REVIEW OF HUMAN FACTORS IN RELIABILITY AND RISK ASSESSMENT

I. A. WATSON
Head of Systems Reliability Service SRS, UKAEA

Human factors can have a significant impact on the reliable operation of technological plant. The impasse in the present state of research into known performance modelling is discussed. This is followed by a review of the techniques of human reliability modelling now being utilised in reliability and safety assessment. The importance of task analysis is illustrated and the problem of incorporating management influences is discussed. An appeal is made to management to recognise the important role that could be played in the development of the subject.

1. INTRODUCTION AND BACKGROUND

It is now commonly accepted by concerned professionals that human factors (HF) can have a significant impact on the safe and reliable operation of technological plant. This understanding is manifest across a variety of industries and technologies e.g., chemicals, processing, nuclear power, aviation, mining, computers and so on. What is still puzzling and controversial is how the matter can be wholly effectively dealt with.

This common concern was expressed in a paper produced on behalf of the Commission of European Community (CEC)(1) surveying research on human factors and man machine interaction and proposing a European Community collaborative research programme. Many probabilistic risk assessment (PRA) reports in the nuclear power industry(1)(2) have shown the tremendous significance of HF and man machine interaction/interfaces (MMI) in nuclear power plant accident sequences. Also HF plays a considerable role in software reliability and common cause failures(3). Its significance now in human computer interaction/interfaces (HCI) is being appreciated in the field of advanced information technology, so it has become a recognised research category in the huge UK, European, USA and Japanese 5th generation computer research projects now underway until 1990. It is well known in the case of aviation that 70%(4) of accidents are due to crew error and similar figures apply to the shipping and chemical industries. The experience of the systems reliability service (SRS) in carrying out reliability assessments for the process industries is that human error (HE) can figure significantly somewhere in many plant or system safety/reliability assessments. An indication of the economic significance of HF can be obtained by a simple calculation based on the loss of availability or mean fractional downtime (D) due to HE and the annual product revenue (APR) i.e., HE cost pa = D x APR

e.g., For D = 1%, APR = £10^6
HE cost pa = £$10^{-2} \times 10^6$
= £10,000

As these are representative figures then clearly it is worth spending a few thousand pounds pa per million pounds worth of product in order to reduce HE. However such trade-off calculations can relate to many aspects of plant design and operation. The moral is that good HF should be part of the whole process of marketing, specification, design, operation and maintenance of plant/systems.

The basis of good ergonomics have been laid down by workers over the past forty years. There is much useful material available relating to design and operation. Unfortunately this is not always utilised in industry, so NCSR in conjunction with the I Chem E is publishing a guidance document(5) which is aimed to help in the application of ergonomics as well as in understanding HF in order to reduce human error. This guide was produced with the aid of the Human Factors in Reliability Group (HFRG) which is supported by the National Centre of Systems Reliability (NCSR).

2. HF RESEARCH

The author of this paper is the chairman of the UK Human Factors in Reliability Group. The work of this group was described in August 1984 issue of the I Chem E "Loss Prevention Bulletin" number 058(8). One of its objectives is to support research and to this end it has members from many UK organisations (CEGB, SSEB, UKAEA, NII, CERL, MRC, HSE, ICI, NCB, BNF, Shell, RRA) and the universities and is in contact with major research projects in Europe and the USA(1)(8). Its members have been involved in many research teams both in the UK and internationally and as a group it is involved in liaisons and co-ordinations of research programmes. The chairman is involved substantially in this and the problem already referred to above has come to light during this activity, particularly in connection with proposing "Summary Guidelines for HF Research"(9) in the UK related to reliability and safety.

Now the controversial issue which has emerged in this document and particularly in its preparation is the clear difference between the perceptions of researchers and those of professional engineers and to some extent practising ergonimists on what are the fundamental issues to be addressed and the overall priorities. I believe that these are symptomatic of even deeper issues. As these differences are now emerging it is timely that we should make an effort to understand and face them.

It is striking that in a keynote address at Interact '84(10), the first International Conference on Human Computer Interaction (HCI), nine substantive areas were listed by Professor Shackel, Director of Husat Research Centre, Loughborough University of Technology, from a survey of "Ergonomics Technology in Europe" as needing research attention. These are listed below; the first five strongly relate to subjects already prioritised by the HFRG.

1. Theory especially in cognitive ergonomics
2. Cognitive/software interface
3. User variables and practical models of users
4. Measurement methods concerning cognitive activities
5. Knowledge for useability design
6. Procedures and tools for designers
7. Work, workplace and systems operation
8. Standardisation issues (including avoidance of premature standards)

9. *Organisational and social issues.*

Researchers in human factors related to safety and reliability and those relating to advanced information technology (AIT) and hence HCI clearly agree that fundamental work on human performance modelling (cognitive ergonomics/modelling user interactions) is necessary to make any substantial progress. One of the problems in communicating and co-ordinating views on relevant research which affect these issues is the lack of an agreed terminology and descriptions in the concerned community. To some extent this is part of the overall problems. It is clear from texts on cognitive psychology(11) that this science is still in an early state of development. Before the 1950's behavioural psychology ("behaviourism") was dominant but a revolution has occurred leading experimental psychologists to turn increasingly to investigation of the mind and so there has been a rebirth of interest in the "cognitive approach" to psychology. This emphasises three major characteristics which distinguish it from behaviourism:-

1. It emphasis "knowing" rather than merely responding as in the behaviourists stimulus-response (S-R) bonds.
2. It emphasises mental structure/organisation which is inherent in all living creatures and provides an important impetus to cognitive development.
3. The individual is viewed as being active, constructive and planful rather than being a passive recipient of environmental stimulation.

Linguists have had a considerable impact by showing that behaviouristic theories could not in principle work for the acquisition and use of language and cognition. Cognitive psychology draws considerably on computer science, particularly analogies with computer structures e.g., memory and processing and from programming analogies with thinking. Also great reliance has been placed on simulation for testing new theories. Out of this has grown a new theory called information processing theory which has contributed mainly to the development of the theory of memory structures. From this has emerged developments in the understanding of language processing, problem solving, reasoning etc. Other voices also argue that more emphasis should be given to understanding the human actions through interpretations of their meanings for the agents (humans) involved and through the elucidation of the purposes, rules, beliefs, reasonings which make these actions appropriate at the time of their performance(6). This is the so-called hermeneutical approach which is very much at odds with a purely mechanistic approach to human behaviour. This approach I believe is important to MMI understanding particularly for engineers and managers who wish to organise their understanding and those of plant operators, i.e., their experience so that the design and operation of the MMI is optimum. However, we need to be careful. It has been observed(11) that when people make decisions they "satisfice" rather than maximise or optimise, that is people accept a choice that is good enough rather than continue to search for the best possible. One reason why Simon(11) is the Nobel prize for economics is that he noted that economic theories often fail to take this into account. They assume that humans have a greater capacity than they actually do to obtain information from the environment, i.e., economic theories assume erroneously that people (and hence corporations) are optimisers or maximisers rather than satisficers. Managers and engineers can use their experience and understanding of plant operators to ensure that a proper understanding is taken into account in MMI design and operation. For this they must communicate effectively with the people involved. Even particle physicists have come to realise that they are in some ways participators in their experiments that they can never be completely isolated observers. Engineers know this from practical experience, but their classical scientific education and general character traits tends to be at variance with an interactive approach to plant personnel. This needs guarding against.

3. HUMAN PERFORMANCE MODELLING

Generic Models

The four stage model originally described by Polya(11) shown in Figure 1 has been updated by cognitive psychologists in a way related to memory working and language comprehension along the lines of modern information processing theory previously mentioned. More recently Norman(12) has produced a specialised version of this for HCI modelling. At the Interact '84 Conference he emphasised that as a professional psychologist he did not think that a scientifically satisfactory HCI model could be offered but engineering required adequate models and he thought that this requirement might be met. He identified four different stages when a person performs an action in an interactive cycle of activities:

- the formation of an intention
- the selection of a method
- the execution of that selection
- the evaluation of the resulting action.

These stages overlap and interact and the feedback or evaluation aspects are crucial, particularly the levels at which these occur and the recognition shown in the system design of this. As an illustration of the design implications of the four stages of user activities relevant to VDU screen layout the following table 1 was presented.

In this paper it is not appropriate to discuss details of the mainly software tools or aids advocated except to suggest that they form some form of guide for the more general MMI design and operation problem. The apparent differences between the first stages of the two models is more apparent than real, since Norman defines intention as "the internal mental characterisation of the desired goal".

