A SET OF COMPUTER BASED TOOLS IDENTIFYING AND PREVENTING HUMAN ERROR IN PLANT OPERATIONS

Dr David Embrey[1], Sara Zaed[2]

,

Abstract

This paper describes a set of techniques, supported by computer based tools, for predicting and preventing human errors in gas plant operations. The first two tools allow an analysis of the task structure and prediction of the errors that could arise at a task or subtask level, together with the potential consequences of these errors. The third tool develops a profile of the factors in the situation (e.g. workload, fatigue, distraction levels) that affect error probability, and the most cost effective interventions to reduce errors. The software is able to provide an estimate of the likelihood of the errors occurring. A simple graphical analysis method is provided as part of the toolset to support the analysis of accident sequences in retrospective analyses. The paper includes case studies illustrating the application of the tools to gas plant operations and the measurement of mental workload of bridge crews in shipping operations.

1. Introduction

There is increasing emphasis by regulators and multinational process industry corporations on proactively assessing human factors issues, and in particular, the likelihood of human errors, as part of formal safety cases and risk assessments. In addition, it is now recognised that incident investigations need to explicitly address the underlying causes of the human errors that are the major contributors to process plant accidents. There is thus a requirement for both proactive and reactive analyses of human errors as part of the management of risks in process safety. Although a number of tools exist for addressing these issues (see for example, Embrey, 1994, Embrey et al 2004, and Embrey, 2005), they are not widely known in the process industries, and up to now have not been available from a single source. This paper describes an integrated set of techniques, supported by a range of software tools, that support a wide range of human factors analyses to reduce human error in process plant operations. These tools have all been applied extensively in practical projects over the past 15 years where they have been shown to make substantial contributions to safety. The software tools are provided in an integrated package called the Human Factors Workbench (HFW). This comprises five separate analytical tools that can be used independently or together depending on the application area. The types of human factors analyses that are carried out in process plant operations and the tools that are available in the HFW to support these activities are summarised in Figure 1:

Areas of application	**Applicable Methodology**	**Supporting software tools in the HFW**
Developing operating procedures and job aids (Proactive)	Hierarchical task Analysis (HTA)	HTA
Developing standardised training methods	Hierarchical task Analysis (HTA)	HTA
Predicting potential human errors and evaluating their consequences	Predictive human error	PHEA

[1] Managing Director, Human Reliability Associates Ltd UK

[2] Founder, Zaed Engineering Brazil

(Proactive)	analysis (PHEA)	
Analysing accident sequences in incident investigations (Retrospective)	Sequential Timed Event Plotting (STEP)	STEP
Assessing the factors influencing the likelihood of errors identified in PHEA to develop specific prevention strategies (Proactive)	Performance Influencing Factors Analysis	Measurement & Investigation Technique to Reduce Errors (MITRE)
Evaluating the factors influencing the likelihood of errors to identify specific and generic prevention strategies (Retrospective)	Performance Influencing Factors Analysis	MITRE
Evaluating the mental workload experienced by operators and its effects on human error	Performance Influencing Factors Analysis	MITRE
Evaluating human error probabilities	Performance Influencing Factors Analysis	MITRE

Figure 1: Types of the Human Factors analysis supported by the HFW

In subsequent sections we will describe each of the analysis methods set out in the tool and the corresponding support provide by the HFW.

2. Development of Operating Procedures and improved training

2.1 Task analysis and the CARMAN methodology

CARMAN (Consensus based approach to Risk Management) is a methodology developed by Human Reliability Associates (HRA) to involve plant operators in documenting their existing working practices and developing best practices for operating the plant using an interactive process called a Consensus Group. The outputs from the consensus group include a Reference Task Description which documents the agreed method of working in a standardised format. This is then used as the basis of the training and competence assessment process. A comprehensive description of CARMAN is provided in Embrey, (2004).

One of the important requirements for reaching a consensus is the existence of a common method for describing tasks in a clear, unambiguous manner, such that there is a shared understanding of the alternative ways of performing a task. In order to achieve this, participants in the consensus groups are trained to document their tasks using a form of task analysis called Hierarchical Task Analysis (HTA). HTA was originally developed for use in training operators in the process industries. It is easy to learn, and it allows tasks to be described at varying levels of detail. The level of detail of the description is based on two criteria:

- Can the risks associated with errors be identified at the current level of detail of the description?
- Is the task described in sufficient detail to allow training specifications, job aids and procedures to be developed which will control the risks?

