1

Introduction: The Role of Human Error in Chemical Process Safety

1.1. INTRODUCTION

1.1.1. Objective

This book has been written to show how the science of human factors can be applied at the plant level to significantly improve human performance and reduce human error, thus improving process safety.

1.1.2. Scope and Organization

The application of the science of human factors to eliminating error in all aspects of process design, management, operation, and maintenance is the focus of this work. Human error has been a major cause of almost all of the catastrophic accidents that have occurred in the chemical process industries (CPI). If one adopts the broad view of human error as being the result of a mismatch between human capabilities and process demands, then clearly management's role is critical in the following areas:

- Defining the process
- Providing the resources to manage, operate, and maintain the process
- Setting up the feedback systems to monitor the processes which are critical to ensuring safe operation

The book begins with a discussion of the theories of error causation and then goes on to describe the various ways in which data can be collected, analyzed, and used to reduce the potential for error. Case studies are used to teach the methodology of error reduction in specific industry operations. Finally, the book concludes with a plan for a plant error reduction program and a discussion of how human factors principles impact on the process safety management system.

The book is organized as follows:

Chapter 1, *The Role of Human Error in Chemical Process Safety*, discusses the importance of reducing human error to an effective process safety effort at the plant. The engineers, managers, and process plant personnel in the CPI need to replace a perspective that has a blame and punishment view of error with a systems viewpoint that sees error as a mismatch between human capabilities and demands.

Chapter 2, *Understanding Human Performance and Error*, provides a comprehensive overview of the main approaches that have been applied to analyze, predict, and reduce human error. This chapter provides the reader with the underlying theories of human error that are needed to understand and apply a systems approach to its reduction.

Chapter 3, *Factors Affecting Human Performance in the Chemical Industry*, describes how a knowledge of "performance-influencing factors" (PIFs), can be used to identify and then eliminate error-causing conditions at the plant.

Chapter 4, *Analytical Methods for Predicting and Reducing Human Error*, contains a discussion and critique of the various methods that are available for analyzing a process for its potential for human error.

Chapter 5, *Quantitative and Qualitative Prediction of Human Error in Safety Assessments*, describes a systematic process for identifying and assessing the risks from human error, together with techniques for quantifying human error probabilities.

Chapter 6, *Data Collection and Incident Analysis Methods*, examines the pitfalls involved in collecting data on human error and suggests possible approaches to improving the quality of the data.

Chapter 7, *Case Studies*, uses examples that illustrate the application of the various error analysis and reduction techniques to real world process industry cases.

Chapter 8, *A Systematic Approach to the Management of Human Error*, explains how the manager and safety professional can use human factors principles in the management of process safety. This chapter also provides a practical plan for a plant human error reduction program that will improve productivity and quality as well.

1.1.3. Purpose of This Book

The objectives of this book are ambitious. It is intended to provide a comprehensive source of knowledge and practical advice that can be used to substantially reduce human error in the CPI. The following sections describe how this is achieved.

1.1.3.1. Consciousness Raising

A major objective is to provide engineers, managers, and process plant personnel in the CPI with an entirely new perspective on human error. In particular, the intention is to change the attitudes of the industry such that human error is removed from the emotional domain of blame and punishment. Instead, a systems perspective is taken, which views error as a natural consequence of a mismatch between human capabilities and demands, and an inappropriate organizational culture. From this perspective, the factors that directly influence error are ultimately controllable by management. This book is intended to provide tools, techniques, and knowledge that can be applied at all levels of the organization, to optimize human performance and minimize error. One of the major messages of this book, with regard to implementing the ideas that it contains, is that methods and techniques will only be effective in the long term if they are supported by the active participation of the entire workforce. To this extent, the consciousness raising process has to be supported by training. The primary focus for raising the awareness of approaches to human error and its control is in Chapters 2 and 7.

1.1.3.2 Provision of Tools and Techniques

This book brings together a wide range of tools and techniques used by human factors and human reliability specialists, which have proved to be useful in the context of human performance problems in the CPI. Although many human factors practitioners will be familiar with these methods, this book is intended to provide ready access to both simple and advanced techniques in a single source. Where possible, uses of the techniques in a CPI context are illustrated by means of case studies.

Chapter 4 focuses on techniques which are applied to a new or existing system to optimize human performance or qualitatively predict errors. Chapter 5 shows how these techniques are applied to risk assessment, and also describes other techniques for the quantification of human error probabilities. Chapters 6 and 7 provide an overview of techniques for analyzing the underlying causes of incidents and accidents that have already occurred.

1.1.3.3 Provision of Solutions to Specific Problems

In addition to raising consciousness and acquainting the reader with a selection of tools for error reduction, this book is also intended to provide assistance in solving specific human error problems that the reader may be experiencing at the plant level. It should be emphasized that no textbook can substitute for appropriate training in human factors techniques or for the advice of human factors specialists. Readers requiring advice should contact professional bodies such as the Human Factors and Ergonomics Society (USA) or the Ergonomics Society (England) who have lists of qualified consultants.

However, given appropriate training, it is quite feasible for personnel such as engineers and process workers to apply techniques such as task analysis (Chapter 4) and audit methods (Chapter 3) to reducing error potential in the workplace.

1.1.3.4. Provision of a Database of Case Studies

The book provides a comprehensive set of examples and case studies that cover a wide variety of process plant situations. Some of these are intended to illustrate the range of situations where human error has occurred in the CPI (see Appendix 1). Other examples illustrate specific techniques (for example, Chapter 4 and Chapter 5). Chapter 7 contains a number of extended case studies intended to illustrate techniques in detail and to show how a range of different techniques may be brought to bear on a specific problem.

1.1.3.5 Cross-Disciplinary Studies

Although this book is primarily written for chemical process industry readers, it also provides a sufficiently wide coverage of methods, case studies and theory to be of interest to behavioral scientists wishing to specialize in process industry applications. Similarly, it is hoped that the a comprehensive description of current theory and practice in this area will stimulate interest in the engineering community and encourage engineers to gain a more in-depth knowledge of the topic. Overall, the intention is to promote the cross-disciplinary perspective that is necessary for effective problem solving in the real world environment.

1.1.3.6. A Complement to Other CCPS Publications

A final objective of this book is to complement other books in this series such as *Guidelines for Chemical Process Quantitative Risk Assessment* (CCPS, 1989b), *Guidelines for Investigating Chemical Process Incidents* (CCPS, 1992d), and *Plant Guidelines for the Technical Management of Chemical Process Safety* (CCPS, 1992a). In the latter volume, human factors was identified as one of twelve essential elements of process safety management. The application to this area of the concepts described in this book is addressed in Chapter 8.

1.2. THE ROLE OF HUMAN ERROR IN SYSTEM ACCIDENTS

After many years of improvements in technical safety methods and process design, many organizations have found that accident rates, process plant losses and profitability have reached a plateau beyond which further improvements seem impossible to achieve. Another finding is that even in organizations with good general safety records, occasional large scale disasters occur which shake public confidence in the chemical process industry. The common

factor in both of these areas is the problem of human error. The purpose of this book is to provide a coherent strategy, together with appropriate knowledge and tools, to maximize human performance and minimize human error.

Human rror is probably the major contributor to loss of life, injury to personnel and property damage in the CPI. Human error also has a significant impact on quality, production, and ultimately, profitability. The publication: *One Hundred Large Losses: A Thirty Year Review of Property Damage Losses in the Hydrocarbon Chemical Industries* (Garrison, 1989), documents the contribution of operational errors to the largest financial losses experienced in the CPI up to 1984. This showed that human errors (defined as errors made on-site that have directly given rise to the losses) account for $563 million of these losses and as such are the second highest cause. If this analysis included off-site errors (e.g., Flixborough, due to an engineering error) human error would be the predominant contributor to these losses. A more recent analysis from the same source, Garrison (1989), indicates that in the period 1985–1990, human error was a significant factor in more than $2 billion of property damage in the CPI. These results are not confined to companies in the West. A study by Uehara and Hasegawa of fire accidents in the Japanese chemical industry between 1968 and 1980 indicated that of a total of 120 accidents, approximately 45% were attributed to human error. If the improper design and materials categories are also assumed to be due to human error, this figure rises to 58%. Little change was observed in this proportion over the twelve years examined. Further details of the study, together with others which indicate the central importance of human error in CPI safety, are given in Table 1.1.

In addition to these formal studies of human error in the CPI, almost all the major accident investigations in recent years, for example, Texas City, Piper Alpha, the Phillips 66 explosion, Feyzin, Mexico City, have shown that human error was a significant causal factor at the level of design, operations, maintenance or the management of the process.

One of the central principles presented in this book is the need to consider the organizational factors that create the preconditions for errors, as well as their immediate causes. Figure 1.1 (adapted from Reason, 1990) illustrates the structure of a general industrial production system. In the context of the CPI, this diagram can be interpreted as representing a typical plant. The plant and corporate management levels determine conditions at the operational level that either support effective performance or give rise to errors. Some of the factors that influence these conditions are given in Figure 1.1.The safety beliefs and priorities of the organization will influence the extent to which resources are made available for safety as opposed to production objectives. Attitudes towards blame will determine whether or not the organization develops a blame culture, which attributes error to causes such as lack of motivation or deliberate unsafe behavior. Factors such as the degree of participation that is encouraged in the organization, and the quality of the communication be-

TABLE 1.1
Studies of Human Error in the CPI: Magnitude of the Human Error Problem

STUDY	RESULTS
Garrison (1989)	Human error accounted for $563 million of major chemical accidents up to 1984
Joshchek (1981)	80–90% of all accidents in the CPI due to human error
Rasmussen (1989)	Study of 190 accidents in CPI facility: Top 4 causes: • insufficient knowledge 34% • design errors 32% • procedure errors 24% • personnel errors 16%
Butikofer (1986)	Accidents in petrochemical and refinery units • equipment and design failures 41% • personnel and maintenance failures 41% • inadequate procedures 11% • inadequate inspection 5% • other 2%
Uehara and Hoosegow (1986)	Human error accounted for 58% of the fire accidents in refineries • improper management 12% • improper design 12% • improper materials 10% • misoperation 11% • improper inspection 19% • improper repair 9% • other errors 27%
Oil Insurance Association Report on Boiler Safety (1971)	Human error accounted for 73% and 67% of total damage for boiler start-up and on-line explosions, respectively.

tween different levels of management and the workforce, will have a major impact on the safety culture. The existence of clear policies that will ensure good quality procedures and training will also impact strongly on error likelihood.

