}$) $= \bar{a}_a^{(x)}$,
Prob (error in event $A^{(x)}$ after success in event $A^{(x-1)}$) $= a_{\bar{a}}^{(x)}$,
Prob (success in event $A^{(x)}$ after success in event $A^{(x-1)}$) $= \bar{a}_{\bar{a}}^{(x)}$.

It is assumed that the influence of recovery dependence is the same in all four cases. The parameter γ is used to express the level of this second type of recovery dependence. The recovery dependence can be positive or negative, just as with the event dependence. This is expressed by γ_+ ($0 \leq \gamma_+ \leq 1$) and γ_- ($0 \leq \gamma_- \leq 1$), respectively. The following formulas are applied for positive dependence:

$$a_a^{(x)} = \gamma_+ + (1-\gamma_+)a;\ \bar{a}_{\bar{a}}^{(x)} = \gamma_+ + (1-\gamma_+)\bar{a} \qquad \text{(Eq. 13)}$$

from which follows

$$\bar{a}_a^{(x)} = (1-\gamma_+)\bar{a};\ a_{\bar{a}}^{(x)} = (1-\gamma_+)a \qquad \text{(Eq. 14)}$$

For negative recovery dependence the formulas become:

$$a_a^{(x)} = (1-\gamma_-)a;\ \bar{a}_{\bar{a}}^{(x)} = (1-\gamma_-)\bar{a} \qquad \text{(Eq. 15)}$$

from which follows

$$\bar{a}_a^{(x)} = \gamma_- + (1-\gamma_-)\bar{a};\ a_{\bar{a}}^{(x)} = \gamma_- + (1-\gamma_-)a \qquad \text{(Eq. 16)}$$

The probabilities satisfy equations similar to Equations (5), (6), (10) and (11). These formulas can also be applied for the probability that a procedure will be chosen. The probability of choosing a procedure or its THESIS event tree is termed 'selection probability'. The selection probability of a recovery tree is assumed to depend only on

the choice of procedure immediately before the recovery attempt. This implies the use of Equations (13) through (16) for the selection probabilities.

Implementation of the model refinements – The refinements described above imply that three influences can affect a probability. The order in which these influences can be applied could influence its value. A specific order must therefore be assumed for application of the refinements:

(1) the variation in the RAP, if present (see first subsection), is applied first;
(2) the event dependence, if relevant to an event (see second subsection), is applied next;
(3) the recovery dependence is finally applied if present (see third subsection).

This specific order is assumed here because it yields the least complex model for calculating the path probabilities. It can be shown that the calculation becomes much more extensive if another order is applied. Since there are no indications that another order gives more reliable results or has any other advantage, the order mentioned above will be applied further on.

The recovery tree 2 of set $4,2^{(1)}$ of Figure 21 is used (Fig. 24) to show how a path probability is calculated. Set $4,2^{(1)}$ implies that the path leading to R_{42} was followed before the recovery attempt. The selection and branch probabilities as depicted in the tree of Figure 24 can be calculated with the previous definitions. Only the right-branch probabilities are depicted in order to simplify the figure. The left-branch probabilities can easily be derived since a left-branch probability and a right one add up to one.

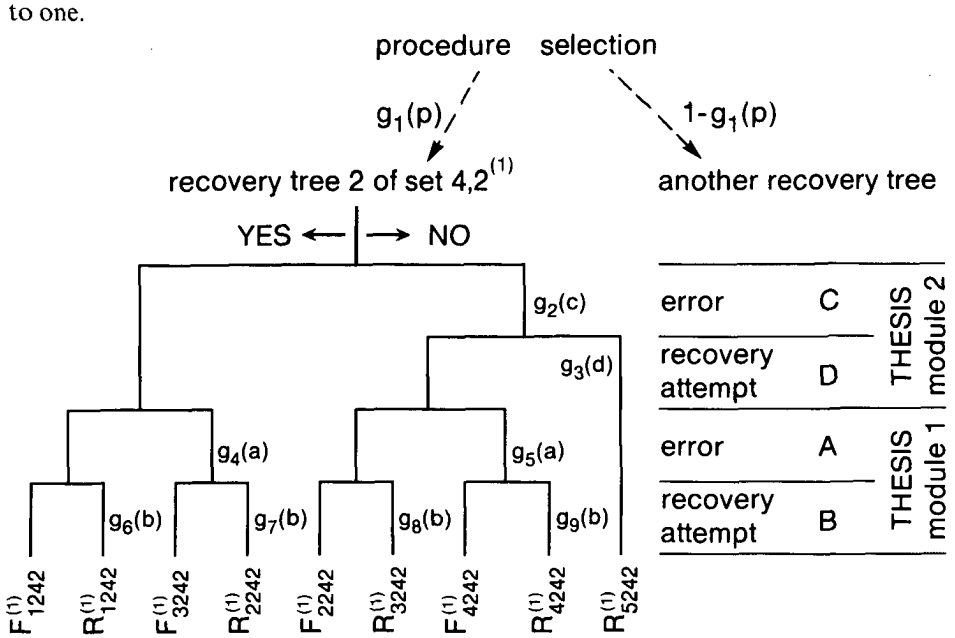


Fig. 24
Recovery tree 2 of set $4,2^{(1)}$. Only the right branch probabilities $g_2(c)$ through $g_9(b)$ are presented. The selection probability of choosing this recovery tree is $g_1(p)$.

It is assumed that there is a positive event dependence between the two specific actions. Parameter α is used to represent the positive event dependence between errors A and C, whereas parameter β is used to represent a positive event dependence between recovery attempts B and D. Furthermore, it is assumed that there is positive recovery dependence, which is represented by γ for events A and C, and by δ for events B and D.

The path probability $f^{(1)}_{2242}$ is calculated and yields, according to Fig. 24:

$$f^{(1)}_{2242} = g_1(p)\, g_2(c)\, [1-g_3(d)][1-g_5(a)][1-g_8(b)] \qquad \text{(Eq. 17)}$$

The following points should be noted:

(1) $g_1(p)$ is influenced only by recovery dependence. Since procedure 2 was carried out before the recovery attempt, it follows that, according to Equation (13):

$$g_1(p) = p^{(1)}_p = \gamma + (1-\gamma)p \qquad \text{(Eq. 18)}$$

(2) $g_2(c)$ is also influenced only by recovery dependence. Because the error is made at event C and because an error was made at C before the recovery attempt, this yields, again by application of Equation (13):

$$g_2(c) = c^{(1)}_c = \gamma + (1-\gamma)c \qquad \text{(Eq. 19)}$$

(3) $g_3(d)$ is influenced by the variation in the RAP and the recovery dependence. According to the order presented earlier, the variation in recovery dependence is considered first. It is assumed that $\eta = d_{min}$ and $\vartheta = d_{max}$ and that ϑ is reached after two errors, so that $\lambda = 2$. Since one error is made before D, i.e. at C in recovery tree 2, the variable y becomes one. This RAP consequently becomes in the first instance, according to Equation (2): $d_{min} + (d_{max} - d_{min})/2 = (d_{max} + d_{min})/2$. Moreover, the influence of recovery dependence is incorporated. Since this is the first recovery attempt, $g_3(d)$ becomes, according to Equation (12):

$$g_3(d) = \delta(d_{max} + d_{min})/2 \qquad \text{(Eq. 20)}$$

(4) $g_5(a)$ is influenced by both event dependence and recovery dependence. The event dependence must be incorporated first. Equation (3) can be applied since an error was made at event C in the same tree and an error is now made at event A. The value is given by: $a_c = \alpha + (1-\alpha)a$. The recovery dependence is then incorporated by using Equation (13), which leads to $g_5(a)$:

$$g_5(a) = \gamma + (1-\gamma)a_c = \gamma + (1-\gamma)[\alpha + (1-\alpha)a] \qquad \text{(Eq. 21)}$$

(5) $g_8(b)$ is influenced by all three factors. The variation in the RAP has reached its maximum ϑ since $y = \lambda$ (error at A and C); it is assumed that $\vartheta = b_{max}$. Furthermore, the event dependence implies the use of Equation (4). The value is given by: $b_{\bar{d}} = (1-\beta)b_{max}$, where β is the parameter for the event dependence between recovery attempts. Finally, the recovery dependence implies that Equation (12) is used again, so that $g_8(b)$ becomes:

$$g_8(b) = \delta(1-\beta)b_{max} \qquad \text{(Eq. 22)}$$

Incorporation of Equations (18) through (22) in Equation (17) yields the path probability for $f^{(1)}_{2242}$.

The other path probabilities of this recovery tree can be calculated in the same way. This can also be done for the other recovery tree of set $4,2^{(1)}$. The path probabilities of the original trees can simply be derived from these by assuming no recovery dependence. The path probabilities of the other sets of recovery trees, following return outcomes other than R_{42}, are obtained in a similar way, as well as the sets for more than one recovery attempt. The path probabilities can subsequently be included in Equation (1) in order to obtain the probability of an outcome in which the recovery attempts are taken into account.

Return level – It was assumed up to now that the total tree is started again after a return outcome but this need not be the case in reality. A first reason is that, after a few actions, it may no longer be possible to return to the top of the THESIS event tree if an irreversible process state has been reached. A second reason is that the motivation of a person to return to the top will decrease when more actions have been performed.

To take this into account, the model is extended by the assumption that a person could possibly return to the top of a certain module of which the THESIS event tree is constructed instead of to the top of the event tree. This is clarified in Figure 25, where THESIS event tree 2 of Figure 21 is presented and where the possible return loops originating from a return outcome are drawn.

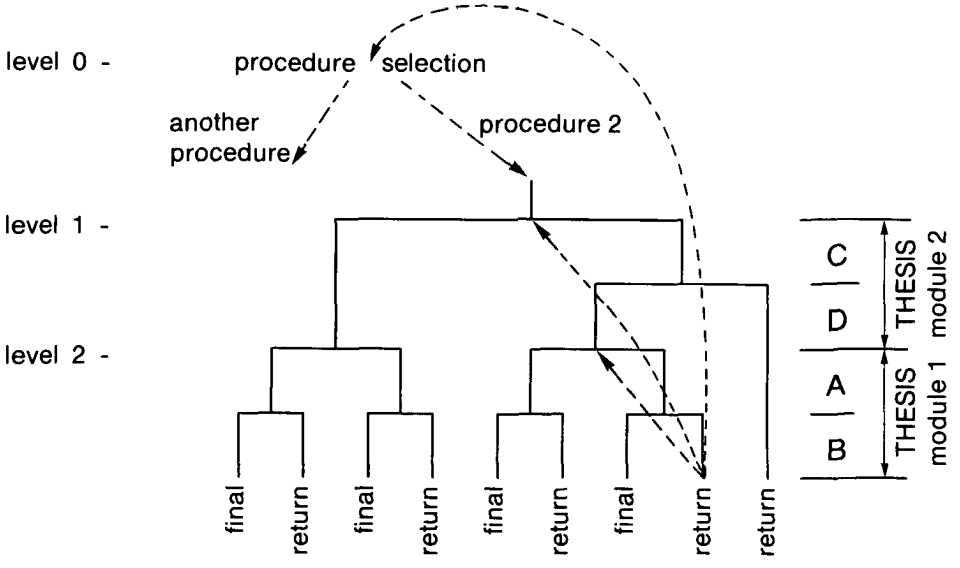


Fig. 25
THESIS event tree 2 of Figure 21 with three return loops from a return outcome going to the procedure selection (level 0), the top of module 2 (level 1) and the top of module 1 (level 2).

Recovery-dependence parameters γ and δ were originally assumed to be independent of the events. Making them dependent on the events, renders it possible to return to the top of a particular module. An example is the return to the top of module 1 from the return outcome in Figure 25, i.e. the return to level 2. This return can be effected by choosing the value for γ of the procedure selection and of event C equal to 1, and the value for δ of event D equal to 0. The return to level 0 then results in return to level 2. This can be understood if one remembers that the return outcome considered in Figure 25 resembles R_{42} of the original tree on the first recovery attempt. By making the value of γ in Equations (18) and (19) equal to 1 and that of δ in Equation (20) equal to zero, the return loop to level 2 is obtained.

Applying values of 1 for γ and 0 for δ implies that no return is made to level 1. By using less extreme values for γ and δ, a compromise between return level and recovery dependence can be made. What is done here for one particular THESIS event tree can also be done for other THESIS event trees if more than one procedure exists (as in the case of Fig. 21 where two procedures are available).

Concluding remarks

A theoretical model based on THESIS event trees was derived in this chapter. Four MRFs (event dependence, recovery attempts, recovery dependence and procedure-selection capability) were incorporated in the model. A general model was derived first, based on the outcome probabilities of the THESIS event trees, followed by some refinements to the model. An essential aspect of the general model was the assumption that the recovery dependence was limited to the THESIS event tree passed through before the recovery attempt. This resulted in a rather compact analytical model. A more complex model would have been arrived at if this assumption had not been made. However, deriving a more sophisticated model, in which recovery dependence is modeled in a more refined way, is probably not worthwhile because of the uncertainty in HEPs.

Several parameters were defined to represent the MRFs. It should be noted that the value of these parameters will, in most cases, be impossible to assess from practical situations. This is due to the fact that several paths may lead to the same outcome, i.e. directly, in the original tree or indirectly, via recovery attempts. This implies that the assessment of the parameters from outcome probabilities obtained in practice becomes difficult. Hence, validation of the model as derived in this chapter will need extensive research which can be done in practice only in specific situations, where each outcome is induced directly by one particular path only. This deeper analysis is, however, not relevant at this stage since the model was derived with the purpose to determine the contribution of certain MRFs by applying a sensitivity analysis. If the contribution of some MRFs is so slight that they can be discarded from the model, validation may become less difficult.

It can be shown that application of the Markov theory instead of THESIS event trees would have resulted in the same analytical model. This is due to the inclusion of the return loops in the THESIS event tree and the definition of event and recovery

dependence. The term 'transition state' as used in the Markov theory (Bhat, 1972) can be compared with the term 'return outcome' used here; another term, i.e. 'absorbing state' can be compared with the final outcome. If the number of recovery attempts is compared to the variable t (time) in the Markov theory, the model can be regarded as a Markov process with a discrete time. Due to the assumption that the probability of a recovery attempt depends upon this time, the process is non-stationary. Hence, the so-called transition matrix (Kemeny & Snell, 1976) as applied in the Markov theory is time-dependent. The two states can be grouped so that the first group represents the final outcomes and the last group the return outcomes of each THESIS event tree. It can be proven that the left-bottom partition of the transition matrix then contains the column vectors of the transpose of $\phi_q^{(i)}$ of Equation (1) and that the right-bottom partition contains the transpose of $\Psi^{(i)}$. A demonstration of the detailed relation between the analytical model and the Markov theory is, however, beyond the scope of this chapter.

An element of one of the matrices in Equation (1), i.e. the path probability of a recovery tree, was calculated analytically at the end of this chapter. It is clear that to do this for all the paths of the THESIS event trees can become very time-consuming, particularly in the case of large trees. Hence, implementation of the analytical model on a computer might be useful and will be discussed in the next chapter.

Chapter 7

Evaluation of the analytical model

Introduction

An analytical model based on the use of THESIS event trees was derived in the preceding chapter. Certain parameters of the model, such as event dependence, recovery attempts, recovery dependence and procedure-selection capability, describe the MRFs. The results of an evaluation performed with this model will now be presented. The effects that combinations of MRFs can have on the probabilities of certain outcomes are therefore quantified. Since it is almost impossible to analyze all the possible combinations, the analytical model will first be evaluated with recovery dependence left out. After that, an attempt will be made to consider all the MRFs that were incorporated in the analytical model. Finally, conclusions are drawn from the results, followed by recommendations for further research.

The effect of recovery attempts without recovery dependence

The effects of the recovery attempts without the presence of recovery dependence, but with event dependence and procedure-selection capability, are analyzed here. It was already demonstrated that the return to an arbitrary point in the THESIS event tree, instead of to the top of the event tree, can be regarded as a form of recovery dependence. The assumption of no recovery dependence therefore implies the return to the top of the THESIS event tree. The assumption also implies that all recovery trees of the different sets (set $j,i^{(x)}$) are quantitatively identical and can simply be replaced by the set containing the original trees. Hence, it holds for Equation (1) that

$$r^{(x)}_{mkji} = r_{mk} \text{ (for each } j \text{ and } i) \qquad \text{(Eq. 23)}$$

$$\text{and } \sum_{k=1}^{u} f^{(x)}_{qkji} = \sum_{k=1}^{u} f_{qk} \text{ (for each } j \text{ and } i) \qquad \text{(Eq. 24)}$$

$\psi^{(x)}_{ki}$ becomes by substituting Equation (23) in Equation (1-F):

$$\psi^{(x)}_{ki} = [\omega_k, \omega_k, \ldots, \omega_k]$$

with length w_i in which the quantity ω_k is given by:

$$\omega_k = \begin{bmatrix} r_{1k} \\ r_{2k} \\ \vdots \\ r_{w_k k} \end{bmatrix}$$

Hence, the matrix $\Psi^{(x)}$ in Equation (1–E) becomes:

$$\Psi^{(x)} = \begin{bmatrix} \omega_1, \omega_1, \ldots, \omega_1 \\ \omega_2, \omega_2, \ldots, \omega_2 \\ \vdots \quad \vdots \quad \vdots \\ \omega_u, \omega_u, \ldots, \omega_u \end{bmatrix} = \Omega \mathrm{I}$$

with length $\sum_{i=1}^{u} w_i$, and containing $u \sum_{i=1}^{u} w_i$ elements.

The parameter Ω is given by Equation (1-C)

and $\mathrm{I} = [1, 1, \ldots, 1]$ with a length of $\sum_{i=1}^{u} w_i$. By substituting Equation (24) in Equation (1-B), $\varphi_{qi}^{(x)}$ becomes: $\varphi_{qi}^{(x)} = [\tau_q^{(0)}, \tau_q^{(0)}, \ldots, \tau_q^{(0)}]$ with length w_i. Hence, the matrix $\phi_q^{(x)}$ in Equation (1-A) becomes: $\phi_q^{(x)} = [\tau_q^{(0)}, \tau_q^{(0)}, \ldots, \tau_q^{(0)}] = \tau_q^{(0)}\mathrm{I}$

with length $\sum_{i=1}^{u} w_i$ Equation (1) thus becomes:

$$\tau_q^{(t)} = \tau_q^{(0)} + \tau_q^{(0)}\,\mathrm{I}\Upsilon + \tau_q^{(0)}\mathrm{I}\Upsilon\,\mathrm{I}\Upsilon + \ldots + \tau_q^{(0)}\mathrm{I}\Upsilon\mathrm{I} \ldots \Upsilon\mathrm{I}\Upsilon \qquad \text{(Eq. 25)}$$

in which the quantity $\mathrm{I}\Upsilon$ means:

$$\mathrm{I}\Upsilon = \sum_{i=1}^{u} \sum_{j=1}^{w_i} r_{ji} = \upsilon$$

The quantity υ is the sum of the return probabilities for the original trees. Equation (25) therefore becomes:

$$\tau_q^{(t)} = \tau_q^{(0)}(1 + \upsilon + \upsilon^2 + \ldots + \upsilon^t).$$

As $\upsilon < 1$,

$$\tau_q = \frac{\tau_q^{(0)}}{1-\upsilon} \qquad \text{(Eq. 26)}$$

follows for $t \to \infty$. Equation (26) can be modified in the special case where not only recovery dependence, but also event dependence is absent. In the case of no event dependence, it can be shown that, if a procedure contains n actions, the parameter υ becomes:

$$\upsilon = r_1 + (1-r_1)r_2 + (1-r_1)(1-r_2)r_3 + \ldots + (1-r_1)\ldots(1-r_{n-1})r_n$$

where r_n is the sum of the return probabilities of the THESIS module of the n^{th} action in the procedure. Hence, it follows that:

$$1-\upsilon = \prod_{i=1}^{n} 1-r_i,$$

so that Equation (26) becomes:

$$\tau_q = \tau_q^{(0)} \prod_{i=1}^{n} \frac{1}{1-r_i} \qquad \text{(Eq. 27)}$$

Equation (27) is the same as to the one derived directly by Heslinga (1984).

The assumption of no recovery dependence obviously changes the complex model of the previous chapter (see Eq. 1) into a simple mathematical model, represented by Equations (26) and (27). This simple model will be discussed thoroughly in the last part of this chapter. The effect of recovery dependence during the recovery attempt is now dealt with.

The effects of recovery attempts with recovery dependence

The effects of all MRFs as incorporated in the analytical model will now be evaluated. This implies an expansion with regard to the approach in the preceding section, since recovery dependence is now included. A simple analytical description could be derived when no recovery dependence was assumed. The analytical description becomes, however, much more complicated if recovery dependence is present.

The need for such an analytical description is questionable. It is certainly possible that the values of a number of MRFs are such that they do not affect the probabilities of certain outcomes at all. This would result in the elimination of certain parameters describing the MRFs, thus providing a model with a much simpler analytical structure. It would therefore be worthwhile to apply a numerical sensitivity analysis to study the effect of the various MRFs.

A computer program, PRESUME, was therefore developed. It is based on the theoretical model derived in the preceding chapter. The program, developed in cooperation with Schoof (1987), allows quantification of the analytical model in its most extensive form, including all the refinements mentioned in the preceding chapter. The input for PRESUME consists of the HEPs for the events and the parameters describing the various MRFs. The output is the set of final outcome probabilities taking into account all possible recovery attempts.

Procedure – The effects of several MRFs really demand to be studied with regard to the long procedures that are present in practice. However, due to computer limitations PRESUME can only handle rather short procedures. THESIS event trees may contain a maximum of 27 events, a number which is too small to handle a real control-room procedure. It might nevertheless be possible to determine the trend in the effect of MRFs by studying relatively short procedures. One could thus extrapolate the effect of certain MRFs on longer procedures, as they appear in actual problems. If it is found that the influence of certain parameters decreases with increasing procedure length, the corresponding MRFs could be disregarded for the longer control-room procedures.

Three cases, with procedure length as the variable, will therefore be analyzed by means of PRESUME. The procedure in case I contains only one human action. The procedure in case II contains two human actions; it is assumed that two sequences,

and therefore two procedures, are possible. Finally, three human actions are considered in case III and three possible sequences (procedures) are assumed to be possible.

Figure 26 shows the three THESIS modules arbitrarily chosen for use in the sensitivity analysis. The THESIS event trees of the procedures for the three cases considered are based on these modules (Fig. 27). The THESIS event tree for case I is similar to THESIS module 1. Since two procedures are possible in case II, there are two THESIS event trees; they are both constructed from THESIS modules 1 and 2. Three procedures are possible in case III; the THESIS event trees of these procedures are constructed from modules 1, 2 and 3. The modules and the construction of the event trees are arbitrary; other approaches are possible, but are not considered here.

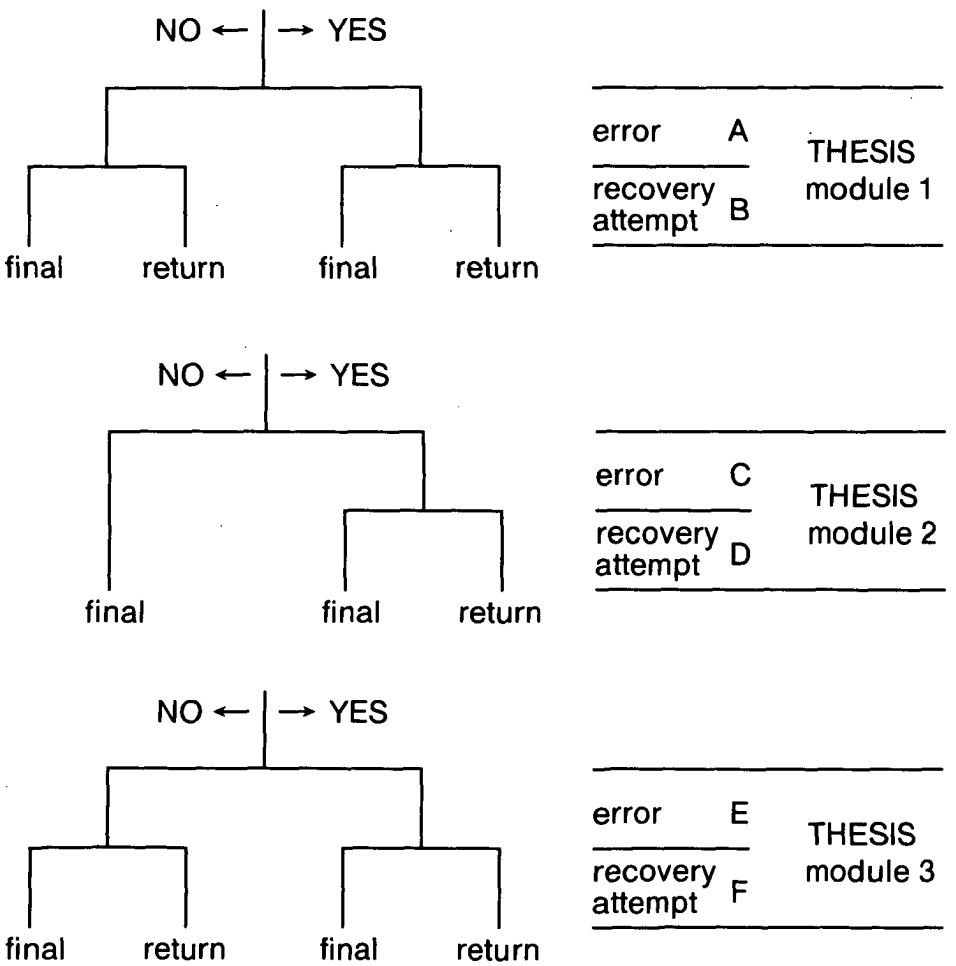


Fig. 26
The three THESIS modules as used for the construction of the THESIS event trees applied in the sensitivity analysis. Although THESIS module 3 has the same structure as module 1, module 3 is regarded as a different module because it contains events that can differ regarding probabilities and dependencies.

