2

Understanding Human Performance and Error

2.1. PURPOSE OF THE CHAPTER

The purpose of this chapter is to provide a comprehensive overview of the main approaches that have been applied to analyze, predict, and reduce human error in industrial systems. The practical application of specific techniques to achieve these goals must be built upon an understanding of the theory that led to the development of these techniques. Just as it would be inadvisable for an engineer to attempt to design a venting system without an underlying knowledge of the behavior of chemical reactions, it is recommended that the user of human factors techniques becomes acquainted with their underlying rationale.

This chapter is organized into four sections, which comprise four complementary approaches to human error in industrial systems:

- Traditional safety engineering
- Factors/ergonomics
- Cognitive systems engineering
- Sociotechnical systems

Prior to the sections that give a detailed description of these approaches, the following overview section provides a summary of the concepts and terminology used in the study of error. This is followed by an introduction to each of the approaches, which are then described in more detail in subsequent sections.

2.2. CONCEPTS OF HUMAN ERROR

A single, all-embracing definition of human error is difficult to achieve. For the engineer, the worker in a system such as a chemical process plant may be

perceived as being there to perform a set of tasks to achieve specific operational objectives. There is therefore relatively little interest in the underlying mechanisms of failure. For the human reliability specialist, however, who is attempting to predict and optimize human performance, the underlying organizational and psychological causes of errors are of considerable importance.

The analysis of accidents and disasters in real systems makes it clear that it is not sufficient to consider error and its effects purely from the perspective of individual human failures. Major accidents are almost always the result of multiple errors or combinations of single errors with preexisting vulnerable conditions (Wagenaar et al., 1990). Another perspective from which to define errors is in terms of when in the system life cycle they occur. In the following discussion of the definitions of human error, the initial focus will be from the engineering and the accident analysis perspective. More detailed consideration of the definitions of error will be deferred to later sections in this chapter where the various error models will be described in detail (see Sections 5 and 6).

2.2.1. Engineering Concepts of Error

From a reliability engineering perspective, error can be defined by analogy with hardware reliability as "The likelihood that the human fails to provide a required system function when called upon to provide that function, within a required time period" (Meister, 1966). This definition does not contain any references to *why* the error occurred, but instead focuses on the consequences of the error for the system (loss or unavailability of a required function). The disadvantage of such a definition is that it fails to consider the wide range of other actions that the human might make, which may have other safety implications for the system, as well as not achieving the required function.

Meister (1977) classified errors into four major groupings:

- Performance of a required action incorrectly
- Failure to perform a required action (omission error)
- Performance of a required action out of sequence (combined commission/omission error)
- Performance of a nonrequired action (commission error)

This classification underscores the inadequacy of the approach common in reliability engineering of simply classifying errors into omission and commission categories.

An additional category related to the above was suggested by A. D. Swain:

- Failure to perform a required action within an allotted time

This is particularly relevant in situations where a human intervention is required in response to a potentially hazardous plant situation.

Although the above descriptions are, strictly speaking, **classifications** rather than **definitions** of error, they share the same characteristics as the first definition in that they describe *what* happened rather than *why* it happened. They are therefore much more easily related to the observable *consequences* of an error than to its causes.

2.2.2. Human Error in Accident Causation

Analysis of accidents and major losses in the CPI indicates that they rarely arise from a single human error or component failure. Often there is a combination of some triggering event (hardware or human) together with preexisting conditions such as design errors, maintenance failures or hardware deficiencies.

It is therefore useful to distinguish between active and latent errors or failures. An *active human error* has an immediate effect in that it either directly causes a hazardous state of the system or is the direct initiator of a chain of events which rapidly leads to the undesirable state.

Example 2.1: Active Human Error (Kletz, 1994b)

A plant worker opened the hatch of a reactor and manually charged it with caustic soda. However, he had failed to check the reactor prior to charging, and the caustic soda reacted with chemicals already present to release a toxic by-product. The worker was overcome, and only survived following emergency treatment.

In the case of a **latent human error** the consequences of the error may only become apparent after a period of time when the condition caused by the error combines with other errors or particular operational conditions. Two types of latent error can be distinguished. One category originates at the operational level and leads to some required system function being degraded or unavailable. Maintenance and inspection operations are a frequent source of this type of latent failure.