The next level represents the organizational and plant design policies, which will also be influenced by senior management. The plant and corporate management policies will be implemented by line management. This level of management has a major impact on the conditions that influence error. Even if appropriate policies are adopted by senior management, these policies may be ineffective if they do not gain the support of line management. Factors that

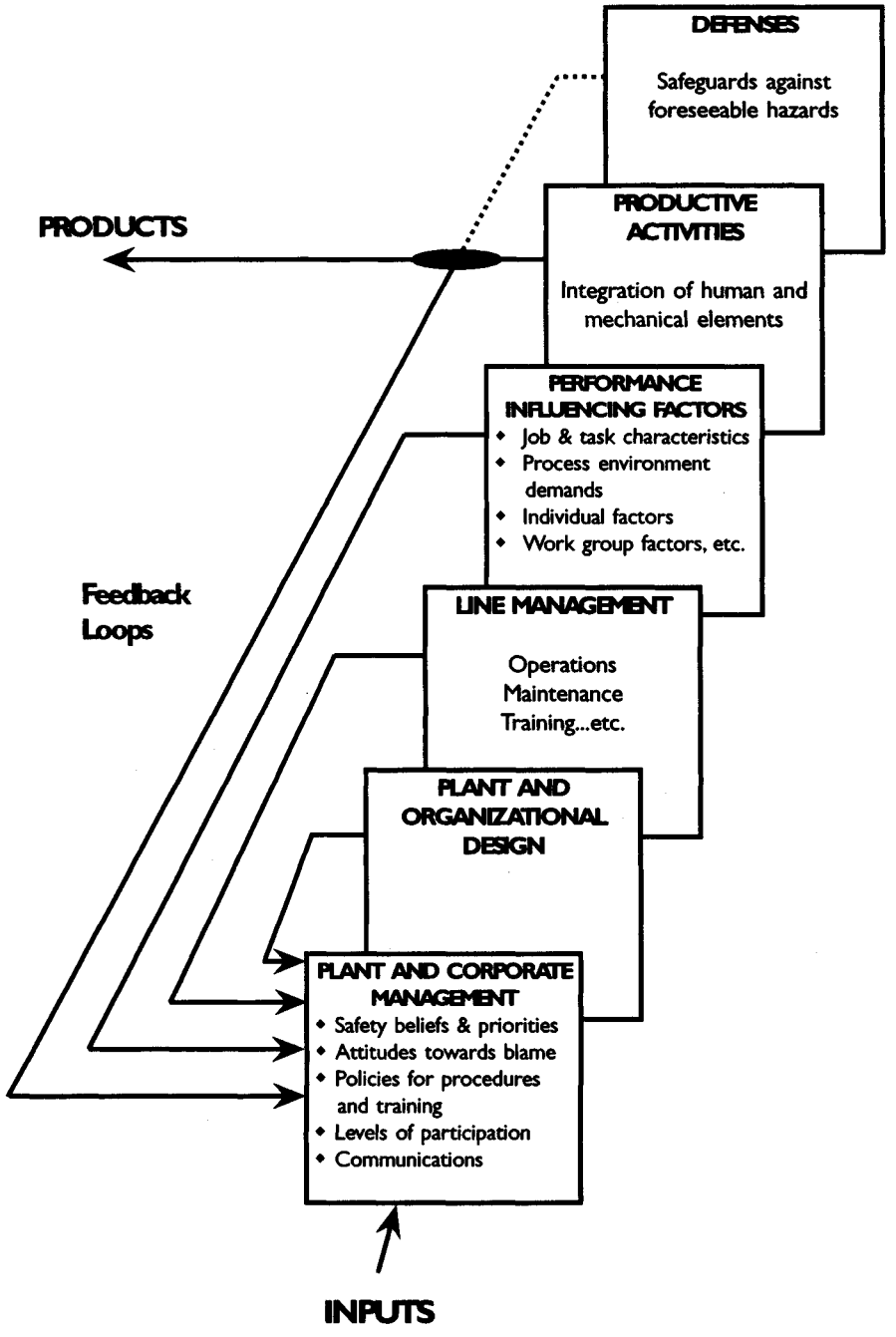

FIGURE 1.1 **Production System Structure (adapted from Reason 1990).**

directly affect error causation are located at the next level. These factors, which include the characteristics of the job performed by the worker (complexity, mental versus physical demands, etc.), and individual factors such as personality, and team performance factors, are called collectively performance-influencing factors, or PIFs. These factors are described in detail in Chapter 3.

The next layer in the production system structure represents the activities carried out at the plant level to make the product. These include a wide range of human interactions with the hardware. Physical operations such as opening and closing valves, charging reactors and carrying out repairs will be prominent in traditional, labor intensive, plants such as batch processing. In modern, highly automated plants, particularly those involving continuous production, there is likely to be a greater proportion of higher level "cognitive" skills involved such as problem solving, diagnosis, and decision making in areas such as process and production optimization. In all facilities, human involvement in areas such as maintenance and repairs is likely to be high.

The final elements of a production system represented in Figure 1.1 are the defenses against foreseeable hazards. These defenses exist in many forms. They may include engineered system features such as emergency shutdown systems, relief valves, bursting disks and valves or trips that operate on conditions such as high pressures or low flows. In addition to these hardware systems, the defenses also include human systems such as emergency response procedures, and administrative controls, such as work permits and training designed to give workers the capability to act as another line of defense against hazards.

The various feedback loops depicted in Figure 1.1 represent the information and feedback systems that should (but may not) exist to inform decision makers of the effectiveness of their policies. In Figure 1.2 the structure of Figure 1.1 is represented from the negative perspective of the conditions that can arise at various levels of the organization that will allow errors to occur with potentially catastrophic consequences. Inappropriate policies at the corporate level or inadequate implementation of correct policies by line management will create conditions at the operational level that will eventually result in errors. The term "latent failures" is used to denote states which do not in themselves cause immediate harm, but in combination with other conditions (e.g., local "triggers" such as plant disturbances) will give rise to active failures (e.g., "unsafe acts" such as incorrect valve operations or inadequate maintenance). If the system defenses (hardware or software) are also inadequate, then a negative or even catastrophic consequence may arise.

This model of accident causation is described further in Figure 1.3. This represents the defenses against accidents as a series of shutters (engineered safety systems, safety procedures, emergency training, etc.) When the gaps in these shutters come into coincidence then the results of earlier hardware or human failures will not be recovered and the consequences will occur. Inap-

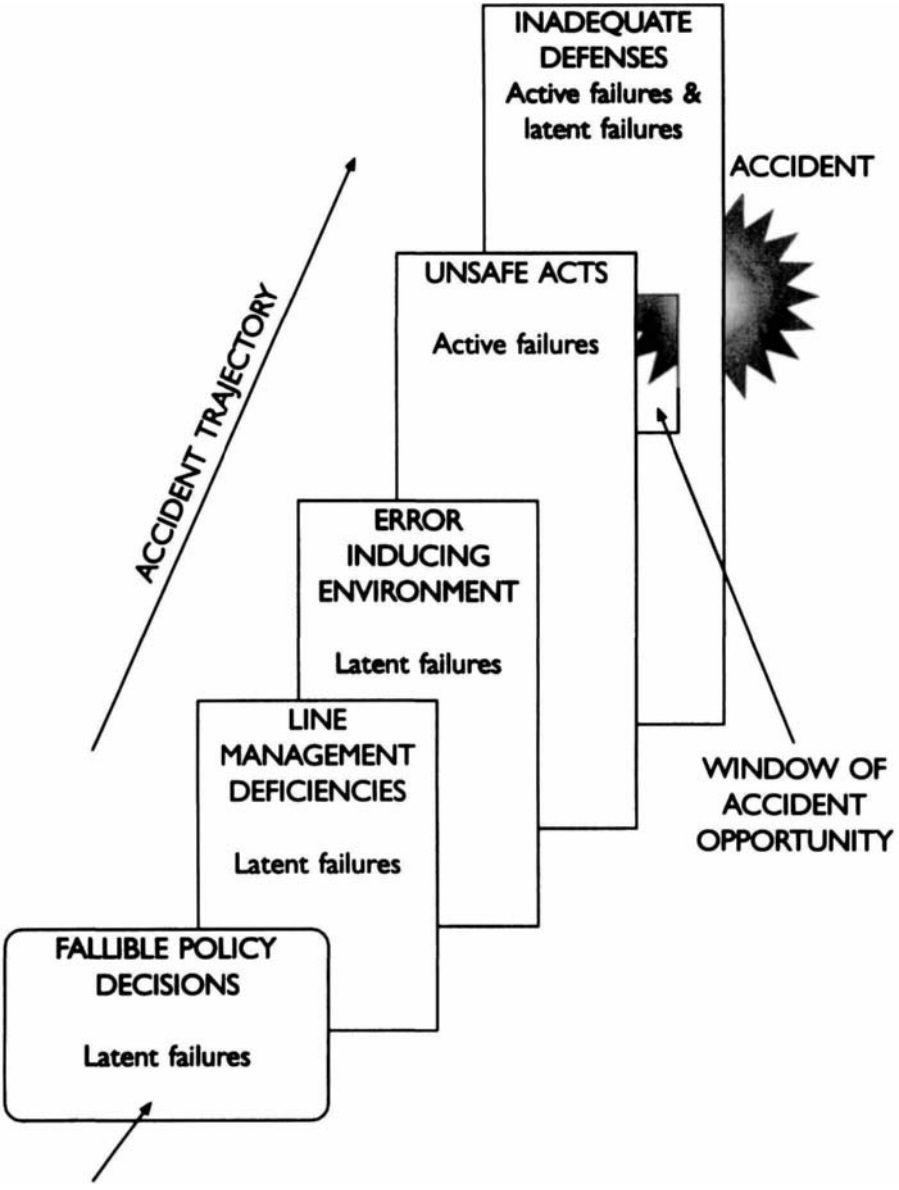

FIGURE 1.2 **Conditions Conducive to Accidents (adapted from Reason, 1990).**

propriate management policies create inadequate PIFs, which in turn give rise to a large number of opportunities for error, when initiated by local triggers or unusual conditions.