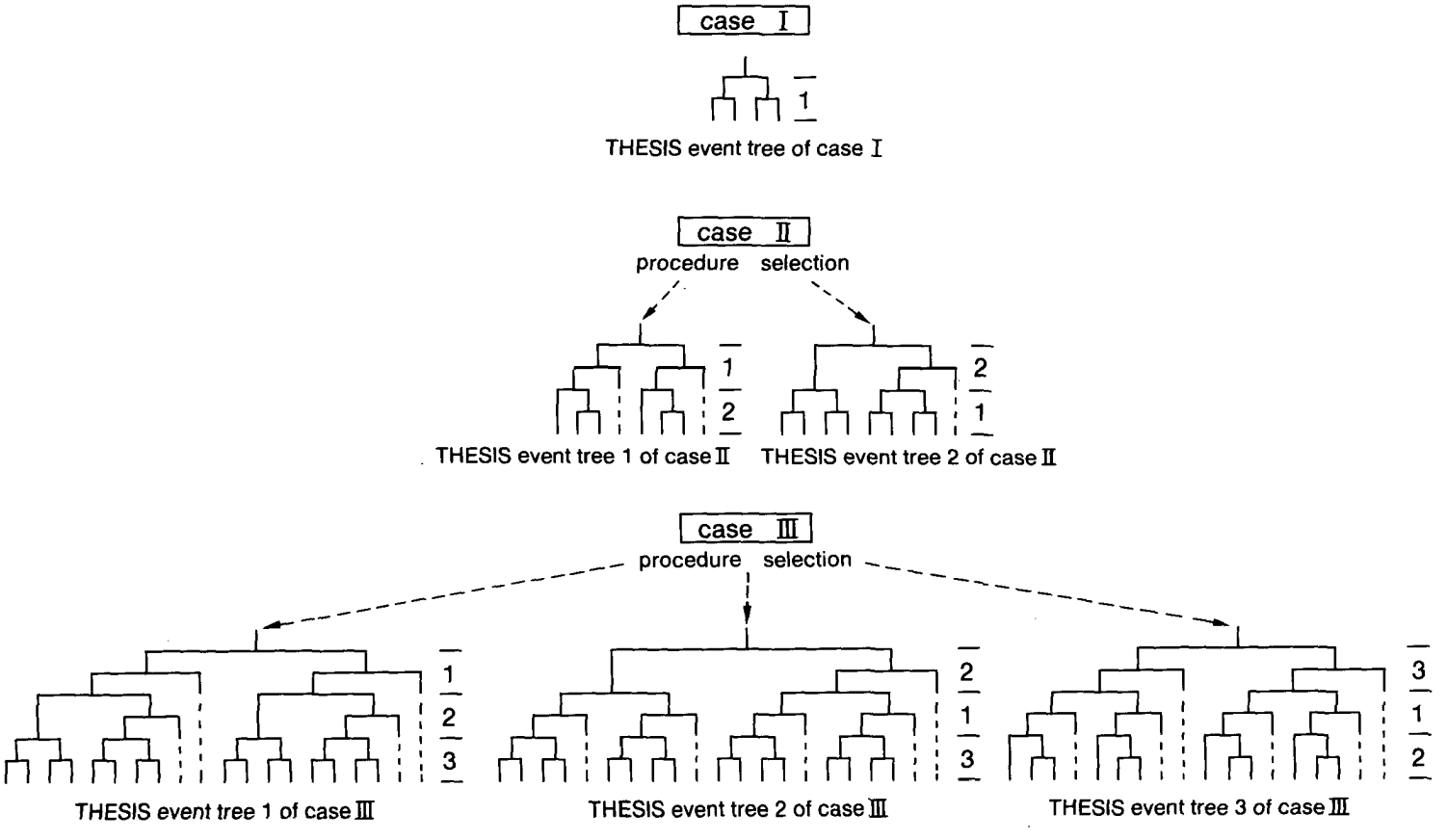


Fig. 27
The THESIS event trees of case I, II, and III. The numbers along the trees show the modules of Figure 26 used to construct the THESIS event trees.

Table 9
The operating point and its extreme values. u represents the number of procedures possible in a certain case; n represents the number of errors that can be made in a procedure (the last equals the number of actions in a procedure since it was assumed that one error can be made per action). RAP represents the return-attempt probability.

parameter		operating point	extreme values
selection probability		1/u	1/u
HEP (a,c,e)		0.01	0.01
event dependence between human errors	α	0.5	0 and 1
event dependence between recovery attempts	β	0.5	0 and 1
recovery dependence between human errors	γ	0.5	0 and 1
recovery dependence between recovery attempts	δ	0.5	0 and 1
return level	ε	0	1, 2 and 3
type of recovery dependence	ζ	positive	negative
minimum RAP (b,d,e)	η	0.0	0.01 and 0.1
maximum RAP (b,d,e)	ϑ	0.5	0 and 0.99
number of errors valid for ϑ	λ	n	1

Since the effect of varying a combination of parameters is not yet known, it would be best to make a sensitivity analysis of all possible combinations. However, such a sensitivity analysis would be extremely tedious, since the model contains many parameters. Moreover, the model appears to be non-linear since the output variables, the outcome probabilities, are a non-linear function of the input variables due to the many multiplications. To provide some insight, a one-dimensional analysis in which only one parameter is varied around a certain operating point whereas other parameters are kept constant, will therefore be performed. Such an analysis implies the definition of an operating point, around which the parameters are varied, one after the other, between extreme values.

Table 9 gives the operating point applied in the analysis and the extreme values. Certain parameters, i.e. selection probability and event probability are not varied, in order to prevent the analysis from being too extensive. Identical generic values are assumed for each human-error probability (HEP) for the sake of convenience. The value for the recovery-attempt probability (RAP) is also assumed to be equal for each recovery attempt.

Results — The computer program calculates the outcome probabilities τ_q taking an infinite number of recovery attempts into account. In practice, however, the contribution of the recovery attempts will decrease asymptotically. The program can therefore be stopped when the asymptotic value τ_q is reached at a specified accuracy: an accuracy of 1% will be used here.

The influence of a specific parameter is calculated by introducing an extension quotient L. This quotient is defined as the ratio between the highest value of τ_q and the

Table 10
Influence of the parameter 9 for the three cases presented in Figure 27. The parameter 9 represents the RAP that is valid when the maximum number of errors possible in a procedure is made. The asterix (*) indicates the operating point.

		case I		case II				case III							
		τ_1	τ_2	τ_1	τ_2	τ_3	τ_4	τ_1	τ_2	τ_3	τ_4	τ_5	τ_6	τ_7	τ_8
ϑ	0.0	9.900 E-1	1.00 E-2	9.851 E-1	4.95 E-3	4.95 E-3	5.05 E-3	9.801 E-1	4.93 E-3	4.10 E-3	8.49 E-4	3.27 E-3	1.68 E-3	2.50 E-3	2.55 E-3
	0.5*	9.928 E-1	7.19 E-3	9.873 E-1	4.65 E-3	4.59 E-3	3.48 E-3	9.823 E-1	4.75 E-3	3.94 E-3	8.26 E-4	3.06 E-3	1.43 E-3	2.02 E-3	1.62 E-3
	0.99	9.963 E-1	3.71 E-3	9.895 E-1	4.29 E-3	4.05 E-3	2.17 E-3	9.845 E-1	4.51 E-3	3.75 E-3	7.56 E-4	2.81 E-3	1.17 E-3	1.59 E-3	9.46 E-4
L		1.01	2.70	1.00	1.15	1.22	2.33	1.00	1.09	1.09	1.17	1.16	1.44	1.57	2.70
L_{max}		2.70		2.33				2.70							

Table 11
Values of L_{max} obtained by varying the parameters of Table 9 for cases I, II and III. The value of L_{max} is replaced by dashes in those cases in which the parameter does not have any meaning. The complete results are presented in Appendix B.

parameter	case I	case II	case III	appendix
α	–	92.21	9026.06	B-1
β	–	1.49	2.01	B-1
γ	1.98	1.51	1.54	B-2
δ	1.13	1.07	1.09	B-2
ε	–	1.39	1.52	B-3
ζ	1.43	1.20	1.16	B-3
η	1.06	1.03	1.05	B-4
ϑ	2.70	2.33	2.70	B-4
λ	1.00	1.29	1.53	B-4

lowest value for a certain outcome q (q = 1, 2, ..., u). The highest and lowest value of τ_q are obtained by varying a parameter between its extreme values. This is detailed in Table 10, which contains the results of the influence of parameter ϑ on L. The factor L_{max} is defined as the maximum value of L that is reached in a specific case, i.e. either case I, II or III of Figure 27. Table 11 contains the main results for the three cases and appendix B contains all the detailed results.

Analysis of the results – The results are discussed in the context of the values of L_{max} presented in Table 11. Only two cases can be distinguished for parameters α, β, and ε, viz. case II and case III. This is due to the fact that these parameters have no meaning for case I because of the simple structure of the tree. The L_{max} value is larger for case III than for case II for each of the three parameters. The variation of L_{max} for parameter α (the event dependence between human errors) is very large, ranging from 92 to 9026. In contrast, the changes for parameters β (the event dependence between recovery attempts) and ε (the return level) remain rather small: from 1.49 to 2.01 for β, and from 1.39 to 1.52 for ε. Having only two cases for the three parameters is not enough for the derivation of a trend in L_{max}. However, it can still be concluded that the relatively large L_{max} value for α means that the event dependence between human errors is an important parameter in the calculation of certain outcome probabilities. This phenomenon will be investigated more thoroughly in the next section.

It is obvious that the influence of the parameters describing the recovery dependence, viz. γ (the recovery dependence between human errors) and δ (the recovery dependence between recovery attempts), is relatively small. The L_{max} value for γ changes from 1.98, 1.51 to 1.54 and L_{max} for δ changes from 1.13, 1.07 to 1.09 for an increasing procedure length (cases I, II and III subsequently). The results do not show a clear trend of L_{max} for these parameters and no prediction can thus be made about the value of L_{max} for longer procedures. A similar observation applies to the influence of η, the parameter describing the minimum RAP, as L_{max} changes from

1.06 (case I), 1.03 (case II) to 1.05 (case III). A nearly similar situation exists for ϑ, the maximum RAP, as L_{max} varies from 2.70 (case I), 2.33 (case II) to 2.70 (case III).

As opposed to the previous parameters, a trend can be noticed for parameter ζ, that expresses the type of recovery dependence, i.e. positive or negative. The value decreases from case I through case III: 1.43, 1.20 to 1.16. When this trend is extrapolated to longer procedures, the question of whether positive dependence or negative dependence is present in practice is of no relevance for the quantification. An opposite trend can be seen for parameter λ, the number of errors where the maximum RAP is reached. Its value increases from 1.00, 1.29 to 1.53 but the increase is relatively small.

It should be noted that recovery dependence can have an important influence on the structure of the model. If γ can be considered to be zero, and δ to be one, there would be no recovery dependence. This would imply the applicability of the simple Equation (26) instead of the complex model of Equation (1). A more thorough analysis of recovery dependence will therefore be made in the next section.

The influence of event dependence and recovery dependence

The above results are somewhat ambiguous, so that the two parameters, event dependence and recovery dependence, will now be analyzed more thoroughly. Recovery dependence is considered first.

Only a one-dimensional analysis of the influence of γ and δ separately was made thus far. No real trend could be found, but it is of interest to investigate whether a two-dimensional sensitivity analysis in which both γ and δ are varied at the same time from the predefined operating point would lead to similar results. The analytical model for this purpose is non-linear due to the many multiplications of several parameters, so that the results could possibly be different from those of one-dimensional analysis.

The operating point and the extreme values used earlier (Table 9) are applied. Table 12 shows the results with the quotients L and L_{max}. The quotients are used in the same way as in the one-dimensional analysis, now showing the combined influence of both recovery-dependence parameters. It appears that L_{max} varies from 1.99 (case I), 1.55 (case II) to 1.61 (case III). Again, there is no clear trend in these values, but it is obvious that the influence of the parameters is again small.

Event dependence is considered next. Equation (3) is applied to calculate the probability of an event C dependent upon event A:

$$c_a = \alpha + (1-\alpha)c \qquad \text{(Eq. 28)}$$

if positive dependence is assumed to be expressed by α, c is then the probability of event C when no event dependence is present.

The value of c will normally vary between 0.001 and 0.01 for procedural actions (Swain & Guttmann, 1983). This implies that, according to Equation (28), the variation in c_a as a result of a variation in α will be nearly 1. However, since α can vary between zero (no dependence) and one (complete dependence), the variation in c_a as

Table 12
Influence of both recovery dependence parameters for cases I, II and III. Parameters γ and δ represent the recovery dependence between human errors and between recovery attempts, respectively.

		case I		case II				case III							
		T_1	T_2	T_1	T_2	T_3	T_4	T_1	T_2	T_3	T_4	T_5	T_6	T_7	T_8
γ and δ	$\gamma = 0.0$ $\delta = 0.0$	9.950 E-1	5.05 E-3	9.896 E-1	3.81 E-3	3.74 E-3	2.86 E-3	9.852 E-1	4.15 E-3	3.36 E-3	6.51 E-4	2.53 E-3	1.17 E-3	1.61 E-3	1.34 E-3
	$\gamma = 0.0$ $\delta = 0.5$	9.950 E-1	5.04 E-3	9.896 E-1	3.81 E-3	3.73 E-3	2.86 E-3	9.852 E-1	4.15 E-3	3.36 E-3	6.50 E-4	2.53 E-3	1.17 E-3	1.61 E-3	1.34 E-3
	$\gamma = 0.0$ $\delta = 1.0$	9.950 E-1	5.03 E-3	9.896 E-1	3.81 E-3	3.73 E-3	2.85 E-3	9.852 E-1	4.15 E-3	3.36 E-3	6.50 E-4	2.53 E-3	1.17 E-3	1.61 E-3	1.34 E-3
	$\gamma = 0.5$ $\delta = 0.0$	9.925 E-1	7.53 E-3	9.871 E-1	4.68 E-3	4.63 E-3	3.60 E-3	9.822 E-1	4.75 E-3	3.95 E-3	8.37 E-4	3.07 E-3	1.46 E-3	2.07 E-3	1.69 E-3
	$\gamma = 0.5$* $\delta = 0.5$*	9.928 E-1	7.19 E-3	9.873 E-1	4.65 E-3	4.59 E-3	3.48 E-3	9.823 E-1	4.75 E-3	3.94 E-3	8.26 E-4	3.06 E-3	1.43 E-3	2.02 E-3	1.62 E-3
	$\gamma = 0.5$ $\delta = 1.0$	9.933 E-1	6.68 E-3	9.875 E-1	4.62 E-3	4.54 E-3	3.35 E-3	9.825 E-1	4.74 E-3	3.94 E-3	8.12 E-4	3.04 E-3	1.40 E-3	1.97 E-3	1.55 E-3
	$\gamma = 1.0$ $\delta = 0.0$	9.900 E-1	1.00 E-2	9.851 E-1	5.26 E-3	5.26 E-3	4.43 E-3	9.801 E-1	5.11 E-3	4.22 E-3	9.16 E-4	3.39 E-3	1.62 E-3	2.46 E-3	2.16 E-3
	$\gamma = 1.0$ $\delta = 0.5$	9.900 E-1	9.99 E-3	9.851 E-1	5.32 E-3	5.32 E-3	4.31 E-3	9.801 E-1	5.14 E-3	4.25 E-3	9.15 E-4	3.42 E-3	1.62 E-3	2.46 E-3	2.07 E-3
	$\gamma = 1.0$ $\delta = 1.0$	9.900 E-1	9.98 E-3	9.851 E-1	5.41 E-3	5.41 E-3	4.12 E-3	9.801 E-1	5.18 E-3	4.30 E-3	9.12 E-4	3.49 E-3	1.61 E-3	2.44 E-3	1.94 E-3
L		1.01	1.99	1.00	1.42	1.45	1.55	1.01	1.25	1.28	1.41	1.38	1.38	1.53	1.61
L_{max}		1.99		1.55				1.61							

a result of a variation in c can lie between zero and one, according to Equation (28). Hence, c_a is on an average more sensitive to variations in event dependence than to variations in HEPs. Particularly for high levels of event dependence, c_a is less sensitive to HEP variations.

This analysis of event dependence may seem rather trivial, but it indicates a practical problem regarding the knowledge of relevant data. Something is now known about the HEPs (Topmiller et al., 1982; Swain & Guttmann, 1983; Comer et al., 1984; Spettel et al., 1986) but data regarding event dependence remain very scarce. Only Swain & Guttmann (1983) provide a guide of a few pages to the assessment of levels of event dependence. This section shows that the acquisition of data regarding the levels of event dependence is as important as, or even more important than the acquisition of HEPs. To discuss whether an HEP is 0.001 or 0.01 (a difference of a factor 10) is less relevant if a high level of event dependence is present. Only Equation (28) was used here to demonstrate this, but similar considerations account for the other event-dependence equations presented in the preceding chapter (Eqs. 4, 8 and 9).

Discussion

The results will now be evaluated, followed by some conclusions and suggestions for further research.

Evaluation – Certain assumptions regarding the MRFs of THESIS were made in using the complicated analytical model of the preceding chapter. One assumption was that there was no recovery dependence during the recovery attempts. It resulted in simplification (Eq. 26) of this analytical model. Equation (26) can be converted to Equation (27) for the special case of no event dependence.

Sensitivity analyses were performed by varying the parameters of the model from a pre-defined operating point to certain extreme values that could perhaps be possible in practice. The outcome probabilities were calculated, and L_{max}, a measure for the maximum influence of a change in a parameter, was determined. It can be shown that the outcome probabilities for this operating point have a maximum or minimum at the extreme values applied. Hence, it was justified to perform the sensitivity analysis with these extreme values in order to calculate L_{max}.

The one- and two-dimensional analyses showed that the influence of the recovery-dependence parameters γ and δ on the outcome probabilities was small. The sensitivity analyses were performed with procedures much shorter than those actually used by operators. Unfortunately, no trend could be found regarding the influence of the parameters with increasing procedure length. However, one issue, that deals with the uncertainty in HEPs, is important in this context and remains to be discussed.

Point values were used up to now for the HEPs in the analysis. In practice, HEPs have a distribution that expresses, among other aspects, the uncertainty. Swain & Guttmann (1983) have provided information regarding the uncertainty of the HEPs of single events and a set of formulas (their Appendix A) for obtaining the uncertainty of the probability of a combination of events. It can be shown that the uncertainty

of the event sequences increases when several events are combined if this set of formulas is used and if values are applied consistently with the operating point used earlier. The uncertainty of the outcome probabilities will generally be greater for case II than for case I, and greater for case III than for case II. This increase in uncertainty will be greater than the change in L_{max} that was calculated with the one- and two-dimensional analyses where γ and δ were varied. It should be kept in mind that L_{max} can be regarded as an indication of the difference in the outcome probabilities calculated with the complex model of Equation (1) and the simple model of Equation (26). Several values of γ and δ were applied in the sensitivity analysis with the model of Equation (1) to determine L_{max} for variations in γ and δ. Assuming $\gamma = 0$ and $\delta = 1$ implies no recovery dependence and, hence, the application of the simple model of Equation (26). As the increase in uncertainty in the outcome probabilities from case I through case III is greater than the observed change in L_{max}, the use of the simple model of Equation (26) instead of the complex model of Equation (1) becomes justified. This implies that recovery dependence can be neglected although it may be present in actual practice.

No clear trend was observed in L_{max} for variations in γ and δ if point values were used. A consideration of this L_{max} in combination with the uncertainty nevertheless led to the decision to use the simple model. Some restrictions must be made in this context. The results were obtained by application of a one-dimensional sensitivity analysis and, partly, by application of a two-dimensional sensitivity analysis in which the values of the parameters deviated from a particular operating point. Although the selection of this operating point was carefully based on average values for the parameters that were taken to be valid for procedural actions, only one operating point was tested. Moreover, the procedures that were analyzed contained at most three human actions, and the THESIS module of each human action contained only one human error and one recovery attempt. Furthermore, one particular structure was assumed for the THESIS event trees.

Different results might be obtained if another operating point, other extreme values, longer procedures or a multi-dimensional sensitivity analysis were applied. The results reported by Schoof (1987), for instance, show an important contribution of the recovery-dependence parameters. However, this author used less realistic values for the RAPs. The conclusion must be that care is needed when Equations (26) and (27) are applied to cases where recovery dependence is present; one should be aware of the extent to which the conditions under which the results were obtained are violated. Experience in making an HPSA is thus of the utmost importance.

Replacing the model of Equation (1) by that of Equation (26) has important implications. Since the use of this equation implies that recovery dependence is assumed to be absent, the parameters 'return level' and 'type of recovery dependence' become unimportant. This implies that to obtain quantitative knowledge about the value of these parameters is no longer relevant.

Since Equation (26) can, under certain conditions, be regarded as a new basis for calculations of human-performance safety, this equation is now discussed further. Two probabilities are important in this equation, i.e. $\tau_q^{(0)}$ (the probability of reaching final

outcome q in an original tree) and υ (the sum of all the return probabilities of the original trees). It is reasonable to assume that υ is small, e.g. less than 0.2, as procedural actions are involved. This does not mean, however, that the recovery attempt can be neglected by making the RAP zero. The probability $\tau_q^{(0)}$ is a combination of the probability of making one or more errors and of making a recovery attempt YES or NO. In practice, the RAP can have any value between zero and one. Hence, $\tau_q^{(0)}$ will depend greatly on the RAP. This effect is well illustrated in Table 10 where a value of 0.0 instead of 0.99 for the maximum RAP could result in an error of 270% for case I and case III. Equation (26) implies, however, that – for small values of υ – the probability of reaching final outcome q indirectly, i.e. via the recovery trees, is small as compared to the probability of reaching this outcome directly, in the original tree. Since the RAP plays a role in the calculation of $\tau_q^{(0)}$, the conclusion is that acquisition of data concerning the RAP is essential.

It was shown that, considering the MRF event dependence, probabilities of human errors that depend on other errors can be more sensitive to the choice of the level of event dependence than to the choice of HEPs. However, fewer data are available regarding this event dependence than the HEPs. This may be due to the fact that the event dependence is more situation-specific and more related to behavior phenomena. It implies, nevertheless, that more attention should be paid to the assessment of data regarding the levels of event dependence (Heslinga, 1985c.)

Conclusions – The results can be summarized in the following conclusions.

(1) It is justified, under certain conditions, to ignore the MRF recovery dependence for procedural actions that may be present in practical situations. It should be carefully investigated whether these conditions are fulfilled. Disregarding recovery dependence implies that a number of parameters can be removed from the analytical model and need not be measured.
(2) Because of the relatively great influence of event dependence, more attention should be devoted to data acquisition regarding event dependence than has so far been done.

Further research – A complex model was converted into a simple one. This operation was based on the simultaneous influence of certain recovery-dependence parameters, γ and δ, in combination with the uncertainty in HEPS. However, only relatively short procedures were considered, whereas actual procedures are much longer. It is not entirely clear to what extent the simplification of the model can be extrapolated to longer procedures. It is therefore suggested that sensitivity analysis should be done with longer procedures. As the results obtained thus far were found with a one-and a two-dimensional analysis, it is also suggested that a multi-dimensional analysis should be done in which more than two parameters are varied.

THESIS has so far been used only for a simple case study (chapter 5) and for theoretical considerations (chapters 6 and 7). THESIS should be evaluated in actual situations, for which longer procedures exist. An HPSA of the start-up procedure of an actual plant by using THESIS will therefore be discussed in the next chapter.

Chapter 8

Application of THESIS to the start-up procedure of an experimental boiler

(a field study)

Introduction

A scheme of the approach to be followed in THESIS was introduced in chapter 4 and is shown again in Figure 28. The scheme was used in chapter 5 to show how THESIS is applied in a case with simple procedures consisting of only two steps. It appeared from this analysis that all paths of the THESIS event tree have to be considered if a correct judgement of the safest procedure is to be arrived at. In particular, an HPSA technique has to be used that considers sequences of human errors. The various consequences that are possible if sequences of human errors are made can thus be analyzed.

The question of the extent to which THESIS can be applied as an HPSA technique to analyze the longer procedures that are present in practice is now raised. The event tree can become rather large – particularly with longer procedures – which will easily make the analysis more complex. The analysis of sequences of human errors, which is one of the purposes of THESIS, may not be feasible in such a case.

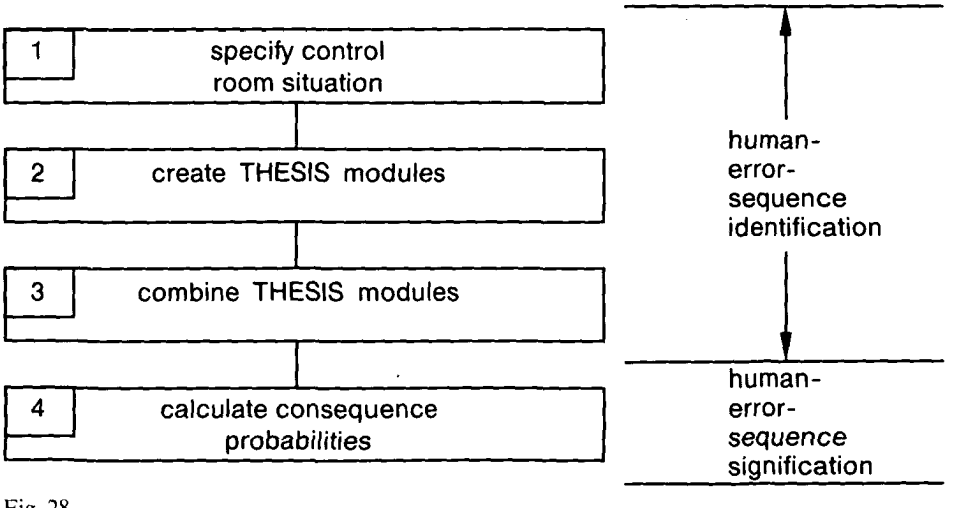


Fig. 28
General scheme of THESIS.

In order to investigate this problem, THESIS was applied to the start-up procedure of the KEMA Experimental Boiler (Willems, 1980). Most of the MRFs mentioned in chapter 4 were assumed to be present, viz. ergonomics, continuous tasks, event dependence and recovery attempts. The influence of the other MRFs, viz. procedure-selection capability, recovery dependence, HEP distributions and correlations, were not present or were ignored. As an example, the influence of recovery dependence was disregarded, as it was clear (see chapter 7) that this feature does not contribute significantly to the probability of certain outcomes and, hence, of certain consequences occurring. Only one procedure as used in the control room under analysis was studied here and the MRF procedure-selection capability was ignored. The two remaining parameters, viz. HEP distributions and correlations, were not considered, as incorporation of these parameters at this stage would not have contributed much to a better insight into the use of THESIS.

The purpose of this chapter is to describe the application of THESIS to the analysis of such a practical control-room procedure, and to investigate the importance of the MRFs just mentioned. Many pragmatic problems tend to emerge during such an analysis, so that the chapter will have a troubleshooting aspect. A summary of the problems arising during the analysis is followed by enumeration of the solutions and the criteria applied. Furthermore, the steps outlined in Figure 28 will be elaborated upon; a detailed scheme, showing the approach used with THESIS in an actual work situation, will thus be developed. The chapter is structured so as to be consistent with the scheme of Figure 28. Each block in this scheme will be dealt with in one section. The advantage to be gained from considering human-error sequences is shown in one of the last sections, by applying and comparing two types of analysis: an extended analysis in which complete human-error sequences are studied and a limited analysis in which only single human errors are considered.

Specification of the control-room situation

Several related matters must be investigated in order to specify the control-room situation: the procedure followed by the operators must be specified, the process must be studied (in particular the part that is relevant to the procedure), and the panel layout must be considered. These three aspects will be dealt with in this section.

The study of the process of the KEMA Experimental Boiler (KEB), in so far as it is relevant to the procedure, includes the process scheme presented in Figure 29. Water is circulated in a closed circuit by pump C. The water flows via a feedwater heater to a boiler, where it is heated to a mixture of steam and hot water. This mixture goes to a test section, where it is used to test several types of equipment. On leaving the test section, the mixture goes to a steam/water separator. The water goes back to the feedwater heater and reaches a collecting vessel via valve E. The steam goes to a condenser via a combination of reducing valves D and F. The latter (F) represents a series of four similar valves (F_1, F_2, F_3, F_4). From the condenser, the water goes to the collecting vessel and is then recirculated. The supply of air and gas to the boiler is regulated by means of two valves (B and G). These two valves can be regulated

directly, but can also be adjusted by control device A. The gas line contains, in addition to valve B, a lock which has two positions ('open' or 'closed'), depending on the water pressure.

The system is controlled automatically under stationary conditions, i.e. some time after the start-up procedure has been completed. This means that most valves are controlled depending on the value of the flow, the temperature and the pressure. However, most variables are controlled manually during the start-up procedure. Most control signals are therefore not shown in Figure 29.

Figures 30 through 32 represent the control-room layout. It should be kept in mind that the control room includes more equipment than shown in these figures: only the part relevant to the analysis is presented. The figures contain not only the control devices that are used if the procedure is followed correctly. The figures also contain the control devices that have a similar layout, and that might be confused with the correct devices and are thus likely to cause selection errors. The letters of the control devices correspond with the letters indicating the components of the process scheme.

