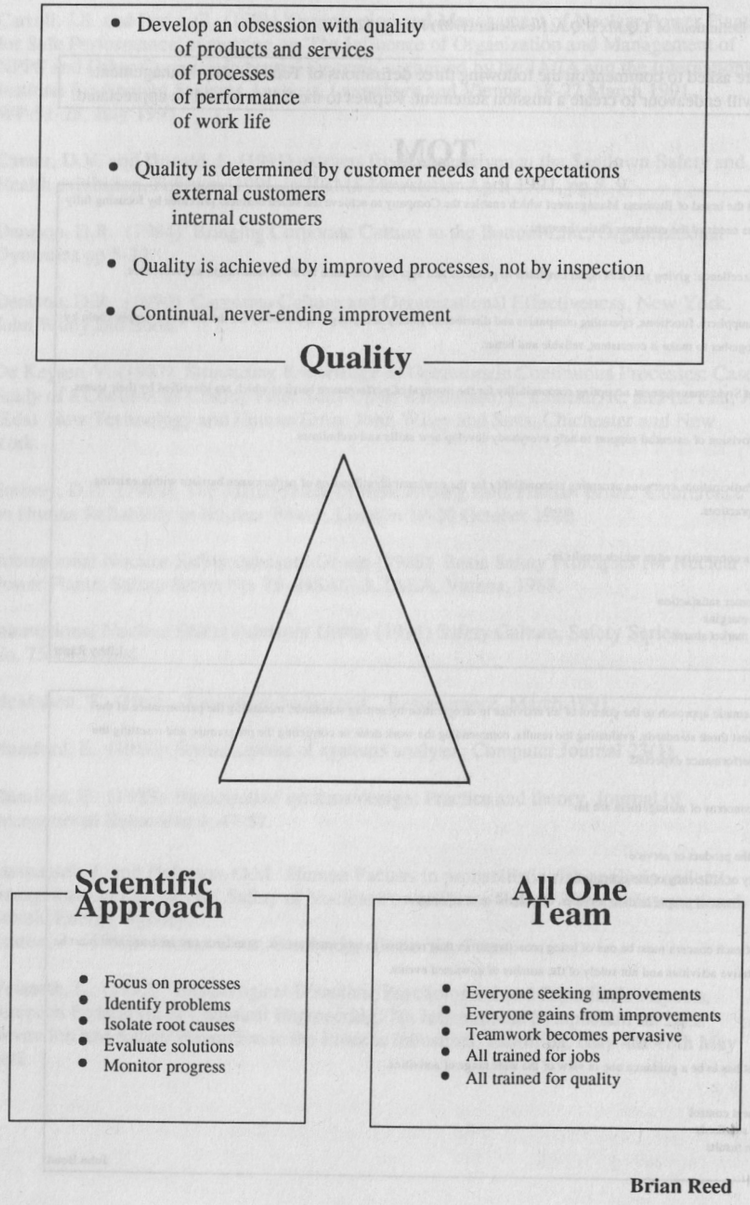

QUANTITATIVE AND QUALITATIVE PREDICTION OF HUMAN ERROR IN SAFETY ASSESSMENTS

D. E. Embrey
Human Reliability Associates Ltd., 1 School House, Higher Lane, Dalton, Wigan, Lancs. WN8 7RP.

This paper describes a comprehensive methodology for addressing human error within the context of Quantified Risk Assessment as performed in the chemical and offshore industries. The role of qualitative and quantitative assessments of human reliability in risk assessment is illustrated by means of examples. A detailed description of the qualitative aspects of the methodology is provided, and is illustrated using a chlorine loading example. The importance of addressing human, hardware and organisational aspects of system reliability within an integrated framework is emphasised.
Keywords: Human reliability, risk and safety analysis, human error reduction.

1. INTRODUCTION

There is an increasing requirement by regulatory authorities for companies to conduct formal safety assessments of both onshore processing plants and offshore oil and gas installations. As part of these assessments, risk and reliability analysts are required to perform evaluations of human reliability in addition to the analyses of hardware systems which are the primary focus of a typical safety assessment. Increasing emphasis is being placed on a comprehensive assessment of the human role in system safety following the occurrence of major disasters in the petrochemical industry (Piper Alpha, Feyzin, Bhopal, Texas City) and other industries (Clapham Junction, Chernobyl, Zeebrugge) where human errors were seen as direct or indirect causes.

Many hardware orientated risk analysts view the prospect of evaluating human reliability with some trepidation. Human error is seen as largely random in nature and therefore essentially impossible to evaluate or reduce. However, this is an unnecessarily pessimistic view. Applied psychologists and ergonomists have been working in this area for many years, and considerable progress has been achieved. In this paper, a systematic framework will be described which can assist risk analysts in performing human reliability assessments.

The usual emphasis in human reliability has been on techniques for the derivation of numerical error probabilities for insertion in fault trees (see Kirwan et. al. (1), for a comprehensive review of these techniques). However, in many ways, this emphasis on absolute quantification is misplaced. Many practitioners emphasise the fact that the major benefits of applying a formal and systematic technique to risk assessment are the qualitative insights that emerge with regard to the sources of risk, and where resources should be expended in minimising these risks. Although the quantitative results of the assessment are important in arriving at decisions in specific areas, for example land use applications for onshore plants, it is widely recognised that there are considerable uncertainties in the data available for inclusion in these analyses.

Given these uncertainties, it becomes even more important that a systematic and comprehensive qualitative method is adopted for identifying the sources of risk and the consequences of failures. Such a procedure must ensure that no significant failures are omitted from the analysis. A comprehensive evaluation of the plant from the perspective of its management, procedures, training, communication and other systemic factors also provides insights into how generic failure data should be modified for use in the particular risk assessment of interest. The major focus of this paper is the description of a defensible procedure for qualitative human error prediction which will achieve these objectives. However, the first part of the paper will discuss the implications of qualitative human error analysis for quantitative risk assessment.

2. THE ROLE OF HUMAN RELIABILITY IN RISK ASSESSMENT

2.1 An Illustrative Case Study

To illustrate the role of Human Reliability Assessment in quantitative risk assessment in the chemical and offshore industry, an example of a typical assessment, described by Ozog (2) will be considered. The stages of the risk assessment are as follows:

a) System Description: The system is a storage tank designed to hold a flammable liquid under a low positive nitrogen pressure (see figure 1). This pressure is controlled by PICA-1. A relief valve is fitted which operates if overpressurisation occurs. Liquid is fed to the tank from a tank truck, and is subsequently supplied to the process by the pump P-1.

b) Hazard Identification: A HAZOP was used to identify potential hazards, the most serious of which is an unrecoverable release from the storage tank.

c) Construction of the Fault Tree: The fault tree is constructed based on the system description and initiating events identified in the HAZOP. Figure 2 shows a portion of an extended version of Ozog's fault tree, taken from CCPS (3). The following terminology is used:

B is a Basic or Undeveloped event
M is an Intermediate event
T is the Top event

The events that could give rise to the Major Flammable Release are as follows:

M1: Spill during tank unloading
M2: Tank rupture due to external event
B1: Tank drain breaks
M3: Tank rupture due to implosion (not shown)
M4: Tank rupture due to overpressure (not shown)

d) Quantification: The overall frequency of the top event is calculated by combining together the constituent probabilities and frequencies of the various events in the fault tree using the appropriate logical relationships described by the AND and OR gates (the detailed calculation is given in (3)).