1.3. WHY IS HUMAN ERROR NEGLECTED IN THE CPI?

The evidence presented in the preceding section makes it clear that human performance problems constitute a significant threat to CPI safety. Despite this evidence, the study of human error has, in the past, been a much neglected area in the industry. There are several reasons for this neglect. Part of the problem is due to a belief among engineers and managers that human error is both inevitable and unpredictable. In subsequent chapters this assumption will be challenged by showing that human error is only inevitable if people are placed in situations that emphasize human weaknesses and do not support human strengths.

Another barrier to a systematic consideration of human error is the belief that increasing computerization and automation of process plants will make the human unnecessary. The fallacy of this belief can be shown from the numerous accidents that have arisen in computer controlled plants. In addition, considerable human involvement will continue to be necessary in the critical areas of maintenance and plant modification, even in the most automated process (see Chapter 2 for a further discussion of this issue).

Human error has often been used as an excuse for deficiencies in the overall management of a plant. It may be convenient for an organization to attribute the blame for a major disaster to a single error made by a fallible process worker. As will be discussed in subsequent sections of this book, the individual who makes the final error leading to an accident may simply be the final straw that breaks a system already made vulnerable by poor management.

A major reason for the neglect of human error in the CPI is simply a lack of knowledge of its significance for safety, reliability, and quality. It is also not generally appreciated that methodologies are available for addressing error in a systematic, scientific manner. This book is aimed at rectifying this lack of awareness.

1.4. BENEFITS OF IMPROVED HUMAN PERFORMANCE

The major benefits that arise from the application of human factors principles to process operations are improved safety and reduced down time. In addition, the elimination of error has substantial potential benefits for both quality and productivity. There is now a considerable interest in applying quality management approaches in the CPI. Many of the major quality experts em-

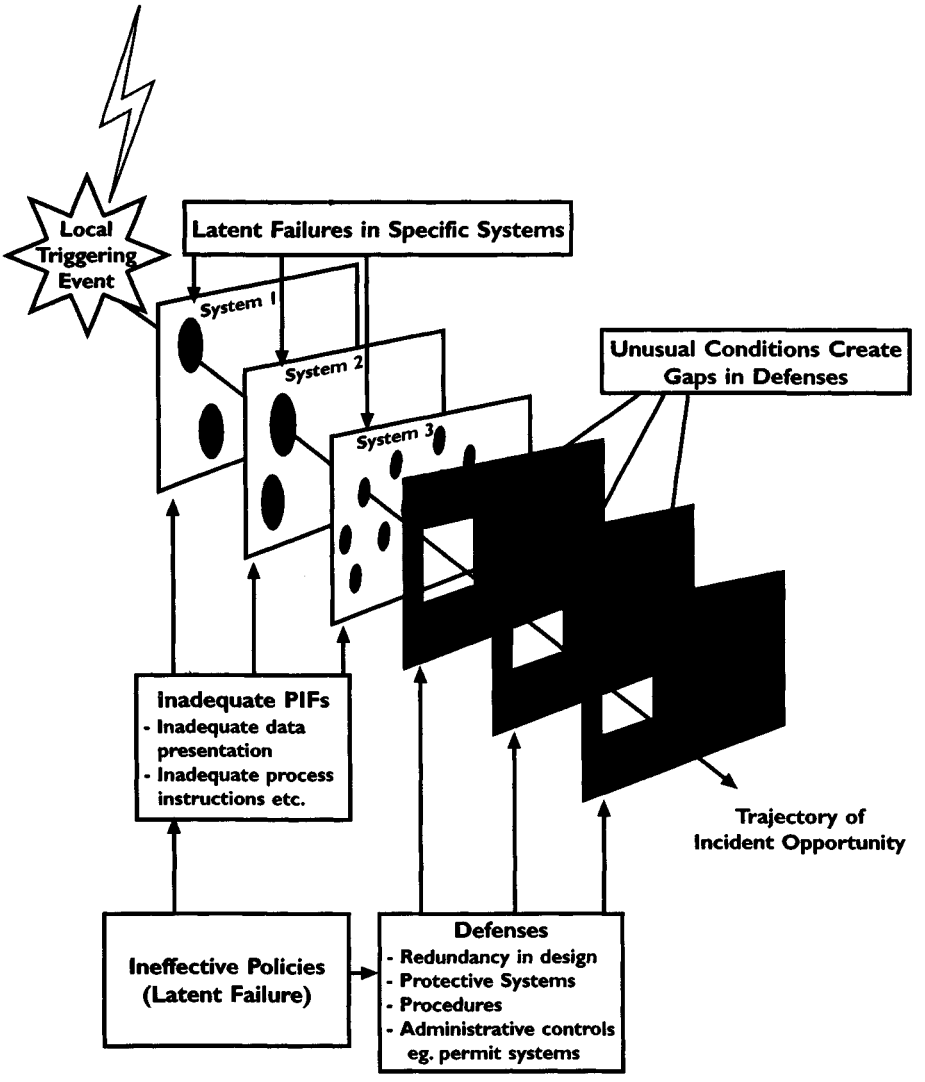

FIGURE 1.3 **The Dynamics of Incident Causation (adapted from Reason, 1990).**

phasize the importance of a philosophy that gets to the underlying causes of errors leading to quality lapses rather than attempting to control error by blame or punishment. Crosby (1984) explicitly advocates the use of error cause removal programs. Other experts such as Deming (1986), and Juran (1979) also emphasize the central importance of controlling the variability of human performance in order to achieve quality objectives. The practical techniques presented in this book could form an integral part of such programs. In Europe

and the United States there has been increasing interest in the relationship between quality and safety (see, e.g., Whiston and Eddershaw, 1989; Dumas, 1987). Both quality and safety failures are usually due to the same types of human errors with the same underlying causes. Whether or not a particular error has a safety or quality consequence depends largely on when or where in a process that it occurs. This indicates that any investment in error reduction is likely to be highly cost effective, since it should produce simultaneous reductions in both the incidence of accidents and the likelihood of quality failures.

An additional reason for investing resources in error reduction measures is to improve the ability of the industry to conform to regulatory standards. It is likely that as the relationship between human error and safety becomes more widely recognized, regulatory authorities will place more emphasis on the reduction of error-inducing conditions in plants. It is therefore important that the Chemical Process Industries take the lead in developing a systematic approach and a defensible position in this area.

Despite the lack of interest in human factors issues in the CPI in the past, the situation is now changing. In 1985, Trevor Kletz published his landmark book on human error in the CPI: *An Engineer's View of Human Error* (revised in 1991). Several other books by the same author e.g., Kletz (1994b) have also addressed the issue of human factors in case studies. Two other publications have also been concerned specifically with human factors in the process industry: Lorenzo (1990) was commissioned by the Chemical Manufacturers Association in the USA, and Mill (1992), published by the U.K. Institution of Chemical Engineers. In 1992, CCPS and other organizations sponsored a conference on Human Factors and Human Reliability in Process Safety (CCPS, 1992c). This was further evidence of the growing interest in the topic within the CPI.

1.5. THE TRADITIONAL AND SYSTEM-INDUCED ERROR APPROACH

From the organizational view of accident causation presented in the previous section, it will be apparent that the traditional approach to human error, which assumes that errors are primarily the result of inadequate knowledge or motivation, is inadequate to represent the various levels of causation involved. These contrasting views of error and accident causation have major implications for the way in which human error is assessed and the preventative measures that are adopted.

The structure of this book is based on a model of human error, its causes, and its role in accidents that is represented by Figures 1.4 and 1.5. This perspective is called the *system-induced error approach.* Up to now, only certain

aspects of this approach have been discussed in detail. These are the concept of performance-influencing factors (e.g., poor design, training, and procedures) as being the direct causes of errors, and the role of organizational and management factors in creating these causes. The other aspect of the model describes how performance-influencing factors interact with basic error tendencies to give rise to errors with significant consequences.

This aspect of the model is illustrated in Figure 1.5. The error tendencies circle represents the intrinsic characteristics of people that predispose them to error. These tendencies include a finite capability to process information, a reliance on rules (which may not be appropriate) to handle commonly occurring situations, and variability in performing unfamiliar actions. These error tendencies are discussed in detail in Chapter 2.

The error-inducing environment circle denotes the existence of conditions (negative performance-influencing factors) which, when combined with innate error tendencies, will give rise to certain predictable forms of error. For example, the finite information processing capabilities of the human means that overload is very likely if the worker is required to perform concurrent tasks. Another form of error, losing place in a sequence of operations, is likely if a high level of distractions are present. In terms of the management influences on these immediate causation factors, policies for planning workload would influence the number of tasks the worker is required to perform. Job design policies would influence the level of distractions.