The value of the above models compared with a more conventional MMI "operator" model as an information processor as shown in Figure 2 is that they are set at a higher cognitive level and emphasise "feedback", which is often more appropriate to modern plant conditions and can be used more widely. With all these models, consideration has to be given to major performance shaping factors (PSF). These will be seen to recur as the discussion of appropriate models develops. Typical PSF are:-

- Level of mental loading
- " " " skill
- Activation and arousal
- Environmental factors
- Perception of risk
- Error correction and feedback.

The last mentioned PSF is probably the most fundamental and has implications at many levels and is consequently being incorporated much more explicitly in actual models. It emphasises the interconnectedness or network situation typical of human activity.

TABLE 1

DESIGN IMPLICATIONS FOR THE STAGES OF USER ACTIVITIES	
STAGE	TOOLS TO CONSIDER
Forming the Intention	Structured Activities Workbenches Memory Aids Menus Explicit Statement of Intention
Selecting the Action	Memory Aids Menus
Executing the Action	Ease of Specification Memory Aids Menus Naming (Command Languages) Pointing
Evaluating the Outcome	Sufficient Workspace Information Required Depends on Intentions Actions Are Iterations toward Goal Errors as Partial Descriptions Ease of Correction Messages Should Depend upon Intention

The Riso National Research Laboratory in Denmark has become well known for the work of Rasmussen and his co-workers in this field and for their useful insights into human performance/error modelling. A much richer model than shown previously has emerged as shown in Figure 3. This has yet to be validated in many respects, but it has stimulated some helpful developments. One of which is shown in Figure 4 that is more related to the practical situation of decision making at the MMI. This model can be more easily understood in terms of a more generalised model related to human information processing shown in Figure 5. This emphasises three basic levels of capability based behaviour that can be directly related to the data processing activities of the previous model.

The human performance models briefly discussed above have concentrated essentially on MMI with emphasis on the lone operator. They are approximations in as yet a poorly developed area of scientific understanding, but they are of practical assistance if used with caution. However they do not really take full into account the interconnectedness and interactions of human activities. A model which takes this more fully into account came out of a Safety and Reliability Directorate (SRD)(7) study of accidents in UK Health and Safety Directorate. This showed many influences at work affecting human performance leading to fatal accidents. The model is shown diagrammatically in Figure 6. From this an accident classification scheme was derived which reflects the principle influences shown in the model. This is illustrated in Figure 7.

The centre of the influence model in Figure 7 is MAN, the modelling of which has been briefly reviewed above. Another is the actual plant concerned. From the reliability and risk point of view this is dealt with by well known reliability techniques related to but not the concern of this paper. The other two i.e., TASK and MANAGEMENT will now be considered.

Task Analysis

The most effective form of reliability analyses involving human operations usually involves some form of task analysis. This is because it is the reliability that can be achieved in the task(s), in which humans are involved, that is the essential concern of risk analysis or reliability assessment. The most useful form of this type of analysis used by ergonomists is hierarchical task analysis(21).

An illustration

To illustrate this process of redescription, consider an operation that might be carried out as one of the duties of a chemical plant operator - 'ensure caustic concentration is within limits specified by manufacturing instructions'. By questioning an informant competent at this operation, we may be able to say that the five sub-ordinate operations in Figure 8 need to be carried out.

But simply listing these five sub-ordinates does not provide a complete redescription of the operation being examined. Their plan must be stated. In this case the plan is most clearly stated in the form of the algorithm in Figure 9.

The same process of redescription can now be applied to each of the five sub-ordinate operations identified in Figure 8. Figure 10 shows how some of these redescriptions may be carried out. Some of the operations so derived may also be treated in a similar fashion.

Control and Monitoring of Tasks

In the NCSR study of common cause failures(3) the importance of control, monitoring and feedback came to be realised in reducing human error, particularly in connection with maintenance. Also the importance of high level controls such as QA, design review and reliability assurance in minimising design error. The essential points are set out in the idealised flow diagram form of task checking model shown in Figure 11.

The p solid line arrows represent stages of work and the p_c and p'_c dotted arrows represent the checking process at various stages, the latter are shown as a feedback function. Making the important assumption that to a large degree these individual actions are independent and the p and p_c symbols are taken as probabilities of error, then assuming that the probabilities are small, the overall probability of failure is given by:-

$$
\begin{aligned}
p_a &= \{[(pp_c + pp_c)\ p'_c + pp_c]\ p'_c + \dots + pp_c\} \cdot p'_c \\
&= pp_c\ p'_c + \text{higher order terms.}
\end{aligned}
$$

Experience has shown that high integrity can be achieved by various means, e.g., high skills, experience, QA. Generally this can be entitled "product assurance". According to the task checking model shown in Figure 11 this involved determining that p'_c, the overall task control element is adequate. Turning now to Figure 12 this represents the upper hierarchy of an overall sub-system CCF modelling structure where CCF models incorporates, maintenance, engineering and random errors (causal mechanisms) as previously discussed. The latter can be divided as shown in Figure 12 and various models have been discussed in the literature for dealing with them. The various generic factors which enter into the estimation of engineering error are shown in Figure 13. These are assumed to be nominally independent, although this may be not entirely true. Studies of plant are have shown that engineering defects decrease by up to an order over a few years(3). The regulatory authorities insist that their experience shows that mandatory codes of practice have a beneficial effect. The three principal types of product assurance shown, i.e., design review, reliability assessment, QA will also contribute perhaps up to an order each improvement in error rate. The thorough implementation of all these factors can obviously have a very significant effect and indicate how a much lower error probability than 10^{-3} may be achievable. Very little data is available to support these predictions except that from aircraft systems.

Management Assessment

This is the most problematic and least developed area from a risk and reliability viewpoint. It is a common influence affecting all aspects of plant operation. Some authorative sources believe that the range from very good to very poor management can produce an order of magnitude increase in risk of accidents. Some analysts believe it can best be dealt with by considering the effects of supervision, training, working environment, etc., and other management controlled factors at the detailed task level. Indeed the existence and performance of overall controls and monitoring as previously described is clearly a major management responsibility in reducing risk and improving reliability. In the aviation world(13) the flight crew training programmes are expanding beyond the traditional role of maintaining piloting skills and providing instruction orientated towards flight deck management crew co-ordination, teamwork and communications.

Flight simulator training(13) now include management programmes focusing on communications and management practices e.g.,

- managerial philosophy
- individual work styles
- communications
- integration of the "four" foundations of management - planning, organising, leading and controlling
- management skills and involvement practices
- specific strategies for the effective exertion of influence.

Flight experts tend to relate aircraft accidents to interpersonnel and management factors far more than lack of systems knowledge or to aircraft related factors. Studies(13) identify a "safety window" in which nearly 83% of accidents involving professional pilots occur beginning at or about the final approach fix and extending through approach and landing. 90% of the accidents that occur in this window appear not to be aircraft related, they are pilot caused and seem to reflect failure to management properly. As a result in training pilots a role change is occurring converting the pilot from a control manipulator to an information processor.

Practically the only technique which has been developed to model and assess management explicitly from the risk viewpoint is the Management and Oversight and Risk Tree (MORT)(14). This system safety programme has been developed and refined by the US Department of Energy (DOE). MORT is a systematic approach to the management of risks within an organisation. It incorporates ways to increase reliability, assess risks, control losses and allocate resources effectively.

The acronym, MORT, carries two primary meanings:

(1) the MORT "tree", or logic diagram, which organises risk, loss, and safety program elements and is used as a master worksheet for accident investigations and program evaluations;

and (2) the total safety program, seen as a sub-system to the major management system of an organisation.

The MORT process includes four main analytical tools. The first main tool, Change Analysis, is based upon the Kepner-Tregoe method of rational decision making. Change Analysis compares a problem-free situation with a problem (accident) situation in order to isolate causes and effects of change.

The second tool, Energy Trace and Barrier Analysis, is based on the idea that energy is necessary to do work, that energy must be controlled, and that uncontrolled energy flows in the absence of adequate barriers can cause accidents.

The third, and most complex, tool is the MORT Tree Analysis. Combining principles from the fields of management and safety and using fault tree methodology, the MORT tree aims at helping the investigator discover what happened and why.

The fourth tool, Positive (Success) Tree Design, reverses the logic of fault tree analysis. In positive tree design, a system for successful operation is comprehensively and logically laid out. The positive tree, because it shows all that must be performed and the proper sequencing of events needed to accomplish an objective, is a useful planning and assessment tool.

An illustration of a MORT "tree" or logic diagram is shown in Figure 14.