Figure 2 shows first level of an HTA for a compressor filter change-over. It can be seen that the task is broken down into a series of tasks and subtasks. The preconditions box specifies the starting assumptions of the analysis, and the plan box the conditions governing the execution of the subtasks (e.g. timing, ordering). It should be emphasised that an HTA is not a flowchart, but is the breakdown of a task into a series of 'goal directed activities'. If a line is drawn below a subtask, this means that the task does not need to be decomposed further, since both of the criteria set out above (i.e. risks identified and sufficient detail for training purposes) are satisfied. An HTA translates very readily into a format suitable for documenting procedures. Breaking complex tasks into a series of

subtasks with clearly defined goals facilitates ease of understanding of the overall structure of a task. This is valuable both during training and for on-line use of the information.

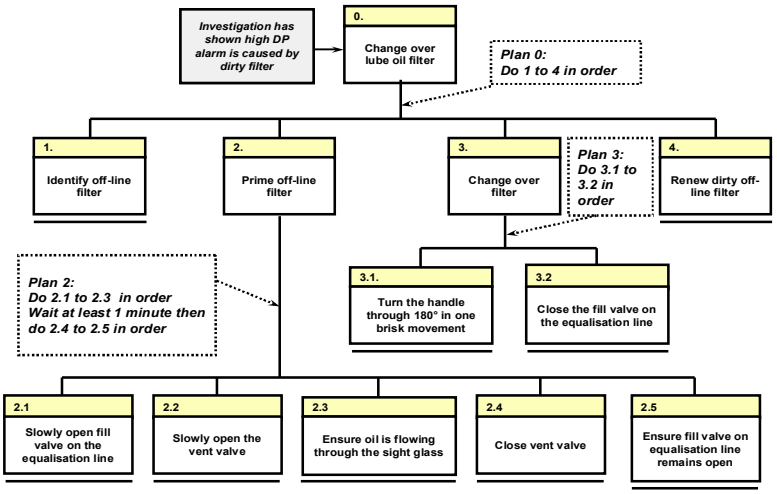
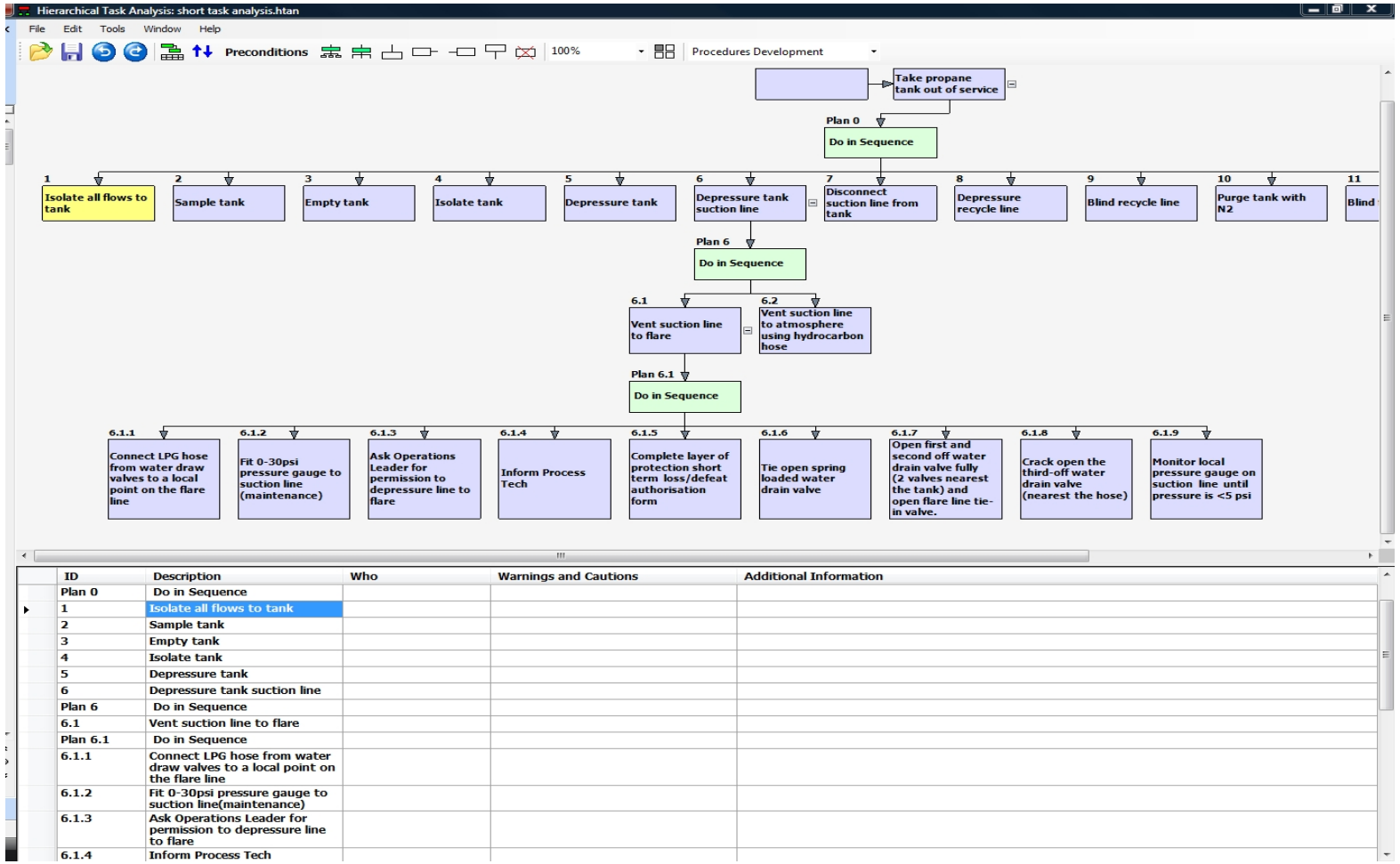


