5

Qualitative and Quantitative Prediction of Human Error in Risk Assessment

5.1. INTRODUCTION

There is an increasing requirement by regulatory authorities for companies to conduct formal safety assessments of hydrocarbon and chemical process plants. 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 (see Bridges et al., 1994, for techniques for including human error considerations in hazard analyses). Emphasis is being placed by regulators 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) where human errors were implicated as direct or indirect causes (see CCPS, 1989b, 1992d for further examples).

The usual emphasis in human reliability has been on techniques for the derivation of numerical error probabilities for use in fault trees (see Kirwan et al., 1988, for a comprehensive review of these techniques). However, in many ways, this emphasis on absolute quantification is misplaced. Many practitioners emphasize 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 minimizing these risks. Although the quantitative results of the assessment are important in arriving at decisions in specific areas, for example the siting of on-shore plants with potentially hazardous processes, it is widely recognized 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 main focus of this chapter is the description of a defensible procedure for qualitative human error prediction that will achieve these objectives.

In addition, the chapter will provide an overview of human reliability quantification techniques, and the relationship between these techniques and qualitative modeling. The chapter will also describe how human reliability is integrated into chemical process quantitative risk assessment (CPQRA). Both qualitative and quantitative techniques will be integrated within a framework called SPEAR (System for Predictive Error Analysis and Reduction).

5.2. THE ROLE OF HUMAN RELIABILITY IN RISK ASSESSMENT

5.2.1. An Illustrative Case Study

Although the main emphasis of this chapter will be on qualitative human reliability methods in risk assessment, this section will illustrate the importance of both qualitative and quantitative methods in CPQRA. An example of a typical assessment, described by Ozog (1985) will be considered. The stages of the risk assessment are as follows:

System Description
The system is a storage tank designed to hold a flammable liquid under a low positive nitrogen pressure (see Figure 5.1). This pressure is controlled by PICA-1. A relief valve is fitted which operates if overpressurization occurs. Liquid is fed to the tank from a tank truck, and is subsequently supplied to the process by the pump P-1.

Hazard Identification
A hazard and operability study (HAZOP) was used to identify potential hazards, the most serious of which is an unrecoverable release from the storage tank.

Construction of the Fault Tree
The fault tree is constructed based on the system description and initiating events identified in the HAZOP. Figure 5.2 shows a portion of an extended version of Ozog's fault tree, taken from CCPS (1989b). The following terminology is used:

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

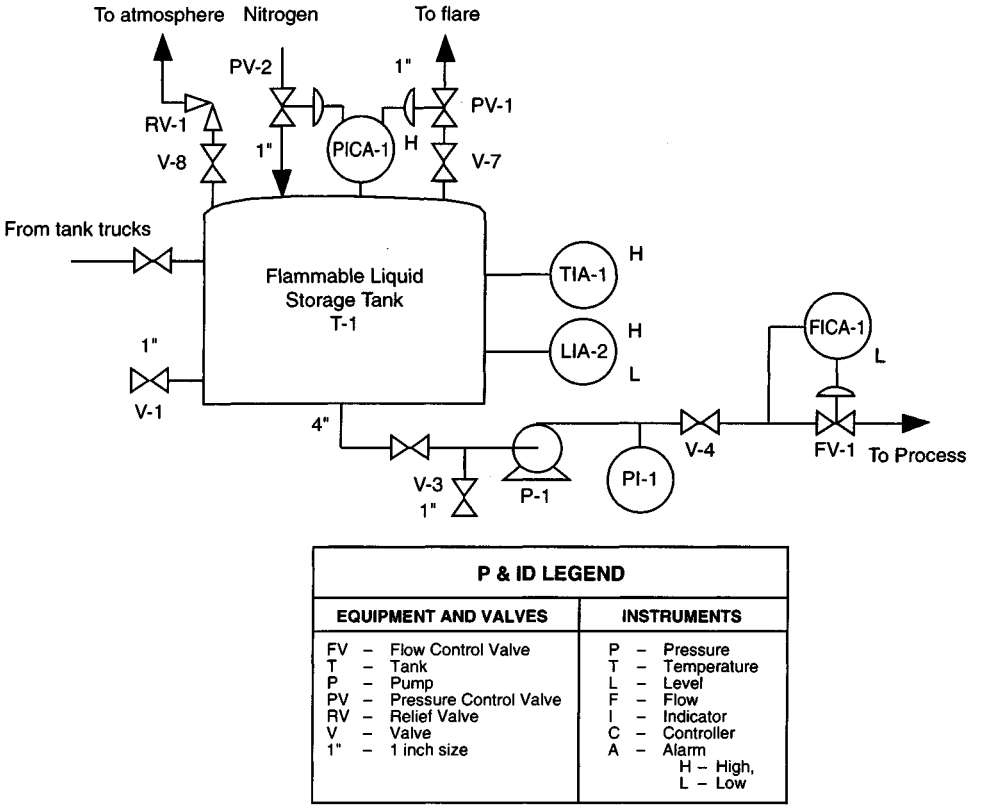

FIGURE 5.1 **Flammable Liquid Storage Tank P&ID (from Ozog, 1985).**

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)

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 CCPS, 1989b).