The start-up procedure can be divided into three main parts:

I bringing the system to the desired pressure rate and desired flow rate;
II heating the water to the boiling point at the desired pressure and flow rates;
III forming high-pressure steam.

The procedure has been thoroughly studied in detail earlier (Van Weersch, 1986a,b,c; Gabriëls, 1987; Godding, 1987; Konings, 1987). The present study will be restricted to part II, since analysis of this part provides the best insight into the applicability of THESIS.

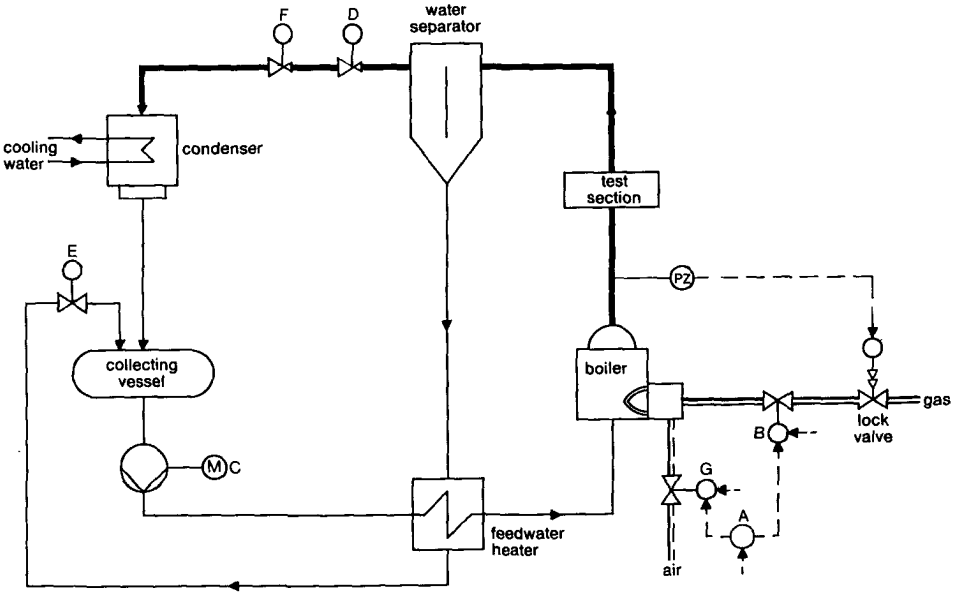


Fig. 29
Process scheme of the process analyzed. Only the components relevant for the analysis of the start-up procedure are shown.

Part II of the procedure consists of the following steps:

(1) opening valve B to a certain position, adjusting the set point of A, igniting the burner, then opening valve B completely;
(2) adjusting the set point of A as a function of the temperature increase;
(3) opening valve D, depending on the increase in pressure; steam will be formed after some time.

In order to allow this part of the procedure to be analyzed with THESIS, the procedure must be broken down into specific actions for which certain criteria must be set. Two essential factors that are relevant at this stage are:

(1) several errors that can be made in following the procedure are observable and may be recovered immediately; these steps might be omitted from the analysis;

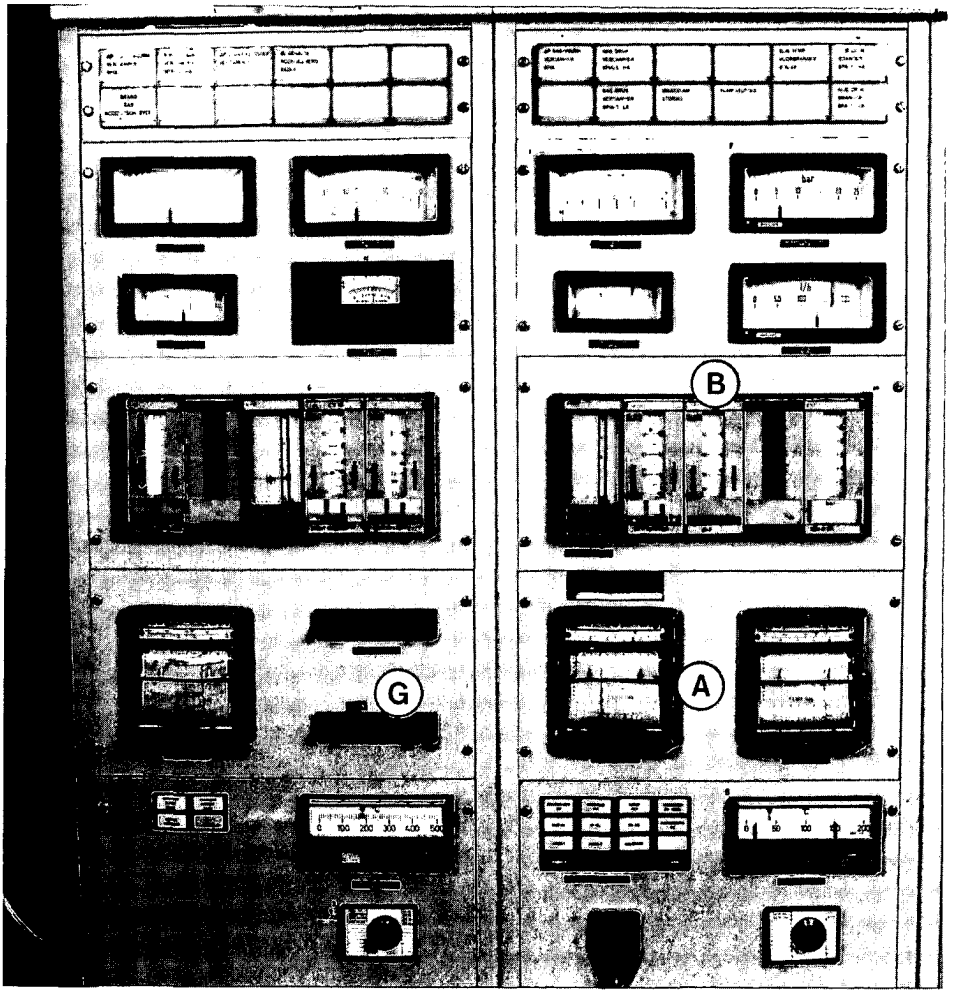


Fig. 30
Part of the control panel dealing with control of the gas/air flow (control devices A, B and G).

(2) the continuous character of the process; this makes the application of event trees more difficult, since the event-tree technique is a discrete technique.

Several criteria were applied to incorporate these two factors. It was assumed, in order to deal with the first factor, that observable and reversible errors were recovered immediately. It was assumed that control devices which had been handled incorrectly, were reset and that the procedure was restarted. Hence, a slight opening of valve B before the ignition of the burner and the ignition of the burner itself, for instance, were omitted since it became clear that errors in these activities would instantly lead to full recovery.

The second factor was dealt with by making the procedure discrete. The two steps of part II of the procedure that can be regarded as continuous are the adjustment of the set point of A (step 2) and the opening of valve D (step 3). It was assumed

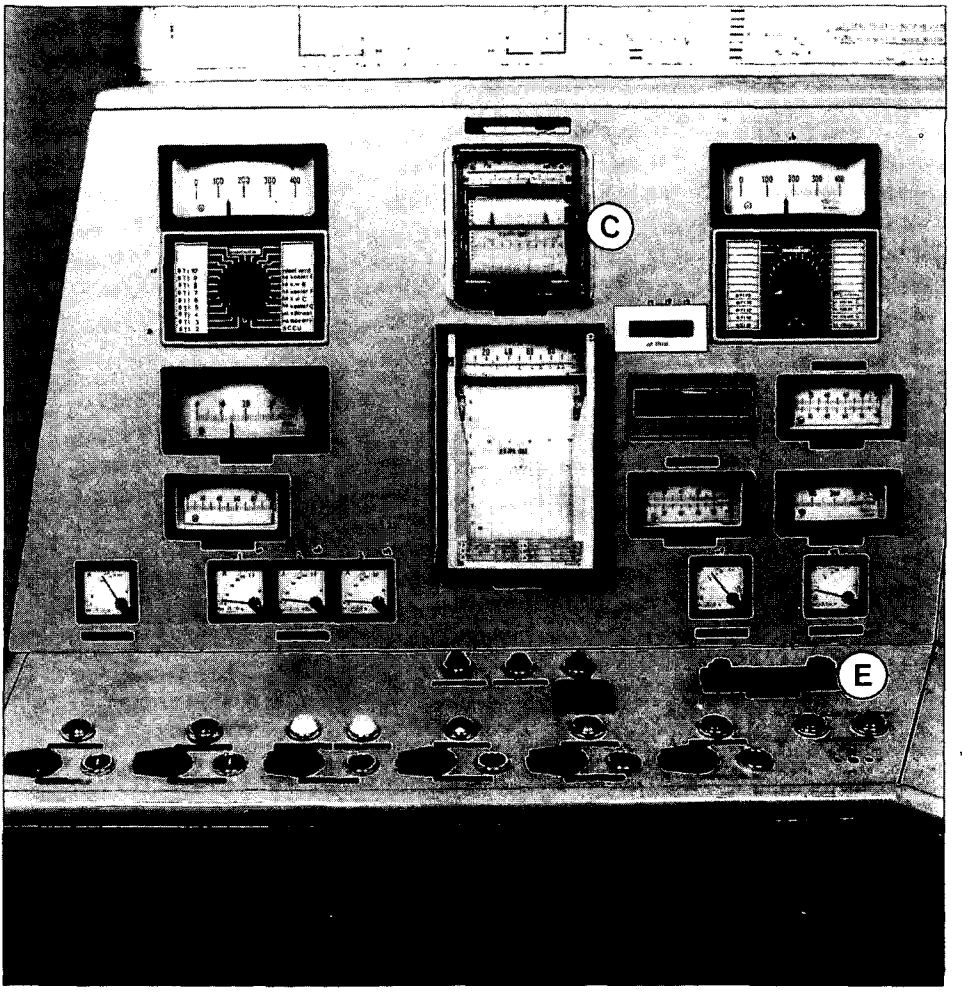


Fig. 31
Part of the control panel dealing with control of the water flow (control devices C and E).

Table 13
The procedure analyzed in the present study.

1:	adjust the set point of A to a certain value.
2:	open valve B completely.
3:	adjust the set point of A.
4:	adjust the set point of A once more.
5:	open valve D once.

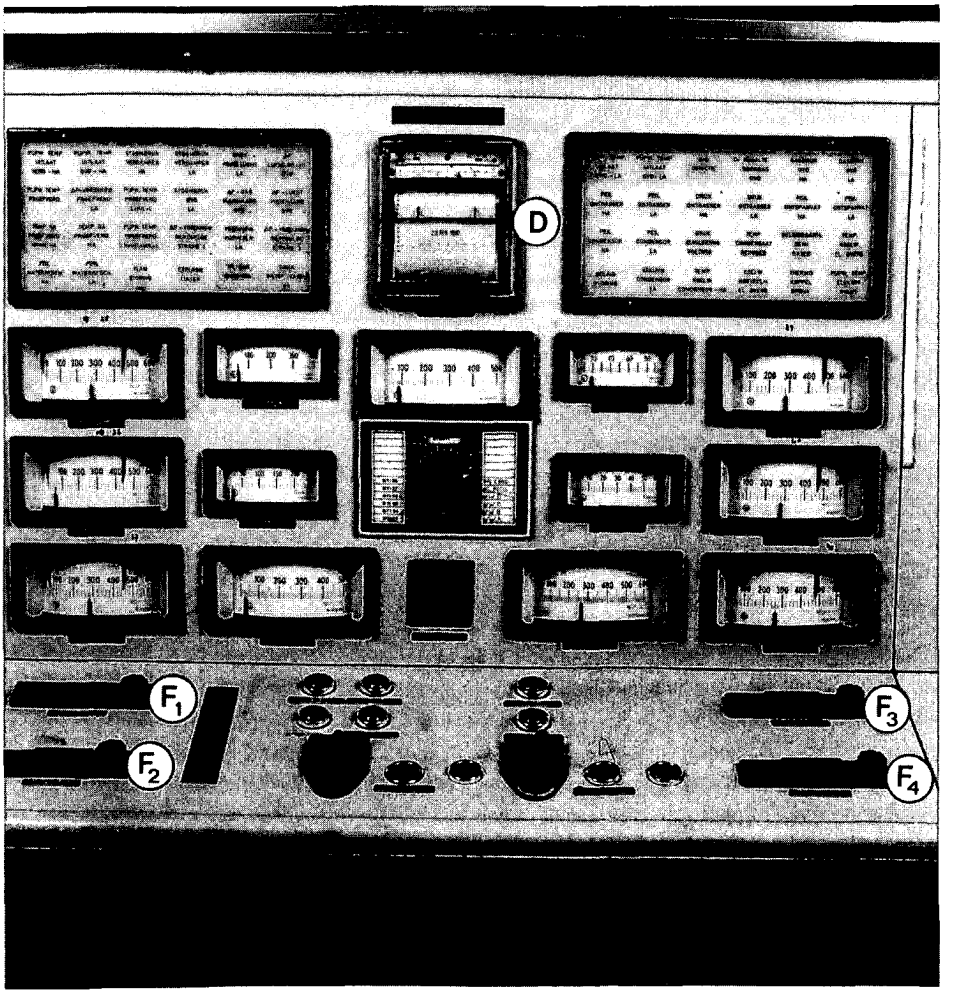


Fig. 32
Part of the control panel dealing with control of the steam flow (control devices D and F_1 through F_4).

that the continuous adjustment of the set point of A could be divided into two discrete steps. This number was regarded as sufficient to perform the analysis, although a greater number of discrete steps could perhaps be distinguished. The opening of valve D occurred only once in most cases, so that it was regarded as one discrete step.

Table 13 contains specific actions of the decomposed procedure that was constructed on the basis of the preceding criteria. In conclusion, Figure 33 summarizes the first three steps of the detailed approach followed in THESIS as presented in this section.

THESIS modules

The second general step in THESIS is the construction of THESIS modules. The specific errors that can be made must be identified so as to make THESIS modules of the specific actions indicated in Table 13. A classification was presented in chapter 2 on the basis of the following general errors: error of omission, selection error, handling error, sequence error and extraneous activity. Several problems arose during the analysis when these errors were specified for the THESIS modules of the specific actions. The three most important problems were the following.

(1) Identification of the control devices that might be selected incorrectly by the operator. It appeared that incorporation of all possible control devices makes the analysis unfeasible.
(2) Determination of the desired positions of the several control devices incorporated in the analysis. It was found that it was rather difficult to specify these positions, as the process studied was an experimental one and the starting situations were often varied.
(3) Specification of the handling errors. Handling errors are all the errors that can be made at the correctly or incorrectly selected control device. Hence, the handling error is more general than the error of omission, the selection error and the sequence error, especially at control devices that can be adjusted with a continuous step size. The handling error may differ according to the control device that is selected.

Several criteria were introduced to overcome these problems. The assumptions related to problem (1) are summarized first.

- The similarity of the control devices was used as a criterion. Control devices were regarded as potential control devices to be confused with the correct ones only if they were equal in size and shape.

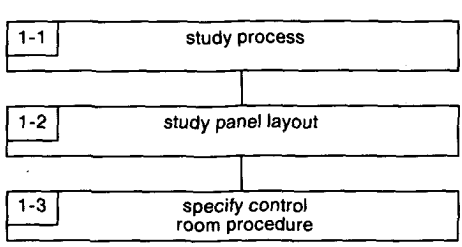


Fig. 33
Detailed description of the first block of Figure 28.

- The proximity of the similar control device was also considered. Only control devices that were within reach were incorporated in the analysis.
- Finally, the immediate consequences of selecting the incorrect control device were taken into account. If it was immediately clear that the selection of the incorrect control device was not of interest, the control device was not incorporated in the analysis.

Problem (2) was overcome by restricting the analysis to the most frequent starting situation of the process. The desired positions of the control devices related to this starting situation could thus be indicated clearly.

The following assumptions to specify the handling error were made for problem (3).

- The desired state of the selected control device and the deviations possible at the selected control device were used as a criterion. The deviations were assumed to follow an ordinal scale (Siegel, 1956); this means that the distances between any two numbers on the scale are not of known size, i.e. a value is only higher or lower than a specific value.
- With relation to the preceding point, it was assumed that a control device could be set in, at most, five different positions, viz. in the desired state, in one of the two extreme states (e.g. a valve in a 'closed' or 'open' state), in a state higher than desired (between the specified state and the extreme state), and in a state lower than desired.
- The direct consequences of handling the selected control device incorrectly were considered; a deviation was not incorporated in the analysis if it immediately became clear that this deviation had no consequences or could be lumped with another deviation.

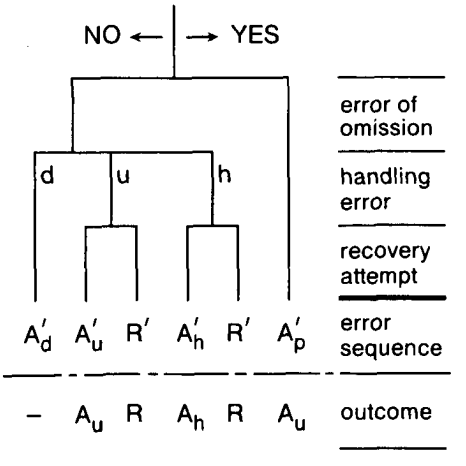


Fig. 34
THESIS module of the first step of Table 13. Both the event sequences and the outcomes are presented.

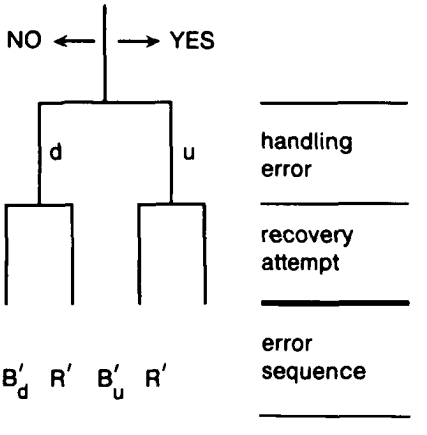


Fig. 35
THESIS module of the second step of Table 13. Only the event sequences are shown, because the outcomes can only be identified through combination with a preceding module.

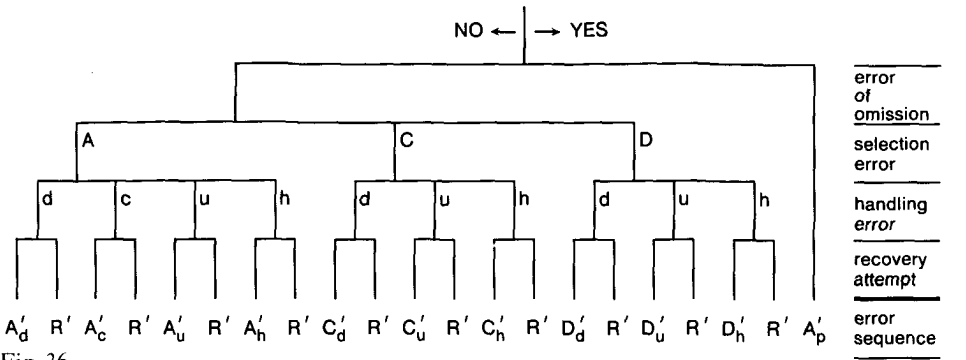


Fig. 36
THESIS module of the third step of Table 13. Only the event sequences are shown, for the same reason as in the preceding figure.

No specific criteria were set with regard to the error of omission. Extraneous activities were omitted from the analysis because incorporation at this stage appeared too difficult and would not contribute significantly to a better insight.

The THESIS modules for the specific actions were drawn on the basis of the criteria presented above. Only the modules for the first three specific actions in Table 13 are shown here (Figs. 34 through 36), as they suffice to explain the approach followed in THESIS. Each tree contains several paths where a recovery attempt is made; these paths are indicated by an R′ at the offshoot. The remaining paths are encoded as described in chapter 5: the selected control device with a capital letter corresponding with the letters in Figure 29; the position of the control device with a subscript. A maximum of six subscripts was used to symbolize the possible positions (c = the first extreme position, e.g. a motor-operated valve closed; u = under desired but higher than a first extreme; d = desired position; h = higher than desired but lower than the second extreme; o = the second extreme position, e.g. a motor-operated valve open; p = a preceding position because of an error of omission). Six subscripts appeared an adequate number with regard to the possible consequences of the positions.

As in chapter 5, a distinction is made between outcome and error sequence; the latter contains an apostrophe in the code. The outcomes are drawn only in the first module (Fig. 34), as they can be derived directly from the error sequences. The outcomes of the modules following this one (Figs. 35 and 36) can only be derived after combination with the preceding module(s), as will be shown in the next section. These modules contain a recovery attempt on the success path, as they will be coupled not only to the success path, but also to the failure paths of the preceding module.

In conclusion, Figure 37 summarizes the detailed approach followed in this section.

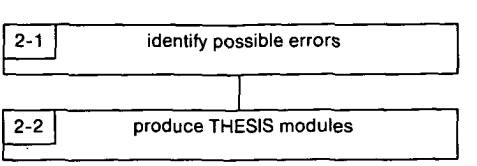


Fig. 37
Detailed description of the second block of Figure 28.

Combination of THESIS modules

The third general step in THESIS is combination of the THESIS modules. This can be done in two ways (also see chapter 5):

(1) by combining the modules into THESIS event trees,
(2) by combining the modules by means of combination matrices.

The following problems arose in the analysis of the coupling of the modules.

(1) A rather rapid increase in the number of error sequences when the modules were coupled to a complete THESIS event tree: the coupling of the modules of the procedure in Table 13 yielded a theoretical total of 2111 error sequences (success path and failure paths).
(2) Prediction of the consequences of several human-error sequences, especially when the error sequences became relatively long: as the operators were assumed to have the best knowledge of the process, they were questioned about the possible consequences. It appeared that they were often able to predict the consequences of a single human error, but not the consequences of sequences of human errors. An example is an error sequence in which, as a first error, the pump control device is selected incorrectly and the pump speed is changed so that the pressure obtained is too high; the second error in this sequence might be a change of valve D to an incorrect position so that, in contrast to the preceding error, a low pressure is obtained. The resulting consequence, a pressure increase or a pressure decrease, is often not known.
(3) The influence of one control device on several process states (Fig. 38): control device A, for instance, was meant to adjust the temperature of the water via H_1, but the pressure in the system is affected together with the temperature, via H_2.

The following method was applied to overcome these problems.

- Specify the possible consequences of human-error sequences on the basis of the consequences that may occur due to single human errors. This approach was allowed as it became clear during the analysis of the KEB process (Godding, 1987; Konings, 1987) that human-error sequences did not introduce other consequences.
- Apply block diagrams (Takahashi et al., 1972) to determine in which way the outcomes, i.e. the adjustments of control devices that could be selected, influence the consequences defined in the preceding step.
- Combine THESIS modules by applying combination matrices and merge the human-error sequences that cause the same consequence(s) into one outcome. Combination matrices were used instead of coupling of the event trees, in order to keep the analysis compact.
- Define final outcomes with which error sequences are cut off. Two outcomes were defined as detailed in chapter 5, viz. a temporary outcome – an outcome after which the analysis is continued – and a final outcome – an outcome after which the analysis is stopped.

Implementation of this method for the procedure of Table 13 leads to specification of the following consequences, classified according to the process variables:

- temperature z_1: lower than desired, as desired, higher than desired, increase too strong (leading to a thermal shock);
- flame conditions z_2: desired, undesired (leading to incomplete combustion);
- pressure z_3: much too low (leading to a shut-down), lower than desired, as desired, higher than desired (leading to the possibility of an explosion);
- flow z_4: lower than desired, as desired, higher than desired.

The block diagram of Figure 38 shows all the control devices that might be selected, correctly or incorrectly, and the possible effects they might have on the process variables. The block diagram was used to determine the possible effects qualitatively only. No attempt was made to determine the process dynamics, i.e. to obtain exact descriptions of the transfer functions (H_is) in Figure 38. Ordinal scales were used for each control device, so that an exact description was not relevant at this stage.

The modules were coupled by means of combination matrices. The first two modules of the procedure in Table 13 were first coupled. The possible outcomes were derived from this combination. The module of the third step was then combined with the preceding two, again by means of a combination matrix. This process was continued until the last step of the procedure in Table 13 was reached.

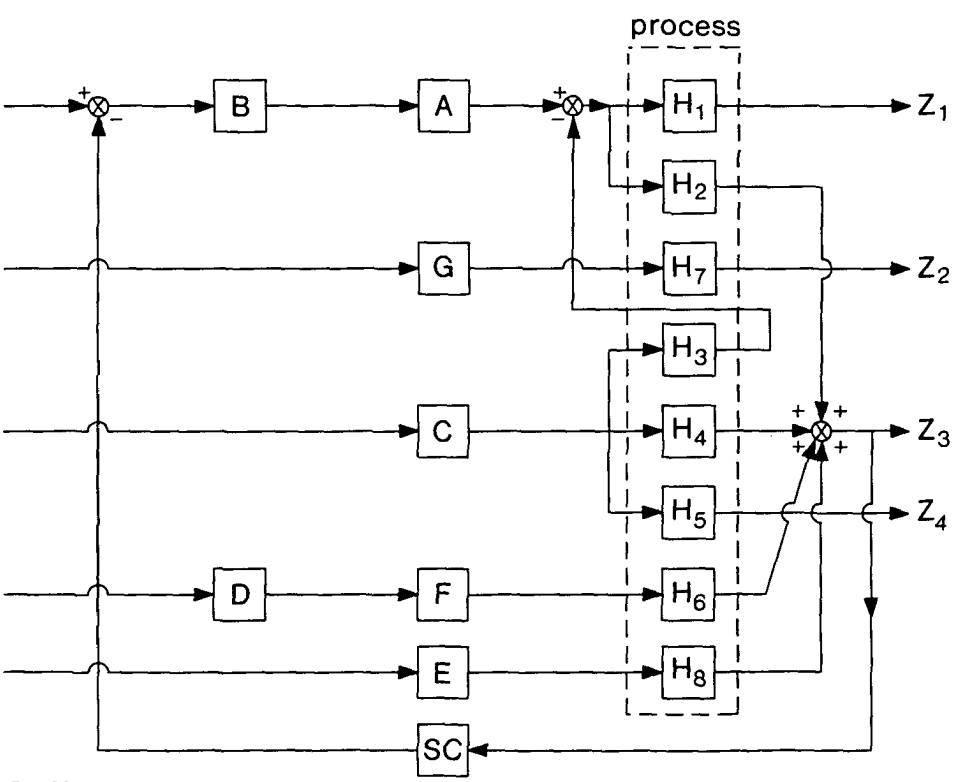


Fig. 38
Block diagram of the process that was studied. A through G indicate the control devices (F is a series of four similar control devices F_1 through F_4), H_1 through H_8 symbolize the transfer functions of the process and SC stands for a safety device.

Table 14
First combination matrix derived by combining the first two actions of the procedure of Table 13. The left column contains the temporary outcomes of the first module (Fig. 34), with the exception of the return outcome, R, since no following module can be attached to this outcome. The top row contains the event sequences of the second module (Fig. 35). The layout is similar to the one used in chapter 5.

step 2 / step 1	B_d'	B_u'	R'
–	– $-B_d'$	B_u $-B_u'$	R $-R'$
A_u	A_u A_uB_d'	B_u A_uB_u'	R A_uR'
A_h	A_h A_hB_d'	B_u A_hB_u'	R A_hR'

Two types of analysis were applied during the coupling; the definition of the final outcomes was related to the type of analysis performed.