Example 2.2: A Latent Error Due to Misplaced Priorities

In an offshore oil production platform, a major accident occurred partly because pump seals failed and therefore an antifoaming agent was not delivered to a crude oil separator. The fact that the pump seals were defective should have been picked up during routine inspections, but the inspections were neglected because of production pressures. The failure to carry out the inspections was a latent error.

The other category of latent failures can occur at the level of engineering design or management policy. For example, the design of a scrubbing system

may not be adequate to handle all credible releases. If an active human error initiates the production of an excessive volume of product the system may allow toxic materials to be released to the environment.

Example 2.3: A Latent Error Due to Lack of Design Knowledge (Kletz, 1994b)

In the Flixborough disaster, one of six reactors in series, through which hot cyclohexane was passed, was removed from service (see Figure 2.1). Each reactor was connected by a short pipe with a bellows at each end to allow for expansion. The fifth reactor was replaced by a temporary bypass pipe with two bends in it to allow for differences in height between reactors 4 and 6. Because the bypass was not properly supported and had a bellows at either end, it moved when there were pressure variations. This movement eventually caused the bellows to fail, releasing 50 tons of cyclohexane which exploded, killing 28 men.

Inadequate ergonomic design in areas such as control panels and the labeling and placement of valves on the plant can also be regarded as a latent failure because it will increase the probability of active errors. For example, a worker may misread process information from a poorly designed display. Poorly labeled and situated valves can cause the wrong valve to be selected, with possibly disastrous consequences.

Management policies are the source of many of the preconditions that give rise to systems failures. For example, if no explicit policy exists or if resources are not made available for safety critical areas such as procedures design, the effective presentation of process information, or for ensuring that effective communication systems exist, then human error leading to an accident is, at some stage, inevitable. Such policy failures can be regarded as another form of latent human error, and will be discussed in more detail in Section 2.7.

Because errors are frequently recoverable, it is also appropriate to define another category of errors, recovery failures. These are failures to recover a chain of events leading to a negative consequence (assuming that such a recovery was feasible) before the consequence occurs. This includes recovery from both active and latent failures.

For the sake of completeness, it is also useful to define at this stage the category of errors known as **violations**. Violations occur when a worker carries out actions that are either prohibited or are different from those which are prescribed by the organization and carry some associated risks. Since violations are deliberate acts, they are not, strictly speaking, errors. However, the violations category is useful when classifying human caused failures.

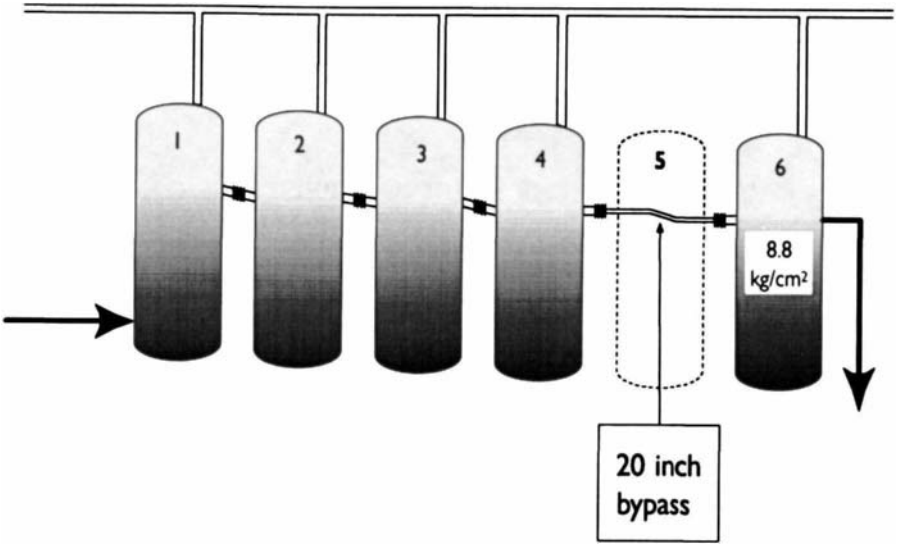

FIGURE 2.1 **Arrangement of Bypass Pipe at Flixborough (Kletz, 1994b).**

2.2.3. Summary of Definitions

Active Error/Failure: An active human error is an unintended action or an intended action based on a mistaken diagnosis, interpretation, or other failure, which is not recovered and which has significant negative consequences for the system.