Figure 2: Hierarchical Task Analysis for a compressor filter change-over

2.2 Support provided for HTA by the HFW

The HTA module of the HFW provides a comprehensive environment for carrying out HTA analyses. The graphical form of the analysis can be easily carried out within a large workspace which allows boxes to be drawn and linked, and decomposed as necessary for the analysis. This graphical representation can be exported as a bitmap or JPEG for use in reports. The program also allows the graphical format to be immediately translated into a text, which in turn can be readily exported as a Reference Task Description in a form suitable for the formal documentation of procedures. This is illustrated in the following case study

The screenshot shown in Figure 3 is an extract from the task of taking a propane tank out of service. This shows how the graphical format of the analysis, suitable for documenting procedures, is automatically generated by the software. The text based output provides columns for the analyst to specify who carries out the various tasks and subtasks, warning and cautions that need to be included in the procedures or job aids, and any additional information. This table, the Reference Task Description (RTD), is then converted to a Microsoft word format document. This can be used to provide the basis for defining a task in full detail for applications such a specifying the training content, or for a step by step procedure if this level of detail is appropriate.



ID	Description	Who	Warnings and Cautions	Additional Information
Plan 0	Do in Sequence			
1	Isolate all flows to tank			
2	Sample tank			
3	Empty tank			
4	Isolate tank			
5	Depressure tank			
6	Depressure tank suction line			
Plan 6	Do in Sequence			
6.1	Vent suction line to flare			
Plan 6.1	Do in Sequence			
6.1.1	Connect LPG hose from water draw valves to a local point on the flare line			
6.1.2	Fit 0-30psi pressure gauge to suction line(maintenance)			
6.1.3	Ask Operations Leader for permission to depressure line to flare			
6.1.4	Inform Process Tech			

Figure 3: Graphical and text based versions of an HTA from the HFW software

Action Errors	
A1	Operation too long / short
A2	Operation mistimed
A3	Operation in wrong direction
A4	Operation too little / too much
A5	Operation too fast / too slow
A6	Misalign
A7	Right operation on wrong object
A8	Wrong operation on right object
A9	Operation omitted
A10	Operation incomplete
A11	Operation too early / late
A12	Operation in wrong order
A13	Misplacement

Checking Errors	
C1	Check omitted
C2	Check incomplete
C3	Right check on wrong object
C4	Wrong check on right object
C5	Check too early / late