The overlap between the error tendencies circle and the error-inducing environment circle represents the likelihood that an error would occur. However, given appropriate conditions, recovery from an error is highly likely. Recovery may arise either if the person making the error detects it before its consequences (accidents, product loss, degraded quality) occur, or if the system as a whole is made insensitive to individual human errors and supports error recovery. These aspects of the system-induced error approach are represented as the third circle in Figure 1.5. Thus, the dark area in the center of the model represents the likelihood of unrecovered errors with significant consequences. At least two major influences can be controlled by the organization to reduce the likelihood of error. The first of these is the design of the system to reduce the mismatch between the demands of the job and the capabilities of the worker to respond to these demands. This area can be addressed by modifying or improving performance-influencing factors that either reduce the levels of demand, or provide greater capability for the humans (e.g., through better job design, training, procedures, team organization). The other area that will have a major impact on error is that of organizational culture. This issue is discussed in Chapter 8.

The system-induced error approach can be restated in an alternative form as an accident causation model (see Figure 1.4). This shows how error-inducing conditions in the form of inadequate PIFs interact with error tendencies to

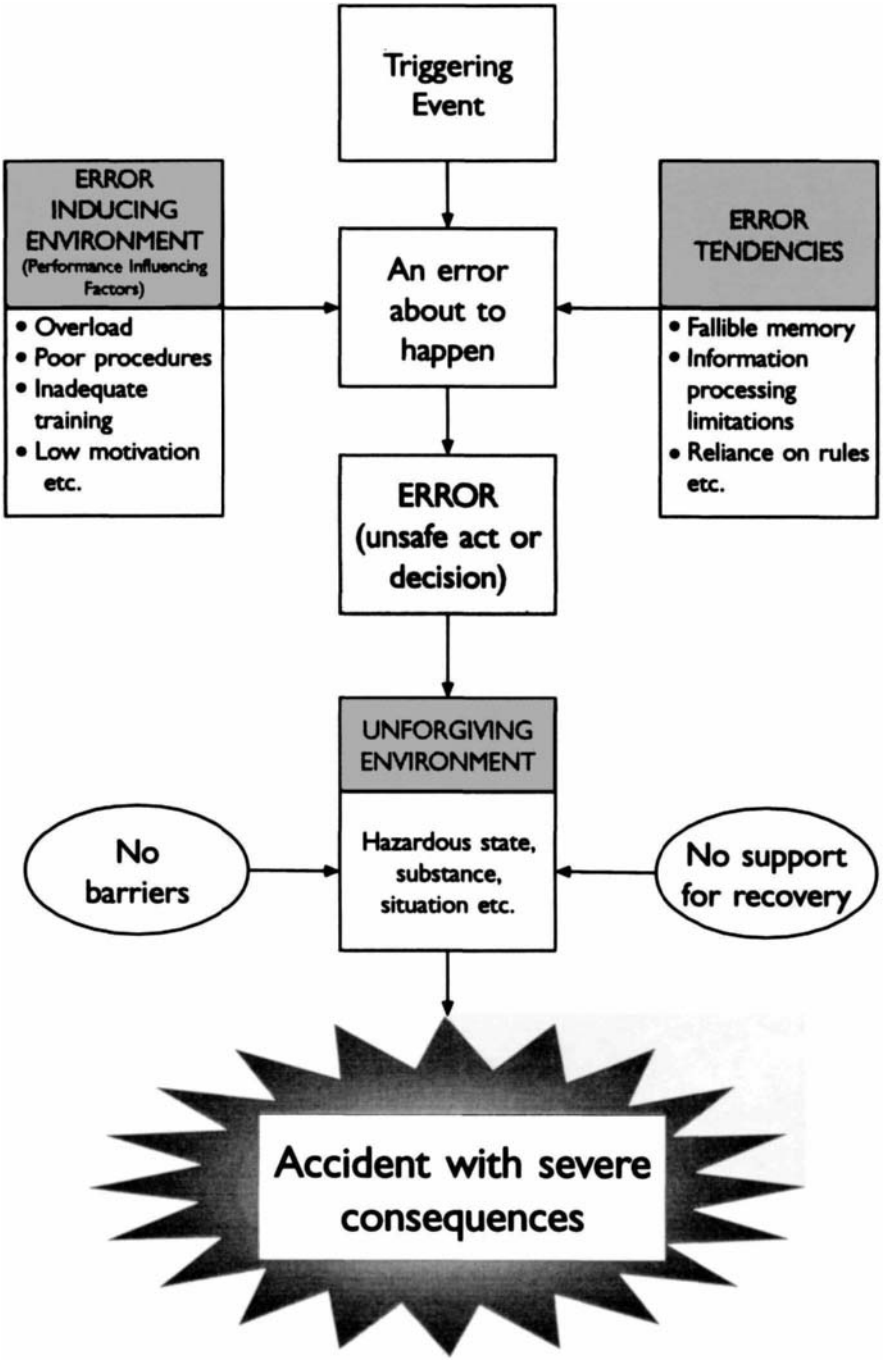

FIGURE 1.4 **Accident Causation Sequence.**

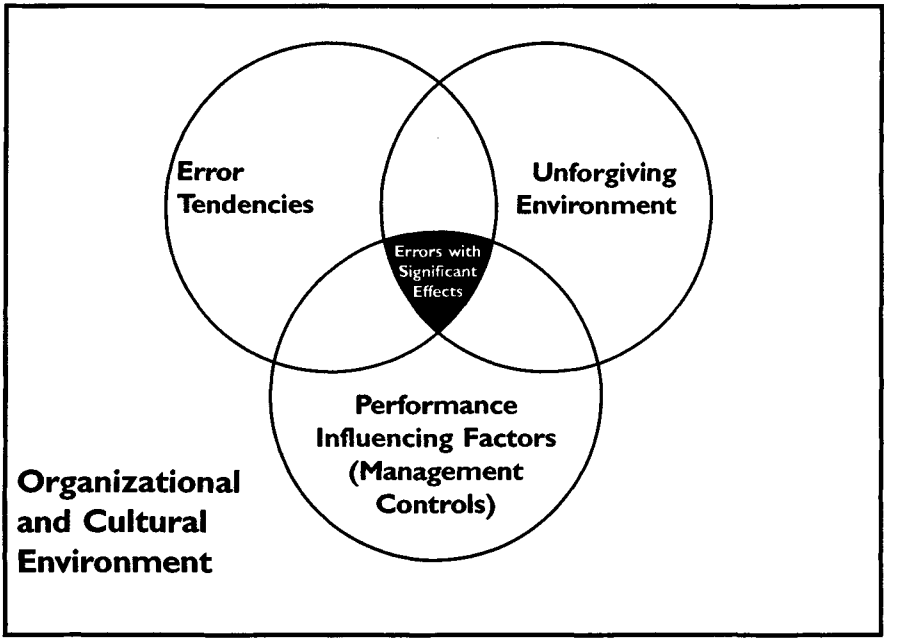

FIGURE 1.5 **System-Induced Error Approach.**

produce an unstable situation where there is a high probability of error. When a triggering event occurs, this gives rise to an error in the form of an unsafe act or decision. This in turn combines with an unforgiving environment that does not support recovery, to give rise to a severe accident. The ways in which the interaction between PIFs and error tendencies gives rise to error are discussed in Chapter 2. A comprehensive description of PIFs is given in Chapter 3.

1.6. A DEMAND–RESOURCE MISMATCH VIEW OF ERROR

A major cause of errors is a mismatch between the demands from a process system and the human capabilities to meet these demands. This is expressed in the model in Figure 1.6. One aspect of the demand side is the requirement for human capabilities that arises from the nature of the jobs in the process plant. Thus, physical capabilities such as craft skills (breaking flanges, welding pipe work, etc.) mental skills (diagnosing problems, interpreting trends) and sensory skills (e.g., being able to detect changes in process information) are all required to a lesser or greater extent by various jobs.

