Reliability Engineering **12** (1985) 63–78

Analysis of Human Reliability on Performing a Specific Action

Gerben Heslinga

Man-Machine Systems Group, Laboratory for Measurement and Control, Delft University of Technology, The Netherlands

(Received: 15 October 1984)

ABSTRACT

To analyse human reliability on performing a specific action, human reliability analysis (HRA) event trees are used involving the breakdown of an action into small elementary steps (events). An example of a specific action, the adjustment of a two-position switch, is analysed and the theory of event trees is explained briefly. The application of event trees in human reliability analysis involves more difficulties than in the case of technical systems, where event trees have been mainly used up until now. The main problem is that the operator is able to rectify his incorrect action, where memory effects play a significant role. In this study these difficulties are dealt with theoretically.

1. INTRODUCTION

This study was commenced following a request to determine the risk (a combination of the probability and the extent of malfunction) of shutting down a nuclear power plant. Since during shutdown many human actions have to be performed, human reliability may influence this risk relatively strongly. Therefore, it is essential to make a detailed analysis of human reliability with regard to failure modes and failure probabilities.

Each procedure to be performed by an operator is built on specific

The work reported is sponsored by the KEMA, Arnhem, The Netherlands.

Reliability Engineering 0143-8174/85/$03·30

actions. Certain actions will be performed several times during the procedure, and it makes sense to analyse each specific action separately. This will be done by making an HRA event tree of that action, after which these trees (modules) can be joined to reflect the entire procedure. Specific actions are, for instance, the adjustment of setpoints, simple two-position switches, multi-position switches, etc.

The use of event trees in human reliability analysis was started by Swain *et al.*[1] and Bell *et al.*,[2] and their work formed the basis for this study. The technique they employed is known as THERP (technique for human error rate prediction) and this is further extended here. With regard to performing a specific action, the technique involves actions being broken down into small elementary steps and each step forms an event in the HRA event tree. For each event a potential error must be identified and a failure probability (human error probability) found. This allows the calculation of the probability of success or failure in an action.

Here the interest is not only directed towards the success paths, but also to the failure paths of the HRA event tree, since these paths may indicate the routes to catastrophic consequences. These consequences are directly related to the risk of incorrect human actions. With the failure paths, the probability of such a consequence is to be calculated.

The aim of this study is therefore to discover whether the use of event trees is a good method for:

(a) the qualitative determination of failure courses of incorrect human actions ending in undesirable consequences;
(b) the quantification of the probabilities of those undesirable consequences occurring.

Important difficulties involved are the dependence among events of the HRA event tree, the capability of the operator in recovering an incorrect action and the influences of memory during recovery. Technical failures are not considered; this study is primarily concerned with human failures.

The object of this paper is to calculate theoretically the probability of occurrence of a particular consequence (failure or success) with regard to:

(a) the influences of dependence and memory mentioned above;
(b) the possibility of recovery;
(c) the carrying out of one specific action.

First, the paper gives a brief explanation of HRA event trees.

2. HUMAN RELIABILITY ANALYSIS EVENT TREES

The HRA event tree described considers an action by which a two-position switch is adjusted. The panel layout given in Fig. 1 is considered and it is assumed that switch 2 has to be changed. The corresponding HRA event tree is given in Fig. 2. On completing the HRA event tree, several consequences are possible: success consequence $\bar{s}$ (the correct

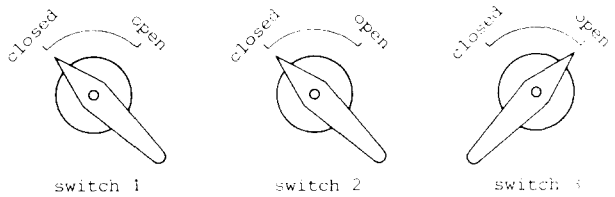


Fig. 1. Panel lay-out of three two-position switches.

switch is adjusted), and failure consequences $\bar{f}_q$ and the recovery consequence $\bar{r}_f$. As opposed to the success and failure consequences, recovery implies that the action does not end but will (partially) be repeated. With regard to Fig. 2 and further research, a symbol with a bar indicates an event or, where appropriate, a consequence, and one without a bar the *probability* of them.

