5th INTERNATIONAL SYMPOSIUM
LOSS PREVENTION AND SAFETY PROMOTION IN THE PROCESS INDUSTRIES
European Federation of Chemical Engineering, 337th event

CANNES, France - 15th-19th September 1986

Incorporating Human Reliability into Probabilistic Risk Assessment

Linda Bellamy, B. Kirwan, R.A. Cox
Technica Ltd, London (G.B.)

ABSTRACT

There is a common mode failure which can bypass design safeguards and is often overlooked in hardware-orientated risk assessment, namely human error. In plant design it is difficult to cater for all human errors, and a risk assessment approach that does not look at human errors explicitly may omit a critical failure path. Many major accidents have occurred which highlight these points, and a few examples are given.

While there is relatively little controversy about the importance of human error, its evaluation is beset by problems of identifying what errors could occur, and by lack of a proven methodology and data for estimating human error rates.

This paper discuses an approach to incorporating human reliability into probabilistic risk assessment, using actual examples. Human reliability analysis revealed important failure modes which would not have been found by the conventional hardware analysis. This led to significant design recommendations. The examples emphasise a system-orientated approach in which the engineering and behavioural science contributions are closely integrated.

It is concluded that human reliability is an essential component of risk assessment and that it is practical to assess human reliability fo specific operations at the design stage.

1. INTRODUCTION

Experience of actual accidents shows that human error is often a contributory factor. Howland (1980) gave several examples of this, and it is a common experience in reviewing data bases of historical accidents in the process industries, that a significant proportion (typically 30-50%) are ascribed to "human error".

In risk or reliability analysis, even those failure modes which are normally treated as spontaneous mechanical failures can often be shown to have root causes in human decisions, lapses of judgement or omissions. Indeed, it can be argued that every failure is ultimately caused by some sort of human error. Current methods of risk analysis for the process industries, however, tend not to treat human error explicitly, but merely include it as one of many possible contributors to failure statistics. Although this means that the overall estimates of risk are unbiased (as far as human errors are concerned) on an industry-wide averaged basis, it remains unsatisfactory because the results of such an analysis are unresponsive to design changes which could be made to reduce the probability of human error. Since human error is a significant contributor to the total risk, it offers a rich potential for the improvement of plant safety, and therefore must be treated explicity and in some degree of detail, in any safety analysis.

Because of the great versatility of human beings, not only in their resourcefulness in dealing with emergencies, but also in the great variety of mistakes that they are capable of making, it is very difficult for the designer of process plant and the man-machine interface to take account of all possible human error, or to deal with these problems by operational management and procedure design. Nevertheless, these are very important tasks which must be attempted in a systematic and scientific manner. The designer therefore needs some method for assessing the merits of any particular design or scheme, and for determining improvements which could be made to the hardware and operating procedures which would have a beneficial effect on that assessment. The ideal way to make such an assessment is to quantify the error rate, and it is an important current challenge to develop accepted methodologies for this purpose.

These aims call for a new collaboration between systems and engineering experts on the one hand and psychologists and ergonomists on the other. In this paper, we describe ways in which these multidisciplinary studies can be structured so as to combine the skills of these experts in an appropriate way, whilst generating results which are of direct utility in the improvement of plant and control room designs, and in the improvement of operational safety. The paper outlines several of the techniques of human factors and total system analysis which may be brought to bear on this question, and gives examples based on experience of real industrial problems.

2. OVERVIEW OF TECHNIQUES

A single method of approach will not suffice for all types of "human factor" risk analysis. The choice of method depends on the level of detail required, the information available, the role of the operator, and the system itself.

The overall logical framework for the analysis is the same as for a "hardware-orientated" risk analysis, but includes contributions from human factors analyses in the manner shown in Figure 1. This shows the general case, in which the operator may appear both as a cause of failure (due to maloperation or maintenance errors) and as a potential preventative factor (by taking 'recovery actions').

The key systems analysis techniques used here are Fault Tree Analysis (Section 5 below) and Event Tree Analysis (Section 6). The former is used to describe causes which lead to the initiation of an accident and the latter is used to describe situations in which a defined event (typically a process failure) could lead to a multitude of different outcomes, dependent upon both human and system factors. Each of these techniques requires definition of particular human actions or errors (e.g. "operator closes valve X instead of valve Y" or "operator does not hear alarm"), and, for each of these, a quantification in terms of probability of error per demand.

Two human factors techniques for identifying human failure modes are Task Analysis (Section 3 below) and "Barrier" Analysis (Section 4). Task Analysis examines the operator and the procedures which he or she is expected to follow. It breaks these down into steps and defines for each step what resources are available and what loads are imposed on the operator. From this, opportunities for human error can be identified. Barrier analysis, on the other hand, considers one particular type of accident and lists all the factors (physical and procedural) which tend to prevent that accident, both before and after the event has been initiated. Failures of each of these, caused by a human error or a failure to take the right recovery action, are examined.

Quantification of human error probabilities is necessary for both Fault Tree and Event Tree analysis. Quantification uses as a basis the qualitative description of the human error derived from a Task Analysis or Barrier Analysis, coupled with a quantification technique such as use of error rate data (e.g. THERP) or influence diagrams coupled with expert judgement. These quantification techniques are described in Section 7.

3. TASK ANALYSIS

Task analysis is a tool for describing in detail what an operator has to do, and the information and controls that are used, available and required to do it successfully. Task analysis is therefore not only a formal way of describing the operator's task, but also a way of examining the task demands in relation to the limitations of the human operator (see Drury, 1983).