2.2 Implications of Human Error for the Analysis

From a human reliability perspective, a number of interesting points arise from this example. Firstly, a simple calculation shows that the frequency of a Major Release (3.2×10^{-2} per year) is dominated by human errors. The major contribution to this frequency is the frequency of a spill during truck unloading (3×10^{-2} per year). An examination of the fault tree for this event shows that this frequency is dominated by event B15: Insufficient volume in tank to unload truck, and B16: Failure of, or ignoring LIA-1. Of these events, B15 can be seen as almost certainly solely due to human error, and B16 would be a combination of instrument failure and human error. (Note however, that we are not necessarily assigning the causes of the errors solely to the operator. The role of management influences on error will be discussed later.) Apart from the dominant sequence discussed above, human-caused failures are likely to occur throughout the fault tree. It is often the case that human error dominates a risk assessment. For example, Bellamy et al (4) present an example from the analysis of an offshore lifeboat system.

These examples suggest that it is critical for the potential human causes of major incidents to be exhaustively identified. Unfortunately, the tools currently used by risk analysts for hazard identification do not adequately address this issue. A commonly used method is the HAZOP approach (Kletz (5), CCPS (6)). Some of the causes of process deviations generated by a HAZOP analysis may indeed be ascribed to human error. However, the analyst is given no explicit guidance within the HAZOP (or any other hazard identification technique) which would enable him or her to identify human causes of these hazards. Although it can be argued that the knowledge and experience of the analyst concerning the system should be sufficient to identify human errors, it is obviously preferable to have a systematic procedure which will ensure a comprehensive identification of possible causes, even if the analyst does not know the system well.

Another danger of an inadequate appreciation of human causes of hazards is that the HAZOP analyst may consider a particular high risk event (identified by a guide word and deviation) to be non-credible, because he or she only takes into account the hardware failures (with an extremely low probability) that could give rise to the event. When human causes are taken into account, the likelihood of the event may actually be quite high.

The framework to be described later in this paper can be seen as a complementary procedure to hardware orientated hazard identification procedures. Ideally, the two approaches should be applied in parallel to a plant evaluation, in order to benefit from the synergy of considering both perspectives.

2.3 Quantification Aspects

In the preceding section, the importance of a comprehensive human reliability modelling approach has been emphasised from the qualitative perspective. However, such an approach is also critical in order to ensure accurate quantification of risk. If significant human contributors to the likelihood of major accidents occurring are omitted, then the probability of the event occurring may be seriously underestimated. Conversely, the role of the human in enhancing the reliability of a system needs to be taken into account. One reason for including humans in engineered systems is that they have the capability to respond to situations which have not been anticipated by the designers of the system. For example, they can prevent an undesirable outcome (e.g. the major flammable release in the situation described earlier) by taking appropriate action an early stage in the event.

These two points can be illustrated in the fault tree in figure 2. Taking the branch dealing with the frequency of the spill during truck unloading, (event M1 and below), a comprehensive analysis might have revealed that other human errors could give rise to a major tank spill (event M5) in addition to events M9 and M10. For example, an evaluation of the procedures during unloading might indicate that V1 could be accidentally opened instead of the valve from the tank truck (because of similar appearance of the valves, poor labelling and unclear procedures). If this probability was deemed to be high (e.g. 1×10^{-3}) on the basis of the evaluation of the operational conditions, then this event would dominate the analysis. M5

would become about 1.1×10^{-3} and the frequency of the flammable release T would become about 3.2×10^{-1} per year, (approximately one release every three years) which would be totally unacceptable.

Although risk assessment usually concentrates on the negative effects of the human in the system, the operator also has the capability to reduce risk by recovering from hardware failures or earlier errors. This can be taken into account in the assessment. Consider the scenario where the operator detects the escape of liquid through the relief valve as soon as overfilling has occurred, and immediately closes the valve to the tank truck. (It is assumed that the alternative error of accidentally opening V1, as discussed above, will not occur.) Although it is still likely that some spillage would occur, this would probably not constitute a major tank spill. If failure of the recovery action is given a conservative probability of 1×10^{-1} and joined by an AND gate to events B15 and B16, then the probability of M9 and M5 becomes 1×10^{-5}. This considerably reduces the overall frequency of a major flammable release (T) to 3.2×10^{-3}.

The analysis set out above demonstrates the importance of a comprehensive evaluation of the human aspects of a hazardous operation, from the point of view of identifying all contributory events and recovery possibilities. It also indicates the need for a complete evaluation of the operational conditions (procedures, training, manning levels, labelling, etc) which could impact on these probabilities.

3. SYSTEM FOR PREDICTIVE ERROR ANALYSIS AND REDUCTION (SPEAR)

The framework to be described in subsequent sections is designed to be used either as a stand-alone methodology, to provide an evaluation of the human sources of risk in a plant, or in conjunction with hardware orientated analyses to provide an overall system safety assessment. The overall structure of the methodology is set out in figure 3. Stages 1 to 4 and 6a of SPEAR comprise the stand alone portions of the methodology, which would be applied if the analyses only addressed the human factors aspects of the system. The remainder of the SPEAR structure would be applied as part of an overall risk assessment in conjunction with hardware orientated assessment techniques. In the following sections the qualitative aspects of SPEAR will be described in detail.

3.1 Critical Human Interaction Identification and Screening Analysis

Because it would be impossible to examine every human activity in a plant, it is necessary to describe where the SPEAR process should be applied to achieve the maximum effect. The first stage of the process is intended to identify all aspects of the system being assessed where errors could lead to consequences which have a major impact on safety. This is achieved in two stages. Firstly, the results of prior hardware oriented analyses (e.g. HAZOPs, FMECAs, Preliminary Operating Hazard Analyses) are collated to specify, as exhaustively as possible, the physical sources of risk in the system being evaluated. Such analyses will usually produce descriptions concerning potentially hazardous substances (e.g. flammable gases, toxic chemicals), states (e.g. high temperatures, pressures), and processes involving these substances (e.g. transport, storage, reaction, compression). The next stage is to identify the human interactions with these processes.

The main types of direct human interactions with the process are specified in table 1 below. This table also indicates some of the major categories of errors that can arise in these interactions.