The advantage of an event tree is that when the probabilities belonging to the separate events are known, multiplication of these probabilities yields the probability of occurrence of a certain consequence. With regard to Fig. 2, where it is assumed that there is no dependence between the separate events, the probability of adjusting the wrong switch 1, consequence $\bar{f}_2$, is

$$f_2 = (1 - D)(1 - C)B(1 - A)$$

and the probability r_2 of ending at the recovery consequence $\bar{r}_2$ is

$$r_2 = (1 - E)D(1 - C)B(1 - A)$$

A quantified example is given in Table 1. Most of the data used there have been taken from Swain *et al.*[1]

Also, when there is dependence between the events, it is possible to determine the probabilities of the consequences occurring by multiplying the separate event probabilities. However, this can only take place if the probabilities of the separate events are adapted so that the dependence is incorporated, resulting in conditional probabilities. The dependence

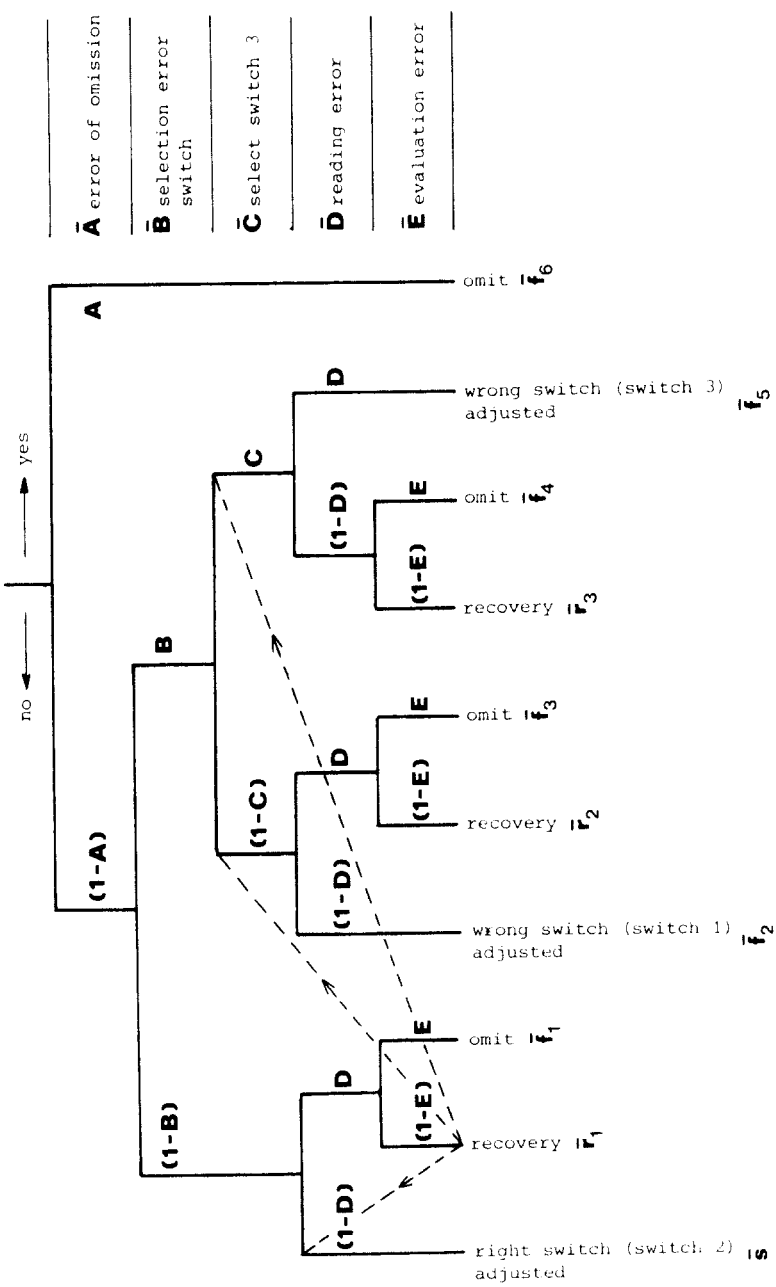
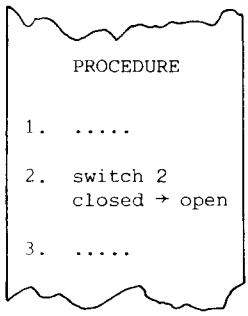
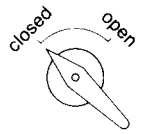
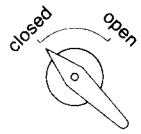