4. QUANTIFICATION OF HUMAN ERROR

In a review(7) of the general approaches to human reliability quantification carried out by the Safety and Reliability Directorate (SRD) of the UK Health and Safety Executive (HSE) three broad categories of approach were described.

The first of these relies primarily on combining together historical data on the probabilities of failure for relatively basic elements of human behaviour such as operating switches, closing valves or reading dials, to give the likelihood of errors for more complex tasks which are aggregations of these basic elements. Such techniques are variously referred to as 'and synthesis', 'reductionist' or 'decomposition' approaches. The next approach are those which attempt to apply classical reliability techniques of time dependent modelling to predict parameters such as probability on a function of time. The third category of techniques makes a much greater use of quantified subjective judgement, supplement the currently inadequate data base of objective data on the probability of human error for various types of task. Also, these methods tend to take a more holistic approach to the evaluation of a task than the decomposition techniques.

Further developments have taken place in some of the specific techniques described in the SRD/HSE report(7), new techniques have appeared and there has been a proliferation of work and PRA reports for the American nuclear power industry utilising many variations of the available methods. It must be emphasised that most of these techniques rest in some way, although often tentatively, on the human performance models previously described. They are loosely based on such models and are techniques to quantify certain kinds of events in probabilistic risk analysis (PRA). They represent an engineering solution to a problem that has resisted solution in the fields of psychology and human factors.

A framework for the systematic application of these techniques has recently been provided through the Electric Power Research Institute (EPRI) of the USA by the NUS Corporation. This is the so-called SHARP (Systematic Human Action Reliability Procedure) framework(15). A description of the method of quantification will be given therefore with reference to this framework.

The SHARP framework is shown in Figure 15 which shows the links between the seven steps involved. The objective of the first step is to ensure that potentially important human influences are included in plant logic diagrams such as event trees (ET) and fault trees (FT). An example of an enhanced fault tree produced after undergoing the detailed procedures of the definition step is shown in Figure 16. The failure "types" referred to in this figure are defined in the SHARP report, but are self-explanatory in the fault tree. In step 2 the objective is to reduce the number of human interactions identified in step 1 to those that might be significant. The application of coarse screening is shown in Figure 17 which is the same fault tree as the previous figure where the analyst has applied generic equipment data and a fixed human error probability, e.g., 1.0. Coarse screening takes into account only those system features that diminish the impact of human interactions on accident sequences. Fine screening goes beyond this by also applying probabilities to human actions. Various examples of suggested screening data have been given in the literature(7)(15). Figure 18 shows a graph based on the Rasmussen model of human data processes and typical malfunctions previously described in Figure 5. The application of such error rates to the fault tree shown in the previous figures is shown in Figure 19. The impact of failure to maintain the breakers is thus seen to be very significant relative to the combination of the failure to scram automatically and manually.

The objective of step 3 is to amplify the qualitative description of each key human interaction identified in step 2. This is essentially done by means of some form of hierarchical task analysis such as previously discussed. Influence parameters, performance shaping factors, ergonomic features (or lack of them) etc., need to be considered to establish a basis for selecting a model basis for representation of the human interactions. This would include organisational factors, quality of information, procedural matters as well as personnel factors.

The steps described so far are usually followed to some limited degree by risk and reliability analysts. Some form of screen or sensitivity analysis is advisable because of the difficulties in carrying out the next steps 4, 5 and 6 concerned which is what is often regarded as human reliability modelling. In fact step 3 and step 4 require human factors specialists as well as risk/reliability assessors whereas the previous steps principally requires systems and reliability expertise. In recent work carried out by NCSR(16) on reactor pressure vessel ultrasonic inspection the ET/FT format was followed. The event tree following the sequence of welding and testing and fault trees was developed for the nodes of the ET each of which involved ultrasonic testing. The fault trees were generated to the level at which reasonable robust human reliability data could be generated as in Figure 20. A similar procedure was devised for human error treatment in major hazard assessment(17) by SRD. An example of an event tree from a typical example is shown in Figure 21.

Human Reliability Modelling

Not all the modelling techniques and data generation methods can be considered here, so only those most relevant to the power and process industries will be considered since their requirements do have considerable similarities. The models and data will be considered together rather than separately, since they are intimately linked. It is worth mentioning here that step 5, impact assessment, of the SHARP procedure allows a re-evaluation of the overall reliability/risk assessment so far and the incorporation of any *insights gained having decided which human reliability models should be used.* The rest of this paper will only be concerned with human reliability modelling and not with the details of the SHARP procedure which essentially only formalises what risk analysts and reliability assessors have been doing to varying degrees anyway.

Operator Action Tree (OAT)

This representation(15) of human decision making is shown in Figure 22. It allows for mis-interpretation by the operator at various key stages in the execution of a task. There are two significant aspects. The first is the limited time which the operator has to carry out the task. The OAT method has a time failure (or non-response) probability relationship. The second is that the operator can take various decision paths and the assessor can determine whether they are key or not. If as shown in the Figure 22 all paths but one lead to failure then they can be grouped together. However if for example failure to diagnose the event correctly could lead to inappropriate action (as evidence indicates has happened since operators often do not follow standard procedures) then the OAT representation should reflect this. Although the OAT representation shown does not show recovery action, it may be appropriate also to allow for this key extension of the tree.

The time related non-response probability data used to quantify OAT is shown typically in Figure 23. The grouping of these curves might tentatively be considered to show the essential character of skill, rule and knowledge based behaviour (moving from L to R across the graph). However further work on the use of simmulator data and human behaviour modelling is required to clearly establish the relationship between human behaviour types and simulator results. The OAT representation potentially is capable of modelling human performance reliability with high levels of problem solving requirement.

Human Reliability Analysis (HRA)

(This technique was formerly called THERP "Technique for Human Error Rate Prediction"). The HRA tree provides a flexible structure for representing the steps of a well defined procedure. Some steps may involve omissions while others may show up as errors of commission. This method has been extensively developed over the past decade. An overview of the procedure involved is shown in Figure 24. Details of the method have been extensively described in a handbook(18) which includes data sets and a procedures guide(19). An illustrative HRA tree together with explanatory glossary and data is shown in Figure 25. The evaluation of performance shaping factors and the procedures for choosing data are explained in detail in the handbook. It may be seen that the HRA tree is similar to the fault tree approach used by NCSR in the reliability analysis of RPV inspections. However there are a variety of methods for generating the data for the basic events in the trees or indeed for whole tasks.

It will be seen from the HRA tree illustrated that it is based on the task analysis approach previously described. Data has been estimated and presented in the handbook for a variety of task elements. The method of estimation was expert judgement by small groups of experts. This data has been verified to a limited extent by a recent simulator study(20). The observed error rates (OER) from the simulator study were compared with the adjusted (allowing for PSFs) human error probability (AHEP) derived from the handbook and found to be largely in agreement. A summary of the results is shown in Table 2. In the case of errors of commission which appeared to be mainly due to operator slips, almost instantaneous error recovery was a significant factor as indicated by the recovery rate in the Table.

TABLE 2 SUMMARY OF OERs

Error Type	OER[a]	AHEP
Whole-Step Omissions		
With Procedures	.0314	.0148 (.0049-.044)
Without Procedures	.0473	.0163 (.0033-.0815)
Within-Step Omissions	.0270	.0155 (.0031-.0775)
General Commission:		
Total:	.00316	.00453 (.0015-.0136)
Unrecovered:	.00042	
Recovery Rate =	.867	

a. Taken from Table 4-4 (reference 20)

Expert Opinion

This has already been referred to in connection with the HRA method which mainly utilised direct numerical estimation by expert groups. It appears to be quite successful and is supported by experience and trials in NCSR. Two other methods are also worthy of serious consideration.

The paired comparison technique was originally developed for psychological scaling and was adopted for human reliability purposes by Hunns and Daniels of NCSR(7). Pairs of tasks from a set of interest are successively judged by each judge in a panel. This procedure is repeated for all possible pairings from the set and a scale of likelihood of failure constructed, based on certain assumed mathematical relationships. The justification for these assumptions are theoretical with very limited experimental evidence. The procedure tends to be long and laborious and has not been used extensively.

SLIM-MAUD

This is the "Success Likelihood Index Methodology"(22) implemented through the use of an interactive computer programme called "Multi-attribute Utility Decomposition".