Types of Interaction	Active errors	Latent errors	Recovery errors
Normal operations	√	√	
Abnormal and emergency operations	√		√
Maintenance		√	√
Plant Changes	√	√	√

Table 1: Main error types associated with different forms of human interaction with a plant

Active errors are inappropriate actions or decisions which give rise to safety significant consequences. Latent errors are actions or decisions which may not have an immediate effect on safety. However, they create vulnerable states which, in combination with subsequent active errors or operational conditions, give rise to safety significant events. Recovery errors are failures to recover a potentially serious situation before the final outcome occurs. Such a situation could arise from previous errors or some abnormal state of the system.

The analyst takes each of the areas of potential hazard and considers the risk potential of the occurrence of each type of interaction and error specified in table 1 with these areas. The earlier example of the flammable liquid storage truck would be identified as a high risk area because of the large inventory of hazardous substances involved and the need for frequent filling operations. The extent to which human interactions occurred in the areas of normal, abnormal or maintenance operations or plant changes would then be considered. In the case of the storage tank, it is obvious that human interactions at the level of normal operations occur extensively during unloading from tank cars. However, there would also be human involvement during plant changes, maintenance or emergency conditions.

The next step is to decide in general terms if any of the error types described in table 1 could occur, and what would be the consequences. If a potentially hazardous activity involves any of the types of human interaction set out in table 1, then this plant area would be specified as being appropriate for more in-depth analysis using the techniques to be described in subsequent sections. Conversely, a section of the plant with few inherently hazardous processes, or which was highly automated and required little maintenance and few plant changes, would probably not be selected.

It should be emphasised that this stage of SPEAR is a broad-brush screening approach designed to minimise the amount of work to be carried out in subsequent stages. Like all screening processes, it carries the risk that some significant hazards may be overlooked. For example the indirect effects of errors in areas such as maintenance and plant changes are easily underestimated. The screening process should therefore be used with caution.

3.2 Qualitative Error Prediction

The quantitative prediction of human errors is focussed on the human interactions with hazardous aspects of the plant identified in the previous phase. Qualitative prediction involves the following stages:

- Task Analysis
- Performance Influencing Factor Analysis
- Screening Analysis

- Predictive Human Error Analysis
- Consequence Analysis
- Error Reduction Analysis

These stages will be described with reference to a simple example, the loading of a chlorine tanker. The overall structure of the qualitative analysis process is set out in figure 4.

3.2.1 Task Analysis Task Analysis is a very general term which encompasses a wide variety of techniques. A comprehensive review of task analysis techniques is provided in Kirwan (7). In this application, the objective of task analysis is to provide a systematic and comprehensive description of the task structure and to give insights into how errors can arise. The structure produced by task analysis is combined with the results of the PIF analysis as part of the error prediction process.

The particular type of task analysis used in SPEAR is called Hierarchical Task Analysis (HTA). This has the advantage that it has been applied extensively in the chemical and other industries. HTA breaks down the overall objective of a task by successively describing it in increasing detail, to whatever level of description is required by the analysis. At each of the levels, a 'plan' is produced which describes how the steps or functions at that level are to be executed. Figure 5 shows an extract from the HTA of the chlorine tanker filling operation which will be used as an example. The first level (numbered 1, 2, 3 etc.) indicates the tasks that have to be carried out to achieve the overall objective. These tasks are then redescribed to a further level of detail as required. As well as illustrating the hierarchical nature of the analysis, Figure 5 shows that plans, such as those associated with operation 3.2, can be quite complex. The term 'operation' is used to indicate a task, subtask or task step depending on the level of detail of the analysis.

A practical advantage of HTA compared with other techniques is that it allows the analysis to proceed to whatever level of detail is appropriate. At each level, the questions can be asked 'could an error with serious consequences occur during this operation?' If the answer to this question is definitely no, then it is not necessary to proceed with a more detailed analysis.

3.2.2 Performance Influencing Factor Analysis Performance Influencing Factors (PIFs) are characteristics of the task, the people and the physical and organisational environment which affect the likelihood that an error occurs. The term Performance Shaping Factors (PSFs) is an older term which often appears in human reliability texts. However, the term PIFs is preferred, since the nature and likelihood of errors is not determined (or shaped) exclusively by these factors. As discussed in Embrey ((8), (9)), these factors interact with existing error tendencies (e.g. limited memory capacity, reliance on usually successful diagnostic rules) to give rise to the human errors such as omitting an action or carrying out the correct action on the wrong object.

Typical task level PIFs are conditions such as the presence of time stress, the quality of training and procedures, and the number of distractions. PIFs associated with the operators themselves include general competence and motivation. All of these factors are in turn influenced by various policy and organisational culture factors (Embrey, (10)). Figure 6 provides a general classification of PIFs which determine the likelihood of errors. This classification is based on a simple demand-resource model of human error. In this model, errors arise as a result of a mismatch between the demands of the task and the resources available to satisfy these demands. The demands arise partly from the process, for example mental or sensory demands such as the requirement to monitor variables, schedule operations, diagnose problems, or physical demands such as locating and operating valves, loading reactors or operating switches. They also arise from individual factors such as the operator's perception of danger, and the social needs of the team carrying out the task. A further source of demands might be events outside the job environment. Management policies influence these demands in several ways.

At a simple level, if there are inadequate staffing levels, or poor training, or if people are asked to perform functions which are intrinsically difficult for humans e.g. keep track of several concurrent tasks at once, then errors are inevitable. The other side of the coin is the availability of resources. For example, if procedures, training and jobs are well designed and work groups are effective, then the resources available to cope with the demands of the job will obviously be enhanced. In addition, to these 'system factors', management have a major influence on individual factors such as motivation.

In a PIF analysis, only the PIFs relevant to the task being evaluated would be assessed. These PIFs are numerically rated at various stages in the analysis, as will be illustrated in later sections. The rating process is supported by means of PIF scales, where descriptions of specific conditions are provided at points along the scales so that the assessor can compare these conditions with those being evaluated.

3.2.3 Screening Analysis Because the prediction of human errors, the next stage of the process, may require considerable resources in some cases, it is essential that the analyst has some guidelines with regard to whether detailed predictive error analyses should be carried out. However, at first sight, it would appear that until the analysis is performed at a more detailed level, it is not possible to anticipate the nature and therefore the consequences of the errors which might be revealed by this more detailed analysis.

One way to address this problem has been described in the initial screening process described in section 3.1. Here, only tasks associated with critical processes are considered. Once the analyst has selected the human involvements with high risk potential processes he or she may still wish to reduce the number of tasks to be considered. This is usually achieved by performing an early coarse PIF analysis for each of the human interactions that have been selected. If the PIFs are rated as being very good, e.g. excellent training, good procedures and information presentation, adequate time available, no competing demands, etc., then the analyst may conclude that the probability of error is sufficiently low such that no further analysis is necessary for that particular task. The other factor that would be taken into account is the overall frequency with which the task is carried out. Obviously, even if an error with a critical outcome only occurred with a probability of 10^{-4}, if this was part of a loading operation which was carried out 5,000 times each year (about 14 times per day) over a number of sites, a major accident could be expected every two years.

