Previous Page

to be asked and the contextual information that should be collected in order to establish root causes and therefore develop effective remedial strategies. In the longer term, it also provides the basis for the evaluation of the effectiveness of these strategies by indicating if the same underlying causes recur even after error reduction measures are implemented (see Chapter 6).

The use of a model of human error allows a systematic approach to be adopted to the prediction of human failures in CPI operations. Although there are difficulties associated with predicting the precise forms of mistakes, as opposed to slips, the cognitive approach provides a framework which can be used as part of a comprehensive qualitative assessment of failure modes. This can be used during design to eliminate potential error inducing conditions. It also has applications in the context of CPQRA methods, where a comprehensive qualitative analysis is an essential precursor of quantification. The links between these approaches and CPQRA will be discussed in Chapter 5.

2.7. THE SOCIOTECHNICAL PERSPECTIVE

The approaches described so far tackle the problem of error in three ways. First, by trying to encourage safe behavior (the traditional safety approach), second by designing the system to ensure that there is a match between human capabilities and systems demands (the human factors engineering approach) and third by understanding the underlying causes of errors, so that error inducing conditions can be eliminated at their source (the cognitive modeling approach). These strategies provide a technical basis for the control of human error at the level of the individual worker or operating team.

The control of human error at the most fundamental level also needs to consider the impact of management policy and organizational culture. The concepts introduced in Chapter 1, particularly the systems-induced error approach, have emphasized the need to go beyond the direct causes of errors, for example, overload, poor procedures, poor workplace design, to consider the underlying organizational policies that give rise to these conditions. Failures at the policy level which give rise to negative performance-influencing factors at the operational level are examples of the latent management failures discussed in Chapter 1 and in Section 2.2.2.

Another way in which management policies affect the likelihood of error is through their influence on organizational culture. For example, a culture may arise at the operational level where the achievement of production objectives is given greater emphasis than safe practices. Of course, no responsible company would sanction such a situation if they knew it existed. However, without effective communications or incident feedback systems, management may never realize that safety is being compromised by an inappropriate culture and the working practices it produces.

Studies of major accidents have shown that they almost always arise from a combination of active errors, latent failures and inappropriate culture. Examples of such analyses from the sociotechnical perspective are available from a number of sources, for example, Reason (1990), Rasmussen (1990), Wagenaar and Groenweg (1987), and Kletz (1994a). These analyses have considered accidents as diverse as Three Mile Island, Chernobyl, the *Challenger* Space Shuttle, Bhopal, Flixborough, and Piper Alpha. Although these accidents may appear to be far removed from the day-to-day concerns of a plant manager in the CPI, they indicate the need to look beyond the immediate precursors of accidents to underlying systemic causes. Methods for addressing these issues during the retrospective analysis of incidents are discussed in Chapter 6.

2.7.1. The TRIPOD Approach

From the point of view of accident prevention, approaches have been developed which seek to operate at the level of organizational factors affecting error and accident causation. One of the most extensive efforts has been the development of the TRIPOD system with the support of the Shell International Petroleum Company. In this system, the direct causes of errors leading to accidents are called "tokens" and the generic management level factors that create latent failure conditions are called "general failure types." (See Wagenaar et al., 1990, and Wagenaar, 1992, for a more detailed description.)

These general failure types are used to produce profiles which indicate the accident potential of a facility on a number of dimensions. An example of these profiles is shown in Figure 2.10 (from Wagenaar, 1992). Scores on these factors are derived from checklists which comprise a series of yes/no questions concerning relevant "indicators." For example, whether or not people have worked 24 hours continuously is taken as an indicator of increased error likelihood. Such a question would be one component of the general failure type "error enforcing conditions." There is a list of questions corresponding to each of the general failure types, which varies depending on the nature of the activity, country or ethnic culture. In the terminology of this book, TRIPOD provides an auditing method which can be used to identify negative performanc-e influencing factors. Those factors which score poorly are used to guide subsequent corrective actions. Wagenaar (1992) states that analyses of accident data show that situations where accidents occur correlate highly with poor scores on the general failure type profiles.

The benefits claimed for the TRIPOD approach are that it provides a consistent method for auditing a situation to identify deficiencies in the factors that are likely to give rise to errors. These deficiencies can then be corrected to reduce the likelihood of accidents occurring in the future.

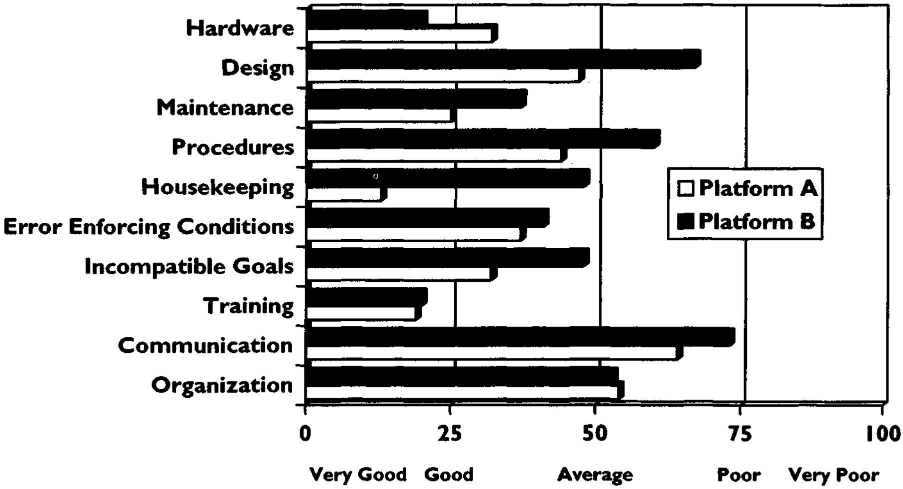


FIGURE 2.10 **TRIPOD Failure-State Profiles of Two Production Platforms (Wagenaar, 1992).**

2.7.2. Human Factors Analysis Methodology

Another strategic initiative in this area is the development of a human factors analysis methodology (HFAM) by a U.S.-based multinational chemical processing company. Preliminary descriptions of this approach are available in Pennycook and Embrey (1993). This methodology is based on the systems-induced error philosophy set out in this book. This states that control of error can be most effectively achieved by attacking the environmental or system causes of error which are under the control of management rather than trying to change behavior directly. HFAM has a similar philosophy to TRIPOD in that it defines a comprehensive set of factors which together address the primary system causes of error. These factors in turn are broken down into a series of diagnostic questions which can be used to make numerical assessments of the dimensions which make up the higher level factors. The current set of factors that make up the HFAM tool are given in Figure 2.11. It can be seen that the factors can be divided into three groups, management level, generic, and job specific.