The basic rationale underlying SLIM is that the likelihood of an error occurring in a particular situation depends on the combined effects of a relatively small set of performance shaping factors (PSFs). In brief, PSFs include both human traits and conditions of the work setting that are likely to influence an individual's performance. Examples of human traits that "shape" performance might include the competence of an operator (as determined by training and experience), his/her morale and motivation, etc. Conditions of the work setting affecting performance might include the time available to complete a task, task performance aids, etc. It is assumed that an expert judge (or judges) is able to assess the relative importance (or weight) of each PSF with regard to its effect on reliability to the task being evaluated. It is also assumed that, independent of the assessment of relative importance, the judge(s) can make a numerical rating of how good or how bad the PSFs are in the task under consideration.

Having obtained the relative importance weights and ratings, these are multiplied together for each PSF and the resulting products are then summed to give the Success Likelihood Index (SLI). The SLI is a quantity which represents the overall belief of the judge(s) regarding the likelihood of success for the task under consideration.

The logarithmic relationship between expert judgements and success probabilities can be expressed with the following calibration equation:

$$\text{log of the success probability} = a\ \text{SLI} + b$$

where: a and b are empirically derived constants.

In general, the field evaluation of the basic SLI methodology has been successful in achieving several objectives. Although it was not possible to verify the accuracy of the human error estimates produced by SLIM because of the absence of sufficient field data on the rare event scenarios being evaluated, the judges involved in the exercise had considerable confidence in the results. It also seemed apparent that SLIM provided a useful structure which assisted the judges in modelling the potential failure modes.

Comments on Human Reliability Modelling

Clearly there are limitations to the extent which psychology can be used to produce well based and useful techniques. It has been shown that there are also other related important considerations. The effect of feedback and error recovery and conditional probabilities can introduce considerable structural complexities into the model. In particular such complexities make the choice of a taxonomy on which modelling and data collection can be based very difficult. There is as yet no universally accepted generic approach to decomposition methods or the corresponding data bases. These have been and should continue to be the subjects of basic research. One way ahead being investigated is to use basic ergonomic research data on the effects of very specific influences such as unfamiliarity, time, poor recovery capability, overload, learning etc., in combination to produce failure data of practical use in reliability assessment. This may lead to a Bayesian methodology. An intermediate step intended by NCSR in conjunction with the HFRG is to produce a longer version of the guide(5) done recently in co-operation with the I Chem E incorporating some of these features. For industries with the capability the use of simulators to verify modelling techniques and derived data will also be extremely useful if not indispensible.

5. RISK PERCEPTION

This is an area not so far mentioned, but which can sometimes be of acute interest and importance to the safety/reliability assessor. It is an area mainly affected by social and political considerations, however the 'human factor' attributes which have been found to influence perceptions of technological risk are listed below(23). They are negatively valued by most people, therefore the stronger the belief that the technology is characterised by these attributes, the less likely people will be to accept it

- involuntary exposure to risk
- lack of personal control
- uncertainty about the probabilities or consequences
- lack of personal experience
- difficulty in conceptualising or imagining
- delayed effects
- infrequent but catastrophic accidents
- the benefits are not highly visible
- the benefits go to others
- accidents caused by human failure.

It would be as well, when risk criteria or targets are being set, to bear these considerations in mind.

6. CONCLUSIONS

A crisis point has been reached in the development and application of human factors related to safety and reliability. This may be overcome by good research management,, but more particularly by a positively sympathetic attitude from engineering management.

The fundamental psychological sciences need considerable development to form a sound basis for technical application in safety and reliability. Techniques are being applied which appear to be adequate, however they have been essentially derived through engineering demand from reliability technology with some limited encouragement by HF specialists. These techniques relate strongly to task analysis and decision making trees which are more central to the problem and can be related to the management, plant and environmental influences. The fundamental decision/task element taxonomies involved in the modelling methods need further development, validation and proving. The dearth of 'real' data is a stumbling block which needs to be overcome. The exact roles which pscyhologists, HF specialists and engineers will play in this is not clear. Management will have to shoulder a major responsibility to ensure that people's experience and their understanding of their work plays a correct role in the formulation and application of HE reduction and assessment methods. They also have a major role to play in ensuring the development of such methods.

REFERENCES

1. WATSON, I. A. et al. "Critical Survey of Research on Human Factors and the Man-machine Interaction" IAEA-SM-26B/29. International Atomic Energy Agency (1984).

2. "The German Risk Study" Rep EPRI-NP-1804 SR Electric Power Research Institute Palo Alto (1981).

3. EDWARDS, G. T. and WATSON, I. A. "A Study of Common Mode Failures", The *Safety and Reliability Directorate* UKAEA SRD R146 (1980).

4. Flight International 22, January (1975).

5. "Guide to Reducing Human Error in Process Operation", Short Version by the Human Factors in Reliability Group. Published by NCSR, UKAEA, Wigshaw Lane, Culcheth, Warrington.

6. GOULD, A., SHOTTER, J. "Human Action and its Psychological Investigation". Routledge and Kegan Paul (1977).

7. "Human Factors in industrial Systems ~ Review of Reliability Analysis Techniques". (Draft available from the HSE, Chapel Street, London).

8. "LOSS PREVENTION BULLETIN" Number 058, August (1984).

9. "HUMAN FACTORS RELATED TO RELIABILITY", Proposed Summary Guidelines for Research. Obtainable from I. A. Watson, Head of SRS, SRD, UKAEA, Wigshaw Lane, Culcheth, Warrington.

10. INTERACT '84 First IFIP Conference on Human-Computer Interaction Conference Papers, September 1984. SHACKEL, B. Keynote Address "Designing for People in an Age of Information" page 6.

11. "Cognitive Psychology" by Darlene V Howard, Macmillan Publishing Co Inc., New York, Collier Macmillan Publishers London (1983).

12. NORMAN, DAVID A. "Four Stages of User Activities" INTERACT '84 (see ref. 13) Page 81.

13. Aviation Week & Space Technology. October 1, (1984) page 99. "Cockpit Crew Curriculums Emphasise Human Factors".

14. "MORT Management and Oversight Risk Tree". International Risk Management Institute, Vol. VI, No. 2, October (1983).

15. "Systematic Human Action Reliability Procedure (SHARP)" EPRI NP-3583 Interim Report, June (1984).

16. WILLIAMS, J. C. et al. "A Method for Quantifying the Effectiveness of Ultrasonic Inspection to Identify and Detect Flaws in Welds", NCSR UKAEA 8th Advances in Reliability Technology Proceedings, University of Bradford, April (1984).

17. "A Suggested Method for the Treatment of Human Error in the Assessment of Major Hazards" Safety and Reliability Directorate SRD R254, UKAEA, Wigshaw Lane, Culcheth, Warrington WA3 4NE.

18. SWAIN, A. D. et al. "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications". Final Report NUREG/CR-1278 Prepared for the US Nuclear Regulatory Agency, August (1983).

19. BELL, Barbara Jean et al. "A Procedure for Conducting a Human Reliability Analysis for Nuclear Power Plants" Final Report NUREG/CR-2254 May (1983). Prepared for the US Nuclear Regulatory Agency.

20. "A Simulator Study-based Study of Human Errors in Nuclear Power Plant Control Room Tasks", NUREG/CR-3309, January (1984). Prepared for the US Nuclear Regulatory Agency.

21. DUNCAN, K. D. et al. "Task Analysis". Training Information Paper No. 6, (1971), HMSO London.

22. SLIM-MAUD: "An Approach to Assessing Human Error Probailities using Structural Expert Judgement" NUREG/CR3518 EMBREY, D. E. et al, March, (1984). Prepared for the US Nuclear Regulatory Commission.

23. "Beyond Acceptable Risk: On the Social Acceptability of Technologies" OTWAY, H. J. Policy Sciences 14, (1982), 247-256. Elsevier Scientific Publishing Co., Amsterdam.