The screening process described above is carried out at two stages of the analysis. It is used to decide whether or not to embark on the detailed prediction of specific human errors, using the techniques described in section 3.2.4. It is also used to decide whether or not a task should be analysed at the next lower level of detail in the task analysis. To recapitulate, it comprises the following steps:

1. Assess safety consequences of one or more errors occurring during the task. (Both direct effects and side effects should be considered.) This is assessed by considering the nature of the process (i.e. its intrinsic hazard potential) and a general consideration of the types of errors that could arise.

2. Evaluate the frequency with which the task is performed.

3. Evaluate the PIFs for the task.

Using this information, a decision table similar to that shown in table 2 below can be constructed.

	High error consequences		Low error consequences	
Quality of PIFs	frequent task	infrequent task	frequent task	infrequent task
High	extend	stop	stop	stop
Low	extend	extend	extend	stop

Table 2: Example decision table indicating criteria for stopping or extending analysis

It should be noted that the table makes the reasonable assumption that the higher the quality of the PIFs then the lower the likelihood of error. The table also makes certain assumptions about the trade-off between the effort required to perform detailed human reliability analyses and the risks that arise from not performing the analyses. This trade-off will depend very much on the severity of the consequences of errors and the tools available (e.g. computer based systems) to support the analyses and hence reduce the time and effort required. Each organisation needs to develop its own version of the decision table in accordance with the specific risks being evaluated.

3.2.4 Predictive Human Error Analysis Predictive Human Error Analysis (PHEA) is the process via which specific errors associated with tasks or task steps are identified. As described in the previous section, normally only those human interactions which have significant consequences if errors occur will be subjected to the PHEA process. The inputs to the process are the task structure and plans, as defined by the task analysis, and the results of the PIF analysis. The process is carried out at each level of the task analysis as required. Because PHEA may be resource-intensive, only those operations not eliminated by the screening analysis will be evaluated. The basic procedure of the PHEA is as follows:

3.2.4.1 Decide on the level of detail to conduct analysis The hierarchical structure of the HTA allows errors to be predicted at a variety of different levels. For example, consider section 2 of the HTA in figure 5. The subtask: 'Prepare tanker for filling' requires subtasks 2.1 to 2.5 to be performed. There are a number of ways in which these subtasks could fail to be performed correctly at this level. For example subtasks 2.3 to 2.5 could be carried out in the wrong order. If there were multiple tankers, 2.1: 'verify tanker is empty' could be carried out on the wrong tanker. It should be noted that this analysis may be quite independent of an analysis at the next lower level, where individual task steps would be analysed.

3.2.4.2 Perform planning error analysis The failure to perform the operations required at the particular level of the HTA being analysed could occur because of deficiencies in the plan. The categories of plan failure that can be defined are as follows:

P1: Incorrect plan selected and executed
P2: Correct but inappropriate plan selected and executed
P3: Correct plan selected but executed too soon / too late
P4: Correct plan executed in wrong order

If the procedures were not regularly updated or were otherwise incorrect, or if training was inadequate, P1 errors could occur. P2 errors would often arise as a result of misdiagnosing a

situation, or if the entry conditions for executing a sequence of operations were ambiguous or difficult to assess and therefore the wrong procedure was selected. It is important to note that if a planning error occurs, then this implies that a detailed analysis needs to be conducted of the alternative course of action that could arise. The analysis needs to consider the consequences of the correct operation not being performed and also the implications of the inappropriate series of actions that might be carried out. In some cases, these may have even more serious consequences than failing to perform the original intended action.

3.2.4.3 Perform operation error analysis This analysis is applied to each operation at the particular level of the HTA being evaluated. Depending on the level of analysis, an operation could be a task, subtask or task step. For each operation, the analyst considers the likelihood that one or more of the error types set out in classification in figure 7 could occur. This decision is made on the basis of the information supplied by the PIF analysis, and the analyst's knowledge concerning the types of error likely to arise given the nature of the mental and physical demands of the task and the particular configuration of PIFs that exist in the situation.

Operation errors are errors associated with one or more actions which change the state of the system, e.g. steps such as open valve A, secure blocking device, etc. These errors can also apply at the level of whole tasks, e.g. disconnect or secure tanker (tasks 4.2 and 4.4 in figure 5). Checking errors are associated with failing to perform a required check, which will usually involve a sensory operation such as verifying a level or state by visual inspection, rather than an action. Retrieval errors are concerned with retrieving information from memory (e.g. the time required for a reactor to fill), or from a visual display or a procedure. Communication or transmission errors are concerned with the transfer of information between people, either directly or via written documents such as permit systems. These errors are particularly pertinent in situations where a number of people in a team have to co-ordinate their activities. Selection errors occur in situations where the operator has to make an explicit choice between alternatives. These may be physical objects (e.g. valves, information displays) or courses of action. It should be emphasised that the categorisation of errors in figure 7 is generic, and may need to be modified for specific industries.

The first stage of the operation error analysis is to determine if any of the error categories in figure 7 apply to the task, subtask or task step being analysed. For example, at the level of individual task steps, operations would be actions performed at each step. If a particular step, e.g. checking a level in a sight glass, did not actually involve actions, then it would not be necessary to consider this category of errors further. The appropriate category in this case would be checking errors. Other applicable categories are Retrieval, Communication or Selection errors.

Once certain categories of error have been ruled out, the analyst decides whether or not any of the errors in the remaining applicable categories could occur within the task, subtask or task step being evaluated.

3.2.4.4 Perform recovery analysis Once errors have been identified, the analyst then decides if they are likely to be recovered before a significant consequence occurs. Consideration of the structure of the task (e.g. whether or not there is immediate feedback if an error occurs) together with the results of the PIF analysis, will usually indicate if recovery is likely.

3.2.5 Consequence Analysis The objective of consequence analysis is to evaluate the safety (or quality) consequences to the system of any human errors that may occur. Consequence Analysis obviously impacts on the overall risk assessment within which the human reliability analysis is embedded. In order to address this issue, it is necessary to consider the nature of the consequences of human error in more detail.

At least three types of consequences are possible if a human error occurs in a task sequence:

a) The overall objective of the task is not achieved.

b) In addition to the task not achieving its intended objective, some other negative consequence occurs.

c) The task achieves its intended objective but some other negative consequence occurs (either immediate or latent), which may be associated with some other system unrelated to the primary task.

Generally, risk assessment has focussed on (a), since the main interest in human reliability was in the context of human actions that were required as part of an emergency response. However, a comprehensive Consequence Analysis has to also consider (b) and (c) since both of these outcomes could be sources of risk to the individual or the plant.

One example of a particularly hazardous type of consequence in category (b) is where, because of misdiagnosis, the operator performs some alternative task other than that required by the system. For example, a rise of pressure in a reactor may be interpreted as being the result of a blockage in an output line, which would lead to attempts to clear the line. If, instead, it was due to impurities causing an exothermic reaction, then failure to attend to the real cause could lead to an overpressurisation accident. With regard to category (c), the operator may achieve the final required objective by a route which has an impact on another part of the process. For example, pipework may be connected in such a way that although the main task succeeds, an accident may occur when another process is started which uses the same pipework.