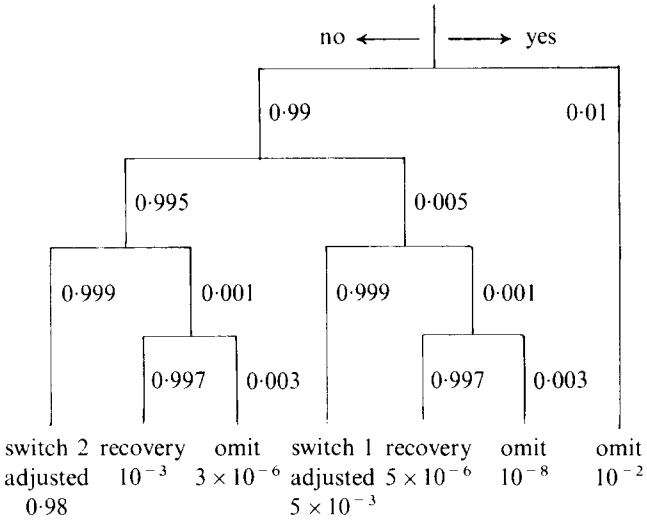
Fig. 2. HRA event tree concerning the adjustment of the two-position switch from Fig. 1. It is presumed that switch 2 has to be adjusted. It is assumed that there is no dependence between the events. The dotted lines represent the recovery lines of which an explanation is given in the text.

TABLE 1
Quantified Example of a Reliability Analysis of One Human Action from a Procedure









error of omission
0·01

selection error
0·005

reading error
0·001

evaluation error
0·003

success	recovery	failure	
switch 2	recovery	switch 1	omit
0·98	10^{-3} 5×10^{-6}	5×10^{-3}	3×10^{-6} 10^{-8} 10^{-2}
0·98	10^{-3}	5×10^{-3}	10^{-2}

between two events means that the failure probability of the second event depends on the success or failure of the first event. The dependence between events in one HRA event tree will be called *internal dependence*. It can be shown that if internal dependence is present, the change of the sequence of events in one tree affects the probabilities of the same consequences. The result is that more HRA event trees have to be formed, each with a selection probability expressing the probability of choosing that particular sequence of events.

In the case of the operator arriving at the recovery consequence, he will usually partially repeat his action and will go back somewhere in the HRA event tree. In Fig. 2, a few *recovery lines* have been drawn. Using one recovery line the operator returns to a particular event in the tree, repeating his action starting at that event. Although the operator does not really recover using a line to the right, these lines are also called recovery lines, and they are also taken into account in the recovery problem.

Theoretically it can be shown that recovery means starting a whole event tree again. This can be simply explained by assuming that there are no influences of memory during recovery and that there is no internal dependence implying one HRA event tree, e.g. Fig. 2. In that figure two recovery lines are drawn starting at a recovery offshoot returning to failure or success of event $\bar{C}$. These lines imply that, during recovery, failure has taken place at the preceding event $\bar{B}$. Therefore, one may draw only one recovery line to the preceding event representing the two recovery lines. In general, the same can be said about two recovery lines going back to failure or success of the preceding event. So, considering all the recovery lines, starting at a particular offshoot carrying the consequence recovery, these lines can be replaced by one recovery line going back to the initiating event of the HRA event tree. This means that, ending at the recovery consequence, the whole HRA event tree is started again. It is assumed that this statement of restarting the whole HRA event tree can also be applied to the practical case with internal dependence, and influences of memory during recovery.