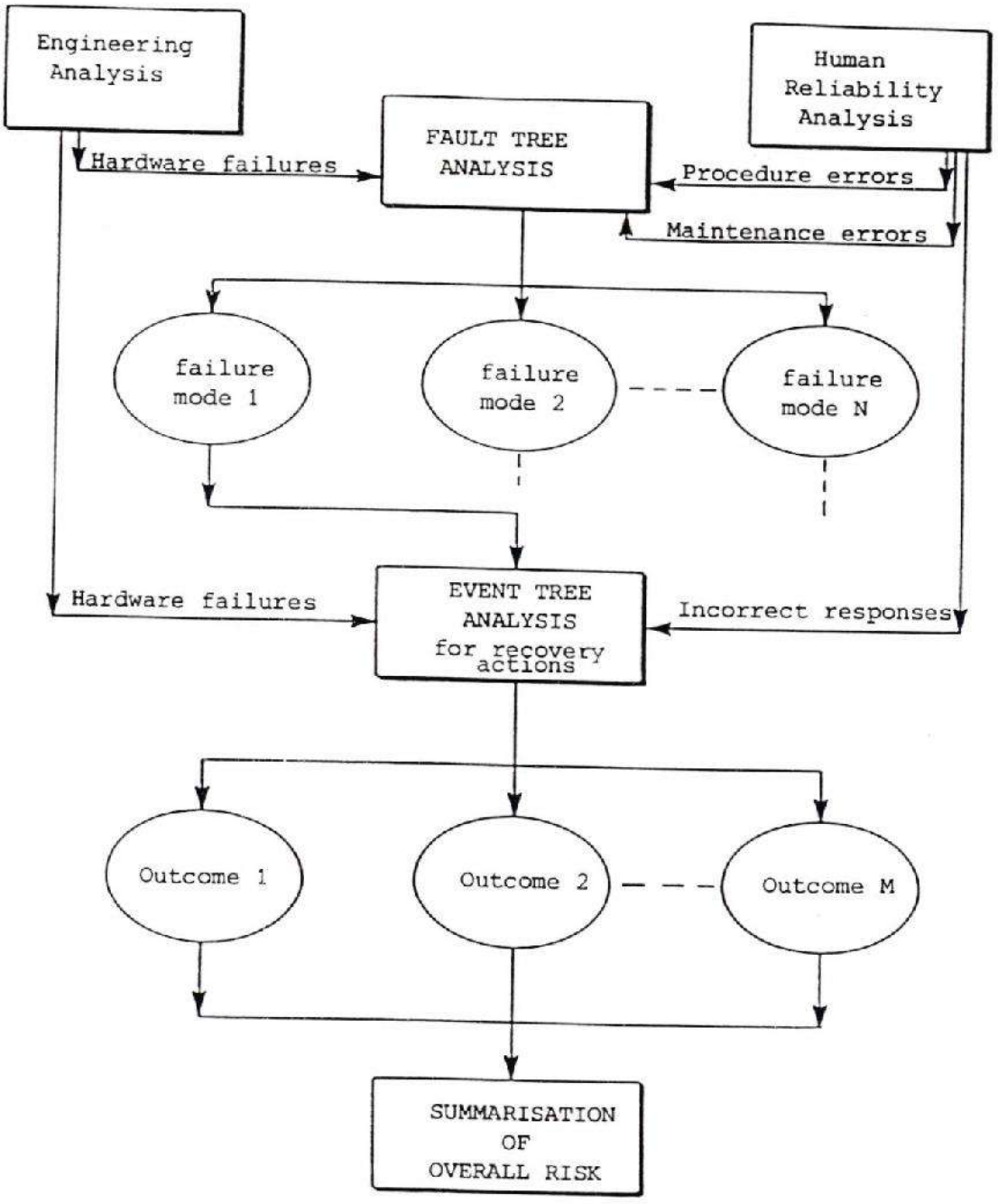

FIGURE 1 - Use of Fault Tree analysis for initial failure modes and Event Tree analysis for operator recovery actions

The major function of task analysis in risk assessment is to identify opportunities for error and sources of error. All task analysis techniques have in common the characteristic that the task is broken down into smaller components of behaviour. This may be done hierarchically, as sub-operations which are progressively broken down into smaller and smaller components, or sequentially. The first stage of a sequential analysis, for example, lists the required sequence of operator actions to achieve the task goal.

The next stage of the method is to determine the demands made on the operator in performing the task components. For the purposes of risk assessment, the interest is principally to determine how the operator could fail to meet these demands and why. For example, the analyst might ask whether the demands on the operator's memory might exceed capacity and therefore result in omitting to perform a particular task component. Consideration of the amount of system support that is given to the operator, such as memory aids, would be relevant when assessing the effect of the design of the system on error.

In order to identify errors, we have used a basic error classification system which includes all possible errors:

Omission:	Omit required behaviour
Commission:	Operation performed incorrectly, (eg. too much, too little), wrong action, action out of sequence.
Action not in time:	Fail to complete an action in time or perform it too late/too early.
Extraneous act:	Perform an action when there is no task demand.
Error recovery failure:	Many errors can be recovered before they have a significant consequence. However, failure to do this can itself be an error.

When defined for a particular task, these errors are expanded in a task-specific form.

An example of a task analysis for closing a valve following a release is shown in Table 1. This analysis was carried out in order to help engineers calculate manual valve closure times following a chemical release.

When applying this technique we have found that, for complex tasks at least, it is best to use an expert with extensive field experience of the operation or system under study, to help in task description, identification of errors and sources of error. In the analysis shown in Table 1, the role of the operations expert was to answer questions such as:

"Are there likely to be any operators nearby if a leak occurs?",
"Will there be an alarm in the control room?",
"Is the reliability of the warning system good ie. will the operators believe it?",
"Is there likely to be a formal procedure to be followed when leaks occur?", etc.