3.2.6 Error Reduction Analysis For those errors with significant consequences where recovery is unlikely, the qualitative analysis concludes with a consideration of error reduction strategies that will reduce the likelihood of these errors to an acceptable level.

3.2.7 Summary of the Qualitative Analysis Process The qualitative analysis process described in previous sections may appear somewhat complex when described in abstract terms. However, in specific cases it will be performed quite rapidly. Computer programs are also available to speed up the process for larger analyses, e.g. Top Down Human Error and Task Analysis (THETA), Embrey, (11).

The hierarchical structure of the process, with a screening analysis at each level provides a much greater likelihood of identifying all errors with significant safety consequences. If the analysis is conducted at a single level, e.g. at the detailed level of task steps such as opening valves, then errors such as the whole task being omitted or carried out too late would not be included.

3.2.8 Case Study Illustrating the Qualitative Analysis Process This example illustrates in a simplified form the steps of the qualitative analysis procedure shown in figure 4 using the chlorine tanker loading case study.

• Select initial level of analysis

The initial level of analysis selected considers tasks 1 to 5 in the task analysis in figure 5.

• Perform task analysis

The task analysis is performed to the next level of detail on tasks 2, 3 and 4, since tasks 1 and 5 were eliminated from the analysis because they did not involve any direct exposure to hazardous substances (from the initial screening analysis described in section 3.1). The first level analysis considers operations 2.1 to 2.5, 3.1 to 3.2 and 4.1 to 4.5 in figure 4.

• Perform PIF analysis

For the purpose of this example, it will be assumed that the PIFs which influence performance in all tasks are identical, i.e.

- Time stress (7)
- Experience / training of operators (8)
- Level of distractions (7)
- Quality of procedures / checklists (5)

These PIFs represent the major factors deemed by the analyst to influence error probability for the operations (coupling hoses, opening and closing valves) and planning activities being carried out within the tasks analysed at this level. In practice, the analyst would need to consider if different types of PIFs applied to the different tasks 2, 3 and 4. The numbers appended to the PIFs represent numerical assessments of the quality of the PIFs (on a scale of 1 to 9) in the situations being evaluated. The ratings indicate that there are negative influences of high time stress and high levels of distractions. These are compensated for by good training and moderate (industry average) procedures. Again, in some cases, these ratings could differ for the different tasks. For example, the operator may be highly trained for the types of operations in some tasks but not for others.

• Perform Screening Analysis

The screening analysis indicates that errors could give rise to severe consequences (chlorine release) in all the tasks. The PIF analysis has identified some negative influences which in turn indicate that the probability of error is not negligible. The loading operation is performed quite frequently (several times a day). These factors indicate that the Predictive Human Error Analysis should be performed for all the tasks.

• Perform detailed Predictive Human Error Analysis (PHEA)

A small subset of the results of the PHEA at this level is shown in figure 8. The possible errors are predicted by considering all possible error types in figure 7 for each operation at this level of the task analysis (2.1, 2.2, etc to 4.5). Planning errors are not included in figure 8, but would be predicted using the appropriate planning error category. Possible error recovery routes are also shown in figure 8.

• Evaluate consequences

Consequence analyses are set out in figure 8.

• Error Reduction Analysis

Figure 9 illustrates some of the possible error reduction strategies available. Apart from the specific strategies set out in figure 9, the PIF analysis also indicates which Performance Influencing Factors should be modified to reduce the likelihood of all error. In the case of the chlorine loading example, the major scope for improvements are the reduction of time stress and distractions and the development of better quality procedures.

The Error Reduction Analysis concludes one complete cycle of the Qualitative Human Error Analysis component of SPEAR. The analyst then repeats the earlier screening process to decide if it is appropriate to perform a more detailed analysis on any of the operations considered at the current level. As a result of this process, operation 3.2: 'Monitor tanker following operation' is analysed in more detail (see steps 3.2.1 to 3.2.6 in figure 5).

The Qualitative Human Error Analysis stages described above are applied to the task steps in subtask 3.2. Examples of the results of this analysis are shown in figure 8, where errors associated with steps 3.2.2, 3.2.3 and 3.2.5 are described. The corresponding error reduction strategies are shown in figure 9.

3.3 Representation

The results of the qualitative analysis can be used to comprehensively represent the human errors that need to be assessed in a risk assessment, as discussed in section 2.2. The form of representation can be in the form of a fault tree, as shown in figure 2, or an event tree (see (4)). The event tree has traditionally been used to model simple tasks at the level of individual task steps, for example in the THERP (Technique for Human Error Rate Prediction) method for human reliability assessment (see Swain and Guttmann (12)). It is most appropriate for sequences of task steps where few side effects are likely to occur as a result of errors.

3.4 Quantification

Since the main focus of this paper is on qualitative analysis, the quantification of the errors identified by the process described earlier will not be discussed here. Comprehensive reviews are available in (1).

3.5 Integration with Hardware Analyses

The integration of the human reliability fault trees with hardware analyses has been illustrated in the early sections of this paper. If human errors are shown to be major contributors to risk, as is usually the case, some of the error reduction strategies derived during the qualitative analysis will be implemented, in order to reduce risk to an acceptable level.

4. CONCLUSIONS

This paper has emphasised the major importance of a systematic approach to the qualitative modelling of human error in risk assessment. A comprehensive methodology to achieve this modelling has been described. The amount of analytical effort required to model human error in detail may appear to be large. However, this effort is still considerably less than is currently focussed on the hardware aspects of risk assessments, where the return on investment in terms of risk reduction is likely to be less. With appropriate training, and support from computer based implementations of the methodology, the use of the qualitative analysis methods advocated in this paper can make a cost effective contribution to risk reduction in the chemical and offshore oil production industries.

5. REFERENCES

1. Kirwan, B., Embrey, D.E. and Rea, K. (1988) Human Reliability Assessors Guide (ed. P. Humphreys). Report no. RTS 88/95Q, Safety and Reliability Directorate, United Kingdom Atomic Energy Authority, Wigshaw Lane, Culcheth, Warrington, WA3 4NE, England.

2. Ozog, H. (1985) Hazard identification, analysis and control. Chemical Engineering, 18th February 161-170.

3. Center for Chemical Process Safety (1989) Guidelines for Chemical Process Quantitative Risk Analysis. Center for Chemical Process Safety, American Institute of Chemical Engineers, 345 East 47th Street, New York, NY 10017.

4. Bellamy, L.J., Kirwan, B. and Cox, R.A. (1986) Incorporating human reliability into probabilistic safety assessment. 5th International Symposium on Loss Prevention and Safety Promotion in the Process Industries, Cannes, France.