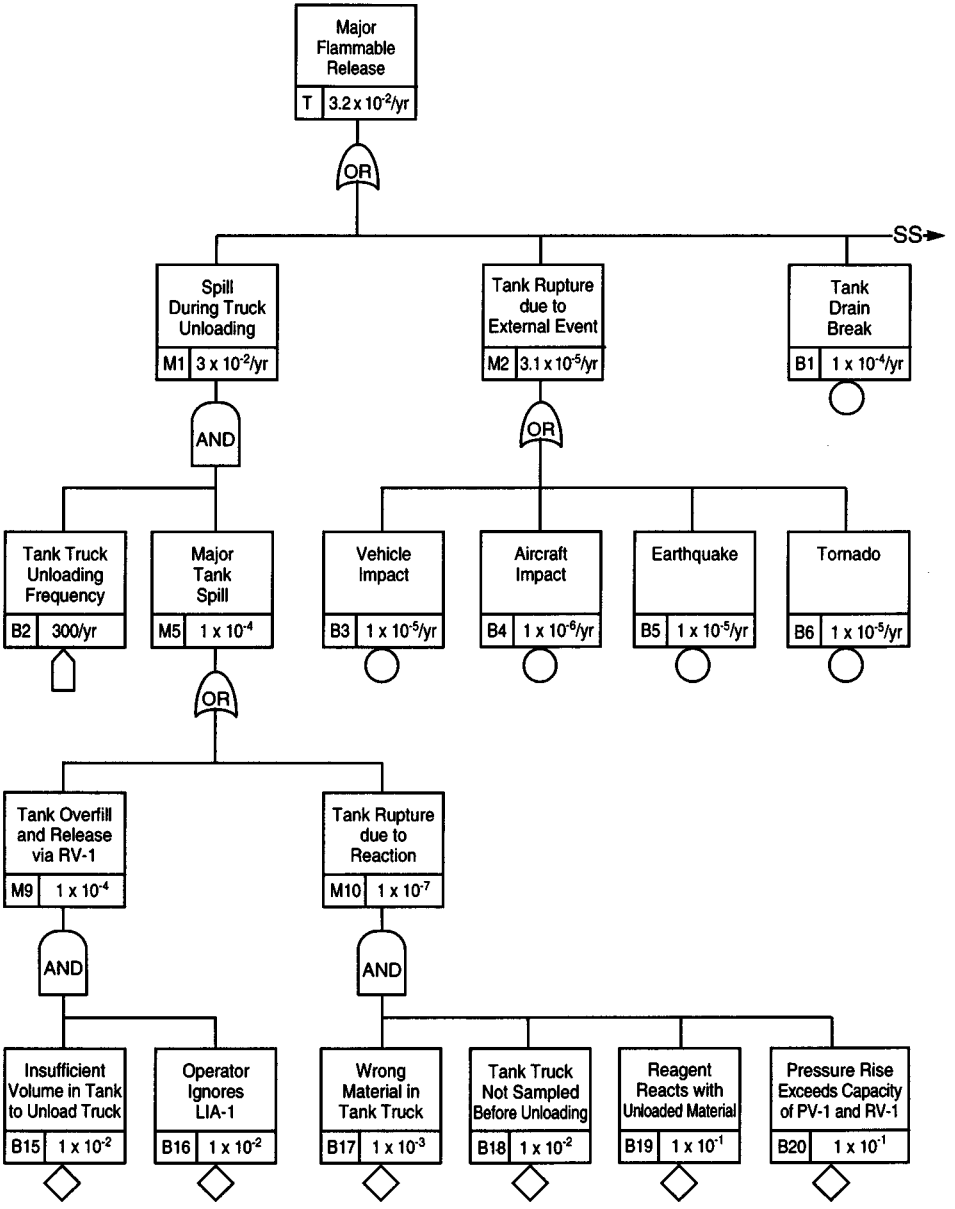

FIGURE 5.2 **Fault tree Analysis of Flammable Liquid Storage Tank (from Ozog, 1985).**