The influences of memory during recovery mean that the probabilities of the same events of an HRA event tree need not be the same during recovery as during the first completion of the HRA event tree. To differentiate between these, the HRA event tree passed through the first time is called the *original tree* and the tree passed through during recovery is called the *recovery tree*. The dependence between the route passing through the recovery tree and the route passing through the original tree,

expressing the influences of memory, will be called *external dependence*. If there is only external dependence (no internal dependence) the number of recovery trees equals the number of paths leading to recovery (each path leading to recovery has its own recovery tree). Just as for the difference between the recovery tree and the original tree, the differences among the recovery trees themselves are reflected by unequal probabilities of the same events, expressing the influences of memory.

3. THEORETICAL ANALYSIS OF RECOVERY

To calculate the probability of success or the probability of a particular failure consequence taking into account the recovery possibility, it is provisionally assumed that there is no internal or external dependence. Thus there is only one original tree and one recovery tree, and both trees are the same. The probability of a particular failure q is f_q, the probability of a particular recovery is r_j and the probability of a success is s. If there are w paths leading to recovery, the probability of starting the tree again after completing the tree for the first time is:

$$\sum_{j=1}^{w} r_j = R$$

So the total success probability then becomes $s + Rs$. Due to the fact that, during recovery, one may end at a recovery consequence again, this continues to infinity. Hence, the success probability finally becomes:

$$S = s(1 + R + R^2 + \cdots) = \frac{s}{1 - R}$$

since R is less than 1. The same applies for a failure q. The probability of a particular failure consequence q is:

$$F_q = \frac{f_q}{1 - R}$$

The same can be done for when both internal and external dependence are present. In this case the terms present tree (the tree being completed at that particular moment) and preceding tree (the tree completed before the

present tree) are defined. The following assumptions are made:

(a) Internal dependence is restricted to the property that a certain event can internally be dependent upon only one other event.
(b) Regardless of the number of times there has been recovery, the same internal dependence is present.
(c) Only between the present tree and the preceding tree is external dependence present.
(d) Regardless of the number of times that recovery takes place, the same external dependence is present.
(e) The selection probability to start a present tree, reflecting the selection of a certain sequence of events in the present tree, depends upon the sequence of events in the preceding tree and upon the route through the preceding tree.
(f) The route through the present tree is dependent upon the route through the preceding tree and upon the selection of a sequence of events in the preceding tree.

An example of the case in which both internal and external dependence are present is given in Fig. 3. It is assumed that there are only two different sequences implying two original trees. After completing the original tree and ending at a recovery consequence, the dotted line indicates the recovery tree that can be selected. The same applies to the selection of a recovery tree if one ends at a recovery consequence again.

The general characteristics can be summarised as follows:

(a) There is more than one original tree. If there are z events, there is a maximum of $z!$ original trees.
(b) Each original tree has a selection probability p_i. If there are u original trees ($i = 1, 2, \ldots, u$), then

$$\sum_{i=1}^{u} p_i = 1$$

(c) If there are u original trees and each tree has w paths leading to recovery, there are u^2w recovery trees or there are $u \,.\, w$ sets each containing u recovery trees each with a different sequence of events.
(d) If path j of the original tree i or the recovery tree i is passed

through, then a recovery tree of set j,i will be passed through ($j = 1, 2, \ldots, w$).

(e) Each recovery tree of set j,i has a selection probability $p_{k|ji}$ ($k = 1, 2, \ldots, u$) for which:

$$\sum_{k=1}^{u} p_{k|ji} = 1.$$

(f) Recovery tree k of set j,i passed through for the nth time of recovery is the same as recovery tree k of set j, i passed through during the first time of recovery.

(g) The failure probability of an internal dependent event is influenced by the failure or success of a previous event in the same tree.

(h) Given failure (success) at the preceding event, then the failure probabilities of the same event in the original tree i and the recovery tree i need not be the same.