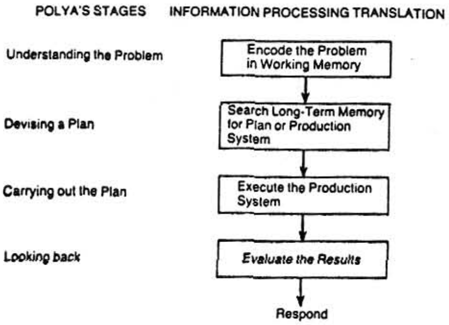


Figure 1 Polya's (1957) four stages of problem solving

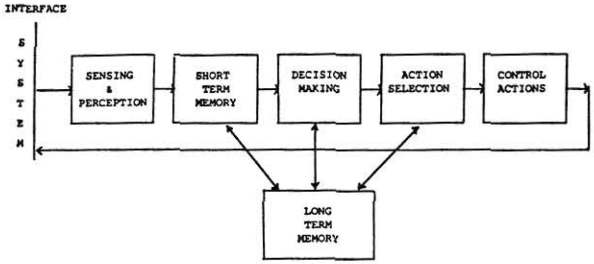


FIGURE 2: FLOW OF INFORMATION THROUGH THE HUMAN OPERATOR

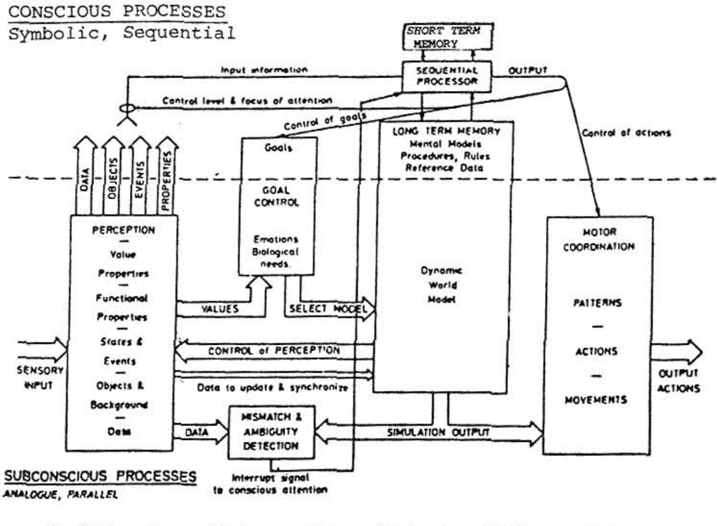


Fig. 3 Schematic map of the human data processing functions which illustrates the important role of the subconscious dynamic world model as part of a complex loop of interactions in conjunction with the perception and goal systems. The world model also forms the basis for a high-capacity efficient feed-forward control of physical actions and serves as a reference for the mismatch detector which activates the conscious processor.

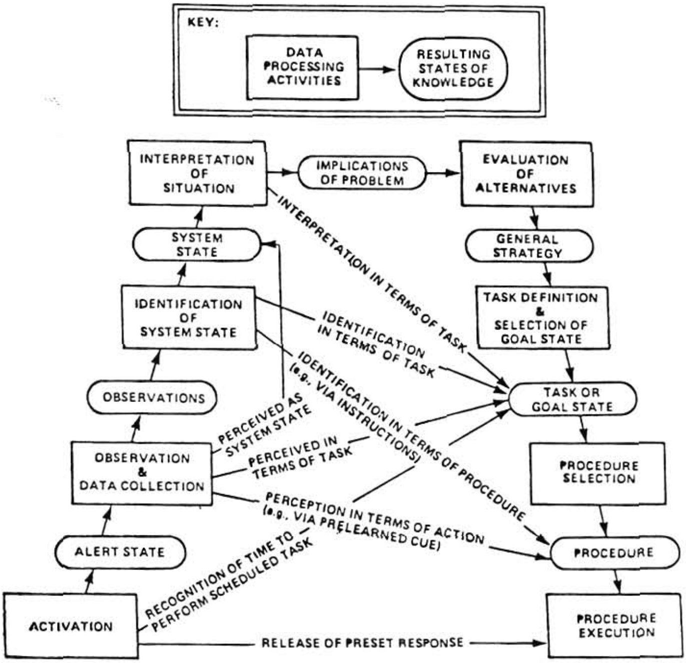


Figure 4 Decision-making Model (Adapted from Rasmussen)

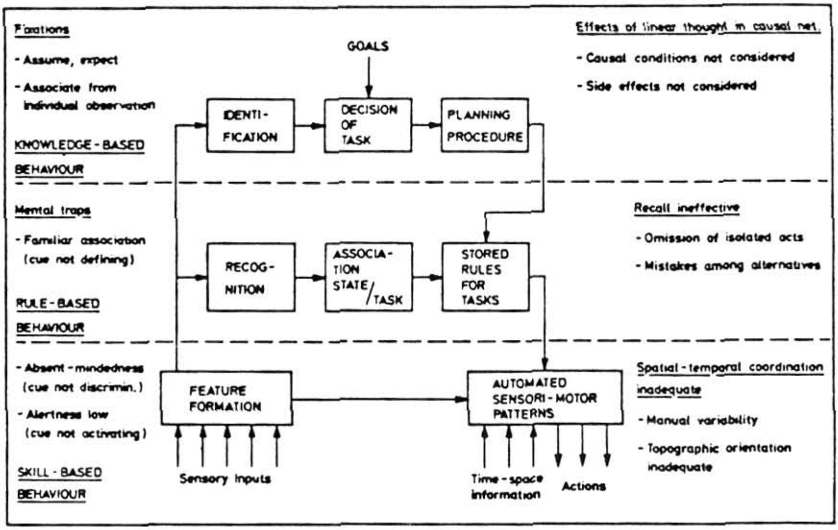


Figure 5 Model of human data processes and typical malfunctions. Reproduced from Rasmussen, 1980