(1) In the first type of analysis, the outcome following a single human error was regarded directly as a final outcome. This type of analysis is called 'limited analysis'.
(2) In the second type of analysis, a complete sequence of human errors was considered. An outcome was then regarded as final if it followed the last step of the procedure or if it led to an undesired consequence. Two consequences were regarded in this study as undesired: a thermal shock and a the possibility of an explosion. This type of analysis is referred to as 'extended analysis'.

The two different types of analysis were performed in order to discover the advantages and disadvantages of analyzing complete human-error sequences rather than single human errors.

Only the first two combination matrices resulting from coupling of the first three actions are presented (Tables 14 and 15), as these are considered sufficient to illustrate the THESIS principle. It appeared that the first two combination matrices are the same for the limited and the extended analysis. This is due to the fact that the limited and the extended analysis contain the same short error sequences at the beginning of the analysis.

The consequences of human errors had to be assessed in order to merge error sequences with the same consequences. This was relatively easy for the first actions of the procedure of Table 13 but the analysis became difficult for the last few actions. This was especially true for the extended analysis where the number of error sequences grew rapidly. The rule was therefore applied that the error sequences that might cause the same process state should be merged under one outcome. As noted before, an outcome is an entity that contains the most essential information regarding control-device positions, information which is needed to predict the influence on the process state, especially with regard to possible undesired consequences.

An example is the merging of the error sequences $-B_u'$, A_uB_u', A_hB_u', for which case it was assumed that the position of valve B was decisive for the value of temperature and pressure. The three error sequences cause qualitatively the same process state

Table 15
Second combination matrix derived from the coupling of action 3 of Table 13 to the preceding actions. The left column contains the temporary outcomes of the first combination matrix (A_h is regarded as a final outcome, since this might lead to a thermal shock in the third step). The R is not included in the left column for the same reason as in the preceding figure. The top row contains the event sequences of the third module (Fig. 36). The layout is similar to the one used in chapter 5.

step 3 / step 1,2	A'_d	A'_c	A'_u	A'_h	C'_d	C'_u	C'_h	D'_d	D'_u	D'_h	A'_p	R'
–	–	A_c	A_u	A_h	A_u	A_uC_u	A_uC_h	A_u	A_uD_u	A_uD_h	A_u	R
	$-A'_d$	$-A'_c$	$-A'_u$	$-A'_h$	$-C'_d$	$-C'_u$	$-C'_h$	$-D'_d$	$-D'_u$	$-D'_h$	$-A'_p$	$-R'$
A_u	A_h	A_c	A_u	A_h	A_u	A_uC_u	A_uC_h	A_u	A_uD_u	A_uD_h	A_u	R
	$A_uA'_d$	$A_uA'_c$	$A_uA'_u$	$A_uA'_h$	$A_uC'_d$	$A_uC'_u$	$A_uC'_h$	$A_uD'_d$	$A_uD'_u$	$A_uD'_h$	$A_uA'_p$	A_uR'
B_u	B_u	A_c	B_uA_u	B_u	B_u	B_uC_u	B_uC_h	B_u	B_uD_u	B_uD_h	B_u	R
	$B_uA'_d$	$B_uA'_c$	$B_uA'_u$	$B_uA'_h$	$B_uC'_d$	$B_uC'_u$	$B_uC'_h$	$B_uD'_d$	$B_uD'_u$	$B_uD'_h$	$B_uA'_p$	B_uR'

because of the position 'under desired' of valve B: the consequence is that temperature and pressure are both lower than desired. Hence, the error sequences are joined under the outcome with symbol B_u; this outcome forms the start of the final row in Table 15.

Table 16 presents the results of the qualitative analysis of this section for both the limited and the extended analysis. The first and second columns show the number of error sequences resulting from coupling of the THESIS modules of the actions in Table 13. This number equals the number of cells per combination matrix, e.g. nine error sequences in the first row since Table 14 contains nine cells.

Columns 3 and 4 contain the number of outcomes per combination matrix. This number is the sum of the number of types of final outcomes, temporary outcomes and the return outcome. For example, there are five outcomes according to Table 14 for the first combination: three temporary outcomes (the outcome –, the outcome

Table 16
The results of the qualitative analysis of the coupling of the THESIS modules of the specific actions in Table 13 to the THESIS module of the preceding action, for both the limited and the extended analysis.

specific-action number in Table 13	number of error sequences in the combination matrix		number of outcomes in the combination matrix		percentages of the outcomes with known process state	
	limited analysis	extended analysis	limited analysis	extended analysis	limited analysis	extended analysis
action 2	9	9	5	5	100	100
action 3	36	36	15	15	36	36
action 4	36	144	15	28	36	22
action 5	39	288	10	18	56	29

A_u and the outcome B_u), one final outcome (the outcome A_h) and the return outcome (the outcome R).

As indicated, the influence of certain outcomes on the process state cannot always be predicted. Columns 5 and 6 show the percentages of outcomes of which the process state can still be foreseen. The percentages include only the temporary and the final outcomes; the return outcome is not included in the calculation of the percentages since this would lead to an unrealistically lower value. The percentage reaches a value of 100 for the first combination (Table 14), since the effect of each outcome on the process state is known: outcomes A_u and B_u lead to a situation with pressure and temperature lower than desired, and to flow/flame conditions that are desired; outcome A_h leads to a thermal shock; and the outcome – leads to the desired situation.

The percentage is less than 100 for the other combinations because of the unknown effects of certain outcomes on the process state. An example is given by outcome A_uC_h (cells 1,7 and 2,7 in the matrix of Table 15). The consequence regarding the temperature is clear: A_u indicates that the temperature will be lower than desired. The consequence regarding the pressure is, however, unclear: A_u indicates a pressure lower than desired because of a temperature lower than desired, but C_h indicates the opposite. The combined effect on the pressure is unclear: the pressure might be lower than desired, as desired, or higher than desired.

Table 16 shows that the number of error sequences grows rapidly with the number of actions for the extended analysis. It also shows that the number of outcomes is greater for the extended analysis. The percentages of outcomes with a known process state are lower for the extended analysis since the process state is less easy to predict for sequences of human errors than for single human errors.

It appears that the number of outcomes decreases at the last action for both the limited and the extended analysis. The last action causes many error sequences that have an unknown effect on the process state. As these error sequences can be merged into one outcome, there are relatively fewer outcomes at the last action compared to the preceding one. The merging of the error sequences with an unknown effect also influences the last two columns. Since there remain relatively more outcomes with a known effect, the percentage of outcomes with a known effect on the process state increases at the last action for both the limited and the extended analyses.

The detailed approach followed in this section is summarized in Figure 39.

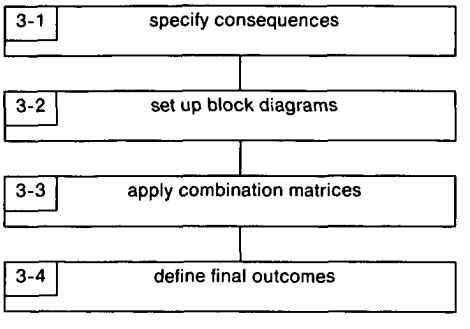


Fig. 39
Detailed description of the third block of Figure 28.

Calculation of consequence probabilities

The PREQUANT program was used to calculate the probabilities of the consequences. This program was described and applied in chapter 5. Contrary to the case study described then, recovery attempts were now included in the calculation of the consequence probabilities. This was achieved by incorporating Equation (26). This equation was derived in chapter 7, under conditions of no recovery dependence. Recovery dependence might, however, be present for the start-up procedure of the KEB. It was nevertheless shown in the sensitivity analysis of chapter 7 that, under certain conditions, the equation might also be valid when recovery dependence is present. Although the results were derived under certain conditions for procedures containing one, two or three specific actions, it was assumed for the following reasons that the formula could also be used for the procedure in Table 13:

- the goal was to perform a comparative study to determine the advantage to be gained from analyzing complete error sequences rather than single human errors;
- calculation of the consequence probabilities should be kept simple;
- the actual conditions at the start-up procedure of the KEB were not known and several MRF parameters were given therefore values corresponding with the values used in chapter 7.

The following three important problems arose when the consequence probabilities were calculated.

(1) The need to assess the probability of human errors and the recovery-attempt probability, as well as the value for event dependence.

(2) PREQUANT only calculates the outcome probabilities. The consequence probabilities are known at once for a one-to-one relationship between the final outcomes and the consequences (chapter 5). However, a one-to-one relationship between final outcome and consequence is not common. How unclear the effect of an outcome on a process state can be was already explained in the preceding section. Hence, the consequence probabilities are some function of the outcome probabilities and this function cannot be quantified, because the positions of the control devices are only defined qualitatively due to the use of an ordinal scale.

(3) Certain consequences may alert the operator, so that recovery can take place. An example is that, if the pressure drops too low, a safety device shuts down the KEB. This will be noticed immediately by the operator and the procedure will consequently be restarted. This sort of recovery is not included in the recovery attempt.

Generic HEPs were applied for the probabilities of the various events in order to meet the first problem. Taking the conditions under which Equation 26 was derived into account, the HEPs for errors that are not dependent upon other errors were assumed to be rather low: 0.01 for an error of omission, 0.001 for a selection error and 0.002 for a handling error; the recovery-attempt probability was assumed to be 0.5. The HEP for an event that depends on another one was assumed to be 0.5, as this value came close to the operating value in the sensitivity analysis; the corresponding oper-

Table 17
Top: the probabilities of the human errors and the recovery attempts applied.
Bottom: the probabilities of the consequences found by means of the extended and the limited analysis.

error of omission	0.01	
selection error	0.001	
handling error	0.002	(no event dependence)
	0.5	(event dependence)
recovery attempt	0.5	
probability of the possibility of an explosion	0.018	(extended analysis)
	0.024	(limited analysis)
probability of thermal shock	0.012	(extended analysis)
	0.011	(limited analysis)

ating value for α was 0.5 and substitution of this value in Equation 3 results in a HEP close to 0.5.

The second problem was overcome by applying the rule that each outcome probability is uniformly distributed over the probabilities of the possible consequences following a certain process variable. Outcome A_uC_h which, as mentioned above, may cause three consequences with regard to the pressure, viz. lower than desired, as desired, and higher than desired, is an example. The consequence probability of the pressure being lower than desired is then one third of the outcome probability. The consequence of the pressure being as desired is also one third of the outcome probability and the same holds for the pressure being higher than desired.

Equation 26 was used again for solving the third problem. The consequences that would definitely lead to a restart of the procedure were regarded as return outcomes. Their probabilities were incorporated in Equation 26 as the return probability. The conditions under which this equation could be used were again assumed to be present.

Table 17 contains the probabilities used for the HEPs as well as the probabilities of the consequences calculated. Only the two consequences that appeared to be highly undesirable, viz. a possibility of an explosion and a thermal shock, are presented. The results of both the limited analysis and the extended analysis are shown.

The steps that were performed to quantify the consequence probabilities are summarized in Figure 40.

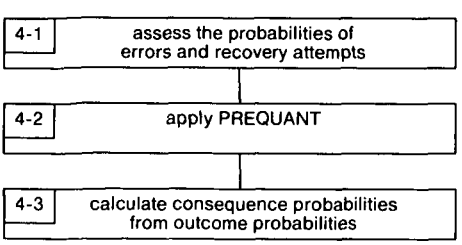


Fig. 40
Detailed description of the fourth block of Figure 28.

Discussion

The method employed and the two types of analysis performed will be discussed here. This is followed by some conclusions concerning the applicability of THESIS and some suggestions to utilize THESIS.

The approach followed in THESIS – Combination of the diagrams of Figures 33, 37, 39 and 40 results in a detailed scheme of the approach followed in THESIS (Fig. 41). The most important part of THESIS is the identification part (human-error-sequence identification). The identification involves the prediction of the type of human errors that may occur and their consequences. Decisions at the start of the identification are very important, since omitting possible errors implies no further analysis of these errors in terms of their consequences. Hence, incorrect decisions at this stage can have an important effect on the final results. The process and the related panel layout, as well as the procedure to be followed, must be studied extensively for an adequate analysis, and this makes the analysis very time-consuming.

Two types of analysis were performed: a limited analysis in which single human errors were considered, and an extended analysis in which sequences of human errors were studied. It was the first time that such an extended analysis was performed and the work was indeed very time-consuming. The extended analysis required a few months, which was approximately eight-fold more than the time required for the limited analysis. The combination matrix grew from 9 to 288 cells for the extended analysis, whereas it finally contained only 36 cells for the limited analysis. It appeared that THESIS was less easily applicable as the procedure became longer, particularly for the extended analysis. THESIS was easier to apply if short human-error sequences were considered.

While the extended analysis may turn out to be time-consuming, it has the important advantage that it provides all possible error sequences and outcomes leading to the consequences identified. According to Table 16, it appeared that eighteen outcomes were possible in the last combination matrix of the extended analysis; as the combination matrix of the limited analysis contained only ten outcomes for the last action, eight of the eighteen outcomes, i.e. 44%, could not be discovered by means of the limited analysis. It should be noted in this context that the consequences identified were the same for both analyses; the possible consequences were based on the consequences that would occur as a result of single human errors (section on the 'combination of THESIS modules'). Although the use of this simpler approach was allowable here, its use may not be generally permissible and a thorough analysis of the consequences of sequences of human errors will be needed.

It became difficult to predict the influences of certain error sequences on the process state as the analyses proceeded. At the last step of the procedure, 56% (Table 16) could be predicted by means of the limited analysis and 29% with the extended analysis. Two reasons can be given for these rather low numbers. First, there was a tight coupling between several control devices and the process variables. Pressure, as an example of a process variable, was influenced by all control devices (Fig. 38). This made the

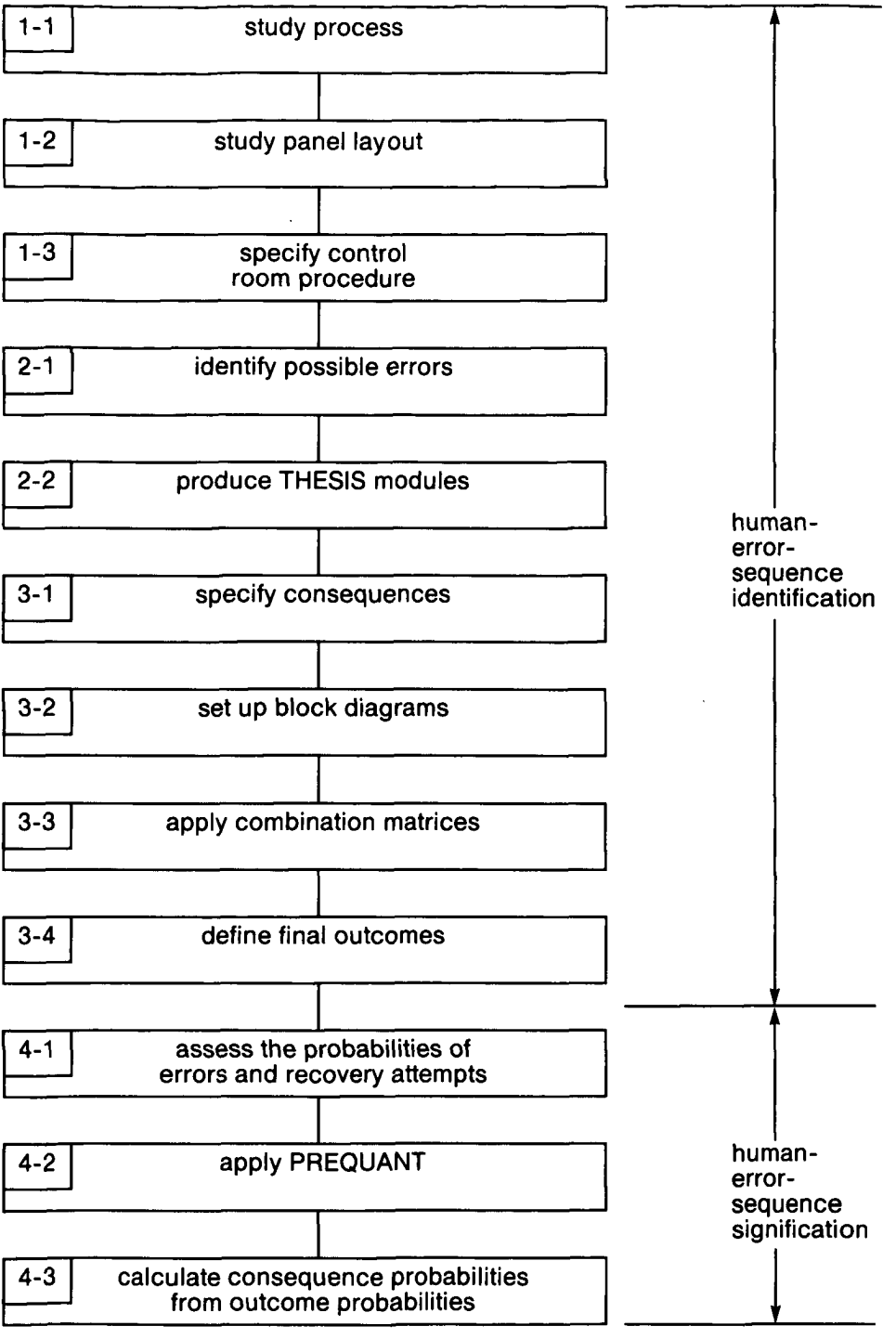


Fig. 41
Detailed scheme of THESIS.

prediction of the course of certain process variables difficult. The second reason is directly related to the former one: an ordinal scale was used for the positions of the control devices. This was done to keep the analysis compact enough that a maximum of five positions per control device had to be analyzed. Analysis of the first steps of the procedure with these scales presented no problem. However, the prediction of the process state became more difficult as the analysis proceeded. Hence, the application of THESIS apparently depended largely on the interaction between control devices and process variables, and on the division of the scales into discrete parts.

A ratio scale (Siegel, 1956) instead of an ordinal scale might have been used in which distances between any two numbers on the scale are of known size and in which a pre-defined 'zero point' is included. Had the continuous scale of the control devices then been divided into a larger number of discrete intervals, the prediction of process states would certainly have been easier. Because of the larger number of control-device positions that would then have emerged, the analysis, particularly the extended one, would, however, have become far too complex and time-consuming. Moreover, the analysis would have been enlarged by the fact that the time-dependent procedural steps of the procedure should then have been divided into an increasing number of specific actions. An example is the adjustment of the set point of A as a function of time. This adjustment was divided roughly into two specific actions, viz. actions 3 and 4 of Table 13. Such a rough division led to no problems for the application of THESIS. A more detailed analysis, in which the scales are divided into a large number of discrete intervals, would require a more detailed division of the procedural steps into discrete specific actions, thus increasing the length of the procedure to be analyzed. This would make the application of THESIS more extensive.

A computer program for human-error signification, i.e. PREQUANT, was used to quantify the consequence probabilities. Generic probabilities were applied as input for PREQUANT. Somewhat different HEPs may be present in practice because of the influence of the performance-shaping factors (Table 3) and the influence of event dependence. As noted in the preceding chapter, event dependence might have a great influence on the quantification. The purpose of the present chapter was, however, not to quantify the consequence probabilities exactly, but to show how THESIS can be applied, and to compare two different types of analysis. Hence, the estimates of the parameters, in particular the 0.5 for event dependence, were not essential at this stage.

The results of the 'signification' gave the probabilities of the undesired consequences, viz. thermal shock and possibility of an explosion. There appeared to be no important difference between the results of the limited analysis and of the extended analysis. Hence, the extended analysis appeared not to present a true advantage over the limited analysis when the probabilities of certain undesired consequences are to be considered. In other words, the conclusion for this case must be that the limited analysis, in which only single human errors are considered, is to be preferred if one is only interested in the probabilities of consequences of incorrect human behavior.

The disadvantage of the limited analysis, however, is that it does not show all possible error sequences and outcomes. If one is interested not only in the consequence

probabilities, but also in the paths leading to these consequences – so that one is able to make correct decisions about optimum man-machine designs – the extended analysis, showing all possible human-error sequences, is to be preferred. The advantages of an extended analysis have been shown in chapter 5 with regard to the selection of the best procedure. The choice depends largely on the results in which the analyst is interested and the time and facilities available. These items direct the cut-off rule that is applied in THESIS to settle the length of the human-error sequences to be studied.

A relatively short procedure was now analyzed but a much longer procedure, containing some thirty specific actions, was actually analyzed in the study. A procedure often contains certain junctions implying no return to the procedural part before this junction, because of irreversible process states. Such a procedure can therefore be divided into certain sub-procedures, thus making the analysis of the total procedure somewhat easier. This characteristic of the procedure implies that, in principle, THESIS is applicable to much longer procedures.

Conclusions – The following conclusions can be drawn about the value and the applicability of THESIS, on the basis of the results discussed.

(1) The value of THESIS lies in its capability to predict the majority of all possible human-error sequences. With regard to the study of complete human-error sequences it appeared that:
   (a) 44% more outcomes were discovered, as opposed to an application in which only single human errors were considered;
   (b) not many differences were found in the present study between the probabilities of certain undesired consequences compared with an analysis in which only single human errors were considered.

(2) The applicability of THESIS is largely influenced by:
   (a) the length of the human-error sequences that are considered, because studying complete human-error sequences is a very time-consuming task;
   (b) the continuity of the tasks, since this can complicate the identification of the specific actions of the procedure;
   (c) the coupling between control devices and the several process variables, since predicting the effect of certain outcomes on the process state becomes difficult if there is a great deal of interaction;
   (d) the character of the procedure concerning the existence of junctions which divide the procedure into units to be analyzed separately.

In general, it appeared that this first application of THESIS to the analysis of complete sequences of human errors had in quantitative terms almost the same value as the analysis of single human errors. Applicability was lower, however, and it took significantly more time to study the complete error sequences and the process dynamics involved. The analysis of complete human-error sequences nevertheless had qualitatively more value, because it provided a better insight into man-machine interactions, as is needed for an optimum design.

Suggestions for further applications of THESIS – It should be kept in mind that the study described in this chapter was a pure research project. The aim was to determine whether THESIS could be used as an HPSA technique to predict the paths leading to undesired consequences that could be regarded as initiating events. A KEB was selected and the operators were asked to cooperate and to predict consequences of the sequences of human errors revealed with THESIS. As most human-error sequences had not yet occurred, the operators were often of the opinion that most of these sequences could not occur. Prediction of the consequences then became difficult in most cases. The results might be different if THESIS were to be applied in a practical situation in response to the order from a client. It is recommended that THESIS be further investigated for application in such a context.

As noted earlier, a more detailed analysis in which more than a maximum of five positions are distinguished per control-device scale might yield better results. Identification of human-error sequences, however, would certainly become very complex. Hence, a computer should be used to complete the identification part of Figure 41 to make it possible to perform a better qualitative analysis of consequences following sequences of human errors. This should be coupled with the acquisition of the dynamics of the process (to obtain information about the H_i,s in Figure 38). This acquisition could be performed by simulation of the process. The computer program DYLAM described in chapter 3 might be a useful tool for the performance of such a part of THESIS. Procedures much longer than the one analyzed in this study might thus be investigated. It is therefore suggested to investigate the possible advantages of DYLAM.

Chapter 9

Variability in human performance

Introduction

Errors in human performance have been quantified so far by means of average HEPs. As mentioned in chapter 4, one of the MRFs that might affect human-performance safety calculations is the variability in human performance. The result of this variability is that the HEPs applied are subject to some degree of uncertainty. This means that distributions instead of point values are present. Little is known about the shape of these distributions but it is usually assumed that they are log-normal (a.o. Swain & Guttmann, 1983). The distribution of HEPs, however, is only occasionally measured. To the author's knowledge only Klemmer & Lockhead (1962) have performed extended measurements to obtain human-error distributions. The distributions they obtained seemed log-normal but the authors did not qualify this.

It has also been noted that, other than the distributions of HEPs, little is known about the correlations between HEPs. A correlation shows how far the HEP of a particular person for one task is consistent with the HEP of the same person for another task. As correlations influence the probability of combined errors, they can also affect the calculations of human-performance safety. It is therefore important to know not only the shape of the distribution, but also the correlations.

This chapter has a twofold aim. First, the correctness of the log-normal assumption for the distributions of HEPs with respect to operator tasks in complex installations will be investigated. Secondly, some insight will be sought concerning the consistency between these human errors, expressed as correlations. Data concerning these distributions and correlations obviously should be obtained in a real, work situation, e.g. in the control room of a complex installation. Representative results can thus be obtained.

Unfortunately, this approach presents various problems (Heslinga, 1985a,b). First, there are often low HEPs in complex installations. This means that measurements must continue for a very long period if reliable data are to be obtained (e.g. for nuclear power plants, one would have to think in terms of decades). Secondly, in order to obtain a distribution, the HEPs of several persons should be measured. However, in practice it may be difficult to gather individual data on human errors and particularly on the number of opportunities to make errors over a longer period of time.

To overcome these problems, a laboratory experiment was set up in cooperation with Wijlhuizen (1986). Participants in this experiment had to perform, one individual at a time, a variety of procedural tasks within a specified period of time. This experiment is described here and the experimental results are analyzed. The analysis focuses on the determination of whether the acquired distributions are log-normal and on the strength of the correlations between the human errors made in the experiment. Group differences are also analyzed as different groups have participated in the experiment.

Method

The experiment was set up in such a way that the actions a participant, termed the 'subject', was to perform, should resemble the procedure in a control room as closely as possible. On the basis of a given code, the subject was to find a meter on a panel and then to read this meter.

Procedure and apparatus – The subjects had available an Apple 2E monochrome monitor and a keyboard (Fig. 42). The procedure involved the following steps:

(1) to read out a four-letter code from the monitor and to try to remember this 'stimulus';
(2) to read out four two-letter codes from the monitor, one after the other; this 'interference task' only served to make it more difficult to remember the stimulus;
(3) to recognize the stimulus among other codes on the monitor and to read out the code recognized; the subject was to recognize the first part of the stimulus in the first column, and the second part of the stimulus in the second column; if the code to be recognized was not present, the N-button (non-presence button) on the keyboard was to be pressed, thus stopping the procedure; the subject was then shown a new stimulus.

Actions 1-3 were called the 'recognition task'; an example with a stimulus is given in Figure 42.

(4) Next, the recognized code was to be applied to find one particular meter on the panel, which contained nine meters. The code that the subject had recognized and read out in the recognition task, whether right or wrong, served as the basis for finding this meter. The first pair from the recognition task marked the rows of a 3x3 matrix and the second pair marked the columns. The matching number was to be entered on the keyboard. Step no. 4 was called the 'search task' (Fig. 42).
(5) Finally, the meter was presented on the monitor. The subject had to check whether the double bar was between the two single ones or not. In the first case the BI-button (from the Dutch word 'binnen', meaning inside) was to be pressed; in the second case the BU-button (from the Dutch word 'buiten', meaning outside) was to be pressed. In addition to pressing a button, the subject had to read out the meter indication. Step no. 5 was called the 'reading task' (Fig. 42).

Together steps no. 1 through 5 formed a 'trial'. The basic position for the participant's

hand in steps no. 4 and 5 was the 0-button. As soon as the image (the matrix or the meter) disappeared, the subject was to move his hand to the selected button as fast as possible. It was important that the 0-button be pressed before presentation of the matrix in step no. 4 or of the meter in step no. 5 (Fig. 42). Moreover, the subject was not to release this button before either the matrix or the meter disappeared. If these two requirements were not met, an error message would appear on the monitor followed by the start of the next trial. An alarm would sound if the subject reacted too late.

A tape recorder was used to make a recording of the verbal responses. Information on the buttons pressed, as well as reaction times and error signals were stored on floppy disk.