Information Retrieval Errors	
R1	Information not obtained
R2	Wrong information obtained
R3	Information retrieval incomplete
R4	Information incorrectly interpreted

Information Communication Errors	
I1	Information not communicated
I2	Wrong information communicated
I3	Information communication incomplete
I4	Information communication unclear

Selection Errors	
S1	Selection omitted
S2	Wrong selection made

Planning Errors	
P1	Plan incorrect because of misdiagnosis
P2	Diagnosis correct but wrong action plan formulat

Figure 4: Classification of error modes in PHEA

3. Predicting potential human errors and evaluating their consequences

Once a HTA has been performed, and a Reference Task Description has been developed based on this task analysis, there will often be a requirement to evaluate this proposed method of performing the task to evaluate the possibility that errors may arise which may have severe consequences for the process and/or the individuals performing the task (occupational safety implications). In order to evaluate these risks, a technique called Predictive Human error Analysis can be applied (Embrey 1994). This technique, which is analogous to the Failure Modes and Effects Analysis, or HAZOP techniques applied in engineering risk analyses, aims to identify possible significant human errors by applying a set of guide words to each subtask or its constituent steps. These guidewords are based on an exhaustive classification of observable failure modes, and hence they do not consider the different

underlying factors that may influence the likelihood of these errors. This issue is considered separately by another tool in the HFW, which will be described in a later section.

The classification scheme used in PHEA is shown in Figure 4 above. Each of these error types is applied to actions, checking operations, information retrieval and communications (person to person communications such as telephone calls), selections (e.g. selecting which pump to maintain) and diagnostic activities. The analyst then evaluates which of the errors is credible given the operational context. For example, an error such as 'right action on wrong object' will be more likely if labelling is poor, or if a control is very close to another that has a different function. A systematic method for evaluating the factors which are likely to influence the likelihood of errors is described in a later section. Figure 5 shows how the PHEA guidewords are applied to the task of taking a propane tank out of service that was described in Section 2. The HFW program provides a drop down list at each task or subtask step. This is used to develop the grid shown in Figure 5 by prompting the analyst to choose a failure mode from the list shown in Figure 4 (if applicable). The first column of the grid is the task step. The second column describes the credible failure modes and Major Accident Hazards that could arise. The next column considers possible risk control measures or recovery opportunities. The final column evaluates the factors that could affect the likelihood of the initial error or the probability that the error could be recovered. This analysis provides a very comprehensive coverage of the possible risks arising from human error in the task, and also suggests possible mitigation measures.

4. Assessing the factors influencing the likelihood of errors

There are many situations where a systematic method is needed for evaluating the factors that affect the likelihood of errors. In the previous section, error modes with severe consequences were identified in PHEA by using a set of guide words that were applied at each task step. However, the actual severity of the risks presented by these failure modes can only be evaluated if they are combined with an evaluation of their associated failure probabilities. In fact there are many difficulties associated with the evaluation of actual human error probabilities (see Embrey (1994) for a discussion of this issue). However, it is quite feasible to identify which factors are likely to have the most significant impact on particular types of errors, and to assess the quality of these factors in the context being assessed. Thus, in a situation where an operator is highly fatigued, has many distractions and is unfamiliar with a task, we would expect the error probability to be greater than when these factors are optimal. In general, these factors are referred to as Performance Influencing Factors (PIFs), and techniques have been developed for identifying these factors and assessing their quality in real tasks. A technique called the Influence Diagram has been applied to developing models of the range of factors influencing error probabilities.

In addition to the primary factors that directly influence the error probability, the Influence Diagram model also specifies the hierarchy of sub-factors that in turn influence these primary factors. A wide range of different types of model have been developed for application in specific domains. For example, a model has been developed in the marine industry for assessing the mental workload (and hence the error probability) of bridge manning teams in ships (see Embrey et al, 2006).

At a qualitative level, the model can be used to provide information to the analyst using the PHEA technique, for example with regard to which factors might affect the likelihood of an 'Action omitted' error for an action step such as 'Close valve 21'. If the Influence Diagram model suggests that the level of distractions, competency, procedures quality and fatigue contribute directly to the likelihood of action errors, these factors would be assessed to evaluate whether or not the likelihood of this failure is high, low or medium. If the result of these evaluations is that all of these factors are at the negative end of their range, then the probability of error and hence the risk arising from this error should be regarded as significant, and appropriate preventative measures should be implemented.