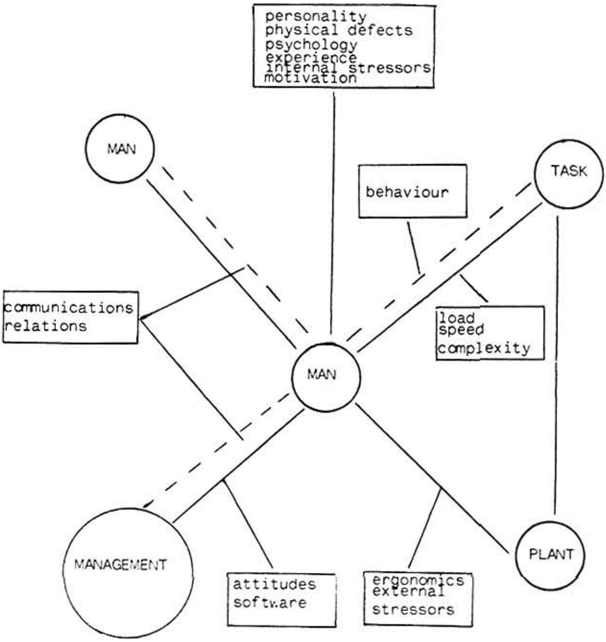


Fig. 6 Influences on man in industry

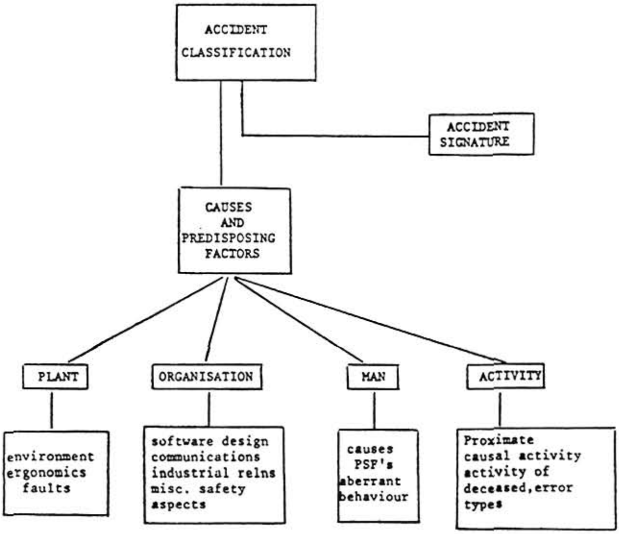


FIG 7: Macro-structure of TAXAC

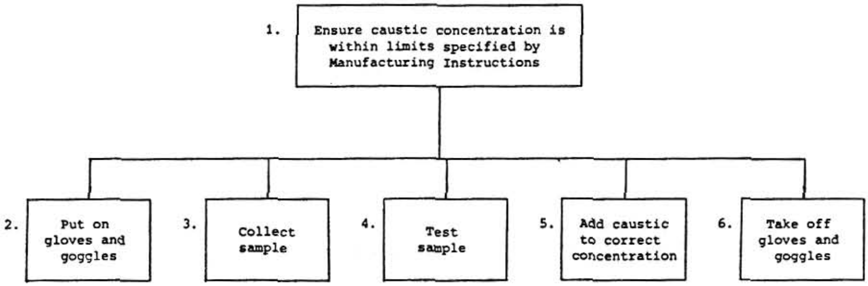


Figure 8

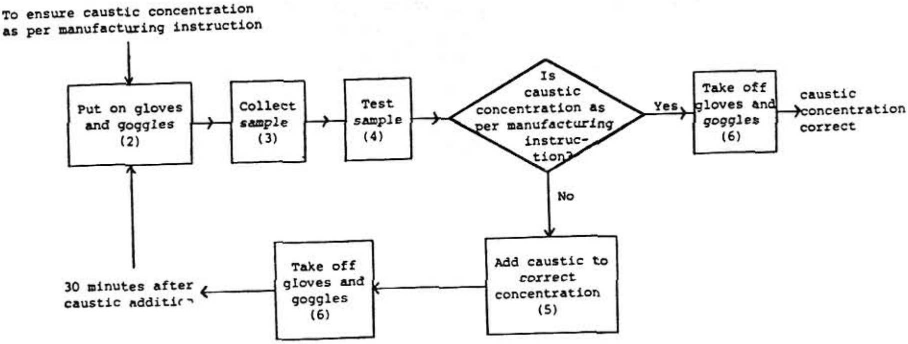


Figure 9

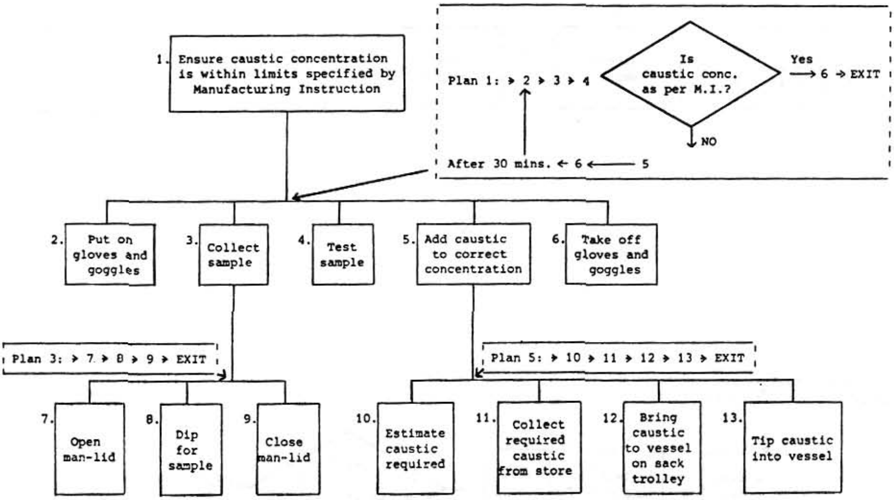

1. Ensure caustic concentration is within limits specified by Manufacturing Instruction
Plan 1: > 2 > 3 > 4
Is caustic conc. as per M.I.?
Yes
→ 6 → EXIT
NO
After 30 mins. ← 6 ← 5
2. Put on gloves and goggles
3. Collect sample
4. Test sample
5. Add caustic to correct concentration
6. Take off gloves and goggles
Plan 3: > 7 > 8 > 9 > EXIT
Plan 5: > 10 > 11 > 12 > 13 > EXIT
7. Open man-lid
8. Dip for sample
9. Close man-lid
10. Estimate caustic required
11. Collect required caustic from store
12. Bring caustic to vessel on sack trolley
13. Tip caustic into vessel

Figure 10

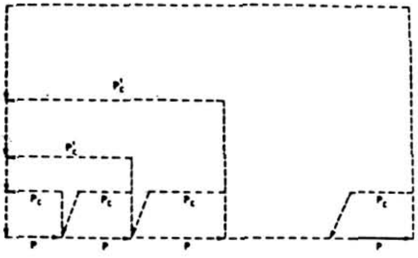


FIG 11 TASK CHECKING MODEL

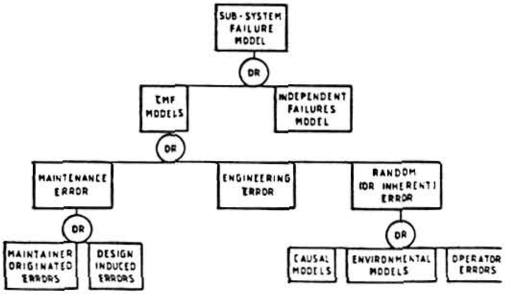


FIG 12 SUB-SYSTEM CCF MODELLING STRUCTURE

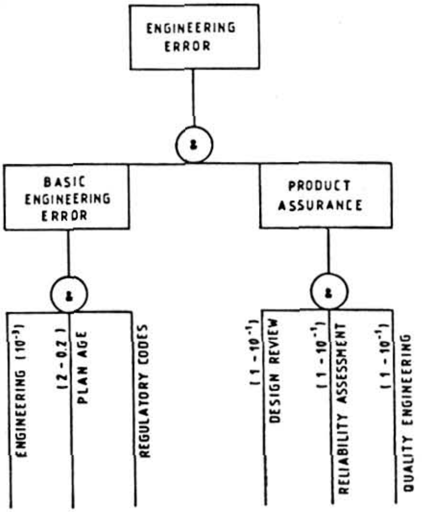
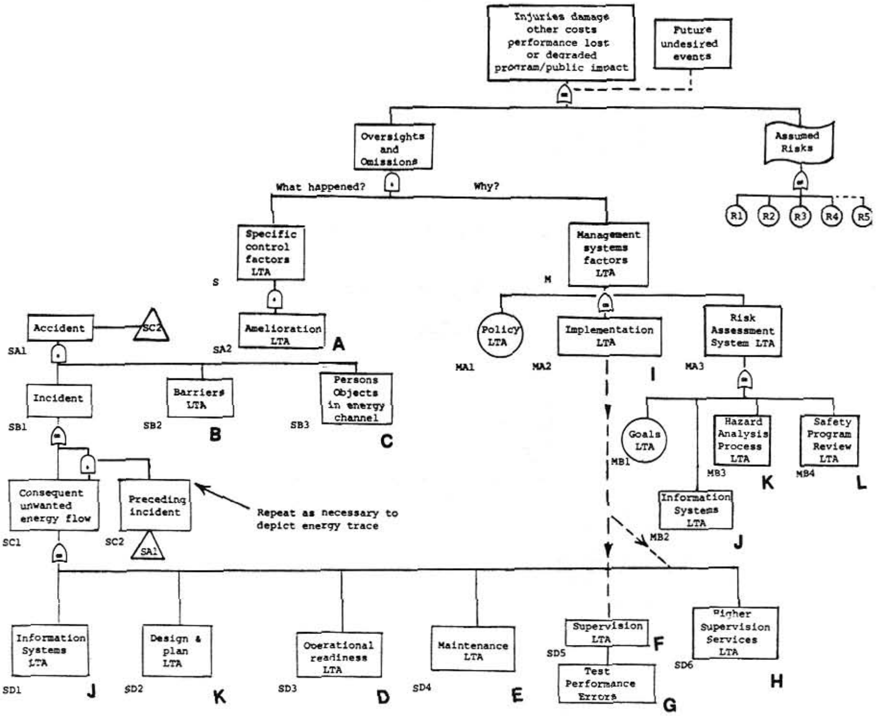


FIG.13 PART OF SUB-SYSTEM CMF MODELLING STRUCTURE



LETTER ABBREVIATIONS

D/N - DID NOT
D/NP - DID NOT PROVIDE
ERDA - ENERGY RESEARCH & DEVELOPMENT ADMINISTRATION
F/ - FAILED FAILURE
F/M - FAILED TO MONITOR
F/M&R - FAILED TO MONITOR & REVIEW
F/T - FAILED TO
HAP - HAZARD ANAL. PROCESS
JSA - JOB SAFETY ANAL.
LTA - LESS THAN ADEQUATE
OSHA - OCCUPATIONAL SAFETY & HEALTH ADMINISTRATION
RSO - REPORTED SIGNIFICANT OBSERVATION
W/ - WITH