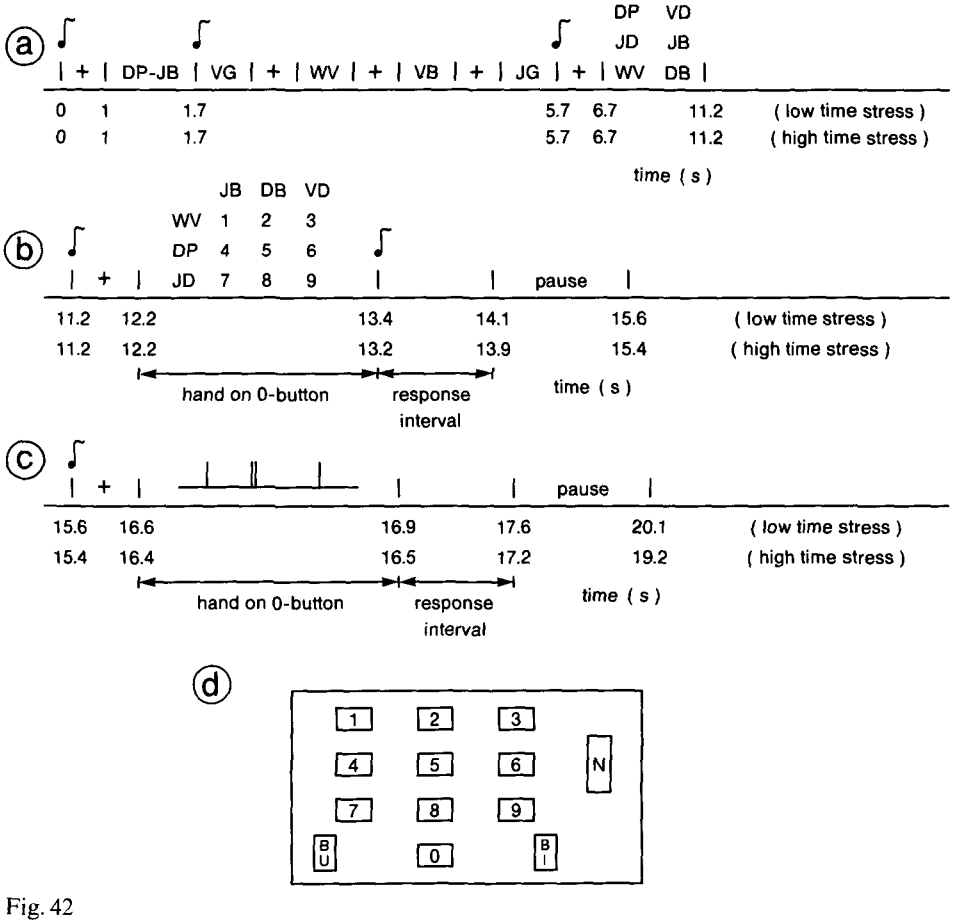


Fig. 42
Set-up for the experiment.
a = recognition task (example); b = search task (example); c = reading task (example); d = keyboard.
The information given between two vertical bars in a, b, and c is shown, in succession, on a monitor. ∫ represents a sound signal. The '+' sign is shown briefly to announce new information. The two time conditions used can be found on the time axis.

Materials – Two types of letters were used that had different sound characteristics. It appears from studies by, among others, Conrad (1964), Wickelgren (1965) and Chechile (1977) that sound plays an essential role when it comes to remembering letters for a short period of time. Recognition errors and recall errors appear more frequently with stimuli consisting of letters which are very similar acoustically. In contrast to recognition errors, no alternatives are presented in the case of recall errors. A study by Wickelgren (1966a) showed that use of an interference task with interference letters that are very similar in sound to the stimulus, results in the stimulus being forgotten sooner than when the letters sound different. It follows from another study by Wickelgren (1966b) that recognition errors will occur sooner when an alternative is presented which is similar in sound to the stimulus.

Four groups of letters were composed on the basis of these findings. The composition of the groups was adapted to the Dutch language as this was the language in which the experiment took place. The groups are presented in Table 18. The letter pairs were constructed from two letters of one group with the following restrictions:

(1) the stimulus consisted of 2x2 letters: the row and the column indication for the matrix – the effect of interference is maximal with 2x2 letters without the limit of the memory capacity being approached too closely; the capacity of short-term memory is sufficient to contain approximately seven elements if these are observed as independent units (Miller, 1956);
(2) a letter pair did not consist of identical letters;
(3) the letter pairs in the stimulus had to differ from each other by at least one letter;
(4) in the recognition task, no column could contain two identical letter pairs so that there would be only one correct response when the matrix was dealt with.

Design – Two independent variables were used to influence the average HEP per task, viz. 'acoustic confusion' and 'time stress'. Acoustic confusion only played a part in the recognition task whereas time stress only influenced the search and reading tasks.

Two experimental conditions were applied with regard to acoustic confusion: the high-confusion condition, in which the code representation was influenced as much as possible by acoustic similarity, and the low-confusion condition, in which the code representation was influenced as little as possible. Two distributions were thus obtained for the recognition task. The conditions were achieved by forming letter pairs from the four groups of letters presented in Table 18.

Table 18
The four groups of letters from which the letter pairs were formed. The letters K, C, E, G and T have not been included. In groups 1 and 2 the letters have a similar sound in the Dutch language; the letters in groups 3 and 4 differ in their sound.

group 1	group 2	group 3	group 4
B	F	X	Q
D	L	U	O
P	M	I	Y
V	N	Y	H
W	R	O	X
J	S	A	Z

All stimuli for the high-confusion condition as well as the alternatives presented in the matrix were taken from group 1 or 2. More specifically, presentations were taken that included either elements from group 1 only or elements from group 2 only. Both groups appeared with the same frequency. The stimuli and the alternatives in the matrix for the low-confusion condition were taken from groups 3 and 4. The interference-task presentations were an exception. Each pair for the interference-task presentation consisted of elements from group 1 or 2. For each trial, two letter pairs for the interference task were made up of letters from group 1 and two letter pairs from group 2.

The second variable, time stress, was obtained by varying the presentation time of the matrix (in the search task) and of the meter (in the reading task). It was assumed that the number of errors in the search task and reading task would increase within certain limits when the presentation time of the matrix or the meter decreased. A 'trade-off' between speed and accuracy takes place (Pew, 1969).

Two time conditions were applied for both the search task and the reading task: the low time stress (long presentation time) and the high time stress (short presentation time). By applying these two different times per task, two distributions were obtained for one task. When the presentation time is long, the distributions occur at a relatively low average HEP and the opposite happens when the presentation time is short.

The determination of both presentation times, i.e. the calibration, was done with the assistance of three subjects. The criterion for calibration was that the error frequency should be less than 20% for both presentation times. Also, there had to be a clear difference between the number of errors made in the short and in the long presentations. This method resulted in the matrix being on the monitor for 1 second for the short presentation, and a search time of 1.2 seconds for the long presentation. The response time allowed was equal for both conditions: 0.7 seconds. The times for the meter were: short presentation, 0.1 seconds and long presentation, 0.3 seconds. The response time permitted was 0.7 seconds for both conditions, as with the matrix.

The subjects were forced to react quickly by the disappearance of the matrix and meter from the monitor when search and reading times had elapsed. Limiting the response time also prevented the subjects from delaying their reactions, which might have led to a substantial overlap in response times under both conditions.

The experiment started with showing of written instructions for about ten minutes. The instructor and the subject subsequently went through the instructions once more together. Next, a number of demonstration trials appeared at a very slow speed. The number varied from six to twelve, depending on whether the subject understood the experiment or not. Seven sessions as described in Table 19 then took place. There was a coffee or tea break of about a quarter of an hour between experimental session no. 2 and training session no. 3. The experiment lasted about 2.5 to 3 hours with each subject.

The variable acoustic confusion was varied within each session, the high- and low-confusion conditions occurring equally frequently but in a random order. The variable time stress was varied between the sessions as shown in Table 19.

The letter pairs in the recognition task, the position of the meter in the matrix,

Table 19
The seven sessions (three training sessions and four experimental sessions) shown in the order in which they took place during the experiment.

number of trials	time (minutes)	experimental condition		session
		acoustic confusion	time stress	
20	13	high, low	very low	training session no. 1
20	10	high, low	low	training session no. 2
50	20	high, low	low	experim. session no. 1
50	20	high, low	low	experim. session no. 2
20	10	high, low	high	training session no. 3
50	20	high, low	high	experim. session no. 3
50	20	high, low	high	experim. session no. 4

and the meter indication had been fixed randomly in advance for the entire experiment. It was arranged that each matrix number in the search task and the meter indication in the reading task would occur in equal numbers. Moreover, it was arranged that the stimulus would be absent in one trial out of ten so that the N-button had to be pressed in 10% of the cases. This was done to avoid bias with respect to pressing the N-button, because ten responses were possible in the recognition task (nine responses due to nine possible codes plus one response due to the code not being present). The experiment was identical for all subjects since all presentations had been set in advance and were read out and presented in a fixed order during the experiment.

Subjects — Two groups participated in the experiment. All subjects had normal hearing and were native Dutch speakers. The first group consisted of fifty students (fifty-three minus the three used for the calibration) from the Delft University of Technology. The fifty subjects were paid for their participation and the three best, with the lowest average HEP, received a bonus. The second group consisted of eighteen operators (both skilled and in training) of a power station. They participated during working hours and received no extra pay.

Results

Processing of the results — All the tapes of the four experimental sessions were listened to a second time so as to check the errors in the recognition task as well as the errors in the verbal response in the reading task. The various counts were then made to determine the HEP per subject for a number of error types. The HEP per subject was determined for each error type by dividing the number of incorrect responses, or the number of 'too late reactions' in a particular task, by the number of times the task in question had to be carried out. The latter is termed the 'number of opportunities'. The number of opportunities could vary per task and per subject as the N-button was pressed; variations in the number of opportunities could also occur if the subject did not press the 0-button or released it too soon.

Table 20
The error types analyzed, classified according to the experimental conditions.

error type	experimental condition
recognition error	low confusion
	high confusion
error in search task	low time stress
	high time stress
error in reading task	low time stress
	high time stress
too late in search task	low time stress
	high time stress
too late in reading task	low time stress
	high time stress

The HEP appeared to be too low to allow further analysis for several error types. The error types included in the analysis are presented in Table 20 in which a distinction is made between the experimental conditions. The results were analyzed by means of the computer program SPSS-X, an extended software package that can be used for statistical analysis of data (Norusis, 1983).

Table 21
Mean values and standard deviations for the HEPs of the operator group and the student group; the P-value of the Mann-Whitney test is also given.

	mean value		standard deviation		P-value
error type	operators	students	operators	students	
recognition error low confusion	0.102	0.041	0.090	0.048	0.00
recognition error high confusion	0.238	0.126	0.099	0.069	0.00
error in search task low time stress	0.160	0.079	0.091	0.083	0.00
error in search task high time stress	0.228	0.146	0.195	0.104	0.17
error in reading task low time stress	0.059	0.062	0.048	0.073	0.63
error in reading task high time stress	0.146	0.145	0.144	0.115	0.52
too late in search task low time stress	0.449	0.184	0.199	0.110	0.00
too late in search task high time stress	0.411	0.167	0.279	0.129	0.00
too late in reading task low time stress	0.424	0.134	0.258	0.104	0.00
too late in reading task high time stress	0.444	0.202	0.314	0.139	0.00

Analysis of the results – The HEPs of both groups were first compared for the tasks listed in Table 20 by means of the Mann-Whitney test (Siegel, 1956). This non-parametric test was used because the distributions of the data were presumably not normal. The results are presented in Table 21. The standard deviation is a measure of the spread in the HEPs due to performance variability. The P-value was determined with the Mann-Withney test. If this value is lower than a predefined level of significance, usually 0.05, the difference between both groups can be considered as significant.

It appears from Table 21 that virtually each mean value for the operators was higher than the corresponding mean values for the students (except for the reading errors under low time stress). It also appears that the standard deviations were greater for the operator data. The last column shows that the differences are significant for most error types, viz. recognition errors, search errors under low time stress and all too late reactions. Since the mean values for the operators were higher, the operators performed these tasks significantly less well than the students. The significant differences for most of the tasks led to the decision not to combine the data for the two groups but to analyze them separately.

HEP distributions were derived from the HEPs per subject for the errors presented in Table 20. The distributions of both groups are presented in Appendix C. The shape of the distributions was tested with the Kolmogorov-Smirnov one-sample test (a non-parametric test; Siegel, 1956). This test compares the theoretical cumulative distribution with the observed cumulative distribution. It was tested whether the observed distributions were log-normal. The results are shown in Table 22. The P-values exceeded the level of significance set, i.e. 0.05, which implies that the hypothesis that the distributions are log-normal cannot be rejected.

Table 22
The results of the Kolmogorov-Smirnov one-sample test. The first two columns show the P-values for the operator group and the student group. The last two columns show the maximum absolute difference between the theoretical log-normal distribution and the distribution measured.

	P-value		maximum absolute difference	
error type	operators	students	operators	students
recognition error low confusion	0.53	0.82	0.191	0.089
recognition error high confusion	0.42	0.98	0.208	0.066
error in search task low time stress	0.47	0.90	0.199	0.081
error in search task high time stress	0.82	0.84	0.150	0.087
error in reading task low time stress	0.99	0.60	0.102	0.108
error in reading task high time stress	0.87	0.79	0.141	0.092
too late in search task low time stress	0.34	0.92	0.222	0.078
too late in search task high time stress	0.95	0.86	0.123	0.085
too late in reading task low time stress	0.69	0.81	0.169	0.090
too late in reading task high time stress	0.92	0.31	0.131	0.136

Correlations were also calculated because, as stated earlier, insight into the correlations is important when making an HPSA. It is important to know whether a person with a high HEP for one task has a high HEP for another task as well. The correlation can have a value between –1 and +1. A high correlation (close to +1) indicates that a high HEP in one task is consistent with a high HEP in another.

Tables 23 and 24 show the correlation between the errors for the operator group and the student group (the Pearson product-moment correlation). The value at the top of each set of data shows the correlation, the number of subjects is presented in the middle, and the P-value – showing the significance of the correlation – is given at the bottom of each set of data. One should use care in interpreting this P-value since its calculation is based on a normal distribution of the data and this is presumably not the case here. A non-parametric measure of correlation, e.g. the Spearman rank correlation (Siegel, 1956), could have been used to avoid this problem. However, the Pearson correlation was selected since this parametric measure of correlation is an important parameter in the function describing the log-normal distribution.

Both groups show several correlations that appear to be far from zero, which is indicative of consistency between the tasks. There are high correlations (> 0.5) for errors in similar tasks that differ only as to the conditions applied. The correlation found between the recognition errors under high- and low-confusion conditions can serve as an example. A subject who made many recognition errors with the letters that were difficult to remember did so also with the letters that were easy to remember. High correlations were also found between errors in the search task with the high and low time stress conditions. The same applies to the reading task.

Relatively high correlations (> 0.4) were found between several too late reactions. A person who was too late in one task was often also too late in another task. In contrast, negative correlations were found under the high time stress conditions between errors in a specific task and too late reactions in this task. It indicates that a subject was either too late and made few errors, or was not so late but made more errors. This applies particularly to the operator group, where these correlations are lower than –0.6.

Discussion

The evaluation of the results will be discussed here. A number of conclusions will be presented and some recommendations for further research will be made.

Evaluation – The first aim of this chapter was to determine the HEP distributions and to discover whether they were log-normal. Testing showed that the hypothesis that the distributions were log-normal could not be rejected. Based on these results, the application of a log-normal distribution for HEPs given in literature cannot be refuted.

The fact that the hypothesis of a log-normal distribution cannot be rejected does not necessarily mean that the hypothesis is true. It is also possible that the distributions are normal (this view is supported by the shape of certain distributions). The hypothe-

Table 23
Correlations between the HEP distributions measured for the operator group (Pearson product-moment correlation).

	recognition error		error in search task		error in reading task		too late in search task		too late in reading task	
	low confusion	high confusion	low time stress	high time stress	low time stress	high time stress	low time stress	high time stress	low time stress	high time stress
recognition error (low confusion)	1.0000 (0) P = .	0.8348 (18) P = 0.000	0.6010 (18) P = 0.004	0.5678 (18) P = 0.007	–0.2316 (18) P = 0.177	–0.0456 (18) P = 0.429	0.5435 (18) P = 0.010	–0.0040 (18) P = 0.494	0.2636 (18) P = 0.145	0.1032 (18) P = 0.342
recognition error (high confusion)	0.8348 (18) P = 0.000	1.0000 (0) P = .	0.4495 (18) P = 0.030	0.3734 (18) P = 0.063	–0.4517 (18) P = 0.030	–0.1869 (18) P = 0.229	0.7858 (18) P = 0.000	0.3593 (18) P = 0.071	0.5751 (18) P = 0.006	0.4623 (18) P = 0.026
error in search task (low time stress)	0.6010 (18) P = 0.004	0.4495 (18) P = 0.030	1.0000 (0) P = .	0.5068 (18) P = 0.016	–0.0029 (18) P = 0.495	0.1508 (18) P = 0.275	0.1183 (18) P = 0.320	–0.1184 (18) P = 0.320	0.0234 (18) P = 0.463	–0.1420 (18) P = 0.287
error in search task (high time stress)	0.5678 (18) P = 0.007	0.3734 (18) P = 0.063	0.5068 (18) P = 0.016	1.0000 (0) P = .	0.2689 (18) P = 0.140	0.4569 (18) P = 0.028	0.1483 (18) P = 0.278	–0.6049 (18) P = 0.004	–0.0730 (18) P = 0.387	–0.3889 (18) P = 0.055
error in reading task (low time stress)	–0.2316 (18) P = 0.177	–0.4517 (18) P = 0.030	–0.0029 (18) P = 0.495	0.2689 (18) P = 0.140	1.0000 (0) P = .	0.7067 (18) P = 0.000	–0.6465 (18) P = 0.002	–0.6649 (18) P = 0.001	–0.6399 (18) P = 0.002	–0.7230 (18) P = 0.000
error in reading task (high time stress)	–0.0456 (18) P = 0.429	–0.1869 (18) P = 0.229	0.1508 (18) P = 0.275	0.4569 (18) P = 0.028	0.7067 (18) P = 0.000	1.0000 (0) P = .	–0.3526 (18) P = 0.075	–0.6489 (18) P = 0.002	–0.4137 (18) P = 0.044	–0.6869 (18) P = 0.001
too late in search task (low time stress)	0.5435 (18) P = 0.010	0.7858 (18) P = 0.000	0.1183 (18) P = 0.320	0.1483 (18) P = 0.278	–0.6465 (18) P = 0.002	–0.3526 (18) P = 0.075	1.0000 (0) P = .	0.5134 (18) P = 0.014	0.7220 (18) P = 0.000	0.6219 (18) P = 0.003
too late in search task (high time stress)	–0.0040 (18) P = 0.494	0.3593 (18) P = 0.071	–0.1184 (18) P = 0.320	–0.6049 (18) P = 0.004	–0.6649 (18) P = 0.001	–0.6489 (18) P = 0.002	0.5134 (18) P = 0.014	1.0000 (0) P = .	0.6748 (18) P = 0.001	0.8314 (18) P = 0.000
too late in reading task (low time stress)	0.2636 (18) P = 0.145	0.5751 (18) P = 0.006	0.0234 (18) P = 0.463	–0.0730 (18) P = 0.387	–0.6399 (18) P = 0.002	–0.4137 (18) P = 0.044	0.7220 (18) P = 0.000	0.6748 (18) P = 0.001	1.0000 (0) P = .	0.8599 (18) P = 0.000
too late in reading task (high time stress)	0.1032 (18) P = 0.342	0.4623 (18) P = 0.026	–0.1420 (18) P = 0.287	–0.3889 (18) P = 0.055	–0.7230 (18) P = 0.000	–0.6869 (18) P = 0.001	0.6219 (18) P = 0.003	0.8314 (18) P = 0.000	0.8599 (18) P = 0.000	1.0000 (0) P = .

The values in the vertical data blocks represent the coefficient, the number of cases and the significance, respectively.
The symbol '.' indicates that a coefficient could not be computed.

Table 24
Correlations between the HEP distributions measured for the student group (Pearson product-moment correlation).

	recognition error		error in search task		error in reading task		too late in search task		*too late in reading task*	
	low confusion	high confusion	low time stress	high time stress	low time stress	high time stress	low time stress	high time stress	low time stress	high time stress
recognition error	1.0000	0.8493	0.5085	0.4850	0.3991	0.4722	0.5353	0.2892	0.3048	0.0783
(low confusion)	(0)	(50)	(50)	(50)	(50)	(50)	(50)	(50)	(50)	(50)
	P = .	P = 0.000	P = 0.000	P = 0.000	P = 0.002	P = 0.000	P = 0.000	P = 0.021	P = 0.016	P = 0.294
recognition error	0.8493	1.0000	0.5433	0.5383	0.3255	0.4374	0.5528	0.3939	0.3324	0.1810
(high confusion)	(50)	(0)	(50)	(50)	(50)	(50)	(50)	(50)	(50)	(50)
	P = 0.000	P = .	P = 0.000	P = 0.000	P = 0.011	P = 0.001	P = 0.000	P = 0.002	P = 0.009	P = 0.104
error in search task	0.5085	0.5433	1.0000	0.5432	0.4343	0.4042	0.2516	0.1733	0.3456	0.0124
(low time stress)	(50)	(50)	(0)	(50)	(50)	(50)	(50)	(50)	(50)	(50)
	P = 0.000	P = 0.000	P = .	P = 0.000	P = 0.001	P = 0.002	P = 0.039	P = 0.114	P = 0.007	P = 0.466
error in search task	0.4850	0.5383	0.5432	1.0000	0.3960	0.5354	0.0761	–0.2340	0.1621	–0.1966
(high time stress)	(50)	(50)	(50)	(0)	(50)	(50)	(50)	(50)	(50)	(50)
	P = 0.000	P = 0.000	P = 0.000	P = .	P = 0.002	P = 0.000	P = 0.300	P = 0.051	P = 0.130	P = 0.086
error in reading task	0.3991	0.3255	0.4343	0.3960	1.0000	0.6238	0.3874	0.1260	0.2234	–0.1709
(low time stress)	(50)	(50)	(50)	(50)	(0)	(50)	(50)	(50)	(50)	(50)
	P = 0.002	P = 0.011	P = 0.001	P = 0.002	P = .	P = 0.000	P = 0.003	P = 0.192	P = 0.059	P = 0.118
error in reading task	0.4722	0.4374	0.4042	0.5354	0.6238	1.0000	0.1407	–0.1725	0.1775	–0.3495
(high time stress)	(50)	(50)	(50)	(50)	(50)	(0)	(50)	(50)	(50)	(50)
	P = 0.000	P = 0.001	P = 0.002	P = 0.000	P = 0.000	P = .	P = 0.165	P = 0.115	P = 0.109	P = 0.006
too late in search task	0.5353	0.5528	0.2516	0.0761	0.3874	0.1407	1.0000	0.7758	0.4316	0.4934
(low time stress)	(50)	(50)	(50)	(50)	(50)	(50)	(0)	(50)	(50)	(50)
	P = 0.000	P = 0.000	P = 0.039	P = 0.300	P = 0.003	P = 0.165	P = .	P = 0.000	P = 0.001	P = 0.000
too late in search task	0.2892	0.3939	0.1733	–0.2340	0.1260	–0.1725	0.7758	1.0000	0.4729	0.7329
(high time stress)	(50)	(50)	(50)	(50)	(50)	(50)	(50)	(0)	(50)	(50)
	P = 0.021	P = 0.002	P = 0.114	P = 0.051	P = 0.192	P = 0.115	P = 0.000	P = .	P = 0.000	P = 0.000
too late in reading task	0.3048	0.3324	0.3456	0.1621	0.2234	0.1775	0.4316	0.4729	1.0000	0.5624
(low time stress)	(50)	(50)	(50)	(50)	(50)	(50)	(50)	(50)	(0)	(50)
	P = 0.016	P = 0.009	P = 0.007	P = 0.130	P = 0.059	P = 0.109	P = 0.001	P = 0.000	P = .	P = 0.000
too late in reading task	0.0783	0.1810	0.0124	–0.1966	–0.1709	–0.3495	0.4934	0.7329	0.5624	1.0000
(high time stress)	(50)	(50)	(50)	(50)	(50)	(50)	(50)	(50)	(50)	(0)
	P = 0.294	P = 0.104	P = 0.466	P = 0.086	P = 0.118	P = 0.006	P = 0.000	P = 0.000	P = 0.000	P = .

The values in the vertical data blocks represent the coefficient, the number of cases and the significance, respectively.
The symbol '.' indicates that a coefficient could not be computed.

sis that the distributions are normal was therefore tested later on as well. It appeared that the hypothesis also could not be rejected for the two groups involved. Furthermore, it appeared that the normal distribution fitted the data better than the log-normal one for some HEP distributions of the operator group. However, the application of a normal distribution cannot be recommended in an HRA or HPSA on the basis of this finding only and deviate in this way from what is customary in literature for a group of operators. The argumentation is that the variance in the results of the group of operators appears to be too large.

Besides HEP distributions, correlations were determined. In general, these correlations can result from personal characteristics of the subjects and/or from experimental factors. Had the correlations resulted from the experiment and, therefore, be experiment-dependent, they would be less applicable to an HRA or HPSA. It appeared, however, that in most cases there was a high positive correlation between similar errors and too late reactions (e.g. errors made under the low- and high-confusion conditions). The impression was gained that, especially for too late reactions, a personal characteristic, i.e. age, was a crucial factor. It also appeared that, in most cases, there were negative correlations between errors in a specific task and too late reactions in that task. Personal judgement was apparently made in these cases between being on time and making several mistakes on the one hand, and not being on time and making few mistakes on the other. This indicates that the correlations were subject- and not experiment-dependent. Whether this interpretation is correct could be shown by further analysis in which dependent errors within a trial are considered. If the experimental factors (e.g. time stress) are such that an error in a trial causes another error in the same trial, dependent errors will be made. However, such an analysis – as performed by Okma (1987) based on part of the student group (30 students) and on part of the trials – has already shown that this is not the case.

It appeared from the results that operators performed most tasks significantly less well than the students. It is noted that this experiment was designed in such a way that a subject had to react as quickly as possible so as to cause errors necessary to obtain HEPs. Because of the necessity to react quickly, the experiment did not entirely fit the practical control-room situation: operators are trained to develop the attitude of first analyzing a specific situation thoroughly and then taking action. Quick and often incorrect reactions have no place in this situation. This would imply that the operators would have lower HEPs for the search and reading tasks. It appears from Table 21, however, that the mean HEP for the search task of the operator group is higher and that there are small differences for the reading task. If one takes more time for the search task, which implies that one is too late more often, it is thus not true that fewer errors will be made in comparison with the fast responders, the students.

The significant differences between the two groups make it impossible to pool the data and to analyze them on the basis of traditional statistics. Nor is it permissible to apply to the operators any conclusions based on the student group. This experiment shows that care must be taken when conclusions drawn from psychological experiments with students as participants are applied to other groups.

Although the operators performed significantly worse than the academic students,

one cannot conclude that the operators' performance in a control room is inferior and that the future control-room operator should be a young academic. A number of reasons can be given for the inferior performance of the operators in this experiment. First, the validity of the experiment is unknown. It is not known to what extent errors made in this experiment by a subject correspond with errors made in a practical control-room situation. There may be practical situations in which reliable operator performance is highly determined by experience and inventiveness, factors which did not play an important role during this experiment. Secondly, the stress effect may have played an important role: being too late often may have been so discouraging that the HEPs became higher for the slower operators. This might explain the higher HEP for the recognition task with no time stress. Finally, students work more often with computers and keyboards, which makes the lower HEPs for their group in this experiment plausible.