TABLE 1 : TASK ANALYSIS FOR OPERATION OF AN ISOLATION VALVE FOLLOWING A RELEASE (to aid calculation of valve closure times)

BEHAVIOURS INVOLVED REQUIRED OPERATOR RESPONSES	POSSIBLE HUMAN ERRORS	PERFORMANCE SHAPING FACTORS
1. DETECT AND INTERPRET ALARM OR WARNING		
o Operator present when warning/alarm occurs.	o No operator present	o Presence of operators in field to hear/see leak. o Control room manning.
o Detect that alarm/warning has occurred	o Alarm/warning not detected	o Man-machine interface design. o Attention-gaining qualities of warning/alarm signals. o Vigilance of operators. o Workload of operators and other stress factors. o Training/knowledge/experience o Communication system
o Interpret meaning	o Meaning interpreted incorrectly.	o Man-machine interface design. o Reliability of warning/alarm system. o Design of diagnostic techniques. o Training/knowledge/experience o Stress factors
2. CLOSE VALVE		
o Identify correct procedure associated with alarm.	o Incorrect procedure identified.	o Procedure design. o Training/knowledge/experience o Stress factors
o Decide to follow procedure	o Decision error (procedure not followed)	o Training/knowledge/experience o Stress factors o Procedure design o Penalties for incorrect action
o Identify correct valve	o Incorrect valve identified	
o Operate valve control correctly	o Incorrect control operation	o Man-machine interface design. o Procedure design.
o Check operation effective	o Fail to check o Checking error	o Stress factors o Training/knowledge/experience
o Correct error(s)	o Error recovery failure	

Apart from its use in risk analysis, Task Analysis is a complete technique in its own right and, if the study has been done to sufficient depth of detail, it can be used to generate recommendations for design of hardware, training and procedures.

4. THE BARRIER APPROACH

Barrier analysis starts by cataloguing hazards, sources of energy etc., which could lead to an accident. It then identifies the barriers preventing these accidents and, by specifying how they function, determines how they may fail. Often, these barriers are physical, but can be circumvented by human action (eg. inhibiting a trip), but some of the barriers are of a non-physical kind themselves. As an example, white lines in the middle of a road and rules about always driving on one side are not physical barriers, and yet they work extremely well in preventing head-on car collisions.

The non-physical barriers are just as susceptible to failure as the physical ones, yet their failure modes are often not investigated thoroughly in risk analyses. The mechanism of failure often results from conflicts of interest which are imposed on the operators. For example, in oil well drilling, too rapid pulling of drill pipe out of the well may result in a 'kick', yet drillers are often given incentive payments for speed of drilling and so may be tempted to violate this procedural barrier. Barrier analysis is particularly useful for identifying such 'extraneous' factors, which might not be found by task analysis.

An example for overcoming some of the physical barriers on an offshore oil platform is shown in Table 2. This uses the actual design features of a particular installation.

The overall approach is as follows:

1) Identify hazards (eg. failure of wellhead)
2) Define barrier function (eg. dropped object protection (DOP));
3) Identify associated design features (eg. DOP deck);
4) Identify associated human errors that could cause barrier failure (eg. leave DOP hatch open);
5) Define barrier recovery functions (eg. restore system to pre-error state).
6) Identify other design features associated with recovery (eg. shutdown systems)

The advantage of this approach to error identification is that it can be used to look at a complete system in a total risk assessment. However, the level of error identification will not normally be as detailed as that derived from a task analysis.

TABLE 2 : EXAMPLE OF THE USE OF A BARRIER APPROACH TO ERROR IDENTIFICATION

BARRIER		BARRIER FAILURE	
Function	Type	Design Features & Assumptions	Human Errors
1.1 Dropped object protection (DOP)	Physical	o Protective decks o Drop out area Assumptions: o Securing of heavy equipment o No design errors	o Drop equipment in areas not protected. o Deck not constructed or installed according to design. o Deck not inspected and maintained according to design. o Inspection error (miss/false alarm). o Maintenance error. o Failure to secure heavy loads/equipment. o Leave DOP hatches open.
1.2 Containment and isolation of flammables	Physical	o Vessels. o Pipework. o Gas/oil tight decks and enclosures o Hydrostatic barriers o Cement o Valves o Blowout preventer(BOP) o Interlocks Assumptions: o No design errors	o Valve operation errors. o Hose connection errors. o Failure to use hot work tent o Failure to maintain hydrostatic well barrier o Inadequate cementing of casing o Equipment not constructed or installed according to design o Inspection error (miss/false alarm). o Maintenance error o Failure to operate BOP or failure to operate it correctly o BOP removed at wrong time o Cutting into/breaking/opening/drilling into live vessel/pipework o Leaving open or propping open gas tight area doors. o Disable interlock.

5. USE OF FAULT TREE ANALYSIS

In a comprehensive risk analysis, fault trees are often used as a means of analysing qualitatively the behaviour of a system under fault conditions, and to provide a method of quantification of failure frequencies. By its nature, fault tree analysis starts from a definition of the unwanted accident, then identifies all the immediate causes of that accident. For each of these immediate causes, further more basic causes are then identified, until the level of detail cannot be further elaborated. In the development of the logic diagram describing the inter-relationships between all of these contributory causes, human errors arise as an inevitable and natural part of the overall logic structure.

Fault tree analysis is, therefore, a very good example of analysis techniques which look at the "total system". It treats the human operator as a component of the system, and it requires consideration of all the relevant failure modes of that operator, and ultimately estimation of the probability of those modes. This method of analysis is particularly suitable for systems in which the part played by the operator can be reasonably well defined, and does not contain too much complexity due to "common mode" faults on the part of the operator. Unfortunately, the latter are quite prevalent, and the analyst has to be very careful to take them into account where they may have a significant effect on the overall analysis.

Once the tree structure has been defined in this way, the next step in a complete analysis is the quantification of the frequencies or probabilities of the base events themselves, and the evaluation of the top event frequency by analysis of the tree. As far as the human errors are concerned, it is obviously just as important that they should be quantified as that the hardware faults be quantified. Methods for doing this are described in Section 7 of this paper.

An example of a man-machine system in which fault tree analysis was a very useful tool is provided by the launching system of a lifeboat designed for an off-shore oil platform. This system incorporated mechanical components such as hooks, wires, winches and dampers, all activated through a hydraulic system of some complexity. In this case, the top event of the fault tree which was of interest could be defined very precisely, i.e., failure to launch the lifeboat at the first attempt". The operation of this system was necessarily under human control, because of the need for judgements and decisions, such as ensuring that all personnel are aboard, properly seated, and that it was actually necessary to launch the boat.

The fault tree for this case is shown in schematic form, with the human causes highlighted, in Figure 2. This diagram shows the complexity of fault trees such as typically arise in process industry or offshore oil and gas industry fault tree analyses. It can be seen that the human errors pervade the entire tree, and contribute a significant proportion of the total number of contributory causes.