HFAM has 20 groups of factors instead of the 10 general failure types of the TRIPOD approach. The reason for this is that all of the 10 TRIPOD GFTs would be applied in all situations, even though the actual questions that make up the factors may vary. In the case of HFAM, it would be rare to apply all of the factors unless an entire plant was being evaluated. HFAM uses a screening process to first identify the major areas vulnerable to human error. The generic factors and appropriate job specific factors are then applied to these areas. For example, control room questions would not be applied to maintenance jobs.

MANAGEMENT-LEVEL FACTORS	OPERATIONAL-LEVEL GENERIC FACTORS	OPERATIONAL-LEVEL JOB-SPECIFIC FACTORS
• Safety priorities • Degree of participation • Effectiveness of communications • Effectiveness of incident investigation • Effectiveness of procedures development system • Effectiveness of training system • Effectiveness of design policies	• Process management • Job design and work planning • Safe systems of work • Emergency response plan • Training • Work group factors • Work patterns • Stress factors • Individual factors • Job aids and procedures	• Computer-based systems • Control panel design • Field workplaces • Maintenance

FIGURE 2.11 **Factors in Human Factors Assessment Methodology.**

The components of each factor can be evaluated at two levels of detail. An example of these levels for the factor "Procedures and Job Aids" is provided in Figure 2.12. If the question indicates that the first level (e.g., content and reliability) is deemed to be inadequate then more questions are available at the next level of detail (the topic level) to provide additional information on the nature of the problem. For each topic, further questions are provided at a greater level of detail. These detailed questions (diagnostics) are intended to pinpoint the precise nature of a deficiency and also to provide insights for remedial action.

Problems identified at the operational level by the generic and job specific factors are regarded as being indicative of a failure of management level controls of that factor. The corresponding management level factor would then be evaluated to identify the nature of this latent failure. Although specific human factors design deficiencies might be identified at the operational level (e.g., inadequacies in control panel design, poor procedures), inadequacies within the higher level management factor, for example, "Effectiveness of design policies affecting human error" would affect a number of the operational level situations. Thus, the process of remedying the problem would not be confined to addressing the specific operational deficiencies identified but would also consider the changes in management policies needed to address these deficiencies across the whole site (or even the company). Figure 2.12 provides an example of how the system can be applied.

In addition to the management level factors which can be specifically linked to operational level factors (procedures, training, and design), the HFAM tool also provides an assessment of other management level factors which will impact upon error likelihood in a less direct way. Some of these factors, for example, "safety priorities" and "degree of participation," are