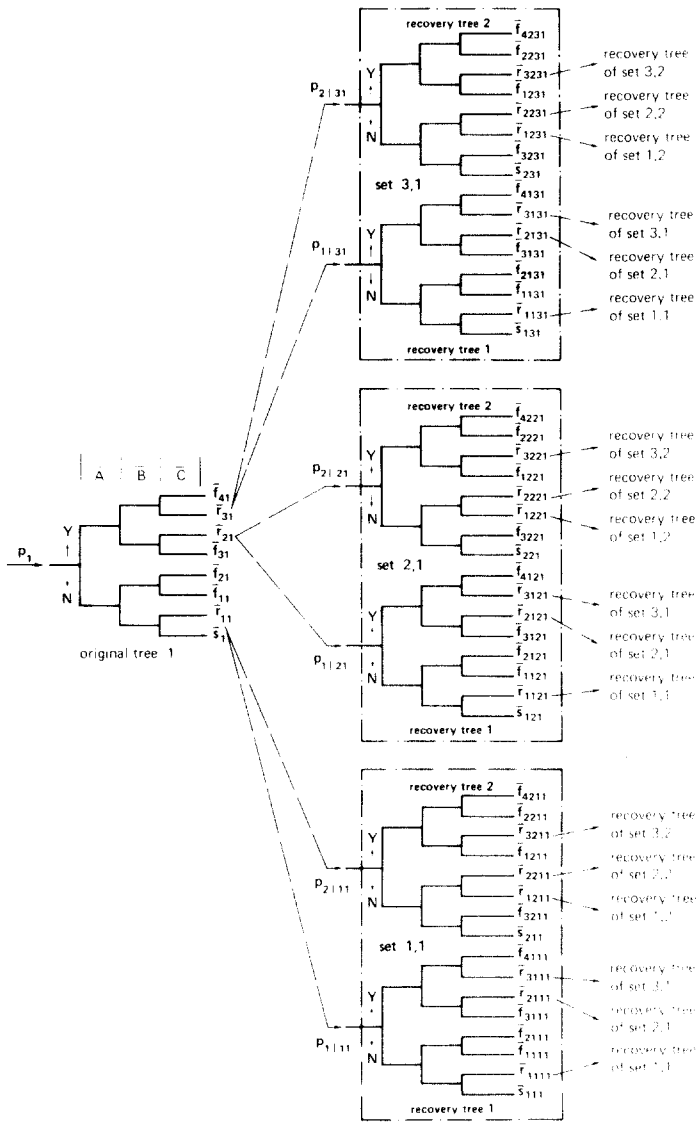
(i) Considering recovery trees with the same sequence of events in the different sets, the failure probabilities of the same events, given failure (success) at the preceding event, need not be the same.

In Fig. 3 $u = 2$ and $w = 3$.

In order to determine the total probability of success and the total probability of failure consequence q, two agreements are made.

The first agreement concerns the original trees. There are u original trees, indicated by the variable i ($i = 1, 2, \ldots, u$) and the selection probability of original tree i equals p_i, respectively. For the *original tree i* accounts:

1. There is one offshoot ending with success $\bar{s}_i$ and the probability of ending up that offshoot is $p_i \,.\, s_i$.
2. There are v offshoots leading to failure with respective consequence q ($q = 1, 2, \ldots, v$). This is at the corresponding offshoot indicated by $\bar{f}_{qi}$ and the probability of ending at that offshoot equals $p_i \,.\, f_{qi}$. In other words the index q indicates the path that has been passed through ending at a failure consequence.
3. There are w offshoots leading to recovery indicated at the respective offshoot by $\bar{r}_{ji}$ ($j = 1, 2, \ldots, w$). The probability of ending at that offshoot equals $p_i \,.\, r_{ji}$. So the index j indicates the path that has been passed through in order to end at a recovery consequence.


A
B
C
original tree 1
recovery tree 2
recovery tree 1
set 3,1
set 2,1
set 1,1
recovery tree of set 3,2
recovery tree of set 2,2
recovery tree of set 1,2
recovery tree of set 3,1
recovery tree of set 2,1
recovery tree of set 1,1