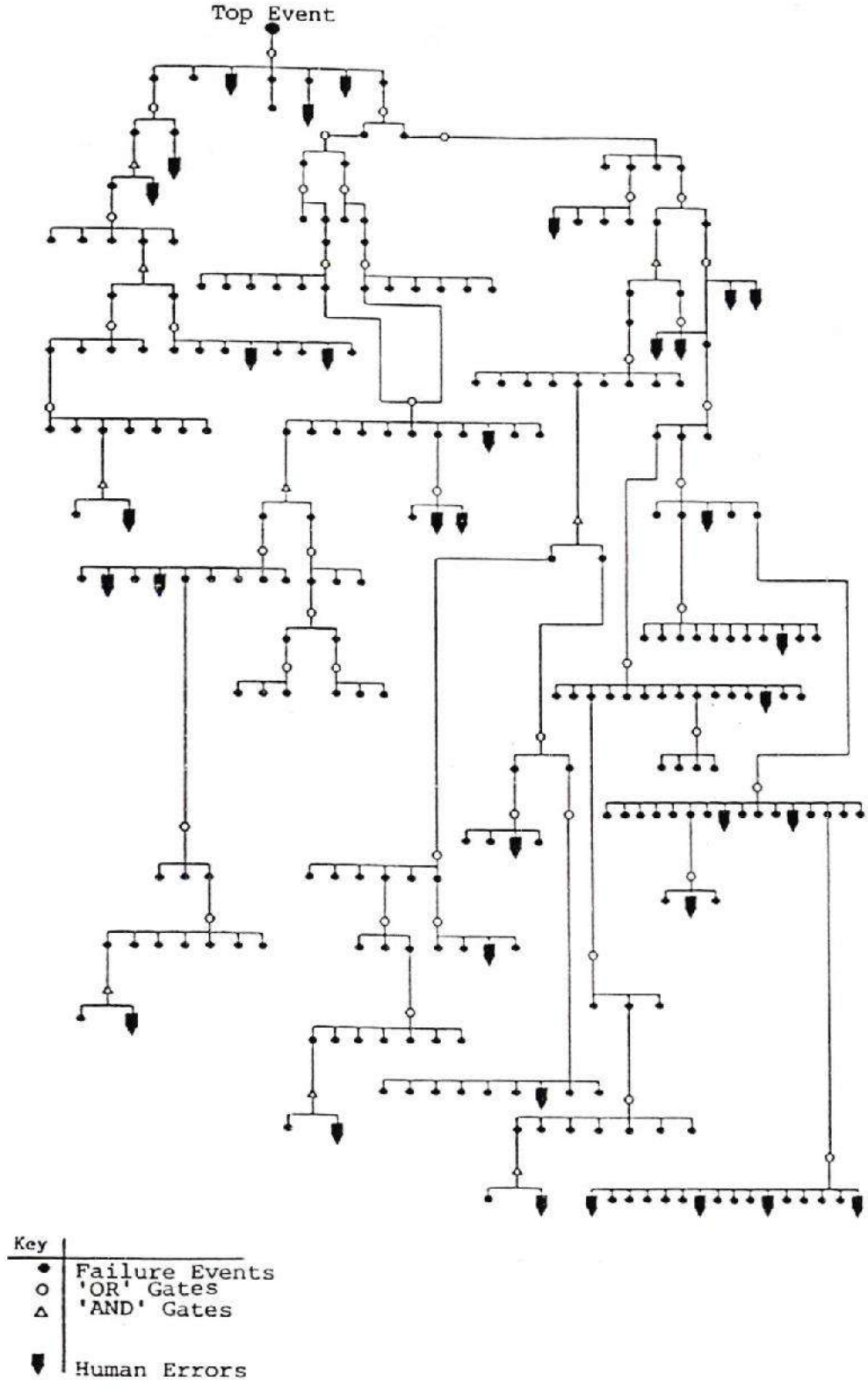

FIGURE 2 - Schematic of Fault Tree for lifeboat launching showing human error causes

Analysis of this case revealed a large number of failure modes, many of which were the direct result of human error in operating the controls. However, since the top event had been carefully defined to include only failure at the first attempt, it was not necessary to take account of error recovery actions, which would have had complicated common cause links to the original errors which they were attempting to recover. These recovery actions by the operators were subsequently taken into account in a separate event tree analysis (see Section 6 below). The specific example of the lifeboat launching system was also a favourable one for application of fault tree analysis because the design of the launching procedure involved quite distinct stages, which were unlikely to give rise to common mode failures. Also, the common mode operator errors which are most likely to be met in the process industries (i.e., operator absent from control room, or incapacitated, or subject to adverse environmental conditions) do not apply in this case.

A study of the reliability of a computer controlled blowdown system on a North Sea platform included human errors as well as hardware failures (Comer and Kirwan, 1985). The top event analysed was "failure to control the system, leading to overload of the flare". As part of the study, a highly detailed fault tree analysis of the Emergency Shutdown (ESD) System was carried out. Over 90% of all failures involved a single maintenance error. The ESD failure frequency was predicted to be once per 120 years. However, if this human error was eliminated, the predicted frequency became once in 1500 years.

The part of the study relating to flare overload also showed human errors in an emergency to be the most likely events leading to the top event. These errors resulted from the lack of coordination and communication between the central control room operators and the local control room operator near the compressors. Another significant problem was use of a misleading colour coding system on the blowdown control panel. This study demonstrated the importance of human errors in both maintenance and emergency response (under stress) in a system for which the hardware itself was otherwise very well designed for its primary function.

6. EVENT TREE ANALYSIS

The technique of event tree analysis, or "operator action trees" (Hannaman, 1983) as they are sometimes called in the context of human error, is very useful for analysing situations where the operator has to react to some unexpected situation. For example, they are appropriate for describing operator response to a control room emergency, or analysing operator recovery actions after some procedural failure.

Many human actions are conditionally dependent on previous actions, and this is especially true in an emergency situation. If an event has been misdiagnosed, all subsequent information will be viewed from the room, perspective of this misdiagnosis, and may itself be misinterpreted. Similarly, the correct performance of actions in an emergency evacuation

can depend on the performance of earlier actions : e.g. the correct launching of a lifeboat may be impeded if several errors are initially made, increasing the stress on those individuals in control.