To discover the learning effect in the results, the data were subjected to a paired T-test later on. For this purpose, the data for each error type were divided into two groups: data obtained towards the beginning of the experiment and data obtained towards the end. The paired T-test showed that there were significant differences between these data groups for certain error types. For the operators 25% of the data groups differed significantly and for the students this value was 17%. Hence, significantly different data were obtained for certain subjects for a few error types in the course of the experiment. This was presumably caused by the learning effect because the error rates for these tasks were on average lower towards the end of the experiment. Although it is important to have no learning effect in most psychological experiments, the question is whether this demand is of great importance in experiments such as the present one. This experiment was intended to represent control-room activities in complex installations and in certain cases there will also be a learning effect when coping with situations that occur less frequently in these installations.

Conclusions – The results described in this chapter lead to the following conclusions:

(1) the log-normal distribution for the HEPs as applied in literature cannot be rejected;
(2) several correlations were found between HEPs which are likely to have been caused by human characteristics and not by experimental factors;
(3) it appeared that the operators performed significantly less well than the university students; interpreting these data in relation to operator performance in a control room is, however, not justified as the validity of the experiment is not yet known;
(4) the experiment showed that caution is needed when conclusions based on results achieved with students as participants in psychological experiments are applied to operators.

Further research – It has been argued that the correlations resulted from personality factors rather than experimental factors. However, this was not proved satisfactorily. An extended analysis in which errors within the trials are considered, as done in part by Okma (1987) should provide a far better insight. It is recommended that such an

analysis be performed.

It is also suggested that other analyses on the data be performed. It was stated that the data for the operators and for the students could not be pooled according to traditional statistics. It might be possible, however, to pool the data by applying Bayesian statistics. A larger group would thus be created to test the hypothesis that HEP distributions are log-normal distributed. A so-called factor analysis might also provide more insight. Such an analysis might show the crucial factors that influenced the results obtained in the experiment.

Moreover, it is recommended that further research be done to discover the validity of the experiment. The validity shows in how far the number of errors made in an experiment by a particular subject is consistent with errors made in actual situations, e.g. in a control room. The validity of the experiment is not yet known and it would be interesting to investigate it since the experiment shows some resemblance with procedural control-room activities. Should the experiment be proved to be of sufficiently high validity, it might be used to select applicants for the job of control-room operator.

Chapter 10

General discussion

Review of the results obtained and conclusions

The aim of this study was to arrive at a technique for qualitative and quantitative prediction of human-error sequences that occur when normal procedures have to be followed (chapter 1). Two methods were described to incorporate the analysis of human errors in risk analyses for systems, viz. the human errors as the basic events of fault trees and the human errors as the initiating events of system event trees (chapter 2). The present study was concentrated on the latter approach and dealt, in particular, with sequences of human errors related to procedural actions being performed. The choice was based on the fact that this aspect had not been considered adequately in previous risk analyses. The present study introduced a technique referred to as 'THESIS', in which event trees are used to analyze the human-error sequences that may lead to various undesired consequences: the initiating events.

It appeared from a review of the existing techniques (chapter 3) that there is, as yet, no adequate technique for the prediction of human-error sequences. It is noteworthy in this context that the techniques reviewed in the present study are techniques known from the HRA literature. Decision trees were therefore not considered. A decision tree is a diagram that shows the various paths in which human decisions interact with their consequences; the related theory can be used in various disciplines to decide on the best strategy to be followed in order to achieve a particular goal. Decision trees were described by, among others, Tribus (1969), Raiffa (1970) and Bunn (1984) for general use, and by Kassirer (1976) and Weinstein & Fineberg (1980) for use in clinical decisions. THESIS event trees are not very different from the decision trees. In fact, the THESIS event trees can be regarded as decision trees that include several extensions, such as sequences of human errors and the possibility of recovery attempts being made.

It appeared that several problems arise when event trees originally used for technical systems are applied to humans. These problems have been referred to as the man-related features (MRFs) of THESIS (chapter 4) and their influence on the application of the so-called THESIS event trees was investigated analytically, by computer simulation, practically and experimentally. The MRFs of which the influence was studied were the procedure-selection capability, the ergonomics of the panel layout, human

actions with a continuous nature, the dependence between human errors (event dependence), the possibility of rectifying an error (recovery attempt), the memory effects during the recovery attempt (recovery dependence), the performance variability, and the correlation between HEPs. Conclusions about the influence of several of these MRFs on the applicability of THESIS were drawn on the basis of several assumptions.

It is obvious from the case study described in chapter 5 that the sequence of actions in a procedure may influence the safety of human actions if event dependence is involved. This means that all procedures used, whether written or non-written, need to be considered when applying event trees if a complete analysis is to be made. It was concluded from the case study that a justified decision about the best man-machine design, e.g. the safest procedure, can only be made if all paths of the THESIS event trees are taken into account, with the probability and extent of the resulting consequences.

The quantitative effect of several MRFs was investigated with a theoretical model (chapters 6 and 7). It appeared that, if there is no recovery dependence, the theoretical description is rather simple and that calculation of undesired consequences due to sequences of human errors is relatively easy. If recovery dependence is present, however, the theoretical description becomes very complicated. Nevertheless, it appeared that, under certain conditions, recovery dependence is not relevant and can be ignored, so that a more simple analytical model, valid in the case of no recovery dependence, can be used (Eq. 26). This analytical model was used in a field study concerning the start-up procedure described in chapter 8. It was also concluded that event dependence greatly influences the quantification, and that too little attention has so far been given to the collection of data regarding this MRF as compared to the collection of HEPs.

The analysis of the start-up procedure in chapter 8 showed the qualitative and quantitative effects of several MRFs on the applicability of THESIS. It appeared that one MRF, namely continuous tasks, had a certain effect because it determined partly the identification of the specific actions of the procedure. It also appeared that, besides this MRF, a technical factor, i.e. the coupling between control input and process variables, had a very large influence on the applicability of THESIS, since predicting the effect of certain human-error sequences became a difficult task when there was much interaction.

Two MRFs, viz. the variability in human performance and the correlation between HEPs, were studied experimentally. It was specifically investigated whether a certain distribution, i.e. the log-normal one, can be used to describe the distribution of the probabilities of human errors. It was concluded that the frequently used, but hardly ever measured, log-normal distribution could not be rejected on the basis of the results obtained. It also appeared that significantly high correlations were sometimes present, presumably caused by human characteristics. These results were not used further in THESIS since point values for the HEPs were used instead of distributions. However, it is obvious, since the standard deviation was often rather high (Table 21), that the variability in human performance in combination with the correlation may have a quantitatively great influence on the results obtained with THESIS.

Not only was the effect of several MRFs determined, but the investigation also

considered the analysis of complete human-error sequences, a topic which was the essential goal of THESIS (chapter 8). This study was performed in the form of an analysis of the difference between complete human-error sequences and single human errors. Quantitatively, there appeared to be no important difference, because the probabilities of the undesired consequences considered did not differ much. Qualitatively, however, there were several differences, since a large number of outcomes following human errors were not discovered by analyzing single errors. Considerable more time was spent on analyzing complete human-error sequences.

THESIS is intended to predict the sequences of human errors leading to undesired consequences. The undesired consequences in the two case studies performed (chapters 5 and 8) were largely determined beforehand and the sequences of human errors leading to these consequences were identified. Obviously, in general, predicting human-error sequences may also lead to the prediction of unforeseen consequences following these error sequences. The feasibility of this aspect was investigated in a study which was not reported on in the preceding chapters. This study involved the analysis of the start-up procedure used at the Nuclear Reactor Institute at Delft, partly by means of THESIS event trees. The analysis was done in co-operation with De Vos (1987).

It appeared from the study at the Nuclear Reactor Institute that it is possible to discover various consequences following sequences of human errors by application of the systematic approach with THESIS event trees. These consequences could not be determined by considering single human errors. The detection of the undesired consequences by means of THESIS led to the recommendation that extra safety devices be introduced near the nuclear section of the installation. Another conclusion was that application of the method demanded considerable effort; many human-error sequences had to be investigated, most of which finally appeared not to contribute to the probability of the undesired consequences. This last result is consistent with the results of the study described in chapter 8.

The main conclusion of this study, based on the results described in the previous chapters, is that THESIS event trees can be used to predict human-error sequences when a normal procedure must be followed, in spite of the problems that appear if event trees originally used for technical systems are used for human-performance safety analysis. It should be borne in mind, however, that this conclusion must be interpreted carefully. It is based on situations where relatively short procedures are followed and where there is a rather simple panel layout, inducing only few possibilities for selection errors. Whether these results are valid for the complex control room of an advanced process should be investigated in an additional research project.

The power of the THESIS event trees lies particularly in the qualitative aspect, as the analysis of complete human-error sequences is a prerequisite for making correct decisions about an optimal man-machine design. However, substantial effort is required to apply the technique, mainly due to the interpretation of the interactions of human-error sequences with the process. It is clear that adequate knowledge about the process in particular and some knowledge about human behavior are fundamental prerequisites if THESIS is to be applied. The technique must, therefore, be carried out by a process or control engineer with adequate knowledge of ergonomics.

As with other techniques related to quantification of the probability of human performance, the lack of data is an essential problem. It implies that, as yet, THESIS can be used only for sensitivity analyses for the screening of man-machine designs. The method has not yet been validated because data are scarce and because the present investigation is the first to have been concerned with complete error sequences leading to various consequences. A lack of validation is, however, a weak point in most techniques concerning probability assessments of human errors (Williams, 1985).

Discussion of the assumptions made and of the method applied

One of the basic assumptions was that rule-based actions were performed. This resulted in the use of rather low HEPs at several points in this study (in the range of 0.001 to 0.01 for events not dependent upon others). It is obvious that this assumption played an essential role in various parts of the study. It appeared, e.g. in the computer simulation described in chapter 7, that certain MRFs had little influence. It was found in the practical study of chapter 8 that there was no great difference between considering complete error sequences and single error sequences regarding the consequence probabilities. The experiment of chapter 9 resulted in long measurement times, despite the fact that the HEPs were increased artificially. The results obtained in chapters 7 and 8 could be different in the presence of higher HEPs, e.g. due to emergency actions. The probability of achieving a return outcome is then higher, which will result in a higher contribution of the recovery attempt to the probability that certain consequences will occur.

Another essential assumption, made at the start of this study, was that a person reaching a return outcome will follow one of the procedures incorporated in the analysis. This may not be true, however, since achieving a return outcome may cause the operator's behavior to shift from rule-based to knowledge-based as defined by Rasmussen (1985). This implies that an operator might follow an entirely different, originally unplanned procedure. This is an essential problem, and it means that the analyst should extend the set of possible procedures that can be followed originally, before any recovery attempt is made, with a set of additional procedures that could be followed after the recovery attempt. This would make the HPSA far more labor-intensive than an HRA, which assumes a return to the existing success path after the return outcome.

Since interest was now generally focused on observable errors, and not on the causes leading to an error, generic values were used for the human errors and the MRF parameters. This was allowable since the values were used only for a sensitivity analysis aimed at increasing insight into the effect of various parameters. The values of the probabilities are obviously critical for safety calculations, and assessment of the exact values is therefore essential. This implies that consideration of observable errors only is not enough in such a case; the causes leading to the errors must be identified to ensure that the correct data for the probability of human errors are used so that correct absolute values can be obtained.

Predictions of human performance in terms of probabilities have been the subject

of much criticism from the beginning. These criticisms can be divided roughly into conceptual and pragmatic criticisms (Meister, 1984). Conceptual criticisms were raised by Adams (1982), Carnino (1985) and Reason & Embrey (1985) among others. In summary, the conceptual criticisms are mostly directed at the attempts to describe overall activities by means of observable, behavioral units to which probabilities must be assigned, just as with technical components. It is not allowable, according to these authors, to do so with humans because of the several problems interfering, that are usually lacking in the case of technical systems.

It must be admitted that THESIS focuses largely on observable errors, and divides human behavior into behavioral units. The trend in psychology that considers only observable human performance and not the internal mechanisms is called behaviorism (Duijker & Vroon, 1981). The consideration of observable errors is, according to Rasmussen (1987b), only fruitful in the case of procedural tasks, since such tasks can be decomposed. The present study is, however, based on this procedural, rule-based behavior. In addition, the study was not focused only on observable errors. Due to the introduction of the MRFs, such as recovery attempts, the study did not involve only the approach of behaviorism.

The problems raised by the application of an event tree to human activities could be studied systematically when the MRFs were introduced. It appeared that certain problems are irrelevant under certain conditions, but that other problems do constitute severe difficulties. It nevertheless appeared that, if these problems are taken into account as MRFs, so as to meet several conceptual criticisms, a technique originally developed for technical systems can be applied to humans within certain limits.

Pragmatic criticisms were raised by Hopkins et al. (1982), Carnino (1985) and Williams (1985). These criticisms are largely related to the scarcity of data and the insufficient validation of the methods. This criticism is justified as regards the attempt to quantify human performance as part of risk analysis; the existing data banks have only limited value due to the many PSFs involved. The setting up of a databank in the near future is a fundamental requirement to quantify human performance in terms of probability, for the valid application of the techniques. Apart from the concept of Comer et al. (1983) that was mentioned earlier, expert judgement (e.g., SLIM-MAUD; see chapter 3) could be a good tool for achieving this. However, if human errors are studied to obtain an idea of how human error might affect a complete system, as was largely done in this study, such a databank is not a prerequisite.

Future research

THESIS is essentially a discrete technique because it divides human actions into possible human errors. It appeared possible to analyze not only discontinuous, but also continuous actions. The continuous actions were therefore divided into several similarly discrete ones. This approach was followed in a study in which the start-up procedure of a boiler was analyzed (chapter 8). The procedure to be analyzed was, however, rather short and the related ergonomics were such that few selection errors could be made.

It is questionable whether the event-tree technique presented here is still applicable if certain practical MRFs are explicitly present, such as a large number of continuous human actions and an ergonomically bad panel layout, the latter causing the possibility of several selection errors. The THESIS event trees might then become too extensive for a feasible analysis with human errors on the component level (B-level in chapter 2), particularly for long procedures. Application of the technique on the system level (A-level in chapter 2) could perhaps be more appropriate in this case. However, it could happen that certain initiating events will not be taken into account then, because selection errors of certain components will no longer be studied in detail. It is nevertheless suggested that THESIS event trees be applied on this higher level for further research because actual control rooms involve the regular presence of these MRFs.

Several MRFs were analyzed in distinct groups in individual chapters. This was done in order not to make the model more complicated than strictly necessary for obtaining sufficient insight into the effects of the various MRFs. It appeared that, in most cases, the distinction allowed valid conclusions to be drawn regarding their effects. It also appeared, however, that it was sometimes necessary to consider more MRFs at the same time. For example, the introduction of the uncertainty of HEPs that was previously disregarded appeared necessary for an understanding of the relevance of recovery dependence in the sensitivity analysis of the analytical model (chapter 7).

The effects of much larger groups of MRFs should be studied. Such an investigation should be combined with the use of a computer program merging the software used in this study, viz. PRESUME and PREQUANT. A combination with other computer programs, such as 'dependent Monte Carlo sampling' – which can be used to combine correlated HEP distributions (Cooke & Way, 1986) – and DYLAM, is recommended for use in further research. The author is aware that this approach may seem rather far-fetched, but is convinced that further analysis of human-error sequences requires a combination of such computer programs because of the demanding nature of the work required for this kind of study of human performance.

Further support for this suggestion is the fact that reset errors have been disregarded up to now. It was assumed at the very beginning of the present study that the system is reset when errors are made and a person makes a recovery attempt. It means that an adjusted control device is set to its starting position during the recovery attempt. This assumption made the analysis less extensive because the number of outcomes remained limited. However, it is entirely possible that incorporating reset errors will lead to additional outcomes, the consequences of which may be undesired. Future research into the feasibility of extending THESIS to include reset errors is therefore suggested.

No attempt was now made to apply the fuzzy-set theory which is characterized by the fact that an entity can be a partial member of a set instead of a complete member; the degree of belonging to a set is described by 'membership functions' (Zadeh, 1965). The theory has already been applied by Terano et al. (1983), Unwin (1984) and Franus (1986) in relation to human factors and reliability calculations. It was considered premature, however, to apply the technique in the present study, because it attempted

to set up an HPSA technique. Moreover, various authors (French, 1984; McCord & Maldonado, 1988) doubt the validity of the fuzzy-set theory if it is used for uncertainty calculation in the likelihood of a combination of human errors: there is, so far, no unambiguous way to calculate the uncertainty with this theory. There is nevertheless a need for research on the application of the theory to the quantification of human performance in terms of probabilities, as human behavior has aspects that can be described well by membership functions.

It is also suggested that technical failures and human errors be studied in combination. It had been assumed up to now that the system to be controlled was perfect and that only human errors could be made. Several accidents in recent years have shown, however, that a combination of technical and human errors can be disastrous. Major accidents caused by human errors only are hardly ever a possibility; many initiating events caused by operators are liable to control by safety devices. However, the consequences may be severe if the safety devices fail as well. One could think in this context of a safety device that fails, leading to obligatory shut-down of the plant, while the same safety device would be needed during shutting down in the case of human errors during the execution of the shut-down procedure.

The question is now raised as to what extent rule-based behavior as investigated here will develop in the near future, in comparison with the knowledge-based behavior that is present when unforeseen situations are dealt with. Most activities have certainly become more and more rule-based, because of the many training exercises conducted in recent years for operators of complex 'installations. On the other hand, several rule-based activities can be automated in some way, making knowledge-based behavior the more essential topic to be investigated. If the latter type of behavior should prevail it could be fruitful to direct the study of human-performance safety from rule-based behavior to knowledge-based behavior.

It has been shown, however, that models for knowledge-based behavior can only describe this kind of behavior in a general or normative way (Stassen et al., 1985). Activities related to this kind of performance cannot be decomposed adequately (Rasmussen, 1987b). It is therefore doubtful whether event trees as used in detail in this study can be applied to knowledge-based behavior. More general techniques may then be necessary to analyze human errors as a part of risk analysis. The suggestion made above to use THESIS event trees on the system level, might be used to tackle this fundamental problem. Since it is well recognized that the underlying mechanisms are essential in this case (Woods et al., 1986), these mechanisms will have to be included in the technique.

References

Adams, J.A. 1982 Issues in human reliability – Human Factors 24(1): 1-10.

Amendola, A. & G. Reina 1984 DYLAM-1. A software package for event sequence and consequence spectrum methodology – Commission of the European Communities Report EUR 9224 EN: 179 pp.

Ang, A.H-S. & W.H. Tang 1984 Probability concepts in engineering planning and design. Volume 2: Decision, risk, and reliability – John Wiley & Sons (New York): 562 pp.

Apostolakis, G. 1985 On the assessment of human error rates using operational experience – Reliability Engineering 12: 93-105.

Apostolakis, G. & S. Kaplan 1981 Pitfalls in risk calculations – Reliability Engineering 2: 135-145.

Bainbridge, L. 1979 Verbal reports as evidence of the process operator's knowledge – International Journal of Man-Machine Studies 11: 411-436.

Baron, S., C. Feehrer, R. Muralidharan, R. Pew & P. Horwitz 1982 A framework for modeling supervisory control behavior of operators of nuclear power plants. *In*: L.S. Abbott (ed.): Proceedings of the workshop on cognitive modeling of nuclear-plant control-room operators (Dedham, Massachusetts, 1982) – Oak Ridge National Laboratory (Oak Ridge) Report ORNL/TM-8614 (also NUREG/CR-3114): 36-51

Beare, A.N., R.E. Dorris, C.R. Bovell, D.S. Crowe & E.J. Kozinsky 1984 A simulator-based study of human errors in nuclear power plant control room tasks – Sandia National Laboratories (Albuquerque) Report SAND83-7095 (also NUREG/CR-3309): 174 pp.

Bell, B.J. & A.D. Swain 1983 A procedure for conducting a human reliability analysis for nuclear power plants. Final report – Sandia National Laboratories (Albuquerque) Report SAND81-1655 (also NUREG/CR-2254): 62 pp. + appendices.

Bello, G.C. & V. Colombari 1980 The human factors in risk analyses of process plants: the control room operator model 'TESEO' – Reliability Engineering 1: 3-14.

Berger, J.L. 1981 Automatische trein beveiliging – Natuur en Techniek 49: 260-279.

Bhat, U.N. 1972 Elements of applied stochastic processes – John Wiley & Sons, Inc. (New York): 414 pp.

Billinton, R. & R.N. Allan 1983 Reliability evaluation of engineering systems: concepts and techniques – Pitman Publishing Limited (London): 349 pp.

Brown, R.G., J.L. VonHerrmann & J.F. Quilliam 1982 Operator action event trees for the Zion 1 pressurized water reactor – Wood-Leaver and Associates, Inc. Report EGG-2201 (also NUREG/CR-2888): 120 pp.

Bunn, D.W. 1984 Applied decision analysis – McGraw-Hill Book Company (New York): 320 pp.

Carnino, A. 1985 Human reliability – Nuclear Engineering and Design 90: 365-369.

Chechile, R. 1977 Storage-retrieval analysis of acoustic similarity – Memory & Cognition 5: 535-540.

CISHC (Chemical Industry Safety and Health Council) 1977 A guide to hazard and operability studies – CISHC (London): 47 pp.

Comer, M.K., E.J. Kozinsky, J.S. Eckel & D.P. Miller 1983 Human reliability data bank for nuclear power plant operations. Volume 2: A data bank concept and system description – Sandia National Laboratories (Albuquerque) Report SAND82-7057/2 (also NUREG/CR-2744/2): 151 pp.

Comer, M.K., D.A. Seaver, W.G. Stillwell & C.D. Gaddy 1984 Generating human reliability estimates using expert judgment – Sandia National Laboratories (Albuquerque) Report SAND84-7115 (also NUREG/CR-3688): 60 pp. + appendices.
Conrad, R. 1964 Acoustic confusions in immediate memory – British Journal of Psychology 55: 75-84.
Cooke, R.M. & R. Waij 1986 Monte Carlo sampling for generalized knowledge dependence with application to human reliability – Risk Analysis 6: 335-343.
DGA (Directoraat Generaal van de Arbeid) 1982 Storingsanalyse. Waarom? Wanneer? Hoe? – DGA (Den Haag) Voorlichtingsblad 2 : 47 pp.
Dhillon, B.S. 1980 On human reliability – bibliography – Microelectronics and Reliability 20: 371-373.
Dhillon, B.S. 1986 Human reliability with human factors – Pergamon Press (New York): 237 pp.
Drury, C.G. 1983 Task analysis methods in industry – Applied Ergonomics 14: 19-28.
Duijker, H.C.J. & P.A. Vroon 1981 Codex Psychologicus – Elsevier (Amsterdam): 589 pp.
Eid, A.M. 1980 Road traffic accidents in Quatar. The size of the problem – Accident Analysis & Prevention 12: 287-298.
Embrey, D.E. 1976 Human reliability in complex systems: an overview – United Kingdom Atomic Energy Authority (Harwell): 85 pp.
Embrey, D.E. 1984 Human reliability. Paper presented at the 1984 Summer School of the Italian Physical Society – Human Reliability Associates Ltd. (Dalton): 33 pp.
Embrey, D.E. 1986 SHERPA: a systematic human error reduction and prediction approach. *In*: Proceedings of the International Topical Meeting on Advances in Human Factors in Nuclear Power Systems (Knoxville, 1986) – American Nuclear Society (Illinois): 184-193.
Embrey, D.E., P. Humphreys, E.A. Rosa, B. Kirwan & K. Rea 1984 SLIM-MAUD: an approach to assessing human error probabilities using structured expert judgment. Volume 1: Overview of SLIM-MAUD – Brookhaven National Laboratory (New York) Report BNL-NUREG-51716 (also NUREG/CR-3518): 29 pp.
Flanagan, J.C. 1954 The critical incident technique – Psychological Bulletin 51: 327-358.
Fragola, J.R. & B.J. Bell 1983 A systematic approach to human error categorization in nuclear power plant tasks – Paper presented at the American Nuclear Society Annual Meeting (Detroit, 1983): 22 pp.
Franus, E.A. 1986 The frame model of reliability. *In*: W. Karwowski & A. Mital (eds.): Applications of fuzzy set theory in human factors – Elsevier Science Publishers B.V. (Amsterdam): 179-189.
French, S. 1984 Fuzzy decision analysis: some criticisms – TIMS/Studies in the Management Sciences 20: 29-44.
Gabriëls, H. 1987 Analyse van de startprocedure (druk maken) van de proefketelinstallatie – N.V. KEMA (Arnhem) Report 30119-MAP-14: 60 pp.
GKN (Gemeenschappelijke Kernenergiecentrale Nederland) 1978 Kernenergiecentrale Dodewaard, technische specificaties – N.V. GKN (Arnhem) looseleaf.
Godding, J.J.M. 1987 Analyse van de startprocedure van de proefketelinstallatie: de vergelijking tussen een uitgebreide en een eenvoudige analyse – N.V. KEMA (Arnhem) Report 30119-MAP-18: 141 pp.
Griffon-Fouco, M. & F. Ghertman 1987 Data collection on human factors. *In*: J. Rasmussen, K. Duncan & J. Leplat (eds.): New technology and human error – John Wiley & Sons Ltd. (Chichester): 193-207.
Hagen, E.W. 1976 Human reliability analysis – Nuclear Safety 17: 315-326.
Hall, R.E., J. Fragola & J. Wreathall 1982 Post event human decision errors: operator action tree/time reliability correlation – Brookhaven National Laboratory (New York) Report BNL-NUREG-51601 (also NUREG/CR-3010): 48 pp.
Hannaman, G.W. & A.J. Spurgin 1984 Systematic human action reliability procedure (SHARP) – NUS Corporation (San Diego): 139 pp.