5.2.2. Implications of Human Error for the Analysis

From a human reliability perspective, a number of interesting points arise from this example. 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 could be due to a prior 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 usually the case that human error dominates a risk assessment, if it is properly considered in the analysis. This is illustrated in Bellamy et al. (1986) with 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, 1992, CCPS, 1992b) as shown in Figure 5.3. Some of the causes of process deviations generated by a HAZOP analysis may actually be ascribed to human error. However, the team doing the analysis is given no explicit guidance within the HAZOP (or any other hazard identification technique) that would enable them to identify human causes of these process deviations. 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 that 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 noncredible, 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 chapter 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.

PROCESS UNIT: DAP PRODUCTION Node: 1 Process Parameter: Flow				
GUIDE WORD	**DEVIATION**	**CONSEQUENCES**	**CAUSES**	**SUGGESTED ACTION**
No	No Flow	Excess ammonia in reactor. Release to work area.	1. Valve A fails closed. 2. Phosphoric acid supply exhausted. 3. Plug in pipe; pipe ruptures.	Automatic closure of valve B on loss of flow from phosphoric acid supply
Less	Less Flow	Excess ammonia in reactor. Release to work area, with amount released related to quantitative reduction in supply. Team member to calculate toxicity vs. flow reduction.	1. Valve A partially closed. 2. Partial plug or leak in pipe.	Automatic closure of valve B on reduced flow from phosphoric acid supply. Set point determined by toxicity vs. flow calculation.
More	More Flow	Excess phosphoric acid degrades product. No hazard in work area.	—	—
Part of	Normal flow of decreased concentration of phosphoric acid	Excess ammonia in reactor. Release to work area, with amount released related to quantitative reduction in supply.	1. Vendor delivers wrong material or concentration. 2. Error in charging phosphoric acid supply tank.	Check phosphoric acid supply tank concentration after charging.

FIGURE 5.3. **Sample of HAZOP Worksheet (CCPS, 1985).**

5.2.3. Quantification Aspects

In the preceding section, the importance of a comprehensive human reliability modeling approach has been emphasized 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 that 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 at an early stage in the event.

These two points can be illustrated in the fault tree in Figure 5.2. 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 labeling 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 3 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 will detect the escape of liquid through the relief valve as soon as overfilling has occurred, and immediately close 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 the recovery action is given a conservative failure probability of 1×10^{-2} and joined by an AND gate to events B15 and B16, then the probability of M9 and M5 becomes 1×10^{-6}. This considerably reduces the overall frequency of a major flammable release (T) to 3.2×10^{-4}.

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, labeling, etc.) which could impact on these probabilities.

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

The SPEAR 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 framework is set out in Figure 5.4.

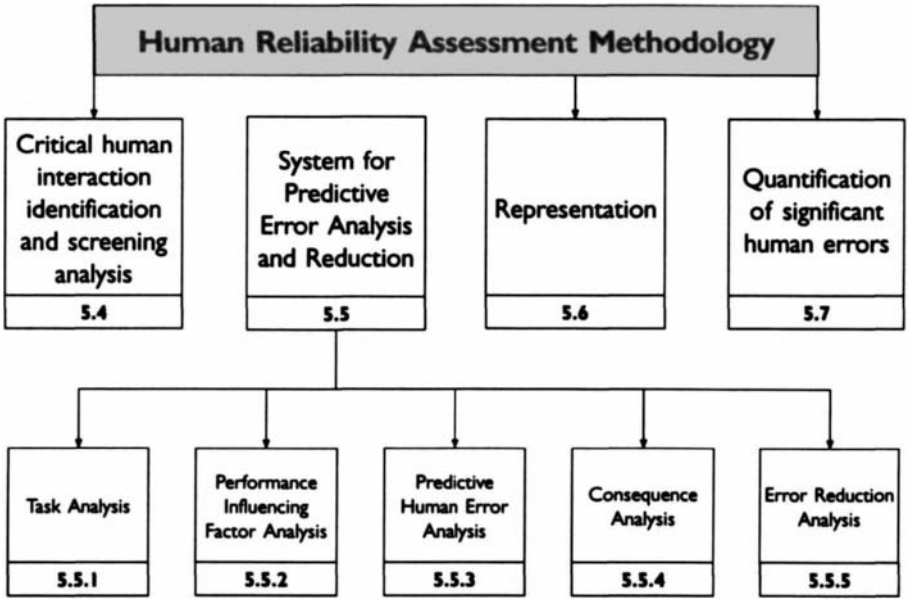

FIGURE 5.4. **System for Predictive Error Analysis and Reduction.**

Critical Human Interaction Identification and Screening (Stage 1)

The process involves identifying and describing human interactions with the system which will have major impact on risk if errors occur. A human interaction can in some cases comprise a single operation, for example, closing a valve or detecting a temperature increase. Usually, however, a human interaction will consist of a task directed at achieving a particular system objective, for example starting up a reactor or responding correctly in an emergency. Human interactions are obviously not confined to operational situations. They may also be involved in maintenance and plant changes. Errors, in these operations, can give rise to latent failures.