5. Kletz, T.A. (1992) HAZOP and HAZAN. Notes on the Identification and Assessment of Hazards. Institution of Chemical Engineers, Rugby, U.K. (3rd edition).

6. Center for Chemical Process Safety (1992) Guidelines for Hazard Evaluation Procedures (2nd edition) Centre for Chemical Process Safety, American Institute of Chemical Engineers, 345 East 47th Street, New York, NY 10017.

7. Kirwan, B. (1992) (ed) A Guide to Task Analysis. London: Taylor and Francis.

8. Embrey, D.E. (1992a) Managing Human Error in the Chemical Process Industries. Proceedings of the 7th International Symposium on Loss Prevention and Safety Promotion in the Process Industries, Taormina, Italy.

9. Embrey, D.E. (1993) in: Guidelines for the Analysis and Reduction of Human Error, Centre for Chemical Process Safety, American Institute of Chemical Engineers, 345 East 47th Street, New York, NY 10017.

10. Embrey, D.E. (1992b) Incorporating Management and Organisational Factors into Probabilistic Safety Assessment. Reliability Engineering and System Safety, September.

11. Embrey, D.E. (1991) THETA (Top-Down Human Error and Task Analysis) Human Reliability Associates, 1 School House, Higher Lane, Dalton, Wigan, Lancs. WN8 7RP, England.

12. Swain, A.D. and Guttmann, H.E. (1983) A Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications NUREG/CR-1278. Washington D.C., U.S. Nuclear Regulatory Commission.