In addition to these qualitative applications, the Influence Diagram also provides mathematical rules which enable the evaluation of the factors at the bottom of the diagram to be combined to provide an overall assessment of the failure likelihood at the top of the tree (see Embrey, (2001) for a more detailed description of this process). If the relative cost of improving the factors is available, the model also allows alternative risk reduction strategies to be assessed from the point of view of relative cost effectiveness.

Task step description	Potential human failures	Potential Major Accident Hazard consequence (MHA) description	Risk Control Measures (RCM)/ Recovery opportunities	Performance Influencing Factor issues	Notes/Actions arising
6.1 Vent suction line to flare	A1 operation too short (not getting pressure down to 5psi as required)	Vent too much propane to atmosphere at next step.	- Ensure limit of 5 PSI clearly stated in checklist - Signature required by Field Leader before proceeding - Local pressure gauge installed	- Passing valves may make this difficult - Custom and practice has been to vent remaining amount to atmosphere	TRAINING POINT: Communicate change to 5psi ACTION: Supervise this part of the process (new requirement for field leader signature)
	A7 Right operation on wrong object (connect wrong suction line to flare)	Time issues. No MAH			
	A7 Right operation on wrong object (Connect the right suction to another line – e.g. jump-over line)	Mainly quality and efficiency issues since the operator is most likely to connect to another propane line.	- NRV prevents backflow into T883.	- Flare line is clearly labelled. - The butane line is around 50-60ft away - Lines are clearly labelled	
	A9 operation omitted (suction leg not vented)	Uncontrolled release (up to maximum build-up in suction leg)	- Stated in procedure - Step 6.2 (vent suction leg to atmosphere) is an opportunity to ensure that there is no pressure in suction line.		
	A10 operation incomplete (failure to return water draw valve to normal state)	Uncontrolled release	- Requirement to complete short term loss/defeat form stated in procedure	- Existing custom and practice is to defeat safety system without completing defeat form	TRAINING POINT: Emphasise the steps necessary when defeating safety critical defence systems
6.2 Vent suction line to atmosphere	A9 operation omitted (failure to clear pressure from line)	Uncontrolled release (up to maximum build-up in suction leg)	- Stated in procedure - Local pressure gauge - GSI for isolation and depressurisation prior to work (Line must be isolated and 2 ways of proving depressurisation must be used) - Operator standby for 1stbreak - Full PPE for Mechanical Technician		TRAINING POINT: How to identify when all pressure has gone
	A10 operation incomplete (failure to clear all pressure from line)	Uncontrolled release (up to maximum build-up in suction leg)	See above		

Figure 5: Example of PHEA analysis for part of the '**Take Propane tank out of service'** scenario