Heising, C.D. & E.I. Patterson 1984 Plant specification of generic human-error data through a two-stage Bayesian approach – Reliability Engineering 7: 21-52.
Henley, E.J. & H. Kumamoto 1981 Reliability engineering and risk assessment – Prentice-Hall, Inc. (Englewood Cliffs): 568 pp.
Heslinga, G. 1983 Human reliability analysis using event trees – Kema Scientific & Technical Reports 1: 19-44.
Heslinga, G. 1984 Analysis of human reliability considering a sequence of independent actions. *In*: Proceedings of the Fourth European Annual Conference on Human Decision Making and Manual Control (Soesterberg, 1984) – Institute for Perception TNO (Soesterberg): 73-86.
Heslinga, G. 1985a A consideration of the problems in obtaining probability density functions of human errors from field studies and simulators – N.V. KEMA (Arnhem) Report WSK/30119-4: 25 pp.
Heslinga, G. 1985b The acquisition of probability density functions of human errors – Paper presented at the Enlarged Halden Programme Group Meeting on Computerised Man-Machine Communication (Göteborg, 1985): 8 pp.
Heslinga, G. 1985c Analysis of human reliability considering a sequence of dependent actions. *In*: J. Stalpaert (ed.): Transactions of the 8th International Conference on Structural Mechanics in Reactor Technology (Brussels, 1985) – North-Holland Physics Publishing (Amsterdam): 491-496.
Heslinga, G. 1986 Reliability analysis of procedural human activities: a case-study – Paper presented at the IFAC Workshop on Reliability of Instrumentation Systems for Safeguarding and Control (Den Haag, 1986): 5 pp.
Hopkins, C.O., H.L. Snyder, H.E. Price, R.J. Hornick, R.R. Mackie, R.J. Smillie & R.C. Sugarman 1982 Critical human-factors issues in nuclear-power regulation and a recommended comprehensive human-factors long-range plan – Human Factors Society, Inc. (Santa Monica) Report DE82 906211 (also NUREG/CR-2833): 2421 pp.
IEEE (Institute of Electrical and Electronics Engineers) 1979 Three Mile Island and the future of nuclear power – IEEE Spectrum November 1979.
INSAG (International Nuclear Safety Advisory Group) 1986 Summary report on the post-accident review meeting on the Chernobyl accident – International Atomic Energy Agency (Wien): 106 pp.
Johnson, W.G. 1980 MORT safety assurance systems – Marcel Dekker, Inc. (New York): 525 pp.
Kassirer, J.P. 1976 The principles of clinical decision making: an introduction to decision analysis – The Yale Journal of Biology and Medicine 49: 149-164.
Kemeny, J.G. & J.L. Snell 1976 Finite Markov chains – Springer (New York): 210 pp.
Klemmer, E.T. & G.R. Lockhead 1962 Productivity and errors in two keying tasks: a field study – Journal of Applied Psychology 46: 401-408.
Konings, A.H.J.M. 1987 Analyse van de startprocedure (temperatuurverhoging) van de proefketelinstallatie – N.V. KEMA (Arnhem) Report 30119-MAP-15: 71 pp.
Kopstein, F.F. & J.J. Wolf 1985 Maintenance personnel performance simulation (MAPPS) model: users' manual – Oak Ridge National Laboratory (Oak Ridge) Report ORNL/TM-9545 (also NUREG/CR-3634): 98 pp.
Leplat, J. 1987 Accidents and indicents production: methods of analysis. *In*: J. Rasmussen, K. Duncan & J. Leplat (eds.): New technology and human error – John Wiley & Sons Ltd. (Chichester): 133-142.
Ligthart, V.H.M. 1979 Shipping accidents in the new Rotterdam Waterway area – a suggested approach towards the setting up of an accident databank – Nederlands Maritiem Instituut (Rotterdam): 56 pp.
Mancini, G. 1985 Modelling humans and machines. *In*: Proceedings of the NATO advanced study institute on intelligent decision aids in process environments (Pisa, 1985) – Commission of the European Communities (Ispra): 18 pp.

Mancini, G. & A. Amendola 1983 Human models and the data problem – Proceedings of the 4th Euredata Conference (Venezia, 1983): 13 pp.
McCord, M.R. & J. Maldonado 1988 Prediction models, subjective probability, and fuzzy membership: results and concerns for transport evaluation – Paper presented at the Fourth International Conference on Utility, Risk and Decision Theories (Budapest, 1988): 31 pp.
McCormick, N.J. 1981 Reliability and risk analysis. Methods and nuclear power applications – Academic Press (New York): 446 pp.
Meister, D. 1984 Human reliability. *In*: F.A. Muckler (ed.): Human factors review – Human Factors Society Inc. (Santa Monica): 13-53.
Miller, G.A. 1956 The magical number seven, plus or minus two: some limits on our capacity for processing information – The Psychological Review 63: 81-97.
Nieuwhof, G.W.E. 1983 Human error – Reliability Engineering 6: 191-192.
Nivolianitou, Z., A. Amendola & G. Reina 1986 Reliability analysis of chemical processes by the DYLAM approach – Reliability Engineering 14: 163-182.
Norman, D.A. 1981 Categorization of action slips – Psychological Review 88: 1-15.
Norusis, M.J. 1983 Introductory statistics guide SPSS X – McGraw-Hill Book Company (New York): 276 pp.
Nuclear News 1986 Chernobyl: the Soviet report – American Nuclear Society (Illinois): 59-66.
NVvE (Nederlandse Vereniging voor Ergonomie) 1988 Ergonomie – Tijdschrift voor Ergonomie 13: (inside cover).
Okma, A.N. 1987 Faalkansverdelingen van menselijke fouten – Technische Hogeschool Delft (Delft) Report N-276: 40 pp.
Pedersen, O.M. 1985 Human risk contributions in process industry: guides for their pre-identification in well-structured activities and for post-incident analysis – Risø National Laboratory (Roskilde) Report Risø-M-2513: 70 pp.
Pew, R.W. 1969 The speed-accuracy operating characteristic – Acta Psychologica 30: 16-26.
Pope, A. 1709 Essay on man and essay on criticism – Parsons and Galignani (Paris, 1806): 1-72.
Raiffa, H. 1970 Decision analysis. Introductory lectures on choices under uncertainty (2nd printing) – Addison-Wesley (Reading): 356 pp.
Rasmussen, J. 1978 Notes on human error analysis and prediction – Risø National Laboratory (Roskilde) Report Risø-M-2139: 53 pp.
Rasmussen, J. 1982a Human reliability in risk analysis. *In*: A.E. Green (ed.): High risk safety technology – John Wiley & Sons Ltd. (New York): 143-170.
Rasmussen, J. 1982b Human errors. A taxonomy for describing human malfunction in industrial installations – Journal of Occupational Accidents 4: 311-333.
Rasmussen, J. 1985 Human error data. Facts of fiction? – Risø National Laboratory (Roskilde) Report Risø-M-2499: 22 pp.
Rasmussen, J. 1987a Human error mechanisms in complex work environments – Risø National Laboratory (Roskilde) Report Risø-M-2679: 23 pp.
Rasmussen, J. 1987b Approaches to the control of the effects of human error on chemical plant safety – Risø National Laboratory (Roskilde) Report Risø-M-2638: 27 pp.
Rasmussen J. & O.M. Pedersen 1982 Formalized search strategies for human risk contributions: a framework for further development – Risø National Laboratory (Roskilde) Report Risø-M-2351: 32 pp.
Reason, J. 1985 Slips and mistakes: two distinct classes of human error? *In*: D.J. Oborne: Comtemporary ergonomics 1985: proceedings of the Ergonomics Society's Annual Conference (Nottingham, 1985) – Ergonomics Society (London): 103-110.
Reason, J. 1987a A framework for classifying errors. *In*: J. Rasmussen, K. Duncan & J. Leplat (eds.): New technology and human error – John Wiley & Sons Ltd. (Chichester): 5-14.
Reason, J. 1987b Generic error-modelling system (GEMS): a cognitive framework for locating common human error forms. *In*: J. Rasmussen, K. Duncan & J. Leplat (eds.): New technology and human error – John Wiley & Sons Ltd. (Chichester): 63-83.

Reason, J.T. & D.E. Embrey 1985 Human factors principles relevant to the modelling of human errors in abnormal conditions of nuclear and major hazardous installations – Human Reliability Associates Ltd. (Dalton): 148 pp.

Rigby, L.V. 1971 The nature of human error – Chemical Technology (December): 712-718.

Rouse, W.B. & S.H. Rouse 1983 Analysis and classification of human error – IEEE Transactions on Systems, Man, and Cybernetics 13: 539-549.

Schoof, F. 1987 Onderzoek van een model van het menselijk handelen volgens een vastgestelde procedure – Technische Universiteit Delft: 70 pp. + appendix.

Seaver, D.A. & W.G. Stillwell 1983 Procedures for using expert judgment to estimate human error probabilities in nuclear power plant operations – Sandia National Laboratories (Albuquerque) Report SAND82-7054 (also NUREG/CR-2743): 119 pp.

SEP (Samenwerkende Elektriciteits-Produktiebedrijven) 1975 Risico-analyse van de splijtstofcyclus in Nederland (RASIN) – N.V. Sep (Arnhem): 4 volumes + summary.

Sheridan, T.B. 1983 Measuring, modeling, and augmenting reliability of man-machine systems – Automatica 19: 637-645.

Siegel, S. 1956 Nonparametric statistics for the behavioral sciences – McGraw-Hill Kogakusha, Ltd. (Tokyo): 312 pp.

Siegel, A.I., W.D. Bartter, J.J. Wolf, H.E. Knee & P.M. Haas 1984 Maintenance personnel performance simulation (MAPPS) model – Oak Ridge National Laboratory (Oak Ridge) Report ORNL/TM-9041 (also NUREG/CR-3626): volume 1 + volume 2.

Spettell, C.M., E.A. Rosa, P.C. Humphreys, and D.E. Embrey 1986 Application of SLIM-MAUD: a test of an interactive computer-based method for organizing expert assessment of human performance and reliability, volume 2 – Brookhaven National Laboratory (New York) Report BNL-NUREG-51828 (also NUREG/CR-4016): 213 pp.

Stassen, H.G., J.J. Kok, R. v.d. Veldt & G. Heslinga 1985 Modelling human operator performance, possibilities and limitations. *In*: G. Johannsen, G. Mancini & L. Martensson (eds.): Analysis, design and evaluation of man-machine systems (2nd IFAC/IFIP/IFORS/IEA conference, Varese, 1985) – Commission of the European Communities (Ispra): 101-106.

Swain, A.D. 1987 Accident sequence evaluation program human reliability analysis procedure – Sandia National Laboratories (Albuquerque) Report SAND86-1996 (also NUREG/CR-4772): 161 pp.

Swain, A.D. & H.E. Guttmann 1983 Handbook of human reliability analysis with emphasis on nuclear power plant applications – Sandia National Laboratories (Albuquerque) Report SAND80-0200 (also NUREG/CR-1278): 698 pp.

Takahashi, Y., M.J. Rabins & D.M. Auslander 1972 Control and dynamic systems (2nd printing) – Addison-Wesley (Reading): 800 pp.

Taylor, J.R. 1979 A background to risk analysis, volume 4 – Risø National Laboratory (Roskilde): 735-856.

Terano, T., Y. Murayama & N. Akiyama 1983 Human reliability and safety evaluation of man-machine systems – Automatica 19: 719-722.

Thomas, B. 1984 Les arrêts de production imprevus du parc REP Français. *In*: Proceedings of the IAEA meeting in Karlsruhe – International Atomic Energy Agency (Wien): 43-61.

Topmiller, D.A., J.S. Eckel & E.J. Kozinsky 1982 Human reliability data bank for nuclear power plant operations. Volume 1: A review of existing human reliability data banks – Sandia National Laboratories (Albuquerque) Report SAND82-7057/1 (also NUREG/CR-2744/1): 217 pp.

Tribus, M. 1969 Rational descriptions, decisions and designs – Pergamon (New York): 478 pp.

Unwin, S.D. 1984 An introduction to fuzzy set theory with a view to the quantification and propagation of vagueness in probabilistic risk and reliability assessment – United Kingdom Atomic Energy Authority (Harwell) Report SRD R301: 25 pp.

USNRC (United States Nuclear Regulatory Commission) 1975 Reactor safety study. An assessment of accident risks in U.S. commercial nuclear power plants – USNRC (Washington) Report NUREG 75/014 (also WASH-1400): 198 pp. + annexes and summary.

USNRC (United States Nuclear Regulatory Commission) 1981 Fault tree handbook – USNRC (Washington) Report NUREG-0492: 207 pp.
USNRC (United States Nuclear Regulatory Commission) 1983 PRA procedures guide. A guide to the performance of probabilistic risk assessments for nuclear power plants – USNRC (Washington) Report NUREG/CR-2300: 2 volumes.
VDEN (Vereniging van Directeuren van Elektriciteitsbedrijven in Nederland) 1981 Analyse van de niet-beschikbaarheid van elektriciteitsproduktiemiddelen – VDEN (Arnhem).
Vestrucci, P. 1988 The logistic model for assessing human error probabilities using the SLIM method – Reliability Engineering and System Safety 21: 189-196.
Vos, A.D.L. de 1986 Een overzicht van de belangrijkste methoden voor de analyse van de menselijke betrouwbaarheid – Technische Hogeschool Delft (Delft) Report S-389: 97 pp.
Vos, A.D.L. de 1987 Bomen bij de HOR, een onderzoek met gebeurtenissenbomen naar de gevolgen van menselijk falen bij de start van de Hoger Onderwijs Reactor – Technische Hogeschool Delft (Delft) Report A-389: 152 pp.
Wagenaar, W.A. 1983 Menselijk falen in de industrie. *In*: Teksten van de gehouden lezingen op het symposium 'Industriële veiligheid' (Noordwijkerhout, 1983) – Bureau Industriële Veiligheid TNO (Rijswijk): 191-195.
Weersch, M.J.H. van 1986a Analyse van de startprocedure van de proefketelinstallatie. Deel 1: Oriëntatie – N.V. KEMA (Arnhem) Report WSK/30119-10: 30 pp.
Weersch, M.J.H. van 1986b Analyse van de startprocedure van de proefketelinstallatie. Deel 2: Kwalificatie – N.V. KEMA (Arnhem) Report WSK/30119-11: 99 pp.
Weersch, M.J.H. van 1986c Analyse van de startprocedure van de proefketelinstallatie. Deel 3: Kwantificatie – N.V. KEMA (Arnhem) Report WSK/30119-12: 43 pp.
Weinstein, M.C. & H.V. Fineberg 1980 Clinical decision analysis – W.B. Saunders Company (Philadelphia): 351 pp.
Wickelgren, W.A. 1965 Acoustic similarity and intrusion errors in short-term memory – Journal of Experimental Psychology 70: 102-108.
Wickelgren, W.A. 1966a Phonemic similarity and interference in short-term memory for single letters – Journal of Experimental Psychology 71: 396-404.
Wickelgren, W.A. 1966b Short-term recognition memory for single letters and phonemic similarity of retroactive interference – Quarterly Journal of Experimental Psychology: 55-61.
Wijlhuizen, G.J. 1986 Faalkansverdelingen van menselijke fouten – Technische Hogeschool Delft (Delft): 40 pp.
Willems, Th.J.A. 1980 Doel, werking, opbouw en specificatie van de proefketelinstallatie – N.V. KEMA (Arnhem) Report WSK/0655-32: 51 pp.
Williams, J.C. 1985 Validation of human reliability assessment techniques – Reliability Engineering 11: 149-162.
Wittenberg, H. 1978 De veiligheid in de luchtvaart en haar bewaking – Technische Hogeschool Delft (Delft) Report LR-260.
Woods, D.D., E.M. Roth & L.F. Hanes 1986 Models of cognitive behavior in nuclear power plant personnel. A feasibility study – Westinghouse Research and Development Center (Pittsburgh) Report NUREG/CR-4532: volume 1 + volume 2.
Zadeh, L.A. 1965 Fuzzy sets – Information and Control 8: 338-353.

Appendix A

List of abbreviations and symbols

This appendix presents the abbreviations frequently used in this study, as well as the symbols frequently used in the case studies (chapters 5 and 8) and the theoretical studies (chapters 6 and 7).

Abbreviations frequently used

DYLAM	dynamic logical analytical methodology
HEP	human-error probability
HPSA	human-performance safety assessment
HRA	human-reliability assessment
KEB	KEMA experimental boiler
MAUD	multi-attribute utility decomposition
MRF	man-related feature
RAP	recovery-attempt probability
PRA	probabilistic risk assessment
PSF	performance-shaping factor
SLIM	success likelihood index method
THERP	technique for human error rate prediction
THESIS	technique for human-error-sequence identification and signification

Symbols frequently used in the case study (chapter 5) and in the field study (chapter 8)

A, B, C, D, E, F, G	control valves/control devices
	F represents a set of four control valves/control devices (F_1 through F_4)
with subscript	outcome
with subscript and apostrophe	event sequence or error sequence
c, d, e, h, o, p, t, u	subscripts denoting control-device positions
H_1 through H_8	transfer functions describing the dynamic properties of the process
I_1, I_2, I_3	weighting factors
K	cost function
R	return outcome
R′	event sequence leading to return outcome
S	success (consequence)

SC	safety component
T	temperature lower than desired (consequence)
U	unacceptably strong temperature increase (consequence)
V	very high pressure (consequence)
z_1	temperature (variable)
z_2	flame conditions (variable)
z_3	pressure (variable)
z_4	flow (variable)
a, a_1 through a_4	probabilities
b_1 through b_3	probabilities
b_{11}, b_{12}, b_{21}, b_{22}	probabilities
b_{31}, b_{32}, b_{41}, b_{42}	probabilities
p_1 through p_4	probabilities

Symbols frequently used in the theoretical study (chapters 6 and 7)

A, C, E	events in the original tree representing a human error YES/NO
$A^{(x)}$, $C^{(x)}$, $E^{(x)}$	events in the recovery tree of set j,$i^{(x)}$ representing a human error YES/NO
B, D, F	events in the original tree representing a recovery attempt YES/NO
$B^{(x)}$, $D^{(x)}$, $F^{(x)}$	events in the recovery tree of set j,$i^{(x)}$ representing a recovery attempt YES/NO
a through f	probabilities to follow the YES-direction at events A through F
(as subscripts)	a dependence upon failure at events A through F, respectively, or $A^{(x)}$ through $F^{(x)}$, respectively
$\bar{a}$ through $\bar{f}$	probabilities to follow the NO-direction at events A through F
(as subscripts)	a dependence upon success at events A through F, respectively, or $A^{(x)}$ through $F^{(x)}$, respectively
$a^{(x)}$ through $f^{(x)}$	probabilities to follow the YES-direction at events $A^{(x)}$ through $F^{(x)}$, respectively
$\bar{a}^{(x)}$ through $\bar{f}^{(x)}$	probabilities to follow the NO-direction at events $A^{(x)}$ through $F^{(x)}$, respectively
i, k	procedure number or THESIS event tree number (i = 1,2,...,u); (k = 1,2,...,u)
j	path number leading to a return outcome in THESIS event tree i (j = 1,2,...,w_i)
m	path number leading to a return outcome in THESIS event tree k (m = 1,2,...,w_k)
q	path number leading to a final outcome (q = 1,2,...,v)
x	variable expressing the number of recovery attempts (x = 1,2,...,t)

y	variable used at the recovery-attempt probability to denote the number of errors made in the THESIS event tree
F_{qi}	final outcome q of original tree i
f_{qi}	probability of F_{qi}
$F^{(x)}_{qkji}$	final outcome q of recovery tree k of set $j,i^{(x)}$
$f^{(x)}_{qkji}$	probability of $F^{(x)}_{qkji}$
L	extension quotient to express the highest influence of a parameter on an outcome probability
L_{max}	maximum L in a specific case (case I, case II, case III)
R_{ji}	return outcome j of original tree i
r_{ji}	probability of R_{ji}
$R^{(x)}_{mkji}$	return outcome m of recovery tree k of set $j,i^{(x)}$
$r^{(x)}_{mkji}$	probability of $R^{(x)}_{mkji}$
r_n	sum of the return probabilities of the THESIS module of the n^{th} action in the procedure in case of no event dependence
α	parameter expressing the event dependence between human errors
β	parameter expressing the event dependence between recovery attempts
γ	parameter expressing the recovery dependence between human errors
δ	parameter expressing the recovery dependence between recovery attempts
ε	return level
ζ	type of recovery dependence
η	minimum value for the recovery-attempt probability
ϑ	maximum value for the recovery-attempt probability
λ	number of errors where ϑ is valid
$\tau^{(0)}_q$	total probability of a final outcome q of the original trees
$\tau^{(t)}_q$	total probability of a final outcome q taking into account that t recovery attempts have been made
τ_q	$\tau^{(t)}_q$ for $t \rightarrow \infty$
υ	sum of the return probabilities of the original trees
$\varphi^{(x)}_{qi}$	row vector containing the outcome probabilities $f^{(x)}_{qkji}$
$\phi^{(x)}_q$	matrix containing the row vectors $\varphi^{(x)}_{qi}$
$\psi^{(x)}_{ki}$	matrix containing the return probabilities $r^{(x)}_{mkji}$
$\Psi^{(x)}$	matrix containing the matrices $\psi^{(x)}_{ki}$
ω_i	row vector containing the return probabilities r_{ji}
Ω	matrix containing the row vectors ω_i
$+$	subscript to denote positive event dependence or positive recovery dependence
$-$	subscript to denote negative event dependence or negative recovery dependence

Appendix B

Results of the sensitivity analysis

This appendix presents the detailed results of the sensitivity analysis (chapter 7) performed with the theoretical model.

Table B-1

Influence of the event dependence for the cases I, II and III. The parameter α represents the event dependence between the human errors; the parameter β represents the recovery dependence between the recovery attempts. The asterix (*) indicates the operating point.

		case I		case II				case III							
		τ_1	τ_2	τ_1	τ_2	τ_3	τ_4	τ_1	τ_2	τ_3	τ_4	τ_5	τ_6	τ_7	τ_8
α	0.0	-	-	9.826 E-1	8.69 E-3	8.60 E-3	7.57 E-5	9.731 E-1	9.00 E-3	8.70 E-3	8.19 E-5	8.75 E-3	8.00 E-5	7.97 E-5	7.29 E-7
	0.5*	-	-	9.873 E-1	4.65 E-3	4.59 E-3	3.48 E-3	9.823 E-1	4.75 E-3	3.94 E-3	8.26 E-4	3.06 E-3	1.43 E-3	2.02 E-3	1.62 E-3
	1.0	-	-	9.919 E-1	5.67 E-4	5.45 E-4	6.98 E-3	9.916 E-1	4.33 E-4	2.67 E-4	3.13 E-4	1.09 E-5	3.79 E-4	4.35 E-4	6.58 E-3
L		-	-	1.01	15.33	15.78	92.21	1.02	20.79	33.33	10.09	802.75	17.88	25.35	9026.06
L_{max}		-		92.21				9026.06							

		case I		case II				case III							
		τ_1	τ_2	τ_1	τ_2	τ_3	τ_4	τ_1	τ_2	τ_3	τ_4	τ_5	τ_6	τ_7	τ_8
β	0.0	-	-	9.879 E-1	4.50 E-3	4.80 E-3	2.78 E-3	9.834 E-1	4.75 E-3	3.85 E-3	7.40 E-4	3.17 E-3	1.34 E-3	1.70 E-3	1.10 E-3
	0.5*	-	-	9.873 E-1	4.65 E-3	4.59 E-3	3.48 E-3	9.823 E-1	4.75 E-3	3.94 E-3	8.26 E-4	3.06 E-3	1.43 E-3	2.02 E-3	1.62 E-3
	1.0	-	-	9.867 E-1	4.80 E-3	4.41 E-3	4.13 E-3	9.814 E-1	4.73 E-3	4.01 E-3	8.96 E-4	2.94 E-3	1.50 E-3	2.35 E-3	2.21 E-3
L		-	-	1.00	1.07	1.09	1.49	1.00	1.00	1.04	1.21	1.08	1.12	1.38	2.01
L_{max}		-		1.49				2.01							

Table B-2
Influence of the recovery dependence for the cases I, II and III. The parameter γ represents the recovery dependence between the human errors; the parameter δ represents the recovery dependence between the recovery attempts. The asterix (*) indicates the operating point.

		case I		case II				case III							
		τ_1	τ_2	τ_1	τ_2	τ_3	τ_4	τ_1	τ_2	τ_3	τ_4	τ_5	τ_6	τ_7	τ_8
γ	0.0	9.950 E-1	5.04 E-3	9.896 E-1	3.81 E-3	3.73 E-3	2.86 E-3	9.852 E-1	4.15 E-3	3.36 E-3	6.50 E-4	2.53 E-3	1.17 E-3	1.61 E-3	1.34 E-3
	0.5*	9.928 E-1	7.19 E-3	9.873 E-1	4.65 E-3	4.59 E-3	3.48 E-3	9.823 E-1	4.75 E-3	3.94 E-3	8.26 E-4	3.06 E-3	1.43 E-3	2.02 E-3	1.62 E-3
	1.0	9.900 E-1	9.99 E-3	9.851 E-1	5.32 E-3	5.32 E-3	4.31 E-3	9.801 E-1	5.14 E-3	4.25 E-3	9.15 E-4	3.42 E-3	1.62 E-3	2.46 E-3	2.07 E-3
L		1.01	1.98	1.00	1.40	1.43	1.51	1.01	1.24	1.26	1.41	1.35	1.38	1.53	1.54
L_{max}		1.98		1.51				1.54							

		case I		case II				case III							
		τ_1	τ_2	τ_1	τ_2	τ_3	τ_4	τ_1	τ_2	τ_3	τ_4	τ_5	τ_6	τ_7	τ_8
δ	0.0	9.925 E-1	7.53 E-3	9.871 E-1	4.68 E-3	4.63 E-3	3.60 E-3	9.822 E-1	4.75 E-3	3.95 E-3	8.37 E-4	3.07 E-3	1.46 E-3	2.07 E-3	1.69 E-3
	0.5*	9.928 E-1	7.19 E-3	9.873 E-1	4.65 E-3	4.59 E-3	3.48 E-3	9.823 E-1	4.75 E-3	3.94 E-3	8.26 E-4	3.06 E-3	1.43 E-3	2.02 E-3	1.62 E-3
	1.0	9.933 E-1	6.68 E-3	9.875 E-1	4.62 E-3	4.54 E-3	3.35 E-3	9.825 E-1	4.74 E-3	3.94 E-3	8.12 E-4	3.04 E-3	1.40 E-3	1.97 E-3	1.55 E-3
L		1.00	1.13	1.00	1.01	1.02	1.07	1.00	1.00	1.00	1.03	1.01	1.04	1.05	1.09
L_{max}		1.13		1.07				1.09							

Table B-3
Influence of the return level, ε, and the type of recovery dependence, ζ. The asterix (*) indicates the operating point.

		case I		case II				case III							
		τ_1	τ_2	τ_1	τ_2	τ_3	τ_4	τ_1	τ_2	τ_3	τ_4	τ_5	τ_6	τ_7	τ_8
ε	0 *	9.928 E-1	7.19 E-3	9.873 E-1	4.65 E-3	4.59 E-3	3.48 E-3	9.823 E-1	4.75 E-3	3.94 E-3	8.26 E-4	3.06 E-3	1.43 E-3	2.02 E-3	1.62 E-3
	1	-	-	9.873 E-1	4.49 E-3	4.49 E-3	3.73 E-3	9.824 E-1	4.65 E-3	3.85 E-3	8.18 E-4	3.02 E-3	1.47 E-3	2.04 E-3	1.76 E-3
	2	-	-	9.855 E-1	4.87 E-3	4.77 E-3	4.82 E-3	9.809 E-1	4.84 E-3	4.07 E-3	7.80 E-4	3.22 E-3	1.57 E-3	2.36 E-3	2.30 E-3
	3	-	-	-	-	-	-	9.804 E-1	4.71 E-3	4.05 E-3	8.30 E-4	3.33 E-3	1.71 E-3	2.50 E-3	2.47 E-3
L		-	-	1.00	1.08	1.06	1.39	1.00	1.04	1.06	1.06	1.10	1.20	1.24	1.52
L_{max}		-		1.39				1.52							

		case I		case II				case III							
		τ_1	τ_2	τ_1	τ_2	τ_3	τ_4	τ_1	τ_2	τ_3	τ_4	τ_5	τ_6	τ_7	τ_8
ζ	pos *	9.928 E-1	7.19 E-3	9.873 E-1	4.65 E-3	4.59 E-3	3.48 E-3	9.823 E-1	4.75 E-3	3.94 E-3	8.26 E-4	3.06 E-3	1.43 E-3	2.02 E-3	1.62 E-3
	neg	9.950 E-1	5.02 E-3	9.891 E-1	4.05 E-3	3.94 E-3	2.91 E-3	9.839 E-1	4.47 E-3	3.62 E-3	7.46 E-4	2.78 E-3	1.29 E-3	1.77 E-3	1.40 E-3
L		1.00	1.43	1.00	1.15	1.16	1.20	1.01	1.06	1.09	1.11	1.10	1.11	1.14	1.16
L_{max}		1.43		1.20				1.16							

Table B-4

Influence of the RAP for the cases I, II and III. The parameter η represents the RAP valid when no errors are made; the parameter ϑ represents the RAP valid when the maximum number of errors possible in a preocedure, n, is made; the parameter λ represents the number of errors where ϑ is valid. The asterix (*) indicates the operating point.

		case I		case II				case III							
		τ_1	τ_2	τ_1	τ_2	τ_3	τ_4	τ_1	τ_2	τ_3	τ_4	τ_5	τ_6	τ_7	τ_8
η	0.0*	9.928 E-1	7.19 E-3	9.873 E-1	4.65 E-3	4.59 E-3	3.48 E-3	9.823 E-1	4.75 E-3	3.94 E-3	8.26 E-4	3.06 E-3	1.43 E-3	2.02 E-3	1.62 E-3
	0.01	9.928 E-1	7.23 E-3	9.872 E-1	4.66 E-3	4.61 E-3	3.48 E-3	9.823 E-1	4.76 E-3	3.95 E-3	8.25 E-4	3.07 E-3	1.44 E-3	2.03 E-3	1.62 E-3
	0.1	9.924 E-1	7.65 E-3	9.870 E-1	4.73 E-3	4.74 E-3	3.50 E-3	9.819 E-1	4.91 E-3	4.05 E-3	8.16 E-4	3.20 E-3	1.47 E-3	2.06 E-3	1.62 E-3
L		1.00	1.06	1.00	1.02	1.03	1.01	1.00	1.03	1.03	1.01	1.05	1.03	1.02	1.00
L_{max}		1.06		1.03				1.05							

		case I		case II				case III							
		τ_1	τ_2	τ_1	τ_2	τ_3	τ_4	τ_1	τ_2	τ_3	τ_4	τ_5	τ_6	τ_7	τ_8
ϑ	0.0	9.900 E-1	1.00 E-2	9.851 E-1	4.95 E-3	4.95 E-3	5.05 E-3	9.801 E-1	4.93 E-3	4.10 E-3	8.49 E-4	3.27 E-3	1.68 E-3	2.50 E-3	2.55 E-3
	0.5*	9.928 E-1	7.19 E-3	9.873 E-1	4.65 E-3	4.59 E-3	3.48 E-3	9.823 E-1	4.75 E-3	3.94 E-3	8.26 E-4	3.06 E-3	1.43 E-3	2.02 E-3	1.62 E-3
	0.99	9.963 E-1	3.71 E-3	9.895 E-1	4.29 E-3	4.05 E-3	2.17 E-3	9.845 E-1	4.51 E-3	3.75 E-3	7.56 E-4	2.81 E-3	1.17 E-3	1.59 E-3	9.46 E-4
L		1.01	2.70	1.00	1.15	1.22	2.33	1.00	1.09	1.09	1.17	1.16	1.44	1.57	2.70
L_{max}		2.70		2.33				2.70							

		case I		case II				case III							
		τ_1	τ_2	τ_1	τ_2	τ_3	τ_4	τ_1	τ_2	τ_3	τ_4	τ_5	τ_6	τ_7	τ_8
λ	n *	9.928 E-1	7.19 E-3	9.873 E-1	4.65 E-3	4.59 E-3	3.48 E-3	9.823 E-1	4.75 E-3	3.94 E-3	8.26 E-4	3.06 E-3	1.43 E-3	2.02 E-3	1.62 E-3
	1	9.928 E-1	7.19 E-3	9.893 E-1	4.13 E-3	3.90 E-3	2.69 E-3	9.860 E-1	4.02 E-3	3.30 E-3	7.59 E-4	2.33 E-3	1.03 E-3	1.53 E-3	1.06 E-3
L		1.00	1.00	1.00	1.13	1.18	1.29	1.00	1.18	1.19	1.09	1.31	1.39	1.32	1.53
L_{max}		1.00		1.29				1.53							

Appendix C

Results of the laboratory experiment

This appendix presents the detailed results of the laboratory experiment (chapter 9) in the form of histograms.