Qualitative Analysis of Human Errors (Stage 2)

This stage involves the prediction of errors that could arise on the basis of performance-influencing factors (PIFs) which exist in the situation, the nature of the human interaction with the system (e.g., actions, checking, communication), and the models of error discussed in Chapter 2. Only if human errors are identified that may have significant consequences (loss of life, plant damage, major production loss) will the subsequent stages of the process be performed. This stage therefore includes a consequence analysis, together with an error reduction analysis.

Representation (Stage 3)
This stage involves representing the structure of the tasks in which errors with severe consequences could occur, in a manner that allows the probabilities of these consequences to be generated. The usual forms of representation are event trees and fault trees.

Quantification (Stage 4)
The quantification process involves assigning numerical probabilities or frequencies to the errors (or error recovery opportunities) that have been identified during the preceding stages. Following the quantification process, the error probabilities will be combined with the hardware analyses to allow an overall measure of risk to be calculated. If this expected level of risk is unacceptable, then changes will be made in the human or hardware systems to reduce it (see Figure 5.5). In the case of human errors this may involve consideration of alternative strategies on the basis of cost-effectiveness considerations.

5.4. CRITICAL TASK IDENTIFICATION AND SCREENING ANALYSIS

The purpose of the Critical Task Identification and Screening analysis is to reduce the amount of analysis required by focusing on tasks that have a significant error potential. The screening process essentially asks the following questions:

Is there a hazard present in the area of the plant (e.g., a reactor, or a complete process unit) being considered?

In this context the term *hazard* is taken to mean "potential to cause harm," and would include any substance or plant item with characteristics such as toxicity, flammability, high voltage, mechanical energy, or asphyxiation potential.

Given that there is a hazard present, are there any human interactions with the plant that could cause the harm potential to be released?

Interactions refers to any jobs, tasks, or operations carried out by people who could directly or indirectly cause the hazard to be released. Direct interactions with the plant might involve breaking open pipework, opening reactors, etc. Indirect interactions would include remote activation of valves from a control room, or the performance of maintenance on critical plant items. Errors that might occur during these interactions could allow the harm potential to be released. This could occur directly (for example, a worker could be overcome by a chlorine release if an incorrect valve line-up was made) or indirectly (for example, if a pump bearing in a critical cooling circuit was not lubricated, as in the example in Chapter 1). The procedure as described above