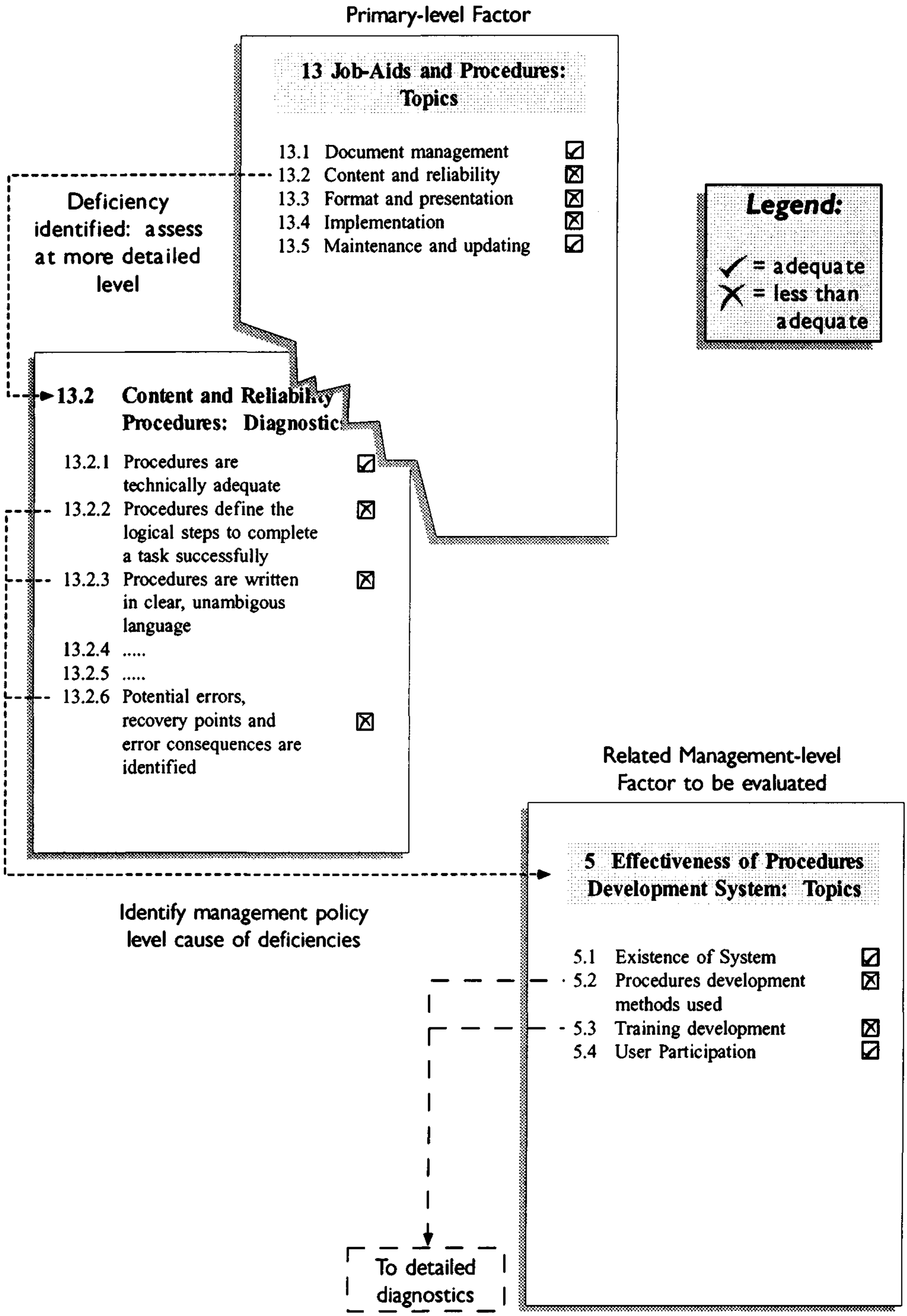

Primary-level Factor
13 Job-Aids and Procedures: Topics
13.1 Document management ☑
13.2 Content and reliability ☒
13.3 Format and presentation ☒
13.4 Implementation ☒
13.5 Maintenance and updating ☑
Legend:
✓ = adequate
✗ = less than adequate
Deficiency identified: assess at more detailed level
13.2 Content and Reliability Procedures: Diagnostic
13.2.1 Procedures are technically adequate ☑
13.2.2 Procedures define the logical steps to complete a task successfully ☒
13.2.3 Procedures are written in clear, unambigous language ☒
13.2.4 .....
13.2.5 .....
13.2.6 Potential errors, recovery points and error consequences are identified ☒
Related Management-level Factor to be evaluated
Identify management policy level cause of deficiencies
5 Effectiveness of Procedures Development System: Topics
5.1 Existence of System ☑
5.2 Procedures development methods used ☒
5.3 Training development ☒
5.4 User Participation ☑
To detailed diagnostics

FIGURE 2.12 **Example of use of HFAM tool for evaluation (Pennycook et al., 1993).**

intended to address conditions that have been found to be good indicators of the quality of the safety culture. The remaining factors, "communications" and "incident investigation" are intended to provide an indication of how effectively information is transmitted vertically and horizontally in the organization, and the capability of the organization to learn lessons from operational experience.

2.7.3 The UK Health & Safety Executive Research Program on Sociotechnical Systems

A program of research has been supported for several years by the United Kingdom Health & Safety Executive (HSE) to address the effects of sociotechnical factors on risk in the CPI. The initial emphasis of this work was to develop a methodology so that chemical process quantitative risk analysis (CPQRA) would take into account the effects of the quality of the management factors of plant being assessed. This work has been described in a series of publications (e.g., Bellamy et al., 1990; Hurst et al., 1991; Geyer et al., 1990; and Hurst et al., 1992).

The project began with an extensive evaluation of 900 reported incidents involving failures of fixed pipework on chemical and major hazard plant. As part of the analysis a failure classification scheme was developed which considered the chief causes of failures, the possible prevention or recovery mechanism that could have prevented the failure and the underlying cause. The classification scheme is summarized in Figure 2.13. A typical event classification would be

> **Corrosion** *(direct cause)* due to **Design error** *(basic or root cause)*
> not recovered by **Inspection** *(failure of recovery)*

These results, together with other research on reactor failures assisted in the development of an audit tool called MANAGER, based on the model shown in Figure 2.14. This allowed an assessment to be made of the different levels of engineering and Sociotechnical factors contributing to the overall risk for a particular plant. The results of this audit process are used to generate a Management Factor for the facility. This is then used to modify the overall risk estimates calculated by traditional CPQRA approaches (e.g., the fault tree analysis) by a factor varying between 10^{-1} and 10^{-3}.

Although the main thrust of the HSE work is directed to providing inputs to the CPQRA process, the audit procedure generates valuable qualitative information regarding both the quality of the overall plant management and also the specific human factors dimensions which affect risk.