Latent Human Error/Failure (operational level): A latent human error is similar to an active error, but the consequences of the error may only become apparent after a period of time or when combined with other errors or particular operational conditions.

Latent Human Error/Failure (management level): A management level human error is an inadequate or nonexistent management policy which creates the preconditions for active or latent human, hardware, or software failures.

Violation Error/Failure: A violation error occurs when an intended action is made which deliberately ignores known operational rules, restrictions, or procedures. However, this definition excludes actions that are deliberately intended to harm the system, which come within the category of sabotage.

Recovery Error/Failure: A recovery failure occurs if a potentially recoverable active or latent error is not detected or remedial action is not taken before the negative consequences of the error occur.

In the above definitions, the term "error" is used for the error event itself, and "failure" for the consequences of the error event.

2.3. AN OVERVIEW OF THE FOUR PERSPECTIVES ON HUMAN ERROR

The four perspectives to be discussed in detail later in this chapter are contrasted in Table 2.1 in terms of the error control strategies that are usually employed, their main areas of application and the frequency that the approaches are applied in the CPI.

2.3.1. Traditional Safety Engineering

The first perspective is the traditional safety engineering approach (Section 2.4). This stresses the individual factors that give rise to accidents and hence emphasizes selection, together with motivational and disciplinary approaches to accident and error reduction. The main emphasis here is on *behavior modification,* through persuasion (motivational campaigns) or punishment. The main area of application of this approach has been to occupational safety, which focuses on hazards that affect the individual worker, rather than process safety, which emphasizes major systems failures that could cause major plant losses and impact to the environment as well as individual injury.

2.3.2. Human Factors Engineering/Ergonomics

The second perspective to be considered in this chapter is the human factors engineering (or ergonomics) approach (HFE/E). This approach, described in Section 2.5, emphasizes the mismatch between human capabilities and system demands as being the main source of human error. From this perspective, the primary remedy is to ensure that the design of the system takes into account the physical and mental characteristics of the human. This includes consideration of factors such as:

- Workplace and job design to accommodate the job requirements of workers with differing physical and mental characteristics
- Design of the human–machine interface (HMI) such as control panels to ensure that process information can be readily accessed and interpreted and that appropriate control actions can be made
- Design of the physical environment (e.g., heat, noise, lighting), to minimize the negative physical and psychological effects of suboptimal conditions
- Optimizing the mental and physical workload on the worker

TABLE 2.1
Comparisons between Various Perspectives on Human Error

SOURCE OF ERROR APPROACH AND CONTROL STRATEGY	MAIN AREAS OF APPLICATION	TYPICAL APPROACHES	CURRENT USE BY THE CPI
Traditional Safety Engineering approach (control of error by motivational, behavioral, and attitude change)	• Occupational safety • Manual operations	• Selection • Behavior change via motivational campaigns • Rewards/punishment	Very common
Human Factors Engineering/Ergonomics approach (control of error by design, audit, and feedback of operational experience)	• Occupational/process safety • Manual/control operations • Routine operation	• Task analysis • Job design • Workplace design • Interface design • Physical environment evaluation • Workload analysis	Infrequent
Cognitive Engineering approach (control of error by design, audit, and feedback of operational experience, with particular reference to mental skills such as problem-solving and diagnosis)	• Process safety • Decision making/problem solving • Abnormal situations	• Cognitive task analysis • Decision support during emergencies • Incident analysis for human error root causes	Rare
Sociotechnical approach (control of error through changes in management policy and culture)	• Occupational/process safety • Effects of organizational factors on safety • Policy aspects • Culture	• Interviews • Surveys • Organizational redesign • Total Quality Management	More frequent in recent years