Conditional probabilities are important in the accurate analysis of human performance after an event has occurred. Event tree analysis is therefore most useful for examining flexible sequences of events which may change course depending upon human, hardware, and environmental responses.

In the case of the lifeboat launching system which was described in Section 5, the top event of the fault tree analysis was described as "failure to launch at the first attempt". It proved possible to group the cut sets of the fault tree for failures at the first attempt into a relatively small number of generic types, characterised by some particular dominant obstacle to success, for which a particular diagnosis and recovery action could be defined. For each of these generic types of failure mode, it was then possible to draw an event tree describing the possible paths which the operators might take in trying to remedy the fault, and also all the mistakes they might make at each stage in this procedure.

An example of one of these event trees is shown in Figure 3. For each branch in the event tree, it is necessary to quantify the probability of the operators successfully completing that step. These probabilities may be quantified by techniques similar to those described in Section 7, and in this particular example, the influence diagram technique was used.

For each path down the event tree, the consequences have to be evaluated, which is essentially an engineering or systems analysis task. In the case of this particular example some of the outcomes amount to total success at the second attempt, while others lead to partial success, and yet others lead to some other kind of catastrophe (see Figure 3).

The overall analysis is completed by quantifying the probabilities of each of these outcomes within each event tree, multiplying by the frequency of the particular original failure mode for which this event tree applies, and then adding up the frequencies of each different type of outcome. Since the outcomes can be broadly classified into only a small number of types, the frequencies of each of these types of outcome can be readily estimated.

With this type of analysis, since both the mechanical and the human errors have been considered and quantified explicitly, including also the performance shaping factors, it is a straightforward matter to evaluate the effect of design changes which may either reduce mechanical failure probabilites or human error probabilities, or give improvements in the environmental conditions. In the case of this example, it was shown that the probability of a successful launch could be fairly easily increased from its initial value of about 78% to about 98%, mostly by means of

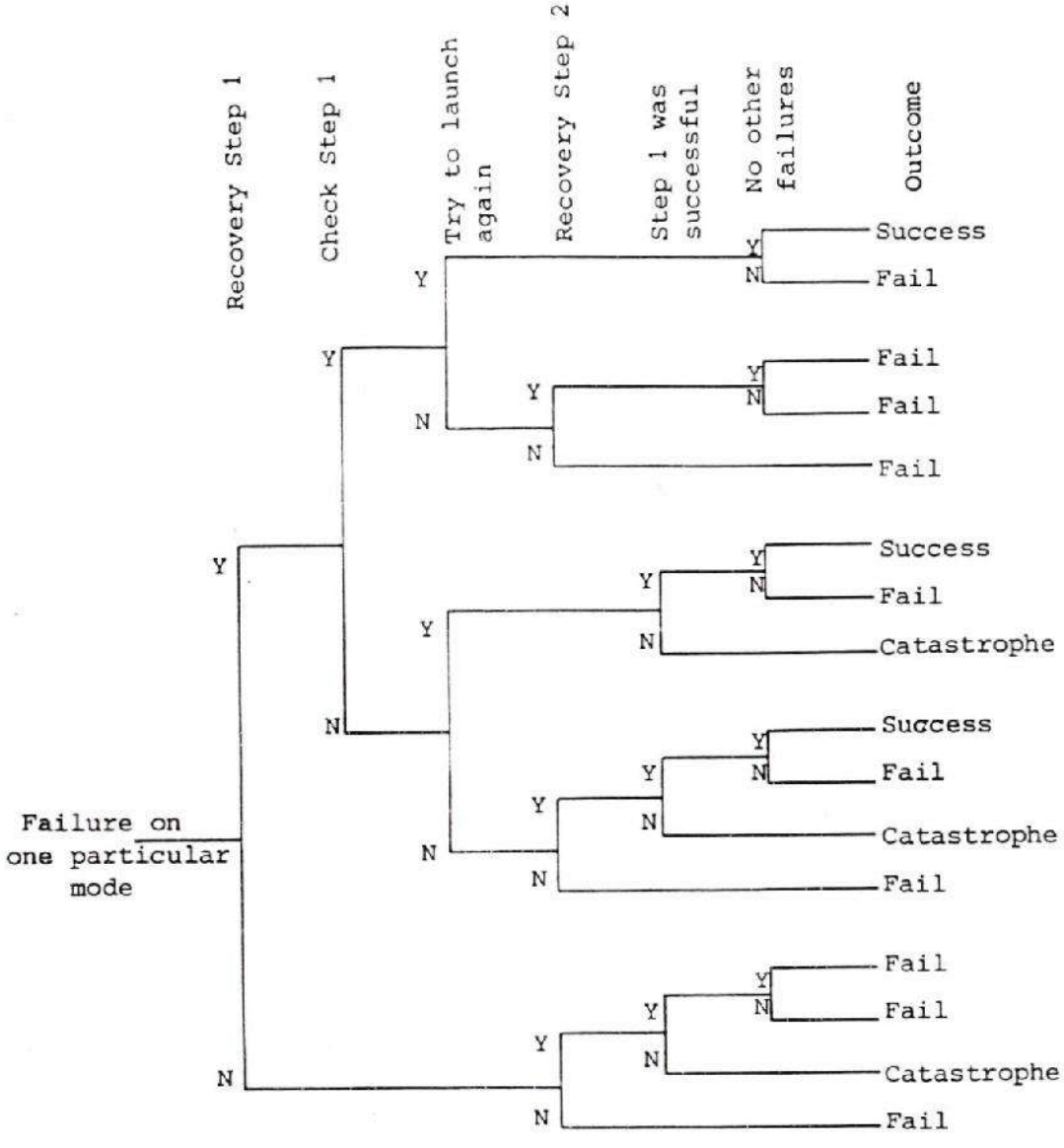

FIGURE 3 - Typical Event Tree for operator response to a failure (example based on failure to launch lifeboat at first attempt)

hardware changes which enabled a single universal procedure to be used for the second attempt at launch, regardless of the failure mode which had caused the failure at the first attempt. These hardware changes were not expensive, but greatly simplified the problem of diagnosis which would have arisen with the original design.