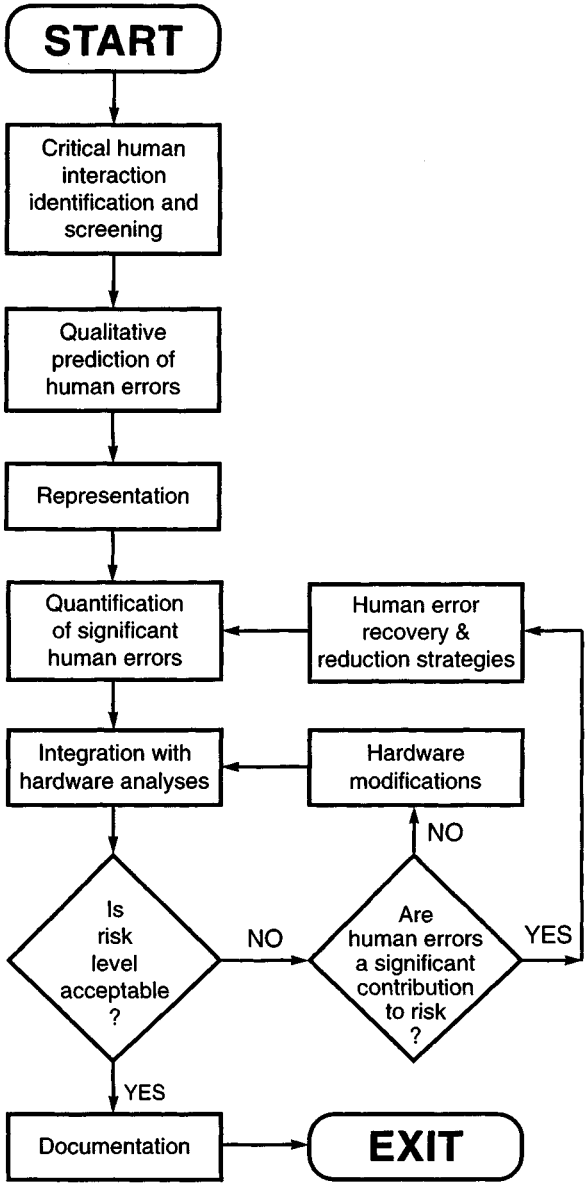

FIGURE 5.5. **Relationship of SPEAR to Human Reliability Assessment Methodology**

is analogous to the process performed for hardware failures in a typical HAZOP (see CCPS, 1992b).

Information on the types of human interactions with hazardous systems that occur would be obtained from sources such as plant operating instructions, job safety analyses and similar sources. These interactions are referred to as **critical tasks (CT)**.

Given that workers interact with hazardous systems, how frequently are they likely to make errors in these critical tasks?

The answer to this question will depend on two factors: the frequency with which the CT occur, and the likelihood of errors arising when performing these tasks. The frequency of the interactions can usually be specified relatively easily by reference to plant procedures, production plans, and maintenance schedules. The probability of error will be a function of the PIFs discussed extensively in Chapter 3 and other chapters in this book. In order to obtain a measure of error potential, it is necessary to make an assessment of the most important PIFs for each of the CT.

In summary, at the screening stage of the SPEAR process, the ranking of tasks in order of potential risk is made on the basis of three criteria:

- The known or hazard severity potential (HSP) that is present in the systems with which the worker is interacting
- The extent to which the nature of the task could allow the hazard to cause harm to workers, the public or the environment (hazard release potential., HRP)
- The frequency (F) with which the task is performed

If these functions are each rated from 1 to 5, a scale of task criticallity can be generated ranging from 0 to 1 as follows:

$$\text{Task Criticality Index (TCI)} = [(\text{HP} \times \text{HSP} \times \text{F}) - 1]/124$$

Each task can then be assessed on this basis to produce a ranking of risk potential. Only those tasks above a predetermined level of the TCI will be subjected to a detailed analysis.

5.5. QUALITATIVE HUMAN ERROR ANALYSIS

Qualitative human error prediction is the most important aspect of assessing and reducing the human contribution to risk. For this reason, it will be described in some detail in this section. The qualitative analysis performed in SPEAR involves the following techniques:

- Task analysis
- Performance-influencing factor analysis

- Predictive human error analysis
- Consequence analysis
- Error reduction analysis

Many of these techniques have been described in Chapter 4. They will be illustrated in this chapter with reference to a simple example, the loading of a chlorine tanker.

5.5.1. Task Analysis

As discussed in Chapter 4, task analysis is a very general term that encompasses a wide variety of techniques. In this context, 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 this example is hierarchical task analysis (HTA) (see Chapter 4). This has the advantage that it has been applied extensively in the chemical and other industries. As described in Chapter 4, 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 that describes how the steps or functions at that level are to be executed.

Figure 5.6 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 broken down to a further level of detail as required. As well as illustrating the hierarchical nature of the analysis, Figure 5.6 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.

5.5.2. Performance Influencing Factor Analysis

During this stage of the qualitative analysis, a PIF analysis is performed that considers those factors which will determine the probability of error for the type of task under consideration. A structured form of PIF analysis such as the HFA tool described in Section 2.7.2 will facilitate this process.

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

1. Park tanker and check documents (not analyzed)

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 ton 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 analyzed)

5. Document and report (not analyzed)

FIGURE 5.6. **Chlorine Tanker Task Analysis.**

5.5.3. Predictive Human Error Analysis

Predictive human error analysis (PHEA) is the process via which specific errors associated with tasks or task steps are predicted. The process also considers how these predicted errors might be recovered before they have negative consequences. 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 basic procedure of the PHEA is as follows:

5.5.3.1. 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 5.6. 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 analyzed.

5.5.3.2. Perform Planning Error Analysis

The failure to perform the operations required at the particular level of the HTA being analyzed could occur because of deficiencies in the plan. The categories of plan failure are shown in Figure 5.7.

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.