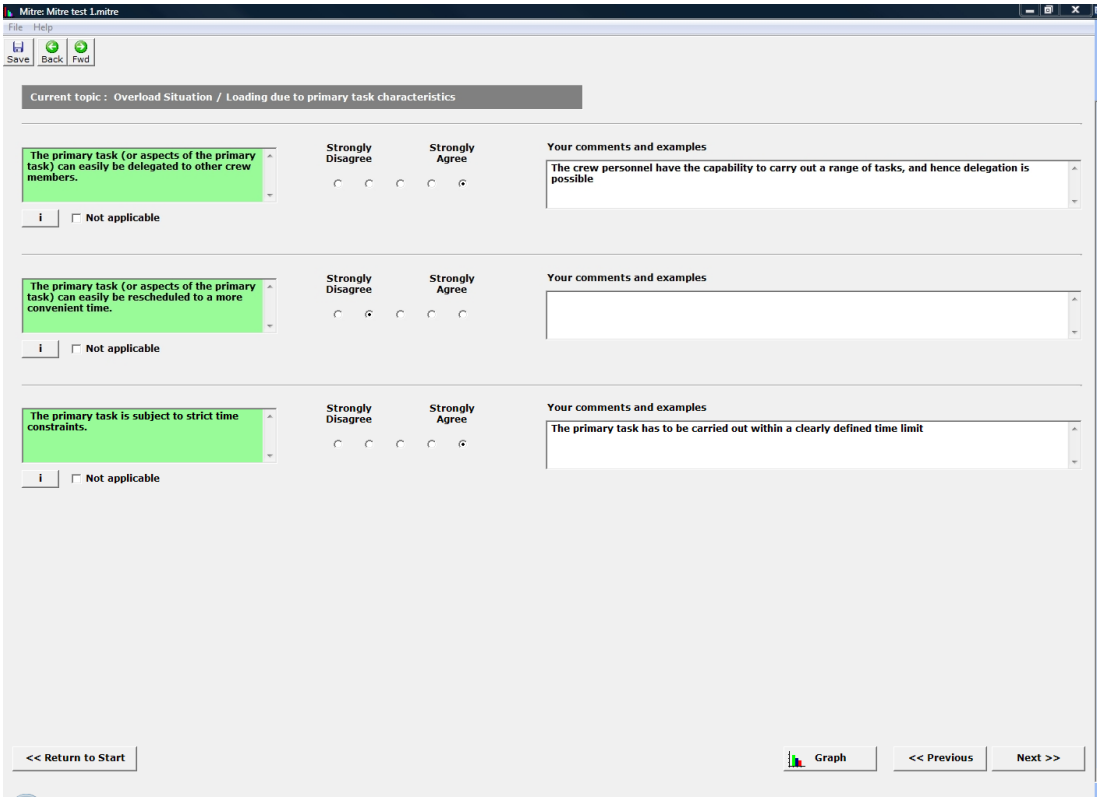


Figure 6 Example of HFW MITRE assessment screen for task loading

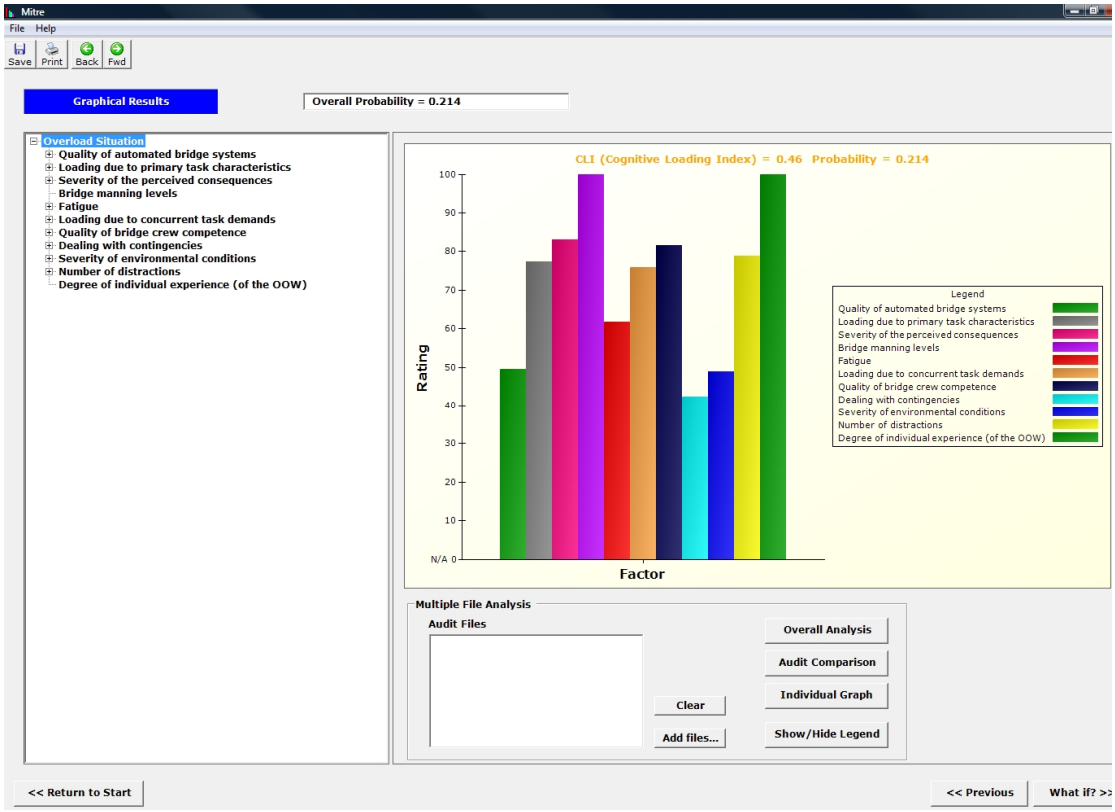


Figure 7: Results of evaluations of the factors affecting human error in a scenario