7. QUANTIFICATION

The quantification of human error poses problems for a number of reasons:

- Many of the quantification techniques have not been validated.

- Incident records rarely describe the environmental conditions (or performance shaping factors) under which the human errors were made. This makes it difficult to generalise from failure data for specific tasks to others that are similar.

- Incident records only reflect errors which have been identified and which resulted in some notifiable consequence. They do not record either opportunities for error or error frequencies with no consequence (eg. because of error recovery). It is not possible to determine, therefore, what the true error rate is although attempts have been made by estimating opportunities for error.

- Techniques which provide data, such as THERP (Swain & Guttmann 1983), do not provide the original data on which the numbers are based.

- Some of the techniques for quantification of human reliability require the use of subjective judgement by experts. Bias in making expert judgements and in judging error probabilities for new designs of systems which have not yet been operated exacerbate the problem, although progress has been made in 'structuring' the judgements in order to reduce the bias.

With these limitations in mind, some attempt at quantification must be made in order to assess the human contribution to risk. It is also necessary to be able to prioritise design improvements which will reduce this risk; the relative values of failure rates are therefore at least as important as the absolute values.

We have found that the most useful method of quantification has the following components:

- A large data base consisting of data points from:
  - o Simulators
  - o Incident records/accident reports (particularly relating to tasks of interest)
  - o Experimental studies
  - o Expert judgement
  - o Generic (i.e. not task-specific) estimates
  - o Quantification techniques which have data (eg. THERP).

- Weightings or multipliers for the effects of performance shaping factors. These values can be derived from the same kinds of sources as the data base.

- A technique which takes account of the effect of interactions between performance shaping factors.

In one study on directional drilling of an oil well, for example, it was necessary to quantify the probability of drilling into a neighbouring well. This requires knowledge about the position of the drill bit, which is determined by a measurement-while-drilling (MWD) instrument providing data to the directional engineer in the form of a printout. This has to be processed by the engineer in order to determine bit position. The MWD instrument is not accurate and this has to be allowed for in estimating a "safe" distance from neighbouring wells whose positions also have to be estimated.

Human errors associated with this task were used in a fault tree. The section of the data base used to quantify these errors is shown in Figure 4. This also lists some of the important performance shaping factors that were used to select values from ranges of possible error rates, with the help of a drilling expert. The actual values used are given in the fault tree in Figure 5. The probability that MWD errors exceed the planned position uncertainty based on known instrument sensitivity and reliabil- ity includes the combination of the probability of instrument error and human error.

Use of influence diagrams to give structure to "expert judgement"

A useful technique for quantification of human errors is to define a logical structure for the human factors which influence the occurrence of those errors, which is usually called an "influence diagram" (Phillips, Humphreys and Embrey, 1983). An example of such a diagram, taken from the study of an offshore lifeboat system referred to in Section 5, is shown in Figure 6. Defining the structure of the influence diagram is a task in which both human factors specialists and other experts with knowledge of the operations involved must collaborate.

In the quantification of an influence diagram, the method adopted is similar to that of fault tree analysis, but uses a more comprehensive description of the states of each of the influences at the base of the logic tree. In the published descriptions of the influence diagram technique (Phillips, Humphreys and Embrey, 1983), these influences are thought of as occupying one of two states, typically "good" and "bad". A team of experts is asked to assign a "weight of evidence" to the proposition that each of the performance shaping factors is in each of these states. The total weight of evidence must add up to 100%.

In practice, we have found that this algorithm for quantifing the influence diagram is unsatisfactory because it does not allow each performance shaping factor to be in an "average" condition at any time, even though this is in fact the most likely circumstance. We have