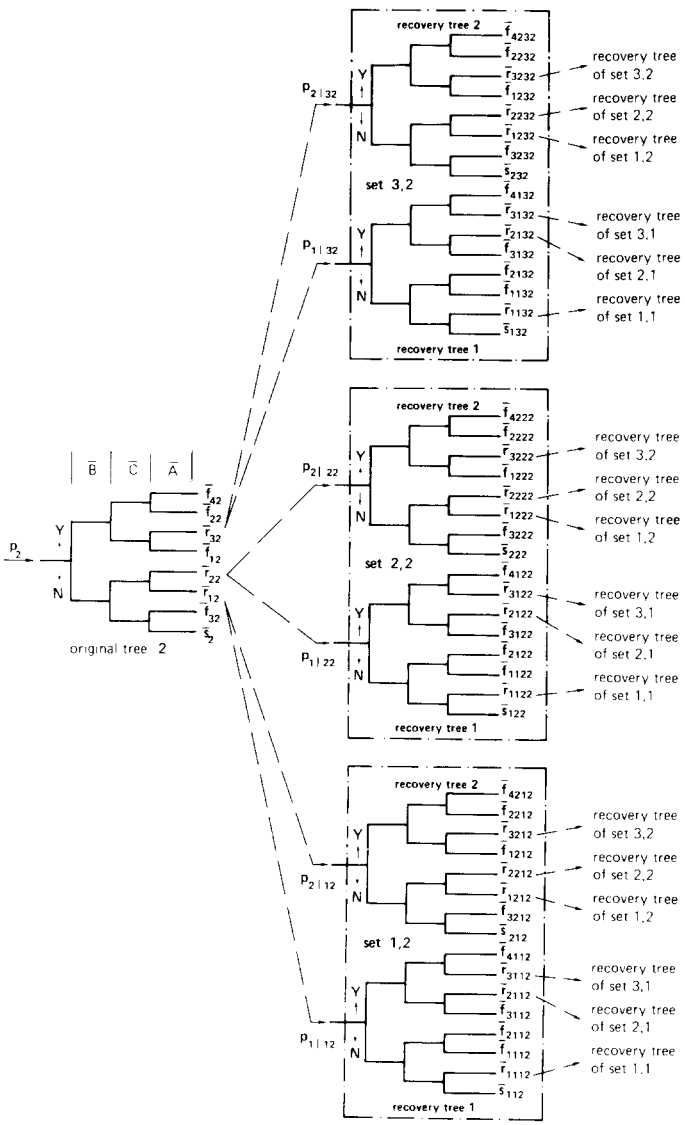


Fig. 3. HRA event trees of three dependent events Ā, B̄ and C̄. For convenience it is assumed that there are only two different sequences: Ā–B̄–C̄ and B̄–C̄–Ā; so there are two original trees. N stands for NO (no failure), Y for YES (failure). At the offshoots the consequences (fictive) are given. At original tree i ($i = 1, 2$), $\bar{s}_i$ reflects success, $\bar{r}_{ij}$ the consequence recovery ($j = 1, 2, 3$) and $\bar{f}_{qi}$ the failure consequence q ($q = 1, 2, 3, 4$). The probability to start original tree i equals p_i. The dotted line indicates the recovery tree to be passed through after completing the corresponding path in the preceding tree. Recovery tree 1 has the sequence Ā–B̄–C̄ and recovery tree 2 the sequence B̄–C̄–Ā. At recovery tree k ($k = 1, 2$) of set j, i, $\bar{s}_{kji}$ reflects success, $\bar{r}_{mkji}$ the consequence recovery ($m = 1, 2, 3$) and $\bar{f}_{qkji}$ the failure consequence q. The probability of starting a recovery tree equals $p_{k|ji}$

The second agreement concerns the recovery trees. There are u. w sets each containing u recovery trees with a different sequence of events. The probability of choosing recovery tree k of set j,i equals $p_{k|ji}$ $(k = 1, 2, \ldots, u)$. For the *recovery tree k of set j,i* accounts:

1. There is one offshoot ending with success $\bar{s}_{kji}$ and the probability of ending at that offshoot equals $p_{k|ji} . s_{kji}$; $p_{k|ji}$ does not include the recovery probability of the preceding tree.
2. There are v offshoots leading to failure with respective consequence q $(q = 1, 2, \ldots, v)$. This is at the corresponding offshoot indicated by $\bar{f}_{qkji}$ and the probability of ending at that offshoot equals $p_{k|ji} . f_{qkji}$. So the index q indicates the path that has been passed through in order to end at a failure consequence.
3. There are w offshoots leading to recovery indicated at the respective offshoot by $\bar{r}_{mkji}$ $(m = 1, 2, \ldots, w)$. The probability of ending at that offshoot equals $p_{k|ji} . r_{mkji}$. So, contrary to index j, actually reflecting the path that has been passed through in the preceding tree i, m indicates the path passing through in the present tree k to end at a recovery consequence.