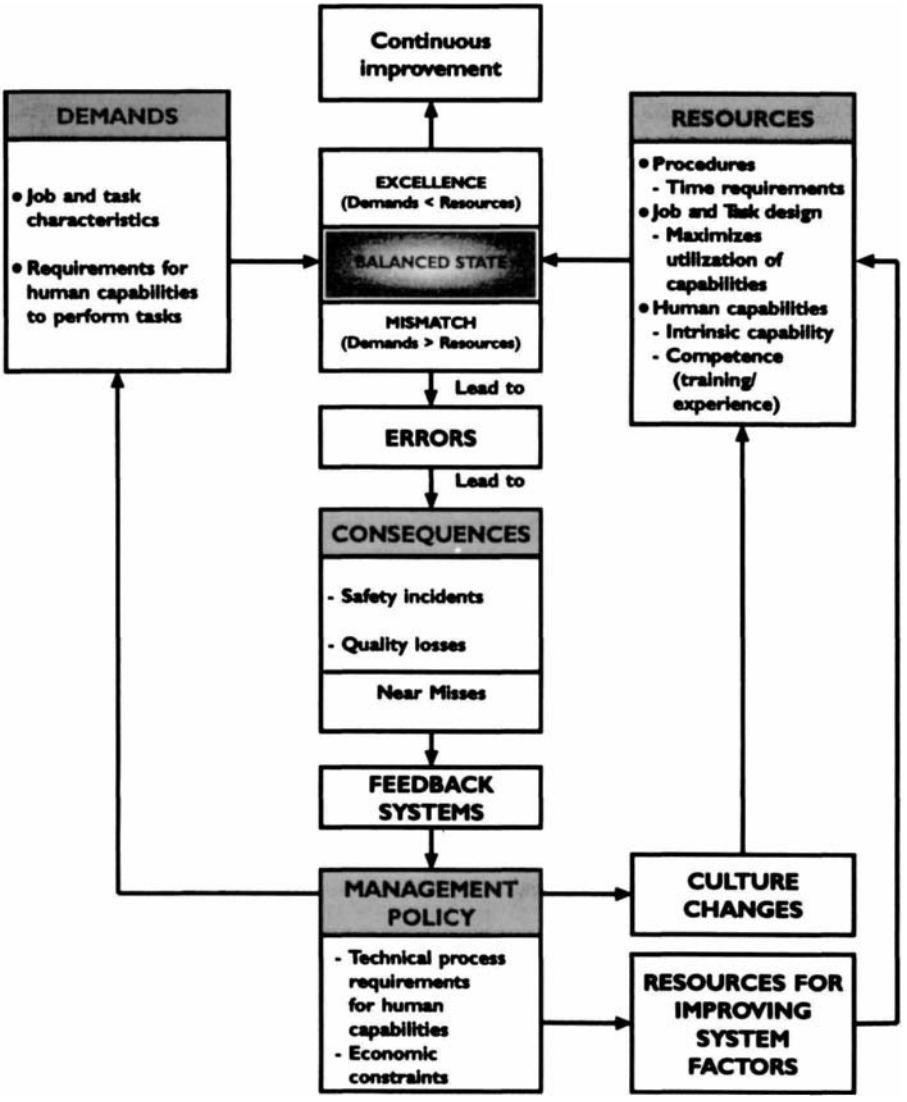

FIGURE 1.6 **A Demand–Resource View of Human Error.**

On the resources side, there are obviously upper limits on human capabilities in these areas. However, these capabilities will be considerably enhanced if the jobs and tasks are designed to utilize human capabilities effectively, if teams are constituted properly in terms of roles, and if personnel with sufficient capability (through training and selection) are available. In addition, these resources will be made more effective if an appropriate culture

exists which releases the "discretionary energy" that is available if workers feel committed to and empowered by the organization.

In Figure 1.6, the relationship between demand and resources can produce three outcomes. Where demands and resources are in balance, errors will be at a low level. If resources exceed demands, the organization can be regarded as "excellent" using the terminology of Peters and Waterman (1982). The spare resources can be used to contribute to a continuous improvement process as defined by Total Quality Management. This means that errors can be progressively reduced over time. The existence of spare capacity also allows the system to cope more effectively when unusual or unpredictable demands occur. It should be emphasized that increasing resources does not necessarily equate to increasing numbers of personnel. The application of various design principles discussed in this book will often reduce errors in situations of high demand without necessarily increasing the size of the workforce. In fact, better designed jobs, equipment, and procedures may enable production and quality to be maintained in a downsizing situation. The third case, the mismatch state, is a major precondition for error, as discussed earlier.

The occurrence of errors gives rise to various consequences. The nature of the underlying causes needs to be fed back to policy makers so that remedial strategies can be implemented. A typical strategy will consist of applying existing resources to make changes that will improve human performance and therefore reduce error. This may involve interventions such as improved job design, procedures or training or changes in the organizational culture. These are shown by the arrows to the right of Figure 1.6. An additional (or alternative) strategy is to reduce the level of demands so that the nature of the job does not exceed the human capabilities and resources currently available to do it. An important aspect of optimizing demands is to ensure that appropriate allocation of function takes place such that functions in which humans excel (e.g., problem solving, diagnosis) are assigned to the human while those functions which are not performed well by people (e.g., long-term monitoring) are assigned to machines and/or computers.

1.7. A CASE STUDY ILLUSTRATING THE SYSTEM-INDUCED ERROR APPROACH

In a batch reaction plant, an exothermic reaction was cooled by water circulating in a jacket. The circulating pump failed and the reactor went out of control causing a violent explosion. A low flow alarm was present but was inoperable. A critical pump bearing had not been lubricated during maintenance, and the collapse of the bearing had led to the pump failure.

The incident report stated that the cause of the accident was human error. Although maintenance procedures were available, they had not been used. The

maintenance technician was disciplined and a directive was issued that in the future more care should be exercised during maintenance and procedures should be used. This report was based on the traditional view of human error. The incident will now be analyzed from the systems-induced error perspective.

1.7.1. Error-Inducing Conditions

1.7.1.1. Design and Culture Factors

There were several reasons why the maintenance procedures, regarding pump bearing lubrication, were not used. They had been supplied by the original manufacturers of the pump and were written in highly technical language. The format of the procedures in terms of layout and typography made it difficult to find the appropriate section. The procedure was bound in a hard cover which made it physically unsuitable for workshop conditions. The nature of the maintenance operations had changed since the procedures were originally written, but these changes had not been incorporated. The general culture in the workshop was that only novices used procedures. Because the technicians had not participated in the development of the procedures there was no sense of ownership and no commitment to using procedures. Training was normally carried out "on the job" and there was no confirmation of competence.

1.7.1.2. Organization and Policy Factors

There were many distractions in the workshop from other jobs. The maintenance technicians were working under considerable pressure on a number of pumps. This situation had arisen because an effective scheduling policy was not in place. No policies existed for writing or updating procedures, or for training. In addition, pump bearing maintenance had been omitted on several occasions previously, but had been noticed before the pumps were put back into service. These occurrences had not been reported because of a lack of effective incident reporting systems for learning lessons from "near misses." The fact that the plant was being operated with an inoperable low flow alarm was also indicative of an additional deficiency in the technical risk management system.

1.7.2. Error Tendencies

The pump maintenance step that was omitted was in a long sequence of task steps carried out from memory. Memory limitations would mean that there was a high probability that the step would be omitted at some stage. The work was not normally checked, so the probability of recovery was low.

The steps for maintenance of the pump involved in the incident were very similar to those for other pumps that did not require bearing maintenance. These pumps were maintained much more frequently than the type requiring

bearing lubrication. It is possible that in a distracting environment, the maintenance technician may have substituted the more frequently performed set of operations for those required. This is a basic error tendency called a **strong stereotype takeover** (see Chapter 2).

1.7.3. Unforgiving Environment

An opportunity for error recovery would have been to implement a checking stage by a supervisor or independent worker, since this was a critical maintenance operation. However, this had not been done. Another aspect of the unforgiving environment was the vulnerability of the system to a single human error. The fact that the critical water jacket flow was dependent upon a single pump was a poor design that would have been detected if a hazard identification technique such as a **hazard and operability study** (HAZOP) had been used to assess the design.

1.8 FROM THEORY TO PRACTICE: TURNING THE SYSTEMS APPROACH TO A PRACTICAL ERROR REDUCTION METHODOLOGY

This chapter has provided an overview of the book and has described its underlying philosophy, the system-induced error approach (abbreviated to the systems approach in subsequent chapters). The essence of the systems approach is to move away from the traditional blame and punishment approach to human error, to one which seeks to understand and remedy its underlying causes.

In subsequent chapters, the various theories, tools, and techniques required to turn the systems approach from a concept to a practical error reduction methodology will be described. The components of this methodology are described in Figure 1.7. Each of these components will now be described in turn, together with references to the appropriate sections of the book.

1.8.1. Performance Optimization

The first component of the systems approach to error reduction is the optimization of human performance by designing the system to support human strengths and minimize the effects of human limitations. The **human factors engineering and ergonomics** (HFE/E) approach described in Section 2.7 of Chapter 2 indicates some of the techniques available. Design data from the human factors literature for areas such as equipment, procedures, and the human–machine interface are available to support the designer in the optimization process. In addition the analytical techniques described in Chapter 4 (e.g., task analysis) can be used in the development of the design.

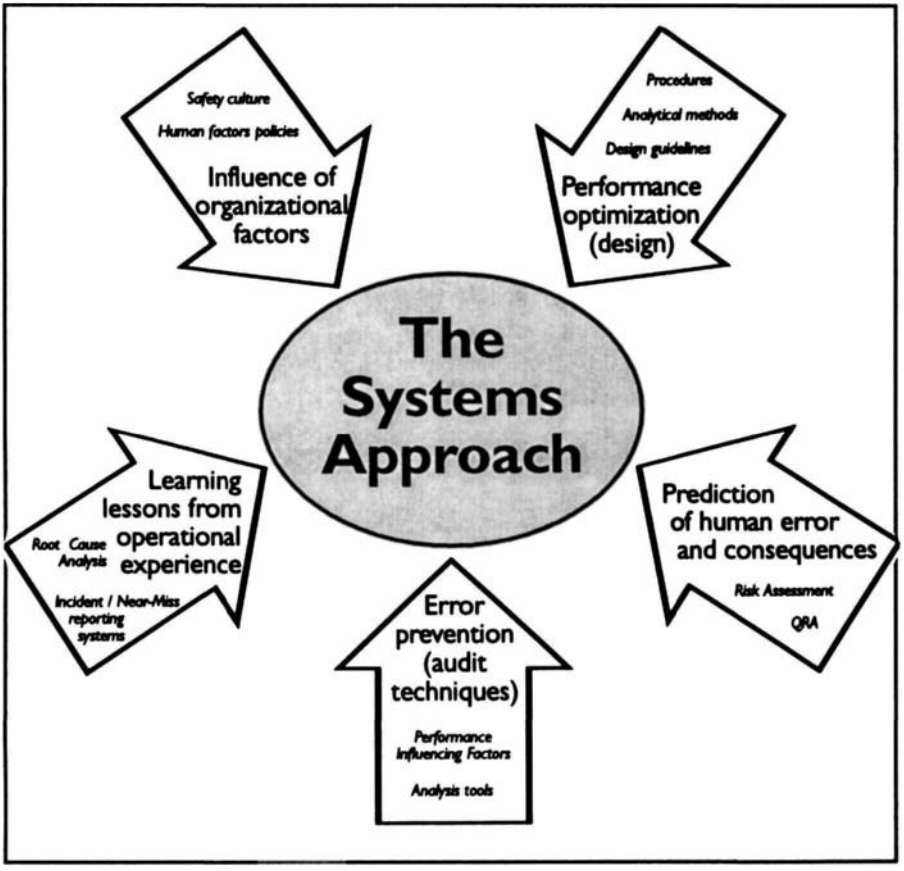

FIGURE 1.7 **Overview of the Systems Approach.**

1.8.2. Prediction of Human Error and Its Consequences

The application of human factors principles at the design stage can reduce the overall probability of errors occurring. However, beyond a certain point, the expenditure that will be required to reduce error rates in general to a very low level may become unacceptable. An approach is therefore required which specifies more accurately the nature of the errors that could occur and their significance compared with other sources of risk in the system. This is achieved by the techniques for the qualitative and quantitative prediction of errors that are described in Chapter 5. In particular, the System for Predictive Error Analysis and Reduction (SPEAR) methodology provides a comprehensive framework for predicting errors and their consequences. By using approaches such as SPEAR, it is possible to make rational decisions with regard to where

resources should be most effectively spent in order to reduce the likelihood of errors that have the most severe implications for risk.