5.5.3.3. Perform Operation Error Analysis

This analysis is applied to each operation at the particular level of the HTA being evaluated. In most cases the analysis is performed at the level of a step, for example, **Open valve 27B.** For each operation, the analyst considers the likelihood that one or more of the error types set out in classification in Figure 5.7 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. The different error categories are described in more detail below:

Operation Errors

Operation errors are errors associated with one or more actions that change the state of the system, for example, steps such as open valve A, secure blocking device. These errors can also apply at the level of whole tasks, for example, disconnect or secure tanker (tasks 4.2 and 4.4 in Figure 5.6).

Action	
A1	Action too long / short
A2	Action mistimed
A3	Action in wrong direction
A4	Action too little / too much
A5	Misalign
A6	Right action on wrong object
A7	Wrong action on right object
A8	Action omitted
A9	Action incomplete
A10	Wrong action on wrong object
Checking	
C1	Checking omitted
C2	Check incomplete
C3	Right check on wrong object
C4	Wrong check on right object
C5	Check mistimed
C6	Wrong check on wrong object
Retrieval	
R1	Information not obtained
R2	Wrong information obtained
R3	Information retrieval incomplete
Transmission	
T1	Information not transmitted
T2	Wrong information transmitted
T3	Information transmission incomplete
Selection	
S1	Selection omitted
S2	Wrong selection made
Plan	
P1	Plan preconditions ignored
P2	Incorrect plan executed

FIGURE 5.7 **Error Classification.**

Checking Errors

These are errors such as failing to perform a required check, which will usually involve a data acquisition process such as verifying a level or state by visual inspection, rather than an action.

Retrieval Errors

These 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

These errors are concerned with the transfer of information among 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 coordinate their activities.

Selection Errors

These are errors that occur in situations where the operator has to make an explicit choice among alternatives. These may be physical objects (e.g., valves, information displays) or courses of action. It should be emphasized that the categorization of errors in Figure 5.7 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 5.7 apply to the task, subtask, or task step being analyzed. 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.

5.5.3.4. 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.

5.5.4. 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:

- The overall objective of the task is not achieved.
- In addition to the task not achieving its intended objective, some other negative consequence occurs.
- 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 focused on the first type of error, 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 other types, since both of these outcomes could constitute sources of risk to the individual or the plant.

One example of a particularly hazardous type of consequence in the second category 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 overpressurization accident. With regard to the third category, the operator may achieve the final required objective by a route that 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 that uses the same pipework.

5.5.5. 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. These strategies can be inferred directly from the results of the PIF analysis, since this indicates the deficiencies in the situation which need to be remedied to reduce the error potential.

5.5.6. Case Study Illustrating Qualitative Analysis Methods in SPEAR

This example illustrates the qualitative aspects of SPEAR, using the chlorine tanker loading case study as a basis.

5.5.6.1. Select Task Steps on the Basis of Screening Analysis

The task analysis is performed on tasks 2, 3, and 4. 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 2.1). The analysis considers operations 2.1 to 2.5, 3.1 to 3.2 and 4.1 to 4.5 in Figure 5.6.

5.5.6.2. Perform Task Analysis

The task analysis is shown in Figure 5.6.

5.5.6.3. Perform PIF analysis

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

- Time stress score (score 7, ideal value 1)
- Experience /training of operators score (score 8, ideal value 9)
- Level of distractions score (score 7, ideal value 1)
- Quality of procedures /checklists (score 5, ideal value 9)

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 analyzed 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) across all task steps 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. It should be noted that as some factors increase from 1 to 9, they have a negative effect on performance (time stress and level of distractions), whereas for the other factors, an increase would imply improved performance (quality of procedures and experience/training).

5.5.6.4. Perform Detailed Predictive Human Error Analysis (PHEA)

A selection of the results of the PHEA is shown in Figure 5.8 for task elements 2.3, 3.2.2, 3.2.3, and 3.2.5. The possible errors are predicted by considering all the possible error types in Figure 5.7 for each element. Planning errors are not included in Figure 5.8, but would be predicted using the appropriate planning error category. Possible error recovery routes are also shown in Figure 5.8.

5.5.6.5. Evaluate Consequences

Consequence analyses are set out in Figure 5.8.

5.5.6.6. Error Reduction Analysis

Figure 5.9 illustrates some of the possible error reduction strategies available. Apart from the specific strategies set out in Figure 5.9, the PIF analysis also indicates which PIFs should be modified to reduce the likelihood of 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 the methodology set out in Figure 5.4. The analyst then decides 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, operations 3.2: **Monitor tanker following operation**, 4.1: **Stop filling operation**, 4.2: **Disconnect tanker**, and 4.4: **Secure tanker** are analyzed in more detail (see Figure 5.6).

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 5.8. The corresponding error-reduction strategies are shown in Figure 5.9.