The emphasis on factors that can be manipulated during the design of a plant has led to the human factors engineering approach being described as "fitting the job to the person." This is in contrast to the approach of "fitting the person to the job," which focuses on training, selection, and behavior-modification approaches. The latter perspective is closer to the traditional safety approach. In fact, training is also usually considered by the human factors engineer, whereas occupational psychologists focus on the selection aspects. The HFE/E approach can be applied to both occupational and process safety and to manual and control room operations. The techniques and data available from the HFE/E approach have been largely developed and applied within the military, aerospace, and power generation sectors in the United States,

although in Europe there has also been a long standing human factors research tradition in the process industries (see, e.g., Edwards and Lees, 1974; Goodstein et al., 1988). The practical application of these approaches to the CPI in both Europe and the United States has, however, been somewhat limited.

2.3.3. Cognitive Systems Engineering

The third approach, cognitive systems engineering (CSE) is described in Section 2.6. This is particularly useful in analyzing the higher level human functions involved in CPI operations, for example, problem solving, decision making, and diagnosis. It also provides an explanation of the underlying causes of errors in a wide range of CPI operations.

The approach developed from a general change in emphasis in applied psychology during the 1970s and 1980s, from viewing the human as a passive black box, analogous to an engineering component, to the view that individuals were purposeful in that their actions were influenced by future goals and objectives. The cognitive systems engineering approach is particularly applicable to activities such as planning and handling abnormal situations. Its methods include cognitive task analysis, which focuses on information processing failures, and the use of decision support systems of varying levels of sophistication to assist in the handling of abnormal situations. To date, the application of the approach has been limited in process plants, although the development of interest in the area by human factors specialists has stimulated research into the nature of the skills possessed by process workers. Nevertheless, this approach is the most comprehensive in terms of evaluating the underlying causes of errors. This means that it has particular relevance to analyzing the causes of recurrent errors and for predicting specific errors that may have serious consequences as part of safety analyses.

2.3.4. Sociotechnical Systems

The fourth approach, the sociotechnical systems perspective, is described in Section 2.7. This arose from a realization that human performance at the operational level cannot be considered in isolation from the culture, social factors and management policies that exist in an organization. For example, the availability of good operating procedures is well known as an important contributory factor in influencing the likelihood of errors leading to major disasters. The existence of good procedures requires a procedures design policy to be implemented by plant management. This should include elements such as participation by the eventual users of the procedures, design of the procedures based on analysis of operational tasks, their preparation in accordance with accepted human factors principles, and a system for modifying the procedures in light of operational experience. All of this requires resources to

be allocated by managers at an appropriate level in the organization. The existence of good quality procedures does not guarantee that they will be used. If a culture exists that encourages workers to take shortcuts not specified in the procedures in order to achieve required production levels, then accidents and losses may still occur. These are typical issues that are considered by the sociotechnical systems approach.

The sociotechnical systems perspective is essentially top-down, in that it addresses the question of how the implications of management policies at all levels in the organization will affect the likelihood of errors with significant consequences. The sociotechnical systems perspective is therefore concerned with the implications of management and policy on system safety, quality, and productivity.

2.3.5. Conclusions

The approaches described in this chapter can be regarded as complementary rather than competing methodologies. They all have a part to play in an integrated approach to the management of human error to reduce accidents in the CPI. Having said this, we will place rather more emphasis on approaches other than the traditional safety approach in this book.

This is partly because the traditional approach is well known and documented in the industry, whereas the other approaches have received very little application to date. In addition, despite the successes of the traditional approach in the area of occupational safety, it may be less applicable in areas such as the prevention of major chemical accidents.

This is because many of the factors that have been shown to be the antecedents of major process accidents (e.g., poor procedures, inadequate training) are not usually under the control of the individual worker. The other approaches can also be applied to improving quality and productivity as well as process safety and can be readily integrated with engineering system safety techniques, as will be described in Chapters 4 and 5.

2.4. THE TRADITIONAL SAFETY ENGINEERING APPROACH TO ACCIDENTS AND HUMAN ERROR

The traditional safety engineering approach to accident causation focuses on the individual rather than the system causes of error. Errors are primarily seen as being due to causes such as lack of motivation to behave safely, lack of discipline or lack of knowledge of what constitutes safe behavior. These are assumed to give rise to "unsafe acts." These unsafe acts, in combination with "unsafe situations" (e.g., unguarded plant, toxic substances) are seen as the major causes of accidents.