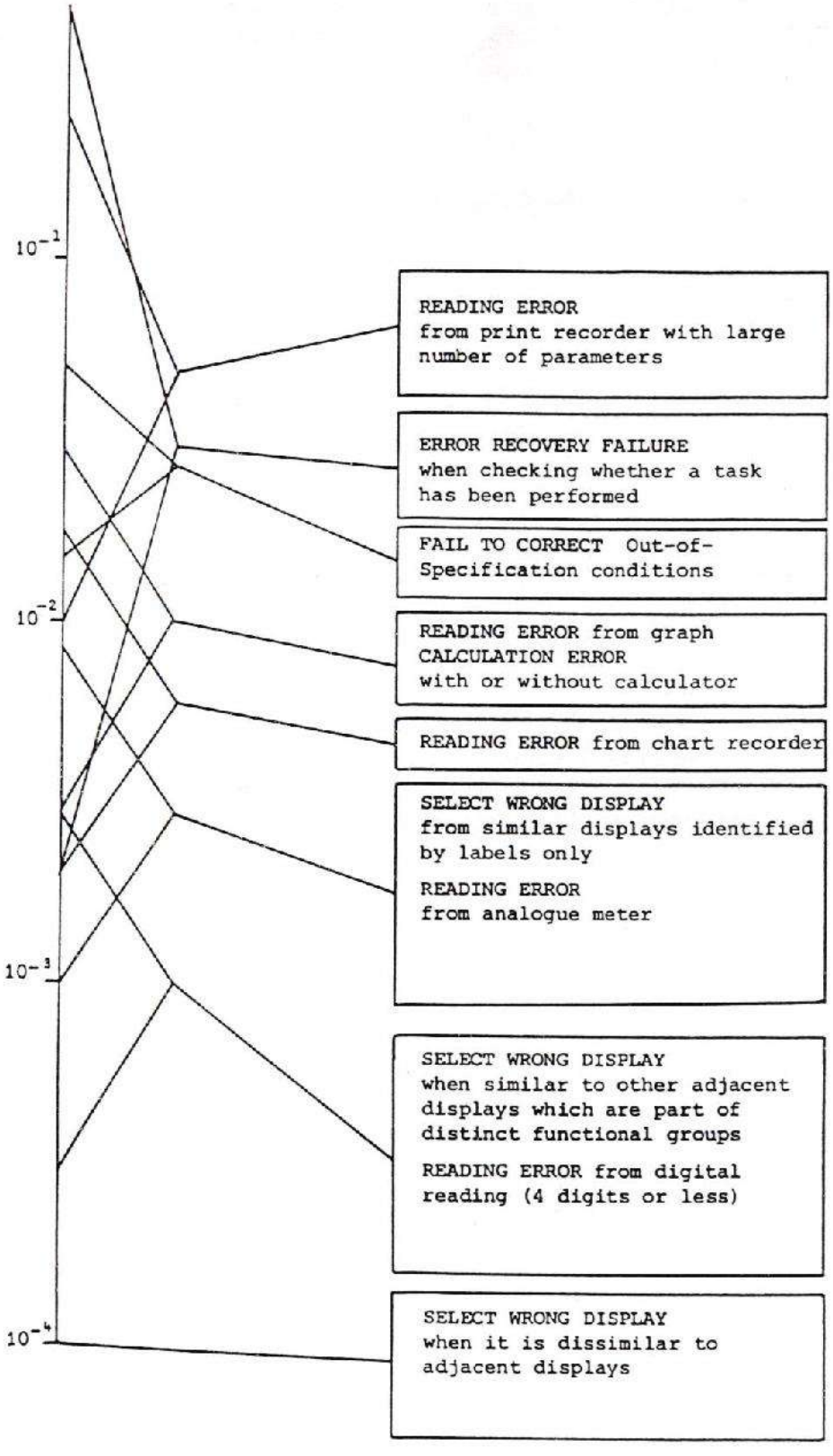

FIGURE 4 - Section of Database used in Directional Drilling Study

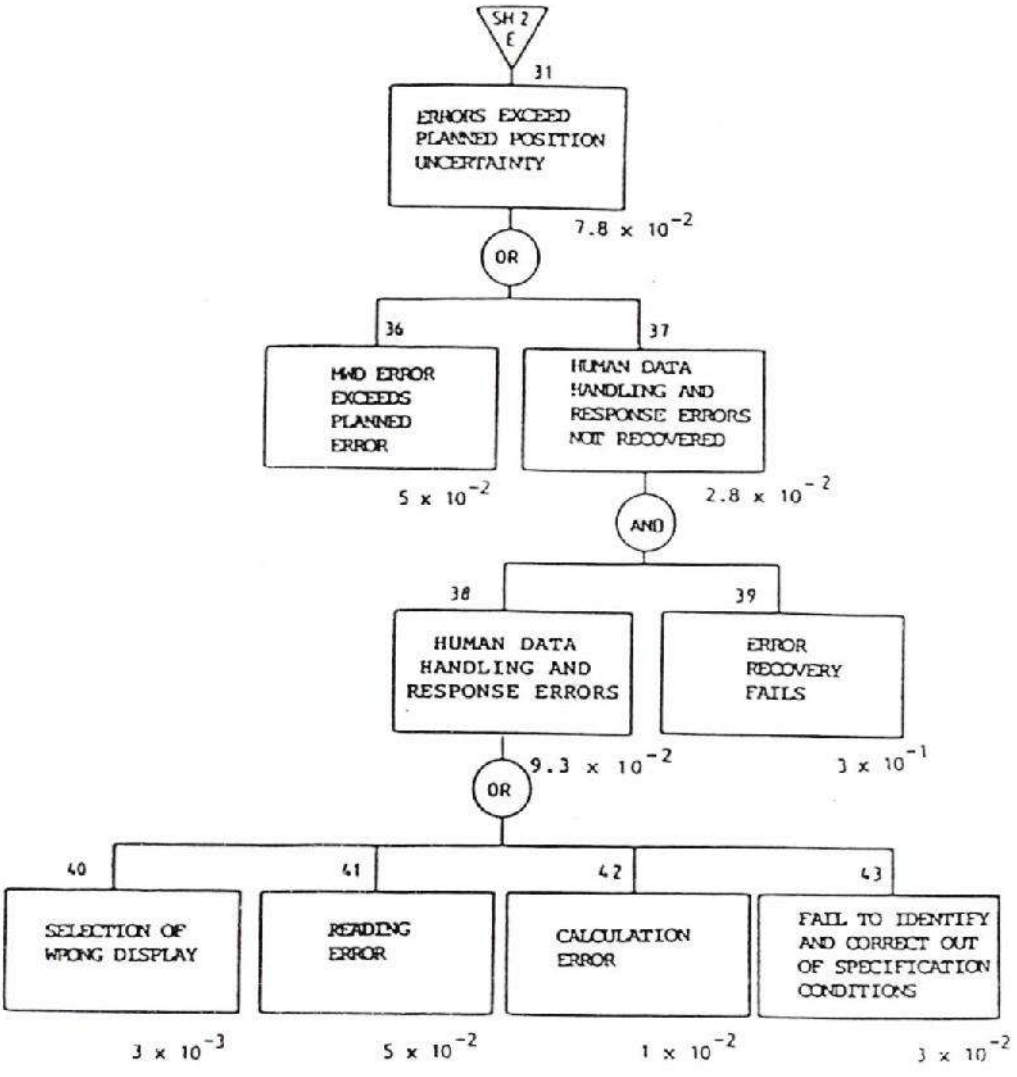

FIGURE 5 - Branch of Fault Tree showing human and equipment measurement-while-drilling (MWD) errors