STEP	ERROR TYPE	ERROR DESCRIPTION	RECOVERY	CONSEQUENCES AND COMMENTS
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 while 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 ton 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
4.1.3 Close tanker valve	Operation omitted (O8)	Tanker valve not closed	4.2.1	Failure to close tanker valve would result in pressure not being detected during the pressure check in 4.2.1
4.2.1 Vent and purge lines	Operation omitted (O8) Operation incomplete (O9)	Lines not fully purged	4.2.4	Failure of operator to detect pressure in lines could lead to leak when tanker connections broken
4.4.2 Secure locking nuts	Operation omitted (O8)	Locking nuts left unsecured	None	Failure to secure locking nuts could result in leakage during transportation

FIGURE 5.8 **Results of Predictive Human Error Analysis.**

5.6. REPRESENTATION

If the results of the qualitative analysis are to be used as a starting-point for quantification, they need to be represented in an appropriate form. The form of representation can be a fault tree, as shown in Figure 5.2, or an event tree (see Bellamy et al., 1986). 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

STEP	ERROR REDUCTION RECOMMENDATIONS		
	PROCEDURES	TRAINING	EQUIPMENT
2.3 **Enter tanker** target weight	Independent validation of target weight.	Ensure operator double checks entered date. Recording of values in checklist	Automatic setting of weight alarms from unladen weight. Computerize 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 tons (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
4.1.3 Close tanker valve	Independent check on action. Use checklist	Ensure operator is aware of consequences of failure	Valve position indicator would reduce probability of error
4.2.1 Vent and purge lines	Procedure to indicate how to check if fully purged	Ensure training covers symptoms of pressure in line	Line pressure indicator at controls. Interlock device on line pressure.
4.4.2 Secure locking nuts	Use checklist	Stress safety implication of training	Locking nuts to give tactile feedback when secure

FIGURE 5.9. **Error Reduction Recommendations Based on PHEA**

assessment, Swain and Guttmann (1983) (see Section 5.7.2.1). It is most appropriate for sequences of task steps where few side effects are likely to occur as a result of errors, or when the likelihood of error at each step of the sequence is dependent on previous steps.

Figure 5.10 shows a detailed fault tree for an offshore drilling operation. The top event of the fault tree is **Failure to use shear rams to prevent blowout.** As with the fault tree in Figure 5.2, the representation combines both hardware