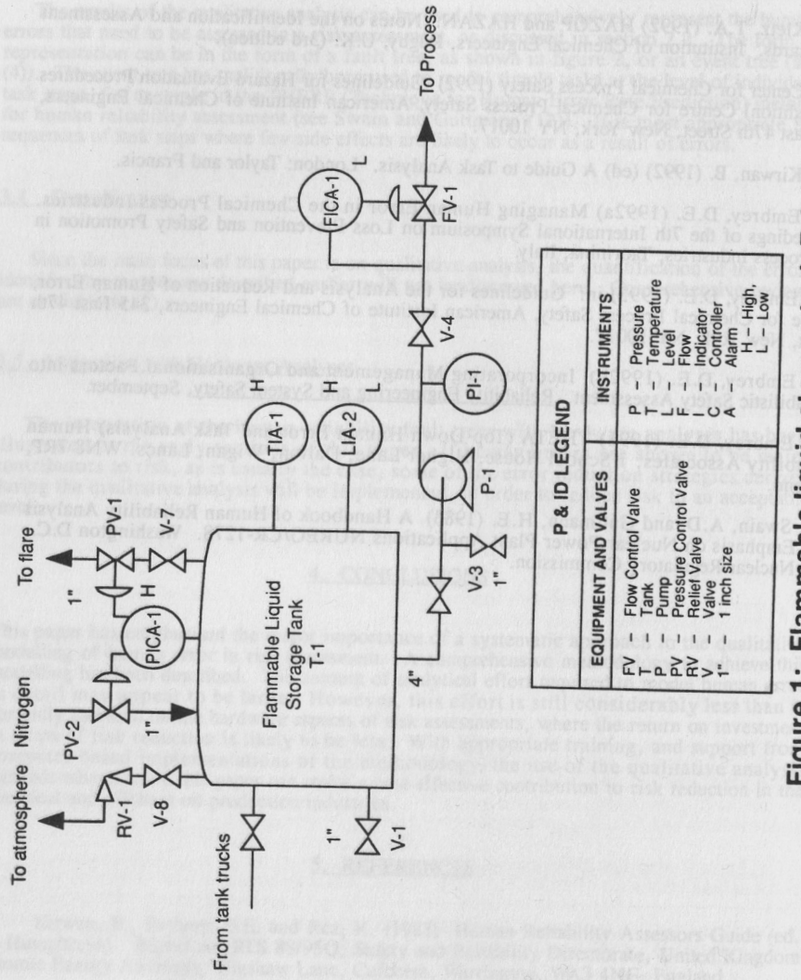

Figure 1: Flammable liquid storage tank P & ID

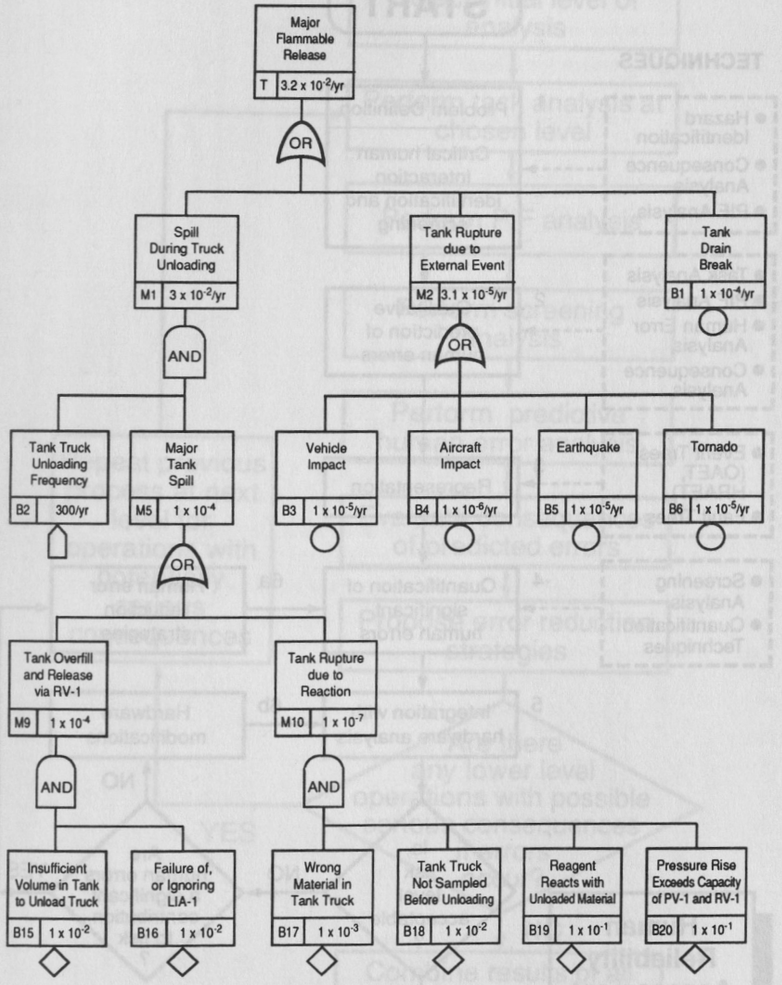

Figure 2. Fault tree analysis of flammable liquid storage tank

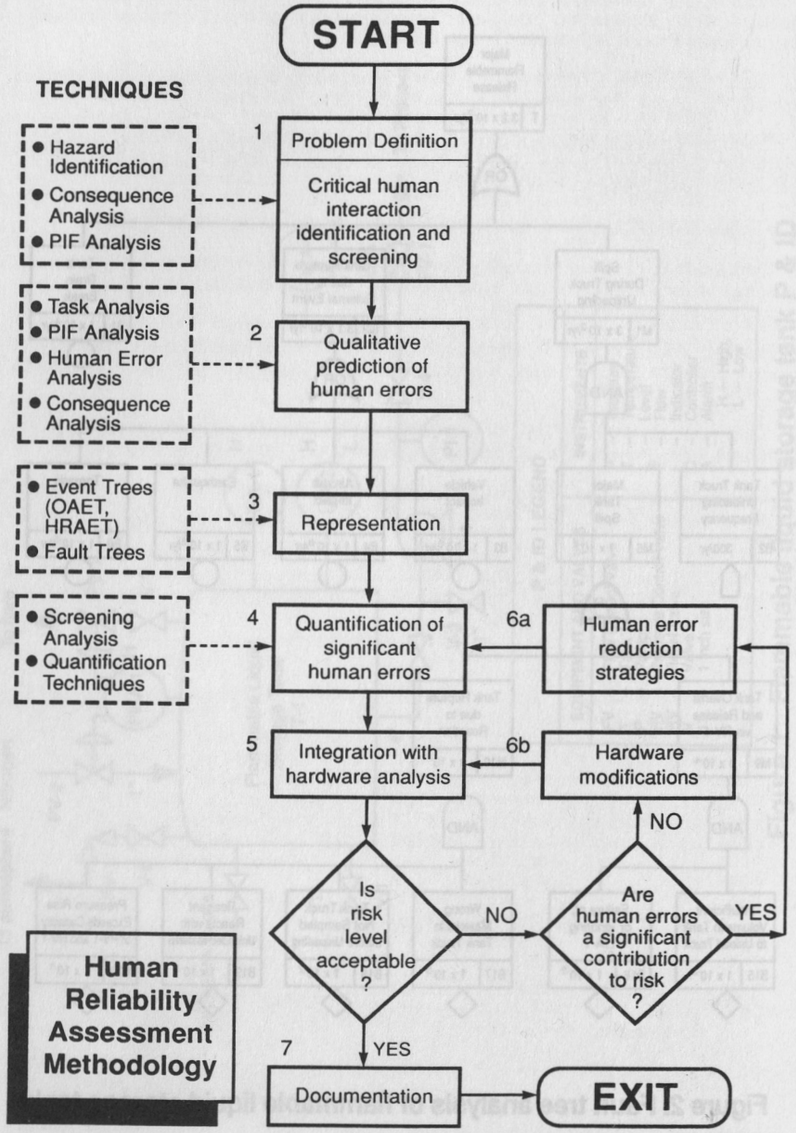

Figure 3: Stages of the Human Reliability Assessment Methodology

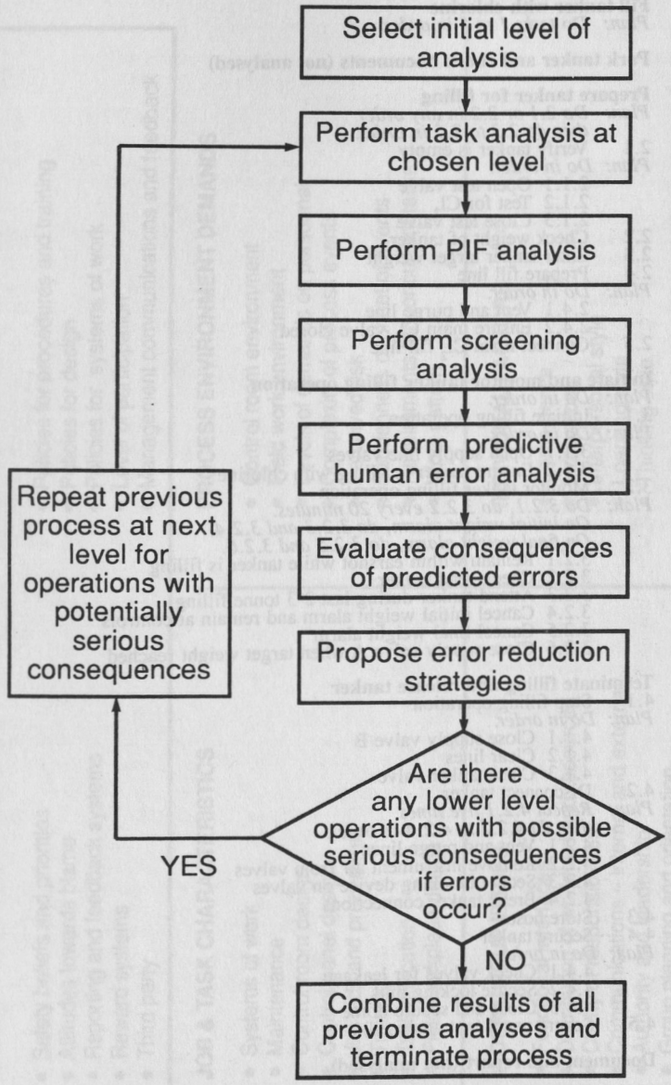

Figure 4. The Qualitative Analysis Process

0. Fill tanker with chlorine
Plan: Do tasks 1 to 5 in order.

1. Park tanker and check documents (not analysed)

2. Prepare tanker for filling
Plan: Do 2.1 or 2.2 in any order
then do 2.3 to 2.5 in order.
2.1 Verify tanker is empty
Plan: Do in order.
2.1.1 Open test valve
2.1.2 Test for Cl_2
2.1.3 Close test valve
2.2 Check weight of tanker
2.3 Enter tanker target weight
2.4 Prepare fill line
Plan: Do in order.
2.4.1 Vent and purge line
2.4.2 Ensure main Cl_2 valve closed
2.5 Connect main Cl_2 fill line

3. Initiate and monitor tanker filling operation
Plan: Do in order.
3.1 Initiate filling operation
Plan: Do in order.
3.1.1 Open supply line valves
3.1.2 Ensure tanker is filling with chlorine
3.2 Monitor tanker filling operation
Plan: Do 3.2.1, do 3.2.2 every 20 minutes.
On initial weight alarm, do 3.2.3 and 3.2.4.
On final weight alarm, do 3.2.5 and 3.2.6.
3.2.1 Remain within earshot while tanker is filling
3.2.2 Check road tanker
3.2.3 Attend tanker during last 2-3 tonne filling
3.2.4 Cancel initial weight alarm and remain at controls
3.2.5 Cancel final weight alarm
3.2.6 Close supply valve A when target weight reached

4. Terminate filling and release tanker
4.1 Stop filling operation
Plan: Do in order.
4.1.1 Close supply valve B
4.1.2 Clear lines
4.1.3 Close tanker valve
4.2 Disconnect tanker
Plan: Repeat 4.2.1 five times
then do 4.2.2 to 4.2.4 in order.
4.2.1 Vent and purge lines
4.2.2 Remove instrument air from valves
4.2.3 Secure blocking device on valves
4.2.4 Break tanker connections
4.3 Store hoses
4.4 Secure tanker
Plan: Do in order.
4.4.1 Check valves for leakage
4.4.2 Secure locking nuts
4.4.3 Close and secure dome
4.5 Secure panel (not analysed)