The MITRE (Measurement and Investigation Technique for Reducing Error) software tool in the HFW provides a very convenient interface for allowing the analyst to assess the quality of the factors affecting error likelihood. The assessment involves answering a series of simple questions regarding the operational conditions, based upon the Influence Diagram model relevant to the type of task being evaluated. An example of the MITRE interface is provided in Figure 6, which is taken from the assessment of mental workload scenarios in the marine industry (Embrey and Blackett 2007). In this assessment, the quality of the automated bridge systems is being assessed, as this contributes to the level of errors arising from overload experienced by the bridge crew on a ship. Figure 7 shows the overall results from the assessment of all the factors contributing to workload during a particular scenario (the berthing of a ship). The tool calculates an index (the CLI), which indicates the overall quality of the factors in the scenario, as assessed by the analysts, and also provides an estimate of the error probability under these conditions (0.278, a very high probability because of the severe conditions in this scenario).

5. Evaluating accident sequences in incident investigations

The final tool provided in the Human Factors Workbench is a simple graphical system for representing accident sequences. This is based on the STEP (Sequential Timed Event Plotting) technique developed by Hendrick and Benner (1987). This is a simple but powerful method for representing accident sequences. The STEP diagram places Agents on the left of the diagram and plots time from left to right. Agents are human or inanimate objects that change their states or interact to create events leading up to the accident outcome (e.g. explosion or injury). The STEP diagram may also include mitigation events after the accident. The first stage in constructing the diagram is to identify the main Agents from the event narrative as elicited from witnesses or other sources. The events associated with these Agents are then plotted on the timeline. The STEP diagram shown in Figure 8 represents the first stage of the Piper Alpha offshore oil production accident that occurred in the North Sea, with the loss of many lives. The critical failures that occurred were the maintenance team not completing their work on a Pressure Relief Valve (PRV) by the end of the day shift at 16.00, and then not informing the incoming Night Shift Operations Supervisor of the faulty valve. The STEP diagram provides a very easy to understand representation of a complex accident sequence.

When investigating accidents using the Human Factors Workbench, the recommended first step is to perform an HTA of the task in which the accident occurred using a consensus group. This supports the construction of a STEP diagram because it provides a more accurate understanding of how the task is really carried out in practice. A PHEA analysis can then be performed to determine if the error giving rise to the failure can be classified using the taxonomy provided by PHEA in Figure 5. The error mode 'Information not communicated', (I1) would be an appropriate classification for the critical failure in the Piper Alpha accident. The MITRE tool described in Section 4 can then be used to evaluate the quality of the Performance Influencing factors in the scenario. Where deficiencies in these contributory factors at both direct and organisational levels can be identified, recommendations can be made for improvements to reduce the likelihood of a future incident.

6. Conclusions

The Human Factors Workbench provides a wide range of tools to support human factors applications in safety critical industries. Most of the tools supported in the HFW have been applied for many years in a wide range of industries, and have been shown to be highly effective. However, by providing an integrated set of tools, both proactive and retrospective error reduction processes can be carried out in a cost-effective manner by both human factors analysts and engineering safety specialists.