The importance of such risk assessment and risk management exercises is being increasingly recognized and can be highly cost-effective if it serves to prevent severe losses that could arise from unmanaged risk. In certain industry sectors, for example, offshore installations in the North Sea, safety cases are being required by the regulatory authorities in which formal risk assessments are documented.

1.8.3. Error Prevention (Audit Techniques)

Measures to reduce human error are often implemented at an existing plant, rather than during the design process. The decision to conduct an evaluation of the factors that can affect error potential at an existing plant may be taken for several reasons. If human errors are giving rise to unacceptable safety, quality or production problems, plant management, with the assistance of the workforce, may wish to carry out a general evaluation or audit of the plant in order to identify the direct causes of these problems.

The identification of the operational level deficiencies that contribute to increased error rates can be achieved by evaluations of PIFs as described in Chapter 3. Although the factors described in that chapter are not exhaustive in their coverage, they can provide a useful starting point for an evaluation exercise. Structured PIF evaluation systems are described in Chapter 2 which ensure that all the important factors that need to be evaluated are included in the exercise.

1.8.4. Learning Lessons from Operational Experience

The next component of the systems approach is the process of learning lessons from operational experience. In Chapter 6, and the case studies in Chapter 7, several techniques are described which can be used to increase the effectiveness of the feedback process. Incident and near-miss reporting systems are designed to extract information on the underlying causes of errors from large numbers of incidents. Chapter 6 provides guidelines for designing such systems. The main requirement is to achieve an acceptable compromise between collecting sufficient information to establish the underlying causes of errors without requiring an excessive expenditure of time and effort.

In addition to incident reporting systems, root cause analysis techniques can be used to evaluate the causes of serious incidents where resources are usually available for in-depth investigations. A practical example of root cause investigation methods is provided in Chapter 7.

1.8.5. Influence of Organizational Factors

The last area addressed by the systems approach is concerned with global issues involving the influence of organizational factors on human error. The major issues in this area are discussed in Chapter 2, Section 7. The two major perspectives that need to be considered as part of an error reduction program are the creation of an appropriate safety culture and the inclusion of human error reduction within safety management policies.

As discussed earlier in this chapter, the main requirements to ensure an appropriate safety culture are similar to those which are advocated in quality management systems. These include active participation by the workforce in error and safety management initiatives, a blame-free culture which fosters the free flow of information, and an explicit policy which ensures that safety considerations will always be primary. In addition both operations and management staff need feedback which indicates that participation in error reduction programs has a real impact on the way in which the plant is operated and systems are designed.

The other global dimension of the systems approach is the need for the existence of policies which address human factors issues at senior levels in the company. This implies that senior management realizes that resources spent on programs to reduce error will be as cost-effective as investments in engineered safety systems.

1.9. APPENDIX: CASE STUDIES OF HUMAN ERROR LEADING TO ACCIDENTS OR FINANCIAL LOSS

1.9.1. Introduction

The intention of this section is to provide a selection of case studies of varying complexity and from different stages of chemical process plant operation. The purpose of these case studies is to indicate that human error occurs at all stages of plant operation, and to emphasize the need to get at root causes. The case studies are grouped under a number of headings to illustrate some of the commonly recurring causal factors. Many of these factors will be discussed in later chapters.

In the shorter case studies, only the immediate causes of the errors are described. However, the more extended examples in the latter part of the appendix illustrate two important points about accident causation. First, the preconditions for errors are often created by incorrect policies in areas such as training, procedures, systems of work, communications, or design. These "root causes" underlie many of the direct causes of errors which are described in this section. Second, the more comprehensive examples illustrate the fact that incidents almost always involve more than one cause. These issues will

be taken up in more detail in later chapters. In addition to the case studies in this chapter, further examples will be provided within each chapter to illustrate specific technical points.

1.9.2. Errors Occurring during Plant Changes and Stressful Situations

Insights into the human causes of accidents for a specific category of process plant installations are provided by the Oil Insurance Association report on boiler safety (Oil Insurance Association, 1971). This report provides a large number of case studies of human errors that have given rise to boiler explosions.

Plants are particularly vulnerable to human error during shutdowns for repair and maintenance. This is partly due to the higher level of direct human involvement with the plant, when errors are likely if procedures and supervisory systems are poor. Errors also occur during high stress situations such as emergency shutdowns. Workers need to be trained in how to handle these situations so that less stress is experienced (see Chapter 3).

Example 1.1

A boiler had been shut down for the repair of a forced draft fan. A blind was not installed in the fuel gas line, nor apparently was a double block and bleed in the fuel line utilized. Gas leaked into the firebox during the repair period and was not removed. A severe explosion occurred during the attempt to light of.

Example 1.2

Low water level had shut down a boiler. Flameout occurred on two attempts to refire the boiler. On the third attempt, a violent explosion occurred. The worker had not purged the firebox between each attempt to fire the boiler and this resulted in the accumulation of fuel–air mixture which exploded on the third attempt to ignite the pilot.

Example 1.3

A boiler house enclosed eight large boilers attended by two men. Failure of the combustion air supply shut down one of the boilers. This boiler shutdown created conditions beyond the control of just two men and lack of proper combustion control equipment finally caused seven of the eight boilers to shut down. Amid the confusion caused by low instrument air

pressure, low steam pressure, constantly alarming boiler panels, the blocking-in of valves and attempts to get the boilers back on line, one boiler exploded. A purge interlock system was provided on the boilers but the individual burner valves were manually operated. The fuel gas header could not be charged until a timed purge period had been completed.

On the boiler that exploded the manual individual burner valves were not closed when the boiler shut down. After the purge period, fuel gas was admitted to the header from remote manual controls in the control room and into the firebox. Low fuel gas pressure tripped the master safety valve after each attempt to pressure the fuel header. Three attempts were made to purge the boiler and on each of these occasions fuel gas was dumped into the furnace through the open manual burner gas valves. On the third attempt a severe explosion occurred.

1.9.3. Inadequate Human–Machine Interface Design

The first set of case studies illustrates errors due to the inadequate design of the human–machine interface (HMI). The HMI is the boundary across which information is transmitted between the process and the plant worker. In the context of process control, the HMI may consist of analog displays such as chart records and dials, or modern video display unit (VDU) based control systems. Besides display elements, the HMI also includes controls such as buttons and switches, or devices such as trackballs in the case of computer controlled systems. The concept of the HMI can also be extended to include all means of conveying information to the worker, including the labeling of control equipment components and chemical containers. Further discussion regarding the HMI is provided in Chapter 2. This section contains examples of deficiencies in the display of process information, in various forms of labeling, and the use of inappropriate instrumentation scales.

1.9.3.1. Inadequate Display of Process Information

Example 1.4

The pump feeding an oil stream to the tubes of a furnace failed. The worker closed the oil valve and intended to open a steam valve to purge the furnace tubes free from oil. He opened the wrong valve, there was no flow to the furnace and as a result the tubes were overheated and collapsed. The error was not due to ignorance. The worker knew which was the right valve but nevertheless opened the wrong one.

This incident is typical of many that have been blamed on human failing. The usual conclusion is that the worker was at fault and there was nothing anyone could do. In fact, investigation showed that:

1. The access to the steam valve was poor and it was difficult to see which was the right valve.
2. There was no indication in the control room to show that there was no flow through the furnace coils.
3. There was no low-flow alarm or low-flow trip on the furnace.

This accident was therefore a typical example of "system-induced error." The poor design of the information display and the inaccessible steam valve created preconditions that were likely to contribute to the likelihood of an error at some time.

Example 1.5

A reactor was being started up. It was filled with the reaction mixture from another reactor which was already on line and the panel operator started to add fresh feed. He increased the flow gradually, at the same time watching the temperature on a recorder conveniently situated at eye level. He intended to start a flow of cooling water to the reaction cooler as soon as the temperature started to rise. Unfortunately, there was a fault in the temperature recorder and although the temperature actually rose, this was not recorded. As a result, a runaway reaction occurred.

The rise in temperature was indicated on a six-point temperature recorder at a lower level on the panel, but the worker did not notice this. The check instrument was about three feet above the floor and a change in one reading on a six-point recorder in that position was not obvious unless someone was actually looking for it.

Example 1.6

When a process disturbance occurred, the plant computer printed a long list of alarms. The operator did not know what had caused the upset and he did nothing. After a few minutes an explosion occurred. Afterwards, the designer admitted that he had overloaded the user with too much information.

1.9.3.2 Poor Labeling of Equipment and Components

Example 1.7

Small leaks from the glands of a carbon monoxide compressor were collected by a fan and discharged outside the building. A man working near the compressor was affected by carbon monoxide. It was then found that a damper in the fan delivery line was shut. There was no label or other indication to show whether the damper was closed or open. In a similar incident, a furnace damper was closed in error. It was operated pneumatically, and again there was no indication on the control knob to show which were the open and closed positions.