In the same way as for when there is no dependence at all, the probability of success or a particular failure consequence taking into account the recovery possibility, can be determined. Here, the calculation will not be shown since this is too extensive and only the answer is presented. The success probability is:

$$S = \Gamma\Lambda + \Omega P[I - R]^{-1} H$$

and the probability of a particular failure consequence q is:

$$F_q = \Gamma Y_q + \phi_q P[I - R]^{-1} H$$

where

$$\Gamma = [p_1, p_2, \ldots, p_u];$$

$$\Lambda = [s_1, s_2, \ldots, s_u]^T;$$

$$Y_q = [f_{q1}, f_{q2}, \ldots, f_{qu}]^T;$$

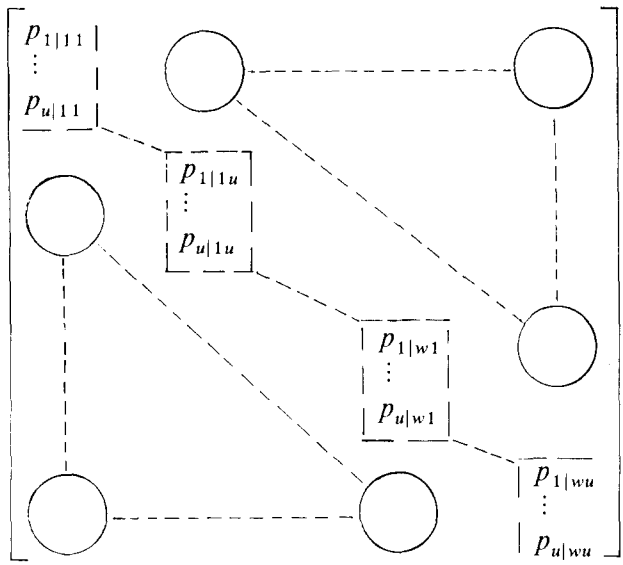
$$\Omega = [s_{111}, \ldots, s_{u11} | \cdots | s_{11u}, \ldots, s_{u1u} | \cdots | s_{1w1}, \ldots, s_{uw1} | \cdots | s_{1wu}, \ldots, s_{uwu}];$$

$$\phi_q = [f_{q111}, \ldots, f_{qu11} | \cdots | f_{q11u}, \ldots, f_{qu1u} | \cdots$$
$$\cdots | f_{q1w1}, \ldots, f_{quw1} | \cdots | f_{q1wu}, \ldots, f_{quwu}];$$

I is a unit matrix with rank $u \cdot w$;

$H = [r_{11}p_1, \ldots, r_{1u}p_u | \cdots | r_{w1}p_1, \ldots, r_{wu}p_u]^T$;

$P =$



$R =$

$$\begin{bmatrix} r_{1111}p_{1|11} & \cdots & r_{111u}p_{1|1u} & r_{11w1}p_{1|w1} & \cdots & r_{11wu}p_{1|wu} \\ \vdots & & \vdots & \vdots & & \vdots \\ r_{1u11}p_{u|11} & \cdots & r_{1u1u}p_{u|1u} & r_{1uw1}p_{u|w1} & \cdots & r_{1uwu}p_{u|wu} \\ & & & & & \\ r_{w111}p_{1|11} & \cdots & r_{w11u}p_{1|1u} & r_{w1w1}p_{1|w1} & \cdots & r_{w1wu}p_{1|wu} \\ \vdots & & \vdots & \vdots & & \vdots \\ r_{wu11}p_{u|11} & \cdots & r_{wu1u}p_{u|1u} & r_{wuw1}p_{u|w1} & \cdots & r_{wuwu}p_{u|wu} \end{bmatrix}$$

4. DISCUSSION

4.1. Results

The THERP has been extended theoretically here to analyse specific actions to be performed by an operator carrying out a written procedure. This has been done with regard to the capability of the operator in

recovering possible failures. Both kinds of recovery (correct and incorrect) have been analysed taking into account dependence among events and memory influences during recovery. This study makes clear that, despite these problems, HRA event trees may form a valid method for structural description of human performance.