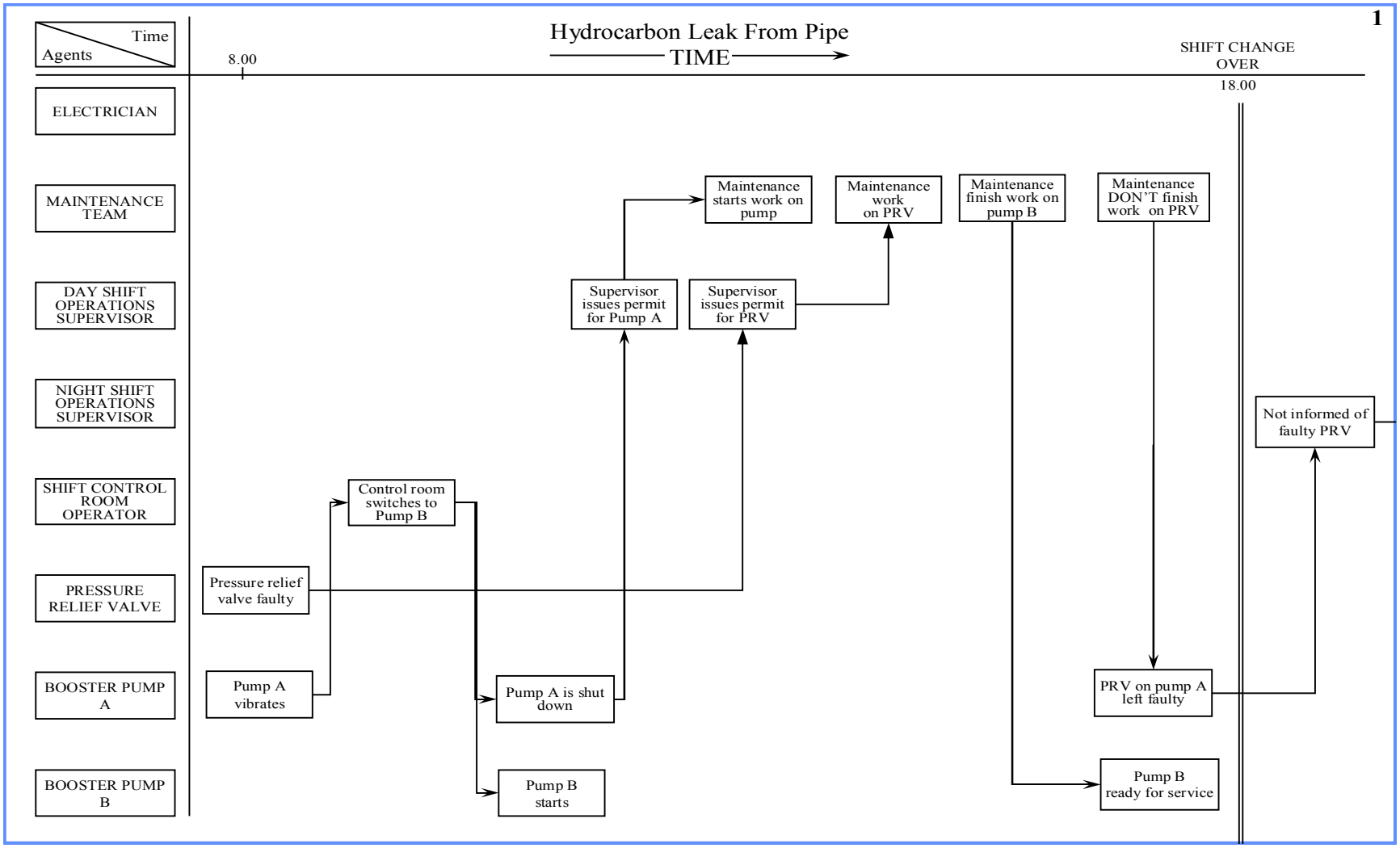


Figure 8: First stage of STEP analysis of Piper Alpha incident

References

EMBREY, D.E. Incorporating Management and Organisational Factors into Probabilistic Safety Assessment. Reliability Engineering and Systems Safety, v. 38, p. 199-208, 1992

EMBREY, D.E, *Guidelines for reducing Human Error in Process Safety* Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, 1994

EMBREY, D.E, Human Reliability Assessment In: ***Human Factors for Engineers*** Sandom, C. and Harvey, R. S. (Eds.) Product Code NS 032 ISBN 0 86341 329 3 Institute of Electrical Engineers Publishing London, 2004

EMBREY, D.E, Preventing Procedures Violations: How to Create a Positive Safety Culture *Petrobras seminar on human factors*, Rio de Janeiro, Brazil, 2004

EMBREY, D. E and BLACKETT, C. A computer based tool for cognitive workload measurement in marine operations. In *Human Factors Issues in Complex System Performance* D. de Waard, G. R. J Hockey and K.A. Brookhuis (Eds.) Shakar Publishing: Maastricht, The Netherlands, 2007

HENDRICK, K. AND BENNER, L. *Investigating Accidents with STEP* Marcel Dekker, New York, 1987