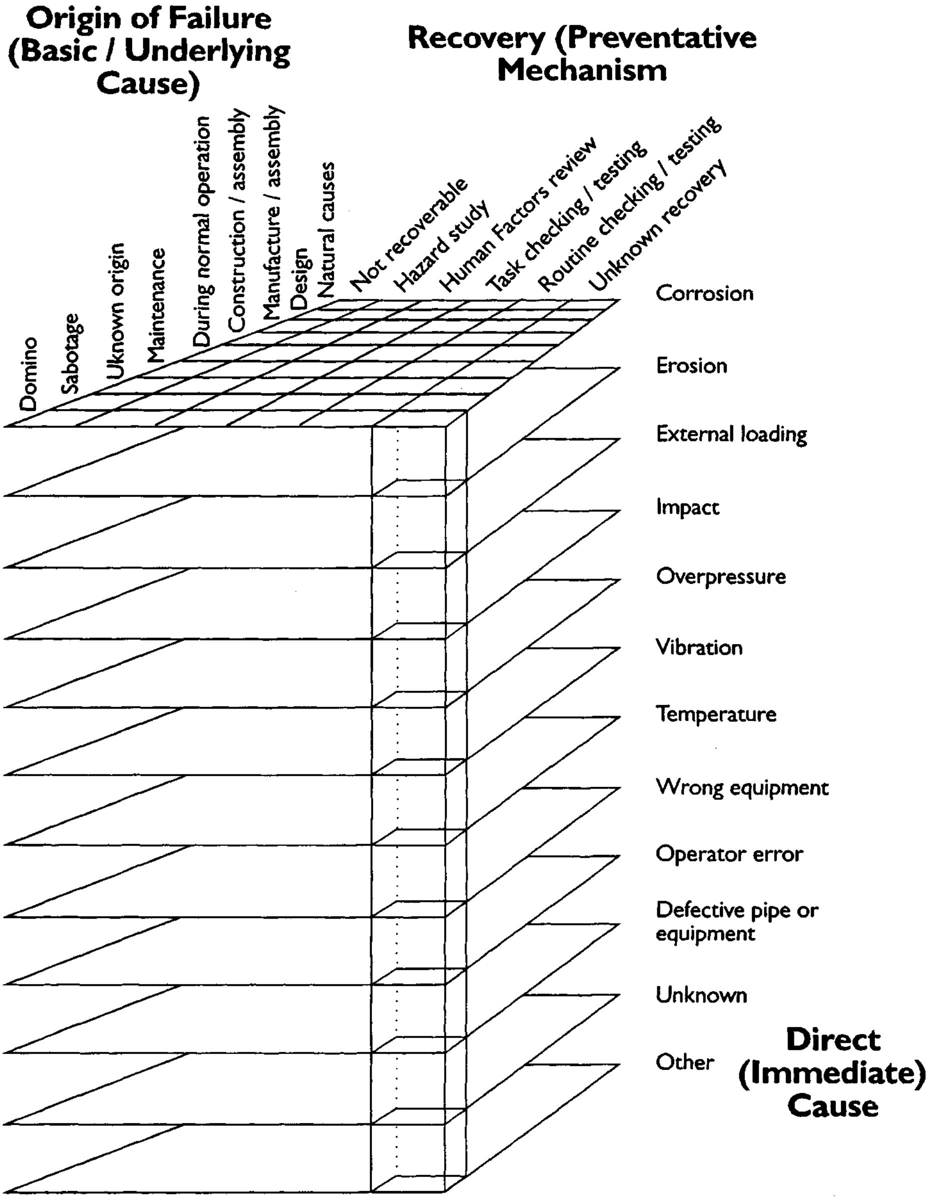


FIGURE 2.13. **Classification of Causal Factors (from Hurst et al., 1992).**

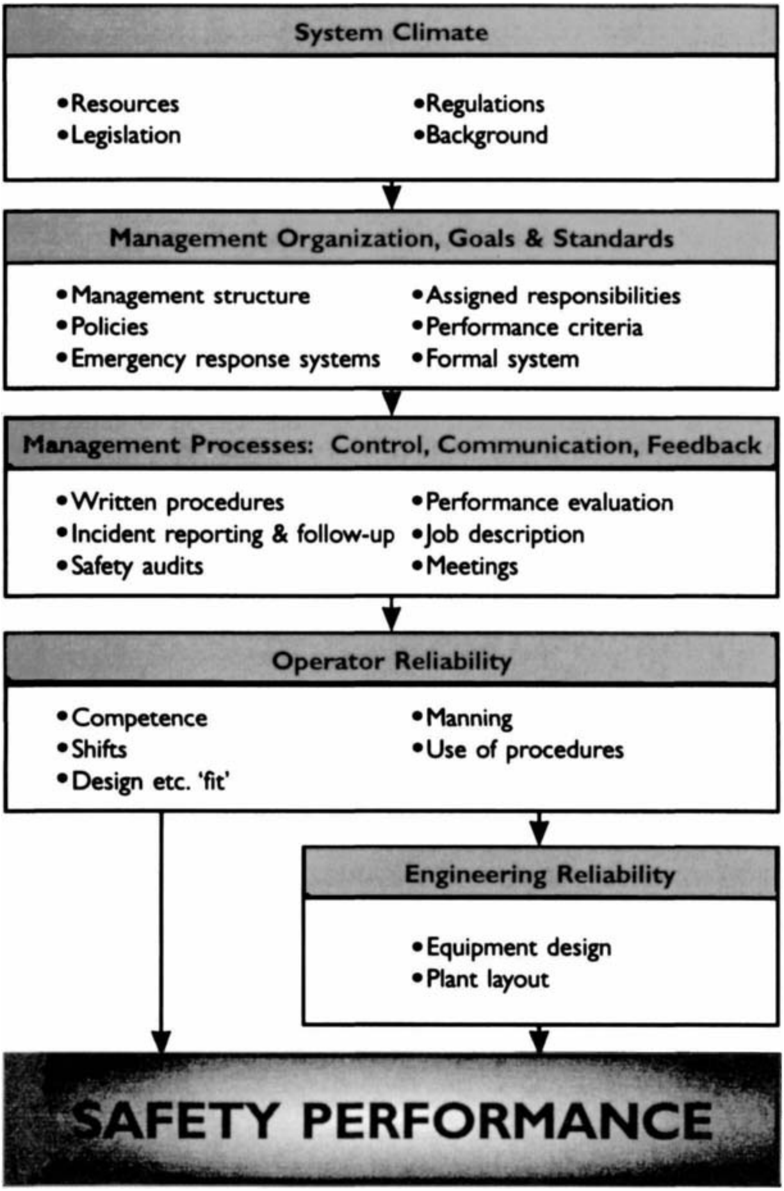


FIGURE 2.14 **Sociotechnical Model Underlying Audit Tool (from Hurst et al., 1992).**

2.7.4. Comparisons among the Sociotechnical Approaches

The similarities between TRIPOD and HFAM are considerable in that they are both based on a systems view of error, and the importance of policy in influencing the immediate causes of error. They have also both been developed iteratively, ιısing extensive field trials. Although both systems are ultimately directed at the reduction of human error leading to accidents, there are differences as how they are applied. It appears that TRIPOD is mainly intended as a proactive evaluation tool which will be used by auditors to evaluate sites and recommend improvement strategies. By contrast, the initial focus of HFAM is to encourage operations staff to evaluate their own environments to identify error potential and develop appropriate remedial strategies. By this means, it is hoped to encourage active participation by individuals with a strong stake in accident prevention as part of the process of continuous improvement. Although both systems are primarily directed at error prevention, they can also be applied as part of the retrospective analysis of accidents that have already occurred.

The focus of MANAGER is somewhat different, in that it was primarily developed to provide a numerical output for use in risk assessment. Nevertheless, the qualitative dimensions included in the audit trail will undoubtedly provide information which can be used as part of an error prevention program.

The fact that these systems exist and have been given considerable support by companies and regulators in the CPI, must be taken as a positive indication of an increasing realization of the importance of human performance in ensuring safe and profitable operation of chemical facilities.