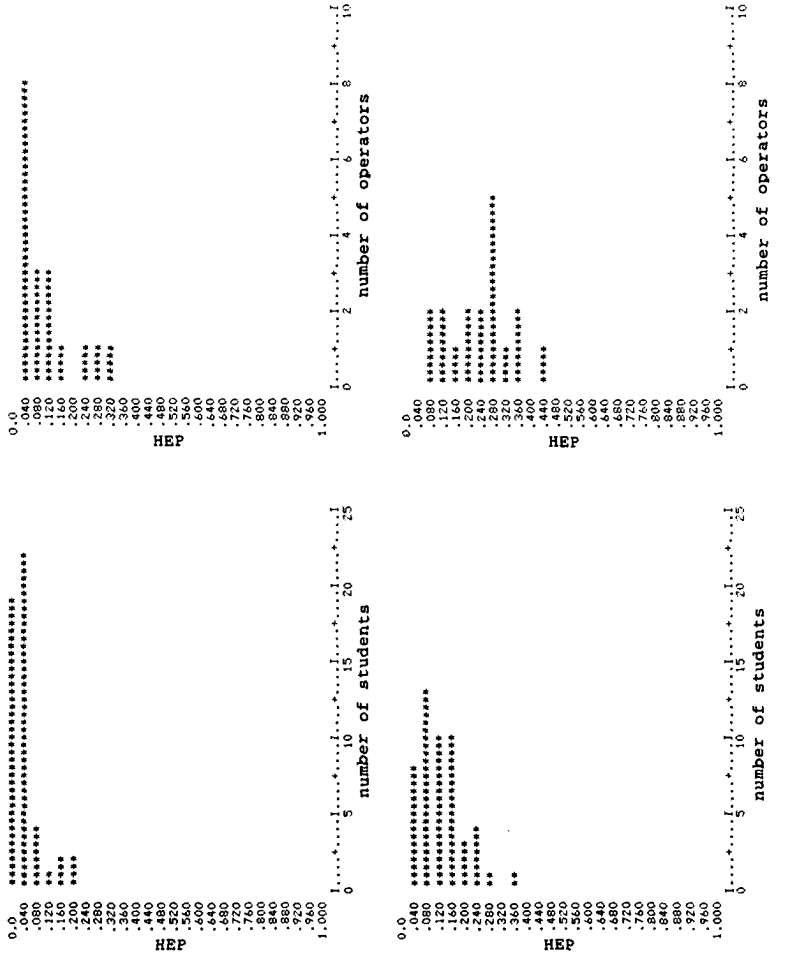


Fig. C-1
Histograms of the recognition errors for the operator group (top) and the student group (bottom). The low-confusion condition is valid for the two distributions on the left; the high-confusion condition is valid for the two distributions on the right.

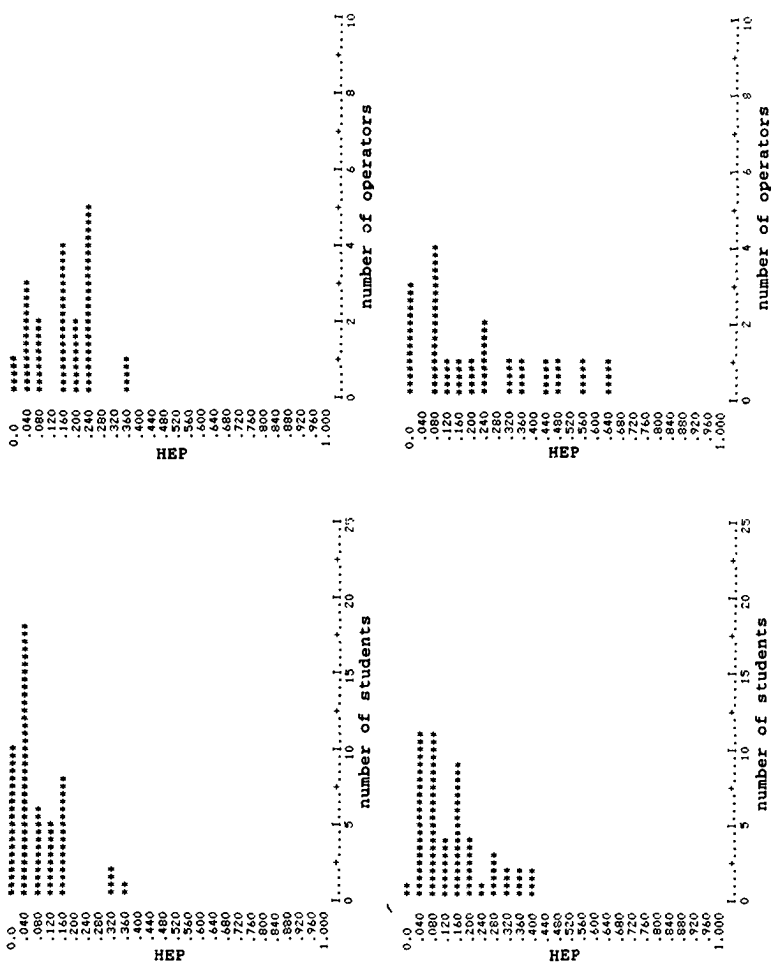


Fig. C-2
Histograms of the errors in the search task for the operator group (top) and the student group (bottom).
Left: low time stress. Right: high time stress.

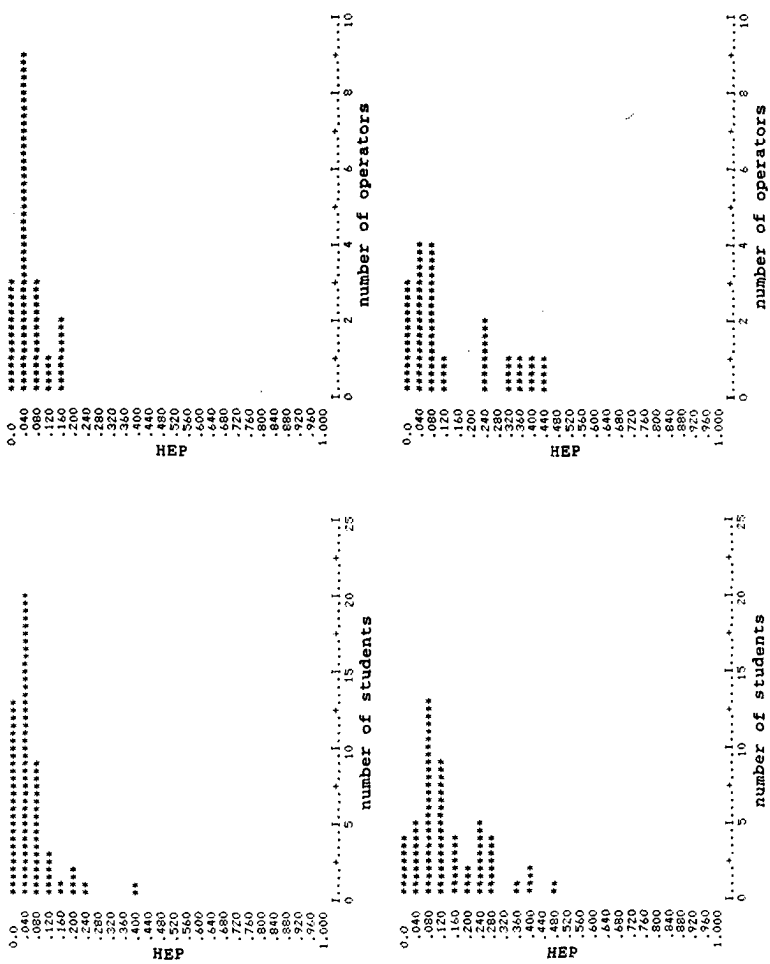


Fig. C-3
Histograms of the errors in the reading task for the operator group (top) and the student group (bottom).
Left: low time stress. Right: high time stress.

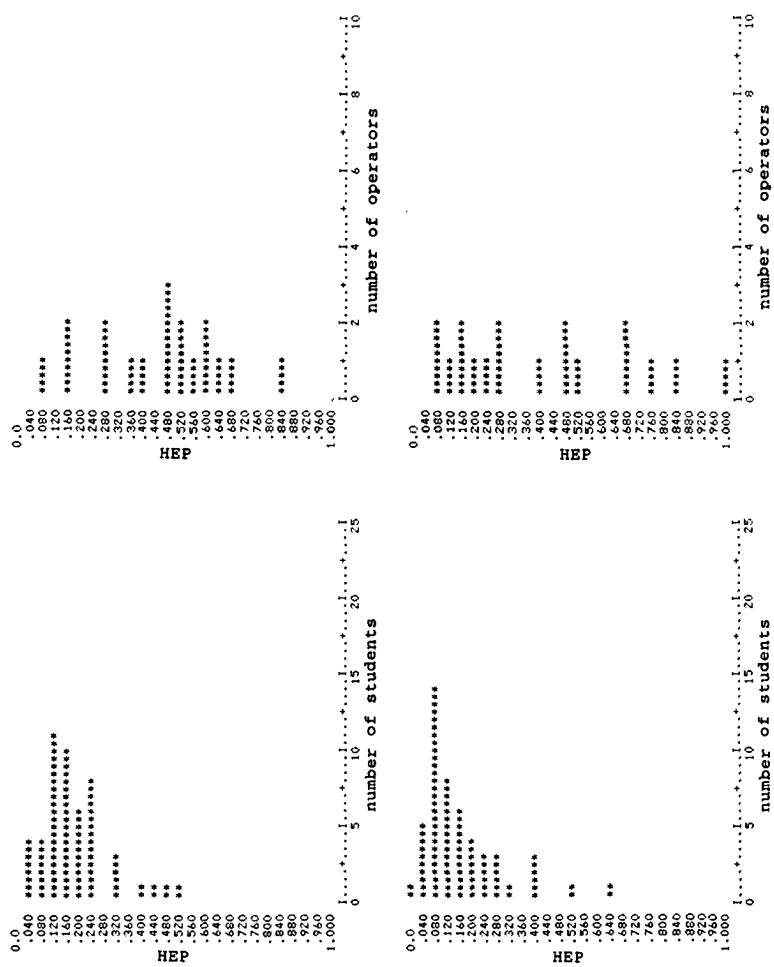


Fig. C-4
Histograms of the too late reactions in the search task for the operator group (top) and the student group (bottom).
Left: low time stress. Right: high time stress.

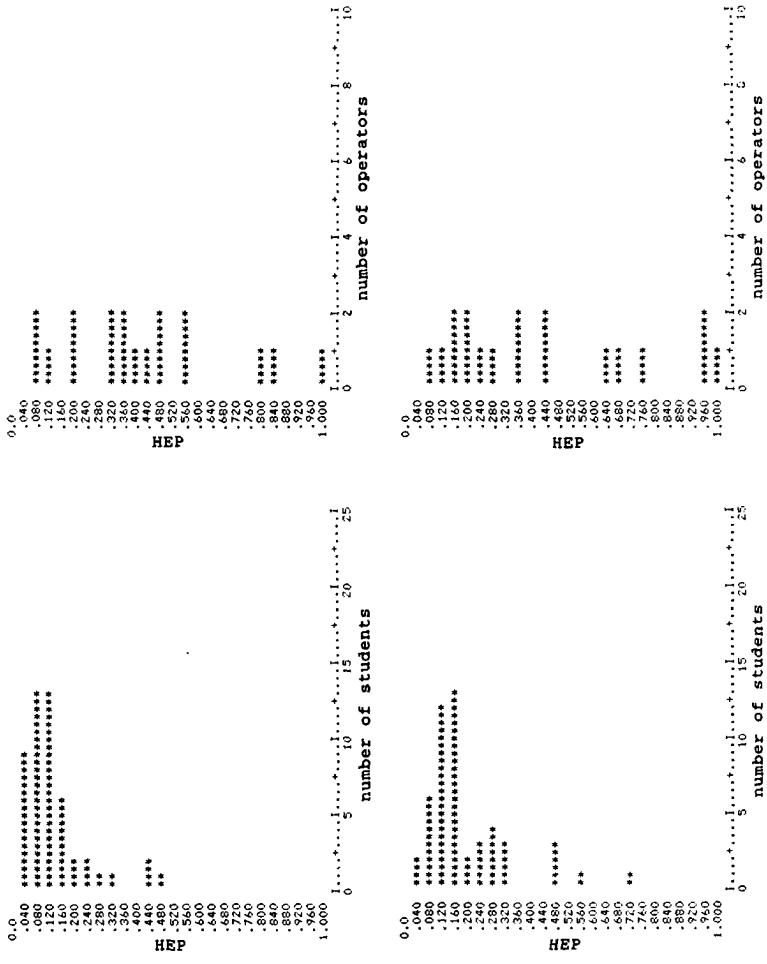


Fig. C-5
Histograms of the too late reactions in the reading task for the operator group (top) and the student group (bottom).
Left: low time stress. Right: high time stress.

Summary

The human factor appears to have an important influence on the safety of complex installations, but much less is known about this factor than about the technical factor. This is particularly true in the case of human performance causing an undesired situation (initiating event) during a change in a process state (start-up and shut-down) according to a given procedure. One of the techniques applied to the analysis of technical failures is the event-tree technique. This method is also used to analyze single human errors. The aim of the present study was to investigate whether the event-tree technique can be used for the analysis of sequences of human errors that could cause initiating events. The scope of the study was limited to a consideration of the performance of procedural actions.

The event-tree technique was modified to adapt it for this study and will be referred to as the 'Technique for Human-Error-Sequence Identification and Signification' (THESIS). The event trees used in this manner, i.e. THESIS event trees, appear to present additional problems if they are applied to human performance instead of technical systems. These problems, referred to as the 'Man-Related Features' of THESIS, are: the human capability to choose among several procedures, the ergonomics of the panel layout, human actions of a continuous nature, dependence between human errors, human capability to recover possible errors, the influence of memory during the recovery attempt, variability in human performance and correlations between human-error probabilities. The influence of these problems on the applicability of THESIS was assessed by means of mathematical analyses, field studies and laboratory experiments.

Mathematical analyses showed that, under certain conditions, the influence of memory during the recovery attempt is only a minor one as concerns probability quantification by means of THESIS event trees. This observation resulted in a highly simplified mathematical model for calculation of the probability that initiating events will occur due to sequences of human errors. The mathematical analyses also showed that the probability of making a recovery attempt can have some influence on the probability quantification and that dependence between human errors can have a rather important effect. In addition to data acquisition on human-error probabilities, of which the necessity is frequently stated in the literature, more attention should therefore be given to data acquisition for the dependence between human errors.

The influence of a number of the Man-Related Features mentioned above was investigated in field studies. It could be concluded that the human capability to achieve a certain goal by means of several procedures is an essential problem if there is dependence between human errors. Ergonomics can also have an important role, since the possibility that many selection errors can be made, renders the THESIS event tree

extensive and unclear. As the THESIS event tree is a discrete technique, continuous actions have to be broken down into small, distinct steps. This proved to be possible in the field studies involved in the present research.

A description for the variability of human performance was sought for in laboratory studies. An experimental setup was used for simulating a control-room procedure. It became clear from the results that the distribution frequently used in the literature but which was not measured explicitly (the log-normal distribution) could not be rejected. Moreover, relatively high correlations were found between a number of human-error probabilities, and these correlations could be assumed to have been due to human characteristics.

The main conclusion to be drawn from the study is that, with certain limitations, event trees can be used to predict sequences of human errors if procedural actions are performed. The limitations are related to the nature of the actions performed, the ergonomics of the panel layout, the existence of several procedures to achieve the same goal and the knowledge of all kinds of data, such as human-error probabilities, return-attempt probabilities, dependence between human errors, variability in human performance and correlations between human-error probabilities.

Samenvatting

De mens blijkt een belangrijke invloed te kunnen hebben op de veiligheid van complexe installaties, maar de kennis van de menselijke invloed is, vergeleken met kennis van de technische factor, vrij klein. Dit geldt in het bijzonder voor het menselijk handelen dat aanleiding is tot het ontstaan van een ongewenste situatie (begin-gebeurtenis) tijdens het veranderen van de toestand van een proces (starten en stoppen) volgens een bepaalde procedure. Eén van de technieken die worden toegepast om technisch falen te analyseren, is de gebeurtenissenboom-techniek. Deze techniek wordt ook toegepast voor de analyse van enkelvoudige menselijke fouten. Het doel van deze studie was na te gaan of de gebeurtenissenboom-techniek eveneens kan worden gebruikt voor de analyse van opeenvolgende menselijke fouten die begin-gebeurtenissen kunnen veroorzaken. Daarbij gaat het voornamelijk om het handelen van de mens bij het uitvoeren van procedurele taken.

De gebeurtenissenboom-techniek is voor deze studie aangepast en 'Technique for Human-Error-Sequence Identification and Signification' (THESIS) genoemd. De aldus gebruikte gebeurtenissenbomen, THESIS gebeurtenissenbomen, blijken bij de toepassing op menselijk handelen een aantal extra problemen met zich mee te brengen, vergeleken met de toepassing van gebeurtenissenbomen op technische systemen. Deze problemen, aangeduid met de term 'Man-Related Features' van THESIS, zijn: de mogelijkheid van de mens om verschillende procedures te kiezen, de ergonomie van de paneel-indeling, de menselijke handelingen met een continu karakter, de afhankelijkheid tussen menselijke fouten, de mogelijkheid van de mens eventuele fouten te herstellen, de geheugenwerking tijdens de herstelpoging, de variabiliteit in het menselijk gedrag en de correlaties tussen menselijke faalkansen. In deze studie is de invloed van deze problemen op de bruikbaarheid van THESIS geanalyseerd door middel van wiskundige analyses, praktijk-studies en laboratorium-experimenten.

Uit wiskundige analyses is gebleken dat de geheugenwerking tijdens de herstelpoging onder bepaalde condities nagenoeg geen invloed heeft op de uitkomsten van de kansberekeningen met THESIS gebeurtenissenbomen. Dit heeft een sterk vereenvoudigd wiskundig model opgeleverd voor de berekening van de kans dat begingebeurtenissen plaatsvinden door opeenvolgende menselijke fouten. Uit de wiskundige analyses is eveneens gebleken dat de kans om herstelpogingen te ondernemen enige invloed kan hebben op de kansberekening en dat de afhankelijkheid tussen menselijke fouten een vrij belangrijke invloed kan hebben. Naast de in de literatuur veelvuldig aangegeven noodzaak tot het verzamelen van meer gegevens over menselijke faalkansen, dient dan ook meer aandacht te worden gegeven aan het verzamelen van gegevens over de afhankelijkheid tussen menselijke fouten.

Met behulp van veldstudies is nagegaan in hoeverre een aantal van de Man-Related Features, zoals hierboven genoemd, een probleem opleverde voor het toepassen van THESIS. Geconcludeerd kan worden dat de mogelijkheid van de mens om een specifiek doel te bereiken door middel van verschillende procedures een belangrijk probleem vormt indien een afhankelijkheid tussen menselijke fouten aanwezig is. Ook de ergonomie speelt een belangrijke rol, daar de mogelijkheid tot veel keuzefouten de THESIS gebeurtenissenboom groot en onoverzichtelijk kan maken. Wegens het specifieke karakter van de THESIS gebeurtenissenboom, moeten continue handelingen worden opgedeeld in kleinere afzonderlijke stappen. In de uitgevoerde veldstudies is dit goed mogelijk gebleken.

Met behulp van laboratorium-studies is nagegaan op welke wijze de variabiliteit in menselijk gedrag kan worden beschreven. Hiertoe is een experimentele opstelling gebruikt waarbij op laboratoriumschaal een regelkamer-procedure is nagebootst. Uit de resultaten is naar voren gekomen dat de verdeling die tot op heden in de literatuur veelvuldig wordt toegepast, maar die niet expliciet gemeten is (de lognormale verdeling), niet kan worden verworpen. Ook zijn relatief hoge correlaties tussen een aantal menselijke faalkansen geconstateerd waarvan het aannemelijk is dat ze door menselijke eigenschappen zijn veroorzaakt.

De belangrijkste conclusie van de studie is dat gebeurtenissenbomen binnen bepaalde beperkingen kunnen worden gebruikt voor het voorspellen van opeenvolgende menselijke fouten bij het uitvoeren van procedurele handelingen. De beperkingen hangen samen met het karakter van de uit te voeren handelingen, de ergonomie van de paneel-indeling, de aanwezigheid van verschillende procedures om hetzelfde doel te bereiken en de kennis over allerlei gegevens, zoals menselijke faalkansen, herstelpogings-kansen, afhankelijkheden tussen menselijke fouten, variabiliteit in menselijk gedrag en correlaties tussen menselijke faalkansen.

Curriculum vitae

The author was born at Sneek on January 21, 1956. He attended high school at the 'Zandvliet Lyceum' in The Hague from 1968 to 1974 ('Atheneum-B' certificate). He then studied mechanical engineering at the Delft University of Technology. This study was completed in the Man-Machine Systems Group of the Laboratory for Measurement and Control in the Faculty of Mechanical Engineering and Marine Engineering.

Since the extended program was followed during attendance at university, the author worked on two research projects. The first project concerned a study into the ability of a mechanism to control coronary blood flow. The second project was a preliminary study into the influence of human performance on system safety. The author received his academic degree in 1983.

There followed employment by the Delft University of Technology from 1983 to 1988 to perform contract research for KEMA at Arnhem. The second project mentioned above was continued during this period. The main results are described in this book.

STELLINGEN

behorende bij het proefschrift

TECHNIQUE FOR HUMAN-ERROR-SEQUENCE IDENTIFICATION AND SIGNIFICATION

1

Het toepassen van de lognormale verdeling bij menselijke faalkansen lijkt gerechtvaardigd.

Dit proefschrift.

2

Te vaak ziet men een menselijke fout pas als een fout als het ongewenste gevolg volgt.

Dit proefschrift.

3

De bewering van Carnino dat het menselijk functioneren per definitie niet kan worden beschreven als dat van een technisch systeem is onterecht; afhankelijk van het abstractie-niveau van het menselijk handelen is zo'n beschrijving wel goed mogelijk.

Carnino, A. 1985 Human Reliability - Nuclear Engineering and Design 90: 365-369.

4

Bij het aannemen van radiologische werkers wordt onvoldoende rekening gehouden met de 'kanker-vatbaarheid'.

Gentner, N.E., D.P. Morrison & D.K. Myers 1988 Impact on radiogenic cancer risk of persons exhibiting abnormal sensitivity to ionizing radiation - Health Physics 55: 415-425.

5

Interstitiële osmolariteit speelt geen dominante rol bij coronaire autoregulatie.

Heslinga, G. 1981 De regelende werking van interstitieel osmotische druk bij coronaire autoregulatie - Delft University of Technology (Delft) Report WBMR A 256-I: 145 pp.

6

Het model zoals toegepast door Avolio et al. ter beschrijving van de hartspier-doorbloeding is fysiologisch onjuist.

Avolio, A.P., J.A.E. Spaan & J.D. Laird 1981 Coronary blood flow regulation and plasma protein concentration: studies in isolated rat hearts and in a control model. In: D. Garlick (ed.): Progress in Microcirculation Research - The University of New South Wales (Kensington): 337-351.

7

Aan de onderlinge afhankelijkheid van fouten, zowel technische als menselijke, wordt bij het verzamelen van gegevens te weinig aandacht besteed.

8

Voor het analyseren van fysiologische systemen wordt onvoldoende gebruik gemaakt van de mogelijkheden die de systeem- en regeltheorie bieden.

9

Om het aantal ongevallen in het verkeer te verminderen kan het geld dat met de verplichte autokeuring is gemoeid beter besteed worden aan het verbeteren van het menselijk handelen in het verkeer.

10

Een gokker is een aanhouder die verliest.

8 december 1988, G. Heslinga