MORT: MANAGEMENT OVERSIGHT AND RISK TREE

Figure 14

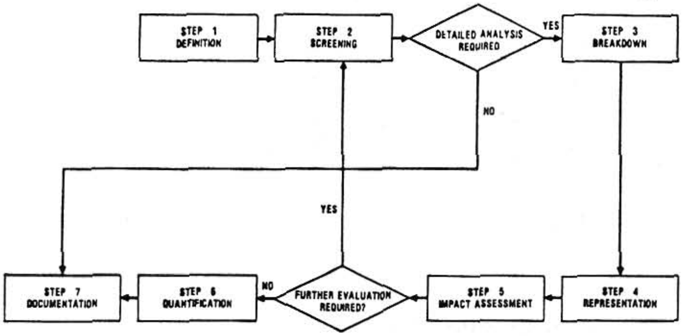


Figure 15 Links Between SHARP Steps

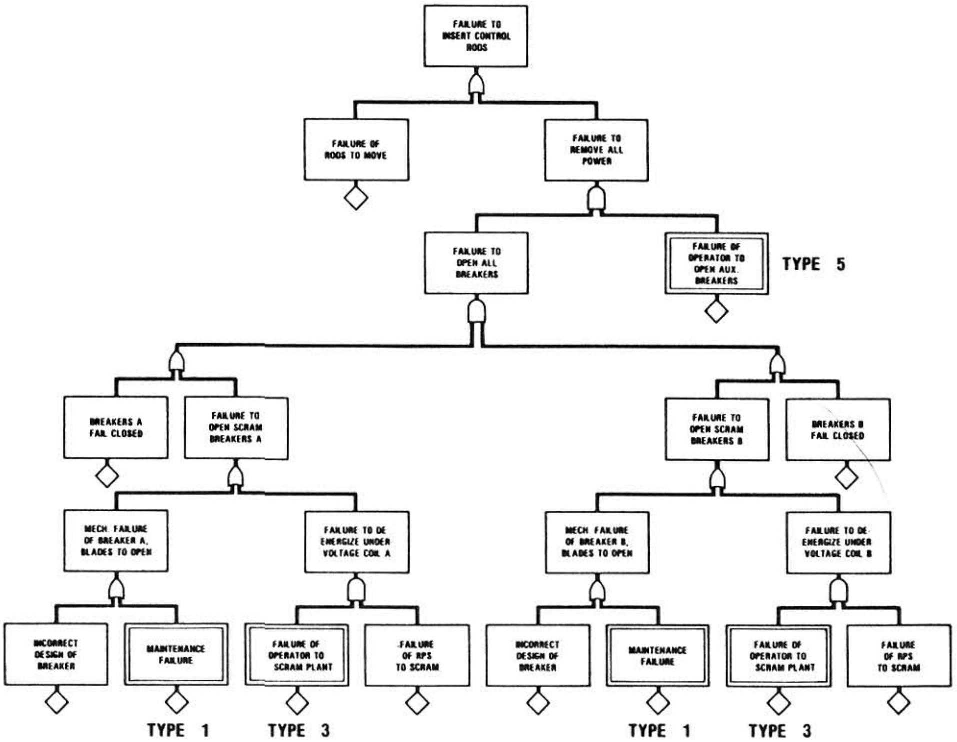


Figure 16 Enhanced Fault Tree

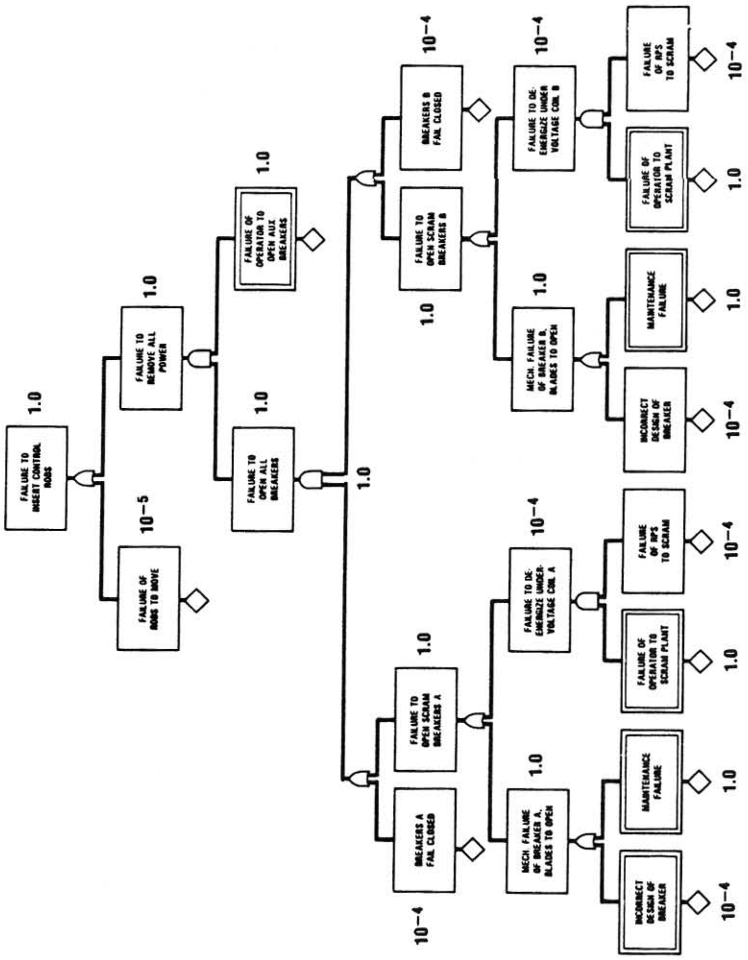


Figure 17 Application of a Coarse Screening Technique

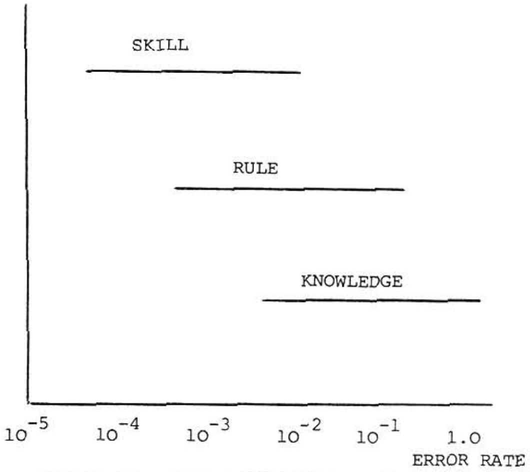


Figure 18 Error Rate Ranges Associated with Human Behaviour

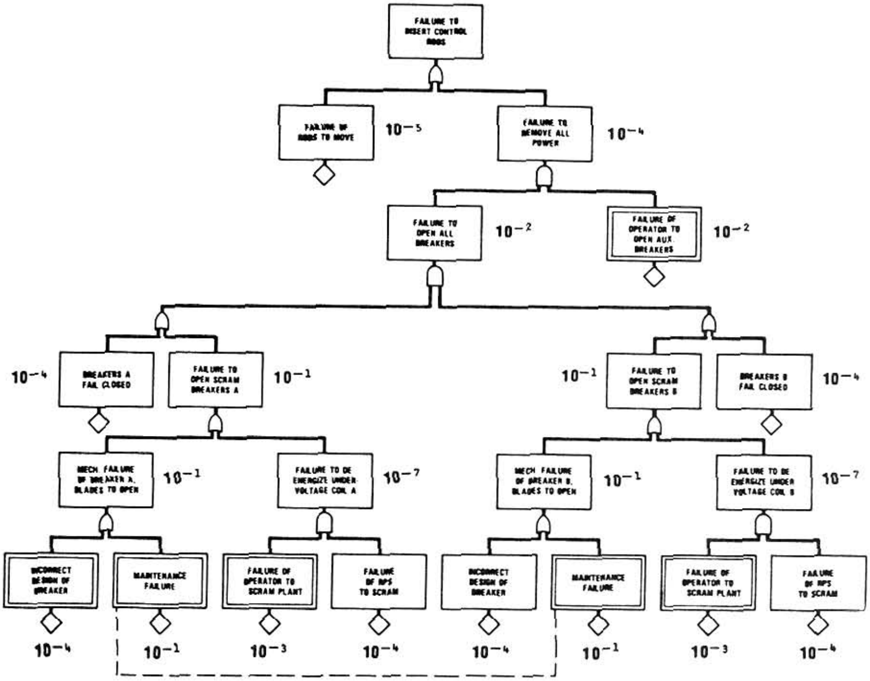


Figure 19 **Application of Screening Using Generic Data, Human and Equipment**

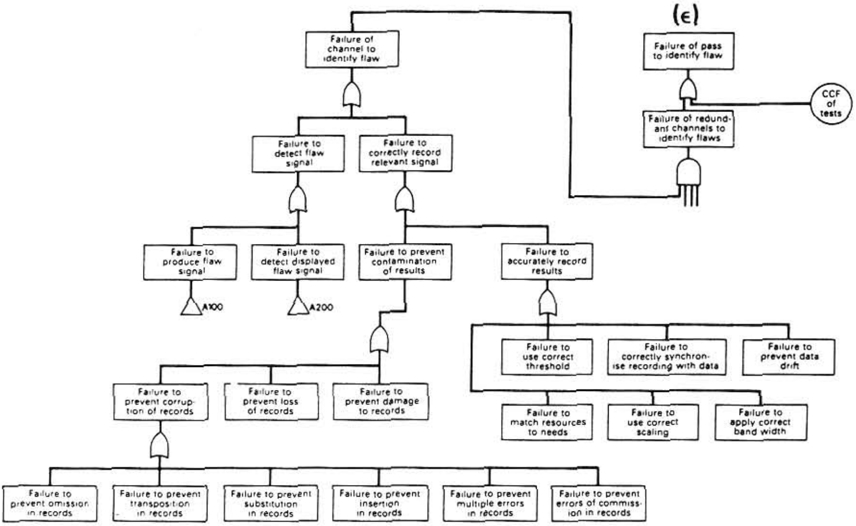
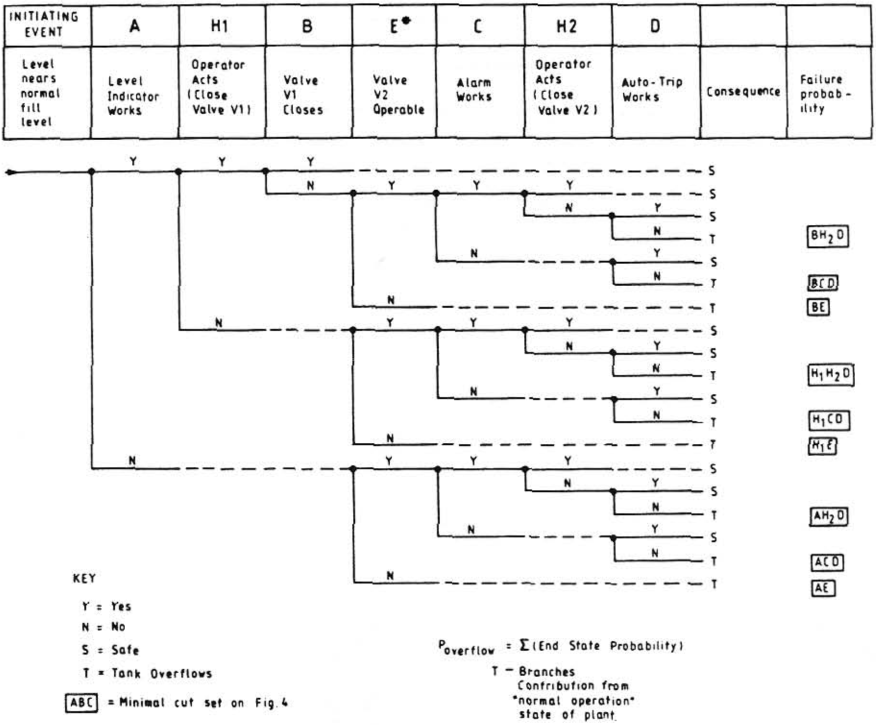


FIG.20 **FAILURE OF PASS TO IDENTIFY FLAW**



$P_{overflow}$ = Σ(End State Probability)

T – Branches
Contribution from
"normal operation"
state of plant.

FIG 21

EVENT TREE FOR SEMI-AUTOMATIC SYSTEM ON FIG. 3

*(Headings Rearranged to account for Common Mode Failure)