2.8. SUMMARY

The intention of this chapter has been to provide an overview of the wide range of strategies available to the CPI for the management of error. The traditional safety approach described in Section 2.4 concentrates on modifying individual behavior, and has been successful in many areas of occupational safety. Section 2.4 provided a review of some of the methods used in this approach and assessed their effectiveness. Section 2.5 considered some of the major technical issues within the human factors engineering approach. Detailed description of the various design approaches and techniques for the optimization of human performance that have emerged from this perspective, will be considered in Chapter 4. The cognitive modeling perspective reviewed in Section 2.6 provides an approach to modeling human errors that can be applied both at the design stage and for deriving the root causes of errors. Both of these applications will be developed in later chapters. Section 2.7 reviewed the organizational perspective, and emphasized the need for error reduction techniques to be supported by a consideration of the role of management policies in influencing the immediate causes of errors—a description was provided of three approaches that have been developed by chemical companies and regulators to provide comprehensive systems for managing error in the CPI.

2.9. APPENDIX 2A: PROCESS PLANT EXAMPLE OF THE STEPLADDER MODEL

In order to explain each box in the stepladder model shown in Figure 2.7 (reprinted on the facing page), we shall use the same batch processing example as in Section 2.6.3.

> *Consider a process worker monitoring a control panel in a batch processing plant. The worker is executing a series of routine operations such as opening and closing valves and turning on agitators and heaters.*

Alert (need for investigation)
An alarm sounds which indicates a problem.

Observe (what is abnormal?)
Scan information sources (dials, chart recorders, etc.). If the pattern of indicators is very familiar, the worker will probably immediately branch to the Execute Actions box (via the thin arrow) and make the usual response to this situation (e.g., pressing the alarm accept button if the indications suggest a nonsignificant event).

Identify Plant State
If the pattern does not fit into an immediately identifiable pattern, the process worker may then consciously apply more explicit "if–then" rules to link the various symptoms with likely causes. Three alternative outcomes are possible from this process. If the diagnosis and the required actions are very closely linked (because this situation arises frequently) then a branch to the Execute Actions box will occur. If the required action is less obvious, then the branch to the Select/Formulate Actions box will be likely, where specific action rules of the form: "if situation is X then do Y" will be applied. A third possibility is that the operating team are unable or unwilling to respond immediately to the situation because they are uncertain about its implications for safety and/or production. They will then move to the Implications of plant state box.

Implications of Plant State
At this stage the implications of the situation will be explored, using the operating team's general functional knowledge of the process. This explicit

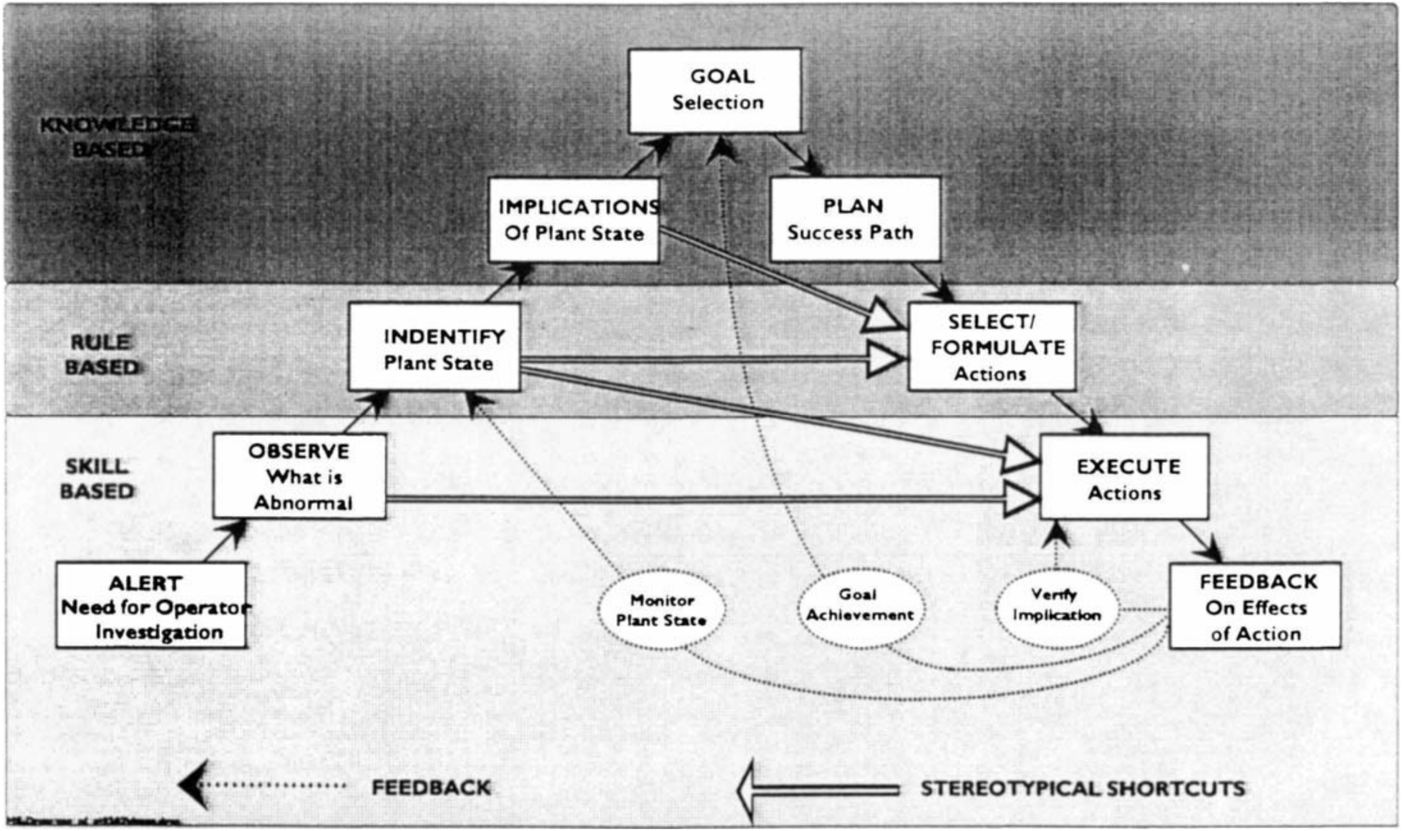


FIGURE2.7. **Decision-Making Model including Feedback (adapted from Rasmussen, 1986).**

evaluation procedure is classified as occurring in the knowledge-based domain, whereas the previous stage was rule based. If the required response to the situation is obvious, that is, there are no alternative goals, then the sequence branches to the Select/Formulate Actions box, where the required actions to achieve the objective are formulated and then acted upon in the Execute Actions box.