Example 1.8

Service lines are often not labeled. A mechanic was asked to fit a steam supply at a gauge pressure of 200 psi (13 bar) to a process line in order to clear a choke. By mistake, he connected up a steam supply at a gauge pressure of 40 psi (3 bar). Neither supply was labeled and the 40 psi supply was not fitted with a check valve. The process material flowed backwards into the steam supply line . Later the steam supply caught fire when it was used to disperse a small leak.

Example 1.9

Nitrogen was supplied in tank cars which were also used for oxygen. Before filling the tank cars with oxygen, the filling connections were changed and hinged boards on both sides of the tanker were folded down so that they read "oxygen" instead of "nitrogen." A tank car was fitted with nitrogen connections and labeled "nitrogen." Probably due to vibration, one of the hinged boards fell down, so that it read "oxygen." The filling station staff therefore changed the connections and put oxygen in it. The tank car was labeled "nitrogen" on the other side and so some nitrogen tank trucks were filled from it and supplied to a customer who wanted nitrogen. He off-loaded the oxygen into his plant, thinking it was nitrogen. Fortunately, the mistake was found before an accident occurred. The customer looked at his weigh scale figures and noticed that on arrival the tanker had weighed three tons more than usual. A check then showed that the plant nitrogen system contained 30% oxygen.

1.9.3.3. Inappropriate Instrumentation Scales

Example 1.10

A workman, who was pressure testing some pipe work with a hand operated hydraulic pump, told his foreman that he could not get the gauge reading above 200 psi. The foreman told him to pump harder. He did so, and burst the pipeline. The gauge he was using was calibrated in atmospheres and not psi. The abbreviation "atm." was in small letters, and in any case the workman did not know what it meant.

Example 1.11

A worker was told to control the temperature of a reactor at 60°C, so he adjusted the setpoint of the temperature controller at 60. The scale actually indicated 0–100% of a temperature range of 0–200°C, so the set point was really 120°C. This caused a runaway reaction which overpressured the vessel. Liquid was discharged and injured the worker.

1.9.3.4. Inadequate Identification of Components

Example 1.12

A joint that had to be broken was marked with chalk. The mechanic broke another joint that had an old chalk mark on it and was splashed with a corrosive chemical. The joint should have been marked with a numbered tag.

Example 1.13

An old pipeline, no longer used, was marked with chalk at the point at which it was to be cut. Before the mechanic could start work, heavy rain washed off the chalk mark. The mechanic "remembered" where the chalk mark had been and he was found cutting his way with a hacksaw through a line containing a hazardous chemical.

1.9.4. Failures Due to False Assumptions

In order to cope with a complex environment, people make extensive use of rules or assumptions. This rule based mode of operation is normally very efficient. However, errors will arise when the underlying assumptions required by the rules are not fulfilled. Chapter 2 discusses the causes of these rule based errors in detail.

Example 1.14

During the morning shift, a worker noticed that the level in a tank was falling faster than usual. He reported that the level gauge was out of order and asked an instrument mechanic to check it. It was afternoon before he could do so. He reported that it was correct. Only then did the worker find that there was a leaking drain valve. Ten tons of material had been lost. In this case an inappropriate rule of the form "If level in tank decreases rapidly then level gauge is faulty" had been used instead of the more general rule: "If level in tank decreases rapidly then investigate source of loss of material."

Example 1.15

Following some modifications to a pump, it was used to transfer liquid. When the movement was complete, the operator pressed the stop button on the control panel and saw that the "pump running" light went out. He also closed a remotely operated valve in the pump delivery line. Several hours later the high-temperature alarm on the pump sounded. Because the operator had stopped the pump and seen the running light go out, he assumed the alarm was faulty and ignored it. Soon afterward there was an explosion in the pump.

When the pump was modified, an error was introduced into the circuit. As a result, pressing the stop button did not stop the pump but merely switched off the running light. The pump continued running-dead-headed, overheated, and the material in it decomposed explosively.

Example 1.16

An ethylene oxide plant tripped and a light on the panel told the operator that the oxygen valve had closed. Because the plant was going to be restarted immediately, he did not close the hand-operated isolation valve as well, relying totally on the automatic valves. Before the plant could be restarted an explosion occurred. The oxygen valve had not closed and oxygen continued to enter the plant (Figure 1.8).

The oxygen valve was closed by venting the air supply to the valve diaphragm, by means of a solenoid valve. The light on the panel merely said that the solenoid had been deenergized not, as the operator assumed, that the oxygen valve had closed. Even though the solenoid is deenergized the oxygen flow could have continued because:

1. The solenoid valve did not open.
2. The air was not vented.
3 The trip valve did not close.

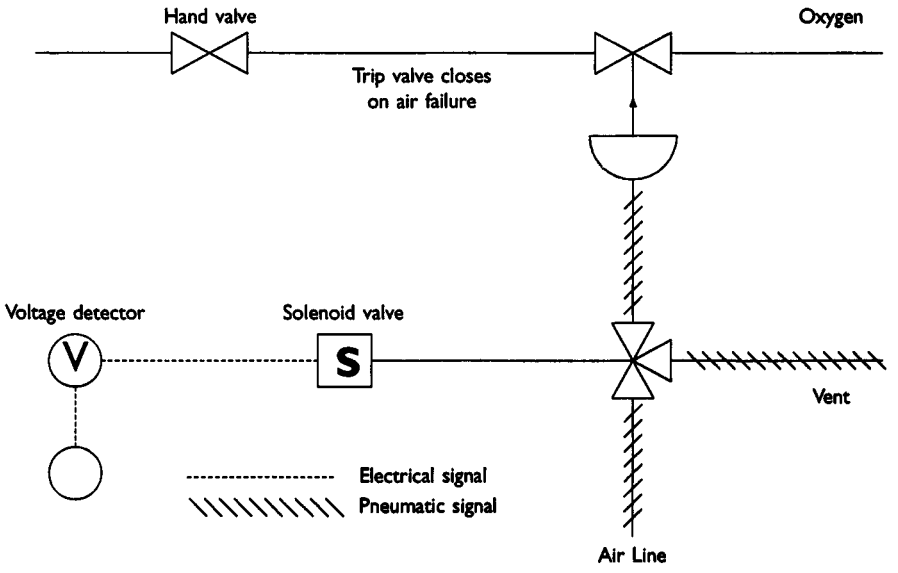

FIGURE 1.8 **The Light Shows That the Solenoid Is Deenergized, Not That the Oxygen Flow Has Stopped (Kletz, 1994b).**

In fact, the air was not vented. The 1-inch vent line on the air supply was choked by a wasp's nest. Although this example primarily illustrates a wrong assumption, a second factor was the inadequate indication of the state of the oxygen valve by the panel light. A similar error was a major contributor to the Three Mile Island nuclear accident.

Example 1.17

A permit was issued to remove a pump for overhaul. The pump was deenergized, removed, and the open ends blanked. Next morning the maintenance foreman signed the permit to show that the job—removing the pump—was complete. The morning shift lead operator glanced at the permit. Seeing that the job was complete, he asked the electrician to replace the fuses. The electrician replaced them and signed the permit to show that he had done so. By this time the afternoon shift lead operator had come on duty. He went out to check the pump and found that it was not there.

The job on the permit was to remove the pump for overhaul. Permits are sometimes issued to remove a pump, overhaul it, and replace it. But in this case the permit was for removal only. When the maintenance foreman signed the permit to show that the job was complete, he meant that the job of **removal** was complete. The lead operator, however, did not read the permit thoroughly. He assumed that the **overhaul** was complete.

When the maintenance foreman signed the permit to show that the job was complete, he meant he had completed the job **he thought he had to do.** In this case this was not the same as the job the lead operative expected him to do.

1.9.5. Poor Operating Procedures

This section gives an example of an error caused by poor operating procedures. In industries such as nuclear power, incident reporting systems indicate that inadequate or nonexistent operating instructions or procedures account for a high proportion of errors. Although there is little hard evidence, because of the incident reporting policies in the CPI (see Chapter 6), this cause probably contributes to many of the incidents discussed in this chapter. The effective design of procedures is discussed further in Chapter 7, Case Study 2.

Example 1.18

When the preparation of a batch went wrong the investigation showed that the worker had charged 104 kg of one constituent instead of 104 grams. The instructions to the worker were set out as shown below (originally the actual names of the chemicals were included).

Operating Instructions	
BLENDING INGREDIENTS	QUANTITY (TONS)
Chemical 1	3.75
Chemical 2	0.250
Chemical 3	0.104 kg
Chemical 4	0.020
Chemical 5	0.006
TOTAL	4.026

1.9.6. Routine Violations

This section is concerned with errors that are often classified as "violations," that is, situations where established operating procedures appear to have been deliberately disregarded. Such violations sometimes arise because the prescribed way of performing the task is extremely difficult or is incompatible with the demands of production. Another cause is lack of knowledge of the

reasons why a particular activity is required. The case studies illustrate both of these causes.

Example 1.19

Experience shows that when autoclaves or other batch reactors are fitted with drain valves, they may be opened at the wrong time and the contents will then discharge on to the floor, often inside a building. To prevent this, the drain valves on a set of reactors were fitted with interlocks so that they could not be opened until the pressure was below a preset value. Nevertheless, a drain valve was opened when a reactor was up to pressure and a batch emptied on to the floor. The inquiry disclosed that the pressure measuring instruments were not very reliable. So the workers had developed the practice of defeating the interlock either by altering the indicated pressure with the zero adjustment screw or by isolating the instrument air supply. One day, having defeated the interlock, a worker opened a drain valve by mistake instead of a transfer valve.

Example 1.20

A small tank was filled every day with sufficient raw material to last until the following day. The worker watched the level in the tank and switched off the filling pump when the tank was 90% full. The system worked satisfactorily for several years before the inevitable happened and the worker allowed the tank to overfill. A high level trip was then installed to switch off the pump automatically if the level exceeded 90%. To the surprise of engineering staff the tank overflowed again after about a year. When the trip was installed it was assumed that:

1. The worker would occasionally forget to switch off the pump in time, and the trip would then operate.
2. The trip would fail occasionally (about once in two years).
3. The chance that both would occur at the time same time was negligible.