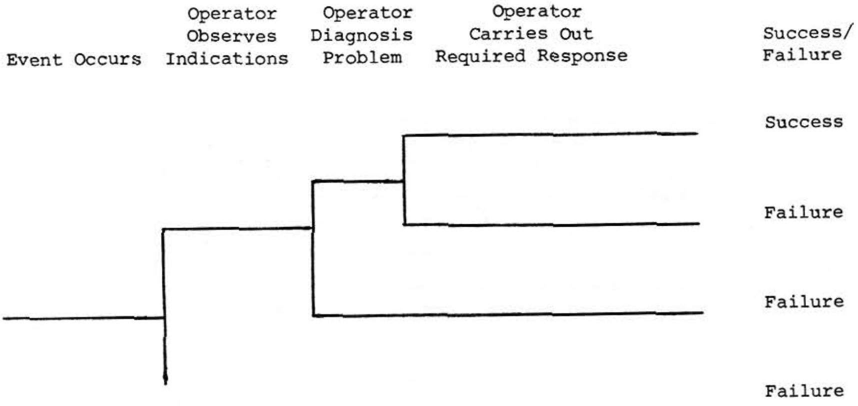


Figure 22 Basic Operator Action Tree

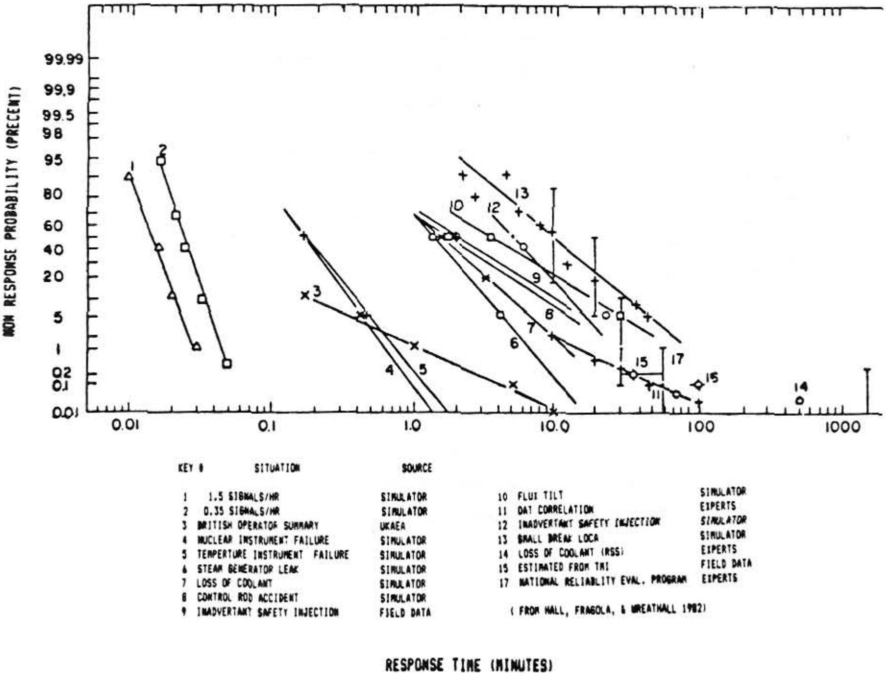


Figure 23 **Non-response Probability Versus Response Time**

Figure 24

An overview of a human reliability analysis

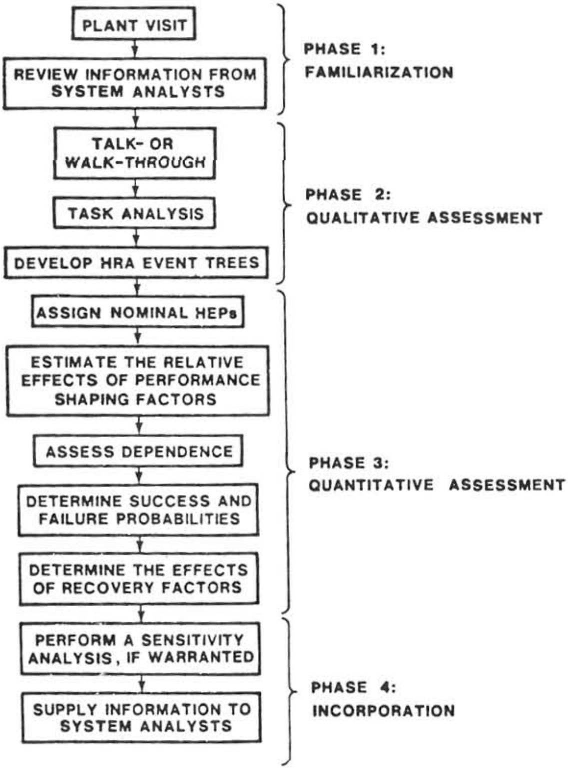
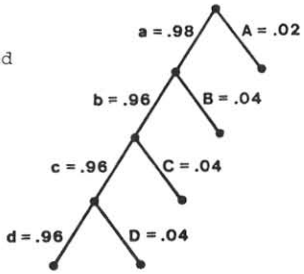


Figure 25

HRA event tree for actions performed outside the control room



Event	HEP	Source
A = Control room operator omits ordering the following tasks	.02 (EF = 5)*	T20-6, #1
B = Operator omits verifying the position of MU-13	.04 (EF = 5)**	T20-8, #3
C = Operator omits verifying/opening the DH valves	.04 (EF = 5)**	T20-8, #3
D = Operator omits isolating the DH rooms	.04 (EF = 5)**	T20-8, #3

* Modified to reflect the effects of moderately high stress

** Modified to reflect the effects of moderately high stress and protective clothing