Goal Selection

During the goal selection stage, the operating team consider alternative objectives which they might wish to achieve. For example, if their assessment of the situation suggested that there was a major potential explosion hazard, then their objective would probably be to shut down the system as quickly as possible. If, on the other hand, the batch was simply off-specification as a result of the abnormal conditions, the strategy of mixing the batch with other batches in a blender might be considered.

Plan Success Path

Having decided on an appropriate objective, the next stage is to plan how to get from the current plant state to the required objective. This could involve deciding whether or not the batch requires cooling, how this would be achieved, what cross couplings are available to connect the reactor to a blender and so on.

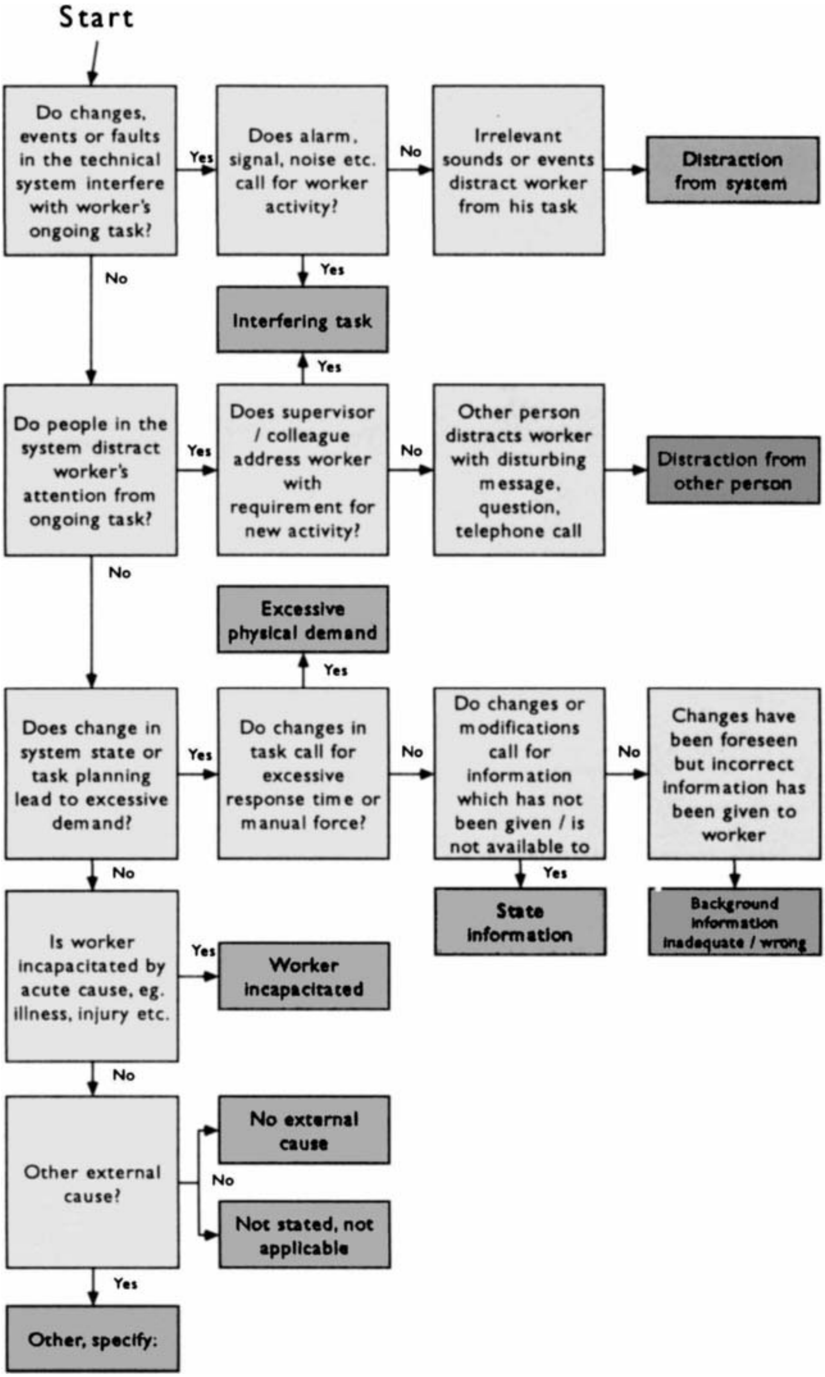
Select/Formulate Actions

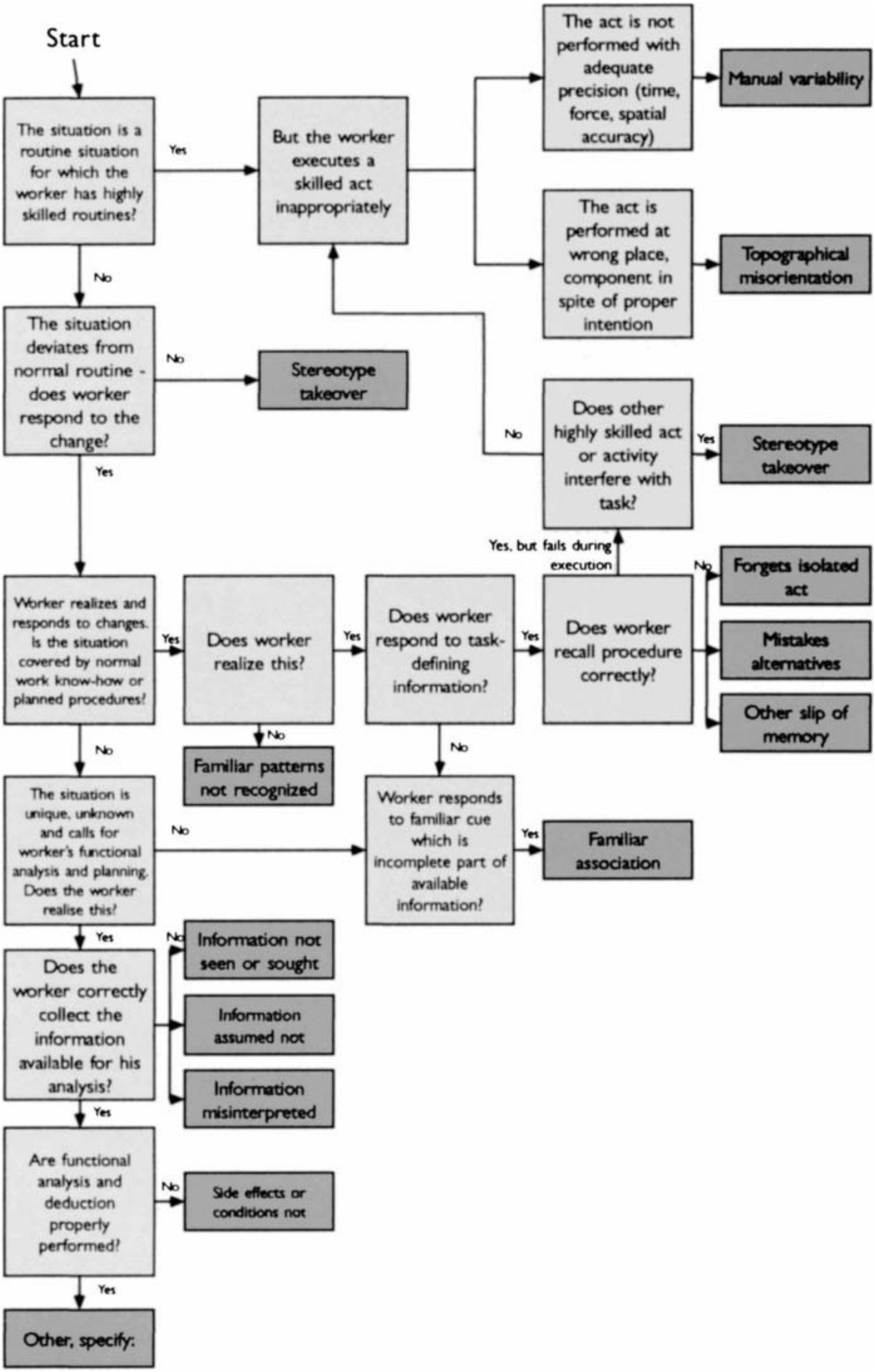
This step involves the formulation of a specific procedure or action sequence to achieve the plan decided upon at the previous stage. This may involve the linking together of an existing set of generic procedures which are employed in a variety of situations (e.g., executing a blowdown sequence). This phase uses action rules of the form "if Y then do Z" as opposed to the diagnostic rules of the "Identify Plant State" box, which is the other component of rule-based processing.

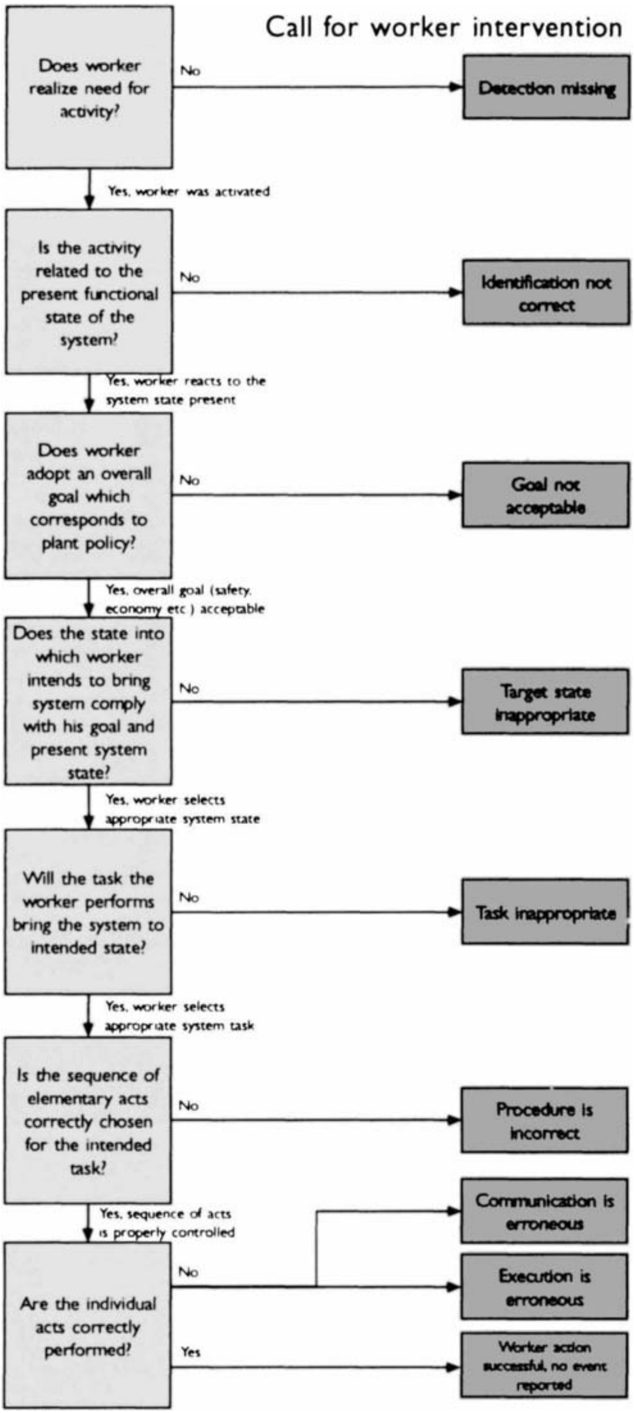
Execute Actions

This box, which is self-explanatory, involves highly practiced actions in the skill-based domain.