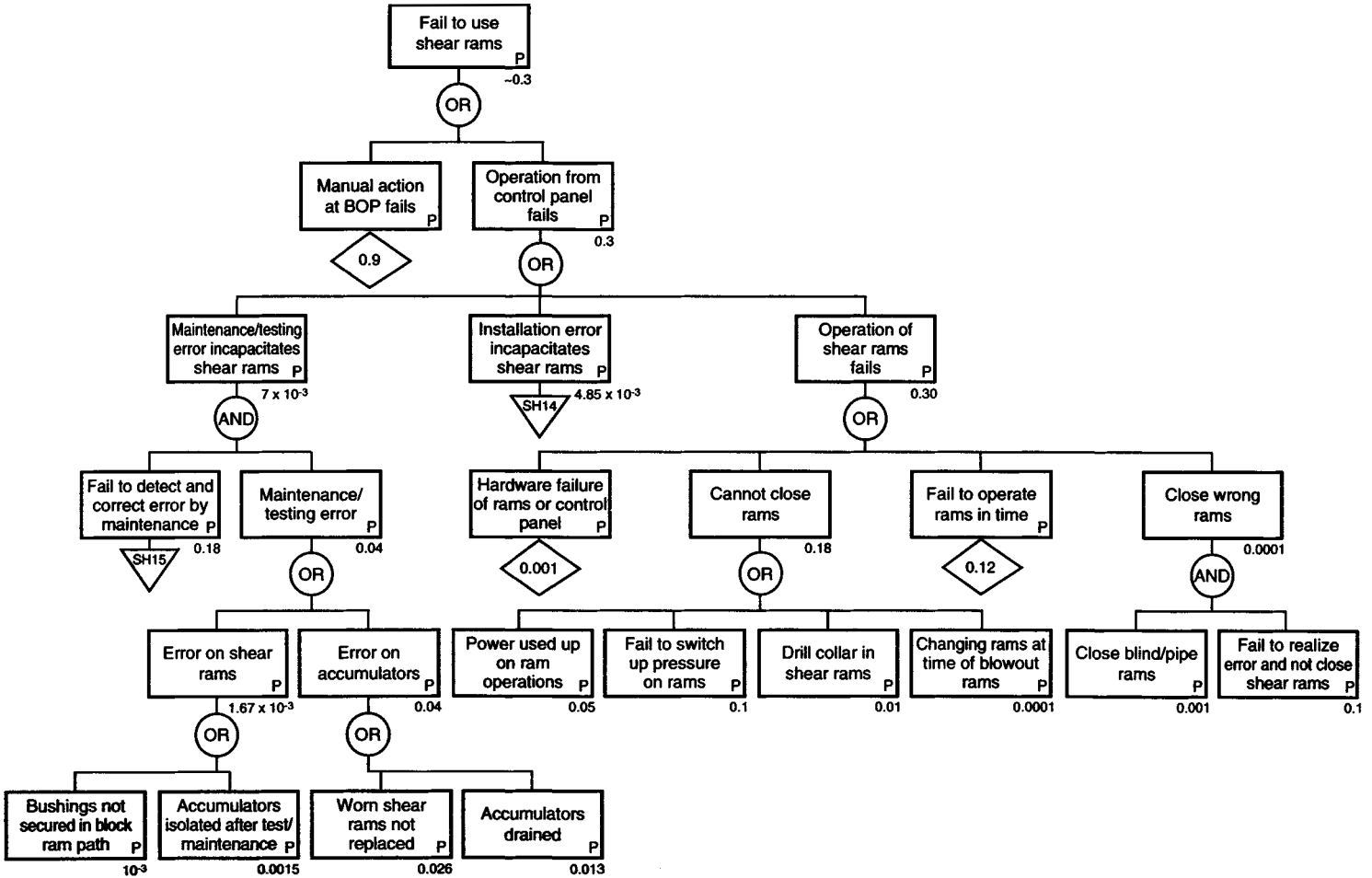

FIGURE 5.10. **Offshore drilling blowout fault tree subtree, "Fail to use shear rams to prevent blowout."**

and human failures. Figure 5.11 is an event tree representation of operator actions involved in an offshore emergency shutdown scenario (Kirwan, 1990). This type of event tree is called an operator action event tree (OAET) because it specifically addresses the sequence of actions required by some initiating event. Each branch in the tree represents success (the upper branch) or failure (the lower branch) to achieve the required human actions described along the top of the diagram. The probability of each failure state to the right of the diagram is the product of the error and/or success probabilities at each node of branch that leads to the state. The overall probability of failure is given by summing the probabilities of all the failure states. The dotted lines indicate recovery paths from earlier failures.

In numerical terms, the probability of each failure state is given by the following expressions (where SP is the success probability and HEP the human error probability at each node):

$$F1 = [SP\ 1.1 + HEP\ 1.1 \times SP\ 1.2] \times SP\ 1.3 \times SP\ 1.5 \times SP\ 1.6 \times SP\ 1.7 \times HEP\ 1.8$$
$$F2 = [SP\ 1.1 + HEP\ 1.1 \times SP\ 1.2] \times SP\ 1.3 \times SP\ 1.5 \times SP\ 1.6 \times HEP\ 1.7$$
$$F3 = [SP\ 1.1 + HEP\ 1.1 \times SP\ 1.2] \times SP\ 1.3 \times SP\ 1.5 \times HEP\ 1.6$$
$$F4 = [SP\ 1.1 + HEP\ 1.1 \times SP\ 1.2] \times SP\ 1.3 \times HEP\ 1.5$$
$$F5 = [SP\ 1.1 + HEP\ 1.1 \times SP\ 1.2] \times HEP\ 1.3 \times HEP\ 1.4$$
$$F6 = HEP\ 1.1 \times HEP\ 1.2$$

Total failure probability T is given by

$$T = F1 + F2 + F3 + F4 + F5 + F6$$

Further details about fault tree and event tree applications in quantitative risk assessment (QRA) are given in CCPS (1989b).

5.7. QUANTIFICATION

Because most research effort in the human reliability domain has focused on the quantification of error probabilities, a large number of techniques exist. However, a relatively small number of these techniques have actually been applied in practical risk assessments, and even fewer have been used in the CPI. For this reason, in this section only three techniques will be described in detail. More extensive reviews are available from other sources (e.g., Kirwan et al., 1988; Kirwan, 1990; Meister, 1984). Following a brief description of each technique, a case study will be provided to illustrate the application of the technique in practice. As emphasized in the early part of this chapter, quantification has to be preceded by a rigorous qualitative analysis in order to ensure that all errors with significant consequences are identified. If the qualitative analysis is incomplete, then quantification will be inaccurate. It is also important to be aware of the limitations of the accuracy of the data generally available

Next Page