However, these assumptions were incorrect. The worker decided to rely on the trip and stopped watching the level. The supervisor and foreman knew this, but were pleased that the worker's time was being utilized more productively. A simple trip fails about once every two years so the tank was bound to overflow after a year or two. The trip was being used as a process controller and not as an emergency instrument. The operating and supervisory staff probably assumed a much higher level of reliability for the trip than was actually the case.

Example 1.21

A permit issued for work to be carried out on an acid line stated that goggles must be worn. Although the line had been drained, there might have been some trapped pressure. The man doing the job did not wear goggles and was splashed in the eye.

Further investigations showed that **all** permits issued asked for goggles to be worn, even for repairs to water lines in safe areas. The mechanics therefore frequently ignored this instruction and the supervisors and foremen tolerated this practice.

Example 1.22

Two men were told to wear breathing apparatus while repairing a compressor that handled gas containing hydrogen sulfide. The compressor had been purged but traces of gas might have been left in it. One of the men had difficulty in handling a heavy valve close to the floor and removed his mask. He was overcome by hydrogen sulfide or possibly nitrogen gas. It was easy to blame the man, but he had been asked to do a job which was difficult wearing breathing apparatus.

1.9.7. Ineffective Organization of Work

Error free operation and maintenance can only occur within an effective management system. At the level of the task itself, this is provided by operating instructions. However, at a more global level, separate tasks have to be organized in a systematic manner, particularly if hazardous operations are involved, and where several individuals need to coordinate to achieve an overall objective. This section illustrates some accidents due to poor organization of work or failure to carry out checks.

Example 1.23

A plumber foreman was given a work permit to modify a pipeline. At 4:00 PM. the plumbers went home, intending to complete the job on the following day.

During the evening the process foreman wanted to use the line the plumbers were working on. He checked that the line was safe to use and he asked the shift mechanic to sign off the permit. Next morning the plumbers, not knowing that their permit had been withdrawn, started work on the line while it was in use.

Example 1.24

A manhole cover was removed from a reactor so that some extra catalyst could be put in. After the cover had been removed, it was found that the necessary manpower would not be available until the next day. The supervisor therefore decided to replace the manhole cover and regenerate the catalyst overnight. By this time it was evening and the maintenance foreman had gone home and left the work permit in his office, which was locked. The reactor was therefore boxed up and catalyst regeneration carried out with the permit still in force. The next day a mechanic, armed with the work permit, proceeded to remove the manhole cover again, and while doing so was drenched with process liquid. Fortunately, the liquid was mostly water and he was not injured.

Example 1.25

A pump was being dismantled for repair. When the casing was removed, hot oil, above its autoignition temperature, came out and caught fire. Three men were killed and the plant was destroyed. Examination of the wreckage after the fire showed that the pump suction valve was open and the pump drain valve was shut.

The pump had been awaiting repair for several days when a work permit was issued at 8:00 AM. on the day of the fire. The foreman who issued the permit should have checked, before doing so, that the pump suction and delivery valves were shut and the drain valve open. He claimed that he did so. Either his recollection was incorrect or, after he inspected the valves and before work started, someone closed the drain valve and opened the suction valve. When the valves were closed, there was no indication on them of **why** they were closed. A worker might have opened the suction valve and shut the drain valve so that the pump could be put on line quickly if required. A complicating factor was that the maintenance team originally intended to work only on the pump bearings. When they found that they had to open up the pump they told the process team, but no further checks of the isolations were carried out.

Example 1.26

While a plant was on-line a worker noticed a blind in a tank vent. The blind had been fitted to isolate the tank from the blowdown system while the tank was being repaired. When the repairs were complete, the blind

was overlooked. Fortunately, the tank, an old one, was stronger than it needed to be for the duty, or it would have burst. The omission of an isolated step at the end of a long sequence of operations is a common failure mode, which often occurs in the absence of formal checklists or operating procedures.

1.9.8. Failure to Explicitly Allocate Responsibility

Many errors have occurred due to failure to explicitly allocate responsibility between different individuals who need to coordinate their efforts. This is illustrated by the case study in this section.

Example 1.27

The following incident occurred because responsibility for plant equipment was not clearly defined, and workers in different teams, responsible to different supervisors, operated the same valves.

The flare stack shown in Figure 1.9 was used to dispose of surplus fuel gas, which was delivered from the gas holder by a booster through valves B and C. Valve C was normally left open because valve B was more accessible. One day the worker responsible for the gas holder saw that the gas pressure had started to fall. He therefore imported some gas from another unit. Nevertheless, a half hour later the gas holder was sucked in.

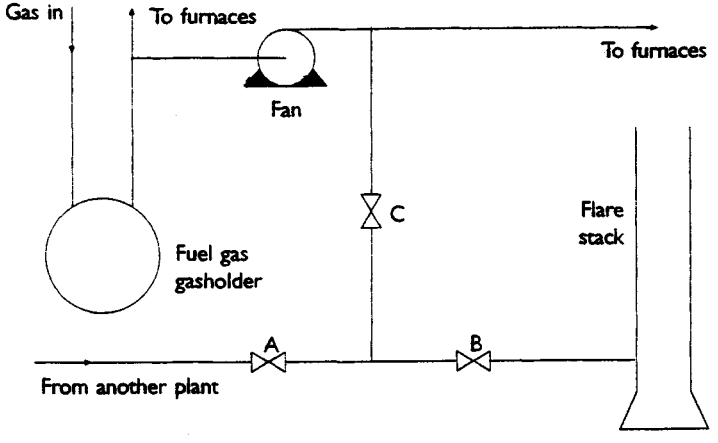

FIGURE 1.9 **Valve B was Operated by Different Workers (Kletz, 1994b).**

Another flare stack at a different plant had to be taken out of service for repair. A worker at this plant therefore locked open valves A and B so that he could use the "gas holder flare stack." He had done this before, though not recently, and some changes had been made since he last used the flare stack. He did not realize that this action would result in the gas holder emptying itself through valves C and B. He told three other men what he was going to do but he did not tell the gas holder worker as he did not know that this man needed to know.

1.9.9. Organizational Failures

This section illustrates some of the more global influences at the organizational level which create the preconditions for error. Inadequate policies in areas such as the design of the human–machine interface, procedures, training, and the organization of work will also have contributed implicitly to many of the other human errors considered in this chapter.

In a sense, all the incidents described so far have been management errors but this section describes two incidents which would not have occurred if the senior managers of the companies concerned had realized that they had a part to play in the prevention of accidents over and above exhortations to their employees to do better.

Example 1.28

A leak of ethylene from a badly made joint on a high pressure plant was ignited by an unknown cause and exploded, killing four men and causing extensive damage. After the explosion many changes were made to improve the standard of joint-making: better training, tools, and inspection.

Poor joint-making and the consequent leaks had been tolerated for a long time before the explosion as all sources of ignition had been eliminated and so leaks could not ignite, or so it was believed. The plant was part of a large corporation in which the individual divisions were allowed to be autonomous in technical matters. The other plants in the corporation had never believed that leaks of flammable gas could ignite. Experience had taught them that sources of ignition were liable to occur, even though everything was done to remove known sources, and therefore strenuous efforts had been made to prevent leaks. Unfortunately the managers of the ethylene plant had hardly any technical contact with the other plants, though they were not far away; handling flammable gases at high pressure was, they believed, a specialized technology and little could be learned from those who handled them at low pressure.

Example 1.29

Traces of water were removed from a flammable solvent in two vessels containing a drying agent. While one vessel was on-line, the other was emptied by blowing with nitrogen and then regenerated. The changeover valves were operated electrically. Their control gear was located in a Division 2 area and as it could not be obtained in a nonsparking form, it was housed in a metal cabinet which was purged with nitrogen to prevent any flammable gas in the surrounding atmosphere leaking in. If the nitrogen pressure fell below a preset value (about ½-inch water gauge) a switch isolated the power supply. Despite these precautions an explosion occurred in the metal cabinet, injuring the inexperienced engineer who was starting up the unit.

The nitrogen supply used to purge the metal cabinet was also used to blow out the dryers. When the nitrogen supply fell from time to time (due to excessive use elsewhere on the site), solvent from the dryers passed through leaking valves into the nitrogen supply line, and found its way into the metal cabinet. The nitrogen pressure then fell so low that some air diffused into the cabinet.

Because the nitrogen pressure was unreliable it was difficult to maintain a pressure of ½-inch water gauge in the metal cabinet. The workers complained that the safety switch kept isolating the electricity supply, so an electrician reduced the setpoint first to ¼ inch and then to zero, thus effectively bypassing the switch. The setpoint could not be seen unless the cover of the switch was removed and the electrician told no one what he had done. The workers thought he was a good electrician who had prevented spurious trips. Solvent and air leaked into the cabinet, as already described, and the next time the electricity supply was switched there was an explosion.

The immediate causes of the explosion were the contamination of the nitrogen, the leaky cabinet (made from thin steel sheet) and the lack of any procedure for authorizing, recording, and checking changes in trip settings. However, the designers were also at fault in not realizing that the nitrogen supply was unreliable and liable to be contaminated and that it is difficult to maintain a pressure in boxes made from thin sheet. If a hazard and operability study had been carried out on the service lines, with operating staff present, these facts, well known to the operating staff, would have been made known to the designers. It might also have brought out the fact that compressed air could have been used instead of nitrogen to prevent diffusion into the cabinet.

The control cabinet did not have to be in a Division 2 area. A convenient location was chosen and the electrical designers were asked to supply equipment suitable for the location. They did not ask if the

cabinet had to be in a Division 2 area. This was not seen as their job. They perceived their job as being to provide equipment suitable for the classification which had already been agreed.