5. Document and report (not analysed)

Figure 5: Chlorine Tanker Task Analysis

MANAGEMENT POLICY AND ORGANISATIONAL CULTURE

- Safety beliefs and priorities
- Attitudes towards blame
- Reporting and feedback systems
- Reward systems
- Third party

- Policies for procedures and training
- Policies for design
- Policies for systems of work
- Level of participation
- Management communications and feedback

JOB & TASK CHARACTERISTICS

- Systems of work
- Maintenance
- Control room design
- Control panel design
- Job aids and procedures
- Training
- Task allocation
- Field workplace design

PROCESS ENVIRONMENT DEMANDS

- Control room environment
- Field work environment
- Levels of demands on personnel
- Complexity of process events
- Perceived risk
- Suddenness of onset of events
- Requirements for concurrent tasks
- Work pattern

WORK GROUP ISSUES

- Functional interfaces
- Distribution of workload and resources
- Clarity of responsibilities
- Communications – internal and external
- Authority and leadership
- Group planning and orientation

INDIVIDUAL FACTORS

- Competence
- Motivation
- Interpersonal style
- Learning style
- Thinking style

Figure 6. Performance Influencing Factors

Planning Errors

P1 Incorrect plan executed
P2 Correct but inappropriate plan executed
P3 Correct plan executed too soon / too late
P4 Correct plan executed in wrong order

Operation Errors

O1 Operation too long / short
O2 Operation mistimed
O3 Operation in wrong direction
O4 Operation too little / too much
O5 Misalign
O6 Right operation on wrong object
O7 Wrong operation on right object
O8 Operation omitted
O9 Operation incomplete

Checking Errors

C1 Check omitted
C2 Check incomplete
C3 Right check on wrong object
C4 Wrong check on right object
C5 Check mistimed

Retrieval Errors

R1 Information not obtained
R2 Wrong information obtained
R3 Information retrieval incomplete

Communication Errors

T1 Information not communicated
T2 Wrong information communicated
T3 Information communication incomplete

Selection Errors

S1 Selection omitted
S2 Wrong selection made

Figure 7: Error Classification

STEP	ERROR TYPE	ERROR DESCRIPTION	RECOVERY	CONSEQUENCES & COMMENTS
2.1 Verify tanker is empty	Check omitted (C1)	Verification omitted	No recovery	Chlorine released when valve is opened
2.3 Enter tanker target weight	Wrong information obtained (R2)	Wrong weight entered	On check	Alarm does not sound before tanker overfills
3.2.2 Check tanker while filling	Check omitted (C1)	Tanker not monitored whilst filling	On initial weight alarm	Alarm will alert operator if correctly set. Equipment fault, e.g. leaks not detected early and remedial action delayed
3.2.3 Attend tanker during last 2 - 3 tonne filling	Operation omitted (O8)	Operator fails to attend	On step 3.2.5	If alarm not detected within 10 minutes tanker will overfill
3.2.5 Cancel final weight alarm	Operation omitted (O8)	Final weight alarm taken as initial weight alarm	No recovery	Tanker overfills

Figure 8: Results of Qualitative Analysis

STEP	ERROR REDUCTION RECOMMENDATIONS		
	PROCEDURES	TRAINING	EQUIPMENT
2.1 Verify tanker is empty	Double check via unladen weight check. Use checklist	Stress importance of verifying tanker is empty	Provide gauge indicating tanker pressure
2.3 Enter tanker target weight	Independent validation of target weight. Recording of values in checklist	Ensure operator double checks entered date	Automatic setting of weight alarms from unladen weight. Computerise logging system and build in checks on tanker reg. no. and unladen weight linked to warning system. Display differences between unladen and current weights
3.2.2 Check Road Tanker while filling	Provide secondary task involving other personnel. Supervisor periodically checks operation	Stress importance of regular checks for safety	Provide automatic log-in procedure
3.2.3 Attend tanker during filling of last 2-3 tonnes (on weight alarm)	Ensure work schedule allows operator to do this without pressure	Illustrate consequences of not attending	Repeat alarm in secondary area. Automatic interlock to terminate loading if alarm not acknowledged. Visual indication of alarm.
3.2.5 Cancel final weight alarm	Note differences between the sound of the two alarms in checklist	Alert operators during training about differences in sounds of alarms	Use completely different tones for initial and final weight alarms

Figure 9: Error Reduction Recommendations

ADVANCES IN GAS CLOUD DISPERSION MODELLING: HEAVY CLOUDS ON SLOPING GROUND

D.M.Webber, S.J.Jones, and D.Martin
SRD, AEA Technology, Wigshaw Lane, Culcheth, Warrington WA3 4NE

A model is presented of the motion of a heavy gas cloud down a uniform slope in calm ambient conditions. The model is derived from solutions of the shallow water equations with appropriate boundary conditions. Its predictions are shown to agree adequately with experimental results in calm conditions, and a possible generalisation to allow for the presence of a wind is discussed.

Keywords: Gas Cloud, Sloping Ground.

1 INTRODUCTION

Integral (or box) models of gas dispersion are now a standard tool for the analysis of flammable and toxic hazards, posed by major industrial plant. Recent developments, including work under the recently completed Major Technological Hazards programme of the Commission of the European Communities, have been aimed at extending the understanding of heavy gas flows to situations where the nature of the terrain, or of structures on it, may have a significant effect on the dispersion. The results of the CEC project have been sumarised by Builtjes (1992) who gives full reference to the more complete reports of the individual participants. This work includes: field trials on propane clouds, with and without momentum at the source, encountering fence and channel obstacles; wind–tunnel experiments involving many repeated releases, clouds encountering fences, and clouds on sloping ground; analysis of earlier data on the interction of clouds with obstacles, and analysis of concentration fluctuations in earlier experiments; and mathematical modelling of some of these processes.

Here we shall focus on some aspects of gas clouds released on sloping ground. The work presented was begun under the above project. Hazardous clouds are very often significantly heavier than air and such sloping terrain is known to have a important effect. Models of the behaviour of a heavy cloud released instantaneously on a slope have recently been presented by Deaves and Hall (1990) and by Nikmo and Kukkonen (1991).

Each of these models is an intuitively appealing generalisation of the flat ground integral model approach to include the effects of slopes. However, in each case the effect of the slope is only found with a numerically computed solution to a set of differential equations. Whilst this situation is quite usual, it is highly desirable to have a more direct understanding of the nature and effects of the assumptions involved in such models.

The importance of such an understanding cannot be overstated. Credible hazard analysis can only come about using models which are well validated on (of necessity) small scale data, and which incorporate sound physical assumptions (and accurate calculational methods) in