2.10. APPENDIX 2B: FLOWCHARTS FOR USING THE RASMUSSEN SEQUENTIAL MODEL FOR INCIDENT ANALYSIS (Petersen, 1985)


Start
Do changes, events or faults in the technical system interfere with worker's ongoing task?
Yes
Does alarm, signal, noise etc. call for worker activity?
No
Irrelevant sounds or events distract worker from his task
Distraction from system
Yes
Interfering task
No
Yes
Do people in the system distract worker's attention from ongoing task?
Yes
Does supervisor / colleague address worker with requirement for new activity?
No
Other person distracts worker with disturbing message, question, telephone call
Distraction from other person
No
Excessive physical demand
Yes
Does change in system state or task planning lead to excessive demand?
Yes
Do changes in task call for excessive response time or manual force?
No
Do changes or modifications call for information which has not been given / is not available to
No
Changes have been foreseen but incorrect information has been given to worker
No
Yes
State information
Background information inadequate / wrong
Is worker incapacitated by acute cause, eg. illness, injury etc.
Yes
Worker incapacitated
No
Other external cause?
No external cause
No
Not stated, not applicable
Yes
Other, specify:


Start
The situation is a routine situation for which the worker has highly skilled routines?
Yes
But the worker executes a skilled act inappropriately
The act is not performed with adequate precision (time, force, spatial accuracy)
Manual variability
The act is performed at wrong place, component in spite of proper intention
Topographical misorientation
No
The situation deviates from normal routine - does worker respond to the change?
No
Stereotype takeover
Does other highly skilled act or activity interfere with task?
No
Yes
Stereotype takeover
Yes, but fails during execution
Yes
Worker realizes and responds to changes. Is the situation covered by normal work know-how or planned procedures?
Yes
Does worker realize this?
Yes
Does worker respond to task-defining information?
Yes
Does worker recall procedure correctly?
No
Forgets isolated act
Mistakes alternatives
Other slip of memory
No
Familiar patterns not recognized
No
No
The situation is unique, unknown and calls for worker's functional analysis and planning. Does the worker realise this?
No
Worker responds to familiar cue which is incomplete part of available information?
Yes
Familiar association
Yes
Does the worker correctly collect the information available for his analysis?
No
Information not seen or sought
Information assumed not
Information misinterpreted
Yes
Are functional analysis and deduction properly performed?
No
Side effects or conditions not
Yes
Other, specify:


Call for worker intervention
Does worker realize need for activity?
No
Detection missing
Yes, worker was activated
Is the activity related to the present functional state of the system?
No
Identification not correct
Yes, worker reacts to the system state present
Does worker adopt an overall goal which corresponds to plant policy?
No
Goal not acceptable
Yes, overall goal (safety, economy etc.) acceptable
Does the state into which worker intends to bring system comply with his goal and present system state?
No
Target state inappropriate
Yes, worker selects appropriate system state
Will the task the worker performs bring the system to intended state?
No
Task inappropriate
Yes, worker selects appropriate system task
Is the sequence of elementary acts correctly chosen for the intended task?
No
Procedure is incorrect
Yes, sequence of acts is properly controlled
Are the individual acts correctly performed?
No
Communication is erroneous
Execution is erroneous
Yes
Worker action successful, no event reported

2.11. APPENDIX 2C: CASE STUDY ILLUSTRATING THE USE OF THE SEQUENTIAL MODEL OF ERROR IN INCIDENT ANALYSIS

A process worker is monitoring the rise in temperature in reactor A. An exothermic reaction occurs producing an alarm requiring the opening of a valve on a circuit which provides cooling water to the reactor. Instead of opening the correct valve, he operates another valve for reactor B, which is the reactor which he monitors on most shifts. Reactor A is destroyed by a runaway reaction.

Initiating Event

At the time that the alarm occurred, the worker was helping a colleague to fix a problem on an adjacent panel. The initiating event was therefore a distraction from another person (see Figure 2.15).

Internal Error Mechanism

Internal error mechanisms can be regarded as intrinsic human error tendencies. The particular error mechanisms that will be triggered depend on the performance-influencing factors (PIFs) in the situation (see Chapter 3). However, use of Figure 2.16 allows certain preliminary conclusions to be drawn.

The fact that the worker normally operated reactor B, and he reverted to this operating mode when distracted, indicates that the internal error mechanism was a **Stereotype Takeover**.

It can be seen that the various boxes in the flowchart can be associated with different stages of the stepladder model. For example, the first box on the left corresponds to skill-based behavior and its associated internal failure mechanisms. The second box illustrates the situation (Stereotype Fixation) where the worker erroneously does not change to a rule-based mode when encountering an unusual situation in the skill-based mode (see also the discussion of the GEMS model in Section 2.6.3).

Performance-Influencing Factors

Performance-influencing factors are general conditions which increase or decrease the likelihood of specific forms of error. They can be broadly grouped into the following categories:

- Operating environment (e.g., physical work environment, work patterns)
- Task characteristics (e.g., equipment design, control panel design, job aids)
- Operator characteristics (e.g., experience, personality, age)
- Organizational and social factors (e.g., teamwork, communications)

All of these factors can influence both the likelihood of various internal error mechanisms, and also the occurrence of specific initiating events. (See Chapter 3 for a comprehensive description of PIFs.)

The PIFs increased the likelihood of the strong stereotype takeover in the case study were the fact that the worker was more used to operating the valve for reactor B than reactor A, together with the distracting environment. In addition, the panel was badly designed ergonomically, and valves A and B were poorly labeled and quite close physically. On the basis of the evaluation of the PIFs in the situation, the internal error mechanisms could be stereotype takeover or spatial misorientation.

Internal Error Mode

This is the actual mental function required by the task that failed (see Figure 2.17). In the case study under consideration the failure was at the **Execute Action** stage of the stepladder model, since the worker intended to operate the valve for reactor A, so there was no question of failure in the selection of actions. The connection with the task characteristics box indicates the fact that action is a function required by the task.

External Error Mode

The external error mode is the observable form of the error. This can often be classified in several ways. In the current example the external error modes were "right action on wrong object" (wrong valve closed) and "action omitted" (the correct valve was not closed). The exact form of the external error mode will obviously depend on the nature of the task. A comprehensive classification of external error modes is provided in Chapter 4.

Consequences

The consequences of an external error mode will depend on the context in which it occurs. Consequences for the same error may be trivial (near misses) or catastrophic, depending on the design of the plant and the recoverability of the error. In the example under consideration, a serious accident occurred.