It has been shown that recovery is equivalent to starting the entire HRA event tree again for the case where there is no internal and no external dependence. This statement has also been used without proof for where internal and external dependence are present. It can be shown, however, that this statement also accounts for that case.

Does recovery make a sizeable contribution to the total probability of a failure consequence? Considering realistic failure probabilities of a maximum of 10^{-2} it has to be noted that this contribution can indeed be neglected in the case of there being no dependence at all. This is easy to show with the above formulae. In the practical case, however, recovery certainly needs to be taken into account since a combination of both internal and external dependence may cause sizeable contributions.

Similar models are presented in other papers (Heslinga[3,4]). These models are different from the model described in this paper because some assumptions about the case where both internal and external dependence are present have been changed. This has meant that the indices of some symbols have had to be extended and changed. Since the assumptions in this paper are less restrictive and more realistic, the model in this paper is to be preferred.

In the model derived in this paper, it has been assumed that the probability to end at a recovery consequence ($p_{k|ji} \cdot r_{mkji}$) remains constant. This implies that infinite times of recovery are considered in this model. If recovery stops after n times, the recovery probability (r_{mkji}) will become zero during the nth time of recovery. Practically, infinite times of recovery will not exist, since the operator will recover one to four times at the most. Because of theoretical difficulties, this feature has not been included in the model of this paper yet.

4.2. Conclusions

The results obtained so far are as follows:

1. In principle, event trees may be used in human reliability analysis despite the fact that there are more difficulties than in the case of technical systems.

2. Although in practice the operator may partially recover his errors, theoretically it can be described as beginning the whole event tree again.
3. Compact formulae have been derived here to calculate the probability of reaching the success consequence or a particular failure consequence on performing a specific action, taking into account the fact that the operator may recover his errors.

4.3. Further research

The study reported needs to be continued with human reliability analysis by combining specific actions representing a written procedure. Not only are more recovery paths possible since the operator may go back somewhere in the procedure for recovery, but also more dependences and memory influences are present compared with only one specific action. These problems mean that such a fundamental approach is to be preferred instead of immediate quantification with unmeasured, estimated human error probabilities. This should all be approached using a sensitivity analysis revealing the way in which the theoretical model has to be extended. In any case, the model should be extended with the possibility that the recovery probability after limited times of recovery can become zero.

In this model only human failures are considered. However, a combination of human failures and technical failures could be disastrous. Therefore, event trees should be made in which these failures are combined. This could be done by regarding a technical failure, like a human failure, as an event in the event tree thus realising a human–technical reliability analysis event tree.

ACKNOWLEDGEMENTS

The author wishes to acknowledge the co-operation provided by the Arnhem institutions of the Dutch electricity utilities and the Delft University of Technology. He also acknowledges the help of Prof. Dr Ir H. G. Stassen of the Delft University of Technology, and Prof. Ir P. Mostert and Ir R. W. van Otterloo of the KEMA.

REFERENCES

1. Swain, A. D. and Guttmann, H. E. *Handbook of human reliability analysis with emphasis on nuclear power plant applications* (*NUREG/CR—1278*). US Nuclear Regulatory Commission, Washington, DC, 1983.
2. Bell, B. J. and Swain, A. D. *A procedure for conducting a human reliability analysis for nuclear power plants* (*NUREG/CR—2254*). US Nuclear Regulatory Commission, Washington, DC, 1983.
3. Heslinga, G. Human reliability analysis using event trees, *KEMA Scientific & Technical Reports*, **1**(3) (1983), pp. 19–44, KEMA, Arnhem, The Netherlands.
4. Heslinga, G. Analysis of human reliability by using event trees, *Proc. Third Europ. Annual Manual* (1983), pp. 243–51, Risø National Laboratory, Roskilde, Denmark.