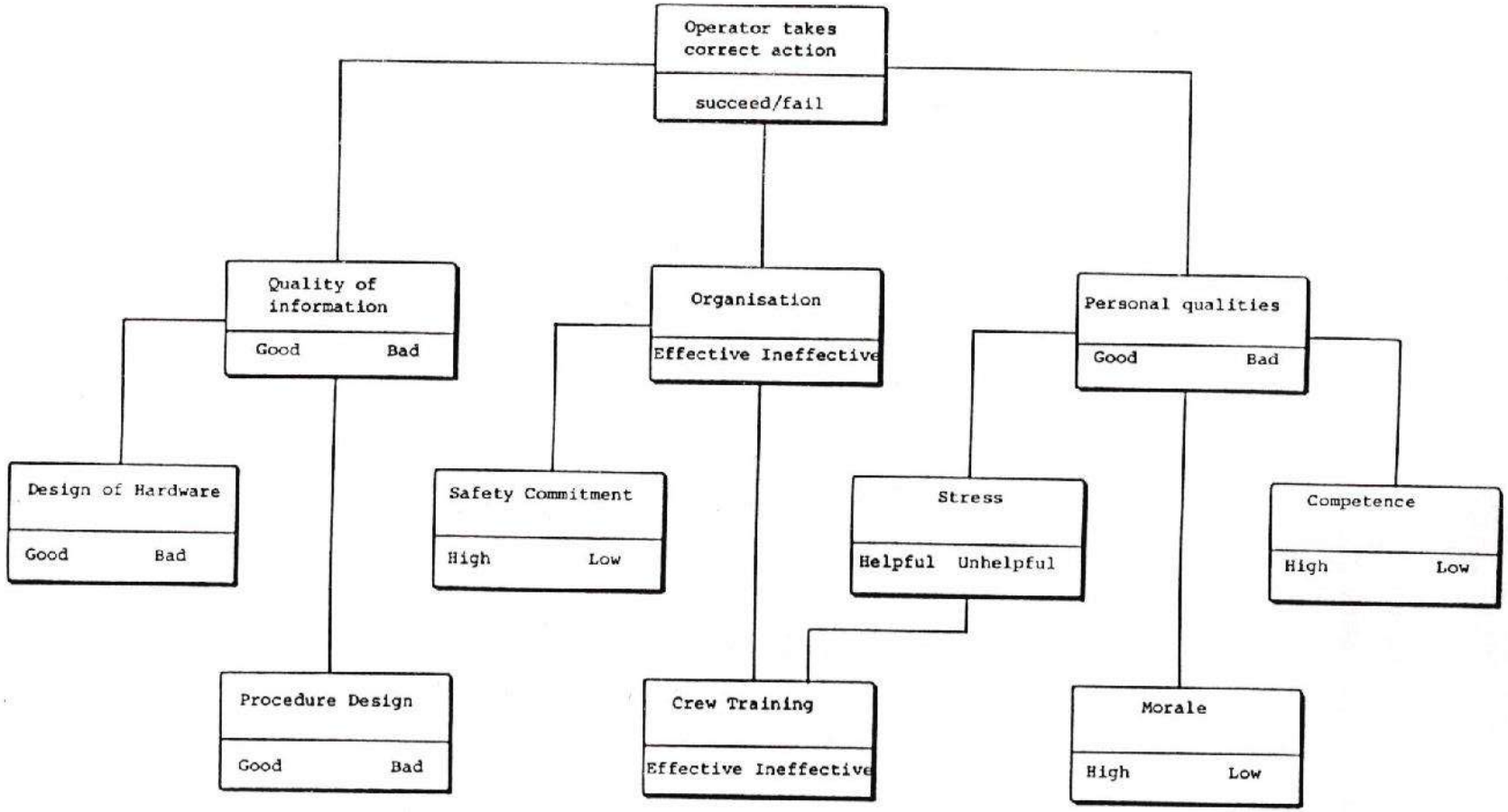

FIGURE 6 - Influence Diagram for Performance Shaping Factors (Lifeboat launching)

therefore modified the influence diagram technique to give it a three point distribution of "weight of evidence" (i.e. "good", "bad" and "average"). Furthermore, since it was observed that the algebra by which weights of evidence were manipulated in the evaluation of the tree was identical to probability algebra, we have simplified the terminology by redefining these weights as "probabilities".

With these transformations, we consider that the influence diagram technique is a very valuable tool for structuring the analysis of human errors in any particular individual procedural step, and, coupled with a degree of necessary expert opinion concerning the probabilities of the performance shaping factors, it can provide a trustworthy technique for quantifing human error probability.

8. CONCLUSIONS

1. Human error is important, and to ignore it may lead to serious underestimation of risk for a human-machine system.

2. Human reliability analysis can be meaningfully incorporated into conventional risk assessments using fault and event trees combined with human reliability and human factors techniques.

3. The incorporation of human reliability assessment into risk assessment with the concomitant recommendations for risk reduction provides the designer with additional means of reducing risk. In addition, quantifiction can be used to prioritise human factors recommendations.

9. RECOMMENDATIONS

1. Data on performance shaping factors and human error from real, as opposed to experimental, situations are extremely hard to find. An effort to categorise and collect such data in a systematic way should be made. This would need a coordinated effort involving a number of organisations that already have, or could collect, such data.

2. Experimental programmes are required to validate human reliability prediction techniques.

3. Risk assessments which include human error components have been made but are rarely published. Publishing more case studies would promote the use of human reliability assessment, facilitate peer review and enhance its acceptability as a tool.

REFERENCES

Comer, P.J., and Kirwan, B. (1985). A reliability study of a platform blowdown system. Symposium on Automation and Safety in Shipping and Offshore Petroleum Operations: Royal Garden Hotel Trondheim, Norway, 25-28 June 1985.

Drury, C.G. (1983). Task Analytic Methods in Industry. Applied Ergonomics, 14.1, 19-28.

Hannaman, G.W. et al (1983). Systematic Human Action Reliability Procedure (SHARP). Electric Power Research Institute Report EPRI-NP-2170-3, EPRI, Pulo Alto. California 92127.

Howland, A.H. (1980). Hazard Analysis and the Human Element, 3rd International Loss Prevention Symposium, Basle, 15-19 September, 1980.

Phillips, L.D., Humphreys, P. and Embrey, D. (1983). A socio-technical approach to assessing human reliability, London School of Economics Decision Analysis Unit, Technical Report 83-4 (July 1983).

Swain, A.D., and Guttmann, H.E. (1983). A handbook of Human Reliability Anlyses with Emphasis on Nuclear Power Plant Applications. NUREG/CR-1298, Washington D.C. 20555.

ACKNOWLEDGEMENTS

In the study of lifeboat launching procedures referred to in this paper, the fault tree analysis was carried out by Alan Miles of Technica (now with BP Exploration Ltd) and the influence diagram work by David Embrey of Human Reliability Associates.