One of the origins of this view of error and accident causation is the theory of accident proneness, which tried to show that a small number of individuals were responsible for the majority of accidents. Despite a number of studies that have shown that there is little statistical evidence for this idea (see, e.g., Shaw and Sichel, 1971); the belief remains, particularly in traditional industries, that a relatively small number of individuals account for the majority of accidents. Another element in the emphasis on individual responsibility has been the legal dimension in many major accident investigations, which has often been concerned with attributing blame to individuals from the point of view of determining compensation, rather than in identifying the possible system causes of error.

2.4.1. Accident Prevention from the Traditional Perspective

Based on this view of accident causation, certain strategies for prevention emerge. The control of unsafe conditions is achieved partly by methods such as eliminating the hazard at its source or by the use of guards or protective equipment. However, the majority of resources are directed at eliminating unsafe acts, either by motivating the worker to change his or her behavior or by retraining, on the assumption that much unsafe behavior is simply due to lack of knowledge, or because the correct way to do things has been forgotten. Retraining, in this context, usually refers to reinforcing existing work practices, or "more of the same."

The basic assumption is that the individual always has the choice of whether or not to behave in an unsafe manner. The implication of this assumption is that the responsibility for accident prevention ultimately rests with the individual worker. It also implies that as long as management has expended reasonable efforts to persuade an individual to behave responsibly, has provided training in safe methods of work, and has provided appropriate guarding of hazards or personal protection equipment, then it has discharged its responsibilities for accident prevention. If these remedies fail, the only recourse is disciplinary action and ultimately dismissal.

In some cases, more subtle approaches to behavior modification have been employed. Applications of behavior modification to safety are discussed in McKenna (1989), Hale and Glendon (1987), and Petersen (1984).

Modern behavior-modification programs rely on the identification and reinforcement of safe behaviors. Considerable improvements in measures of safety performance have been attributed to the introduction of these approaches (see McSween, 1993, for a petrochemical example). However, other studies have indicated that performance may return to its original level if the programs are withdrawn. It is therefore important to maintain a continuing program to ensure that the initial levels of improvements are maintained. Also, the benefits of behavior modification programs have mainly been demonstrated in the context of work activities where there is a high level of

discretion with regard to how tasks are carried out. Thus, existing "unsafe behaviors" can be identified and alternative acceptable behaviors substituted in their place. In the case study cited in Marcombe et al. (1993) for example, the main unsafe behaviors that were cited as precursors to accidents were as follows: not checking out equipment, tools, and the work area; not using personnel protective equipment; and not using the proper body position required by the task. These behaviors were the focus of the program.

2.4.2. Disadvantages of the Traditional Approach

Despite its successes in some areas, the traditional approach suffers from a number of problems. Because it assumes that individuals are free to choose a safe form of behavior, it implies that all human error is therefore inherently blameworthy (given that training in the correct behavior has been given and that the individual therefore knows what is required). This has a number of consequences. It inhibits any consideration of alternative causes, such as inadequate procedures, training or equipment design, and does not support the investigation of root causes that may be common to many accidents. Because of the connotation of blame and culpability associated with error, there are strong incentives for workers to cover up incidents or near misses, even if these are due to conditions that are outside their control. This means that information on error-inducing conditions is rarely fed back to individuals such as engineers and managers who are in a position to develop and apply remedial measures such as the redesign of equipment, improved training, or redesigned procedures. There is, instead, an almost exclusive reliance on methods to manipulate behavior, to the exclusion of other approaches.

The traditional approach, because it sees the major causes of errors and accidents as being attributable to individual factors, does not encourage a consideration of the underlying causes or mechanisms of error. Thus, accident data-collection systems focus on the characteristics of the individual who has the accident rather than other potential contributory system causes such as inadequate procedures, inadequate task design, and communication failures.

The successes of the traditional approach have largely been obtained in the area of occupational safety, where statistical evidence is readily available concerning the incidence of injuries to individuals in areas such as tripping and falling accidents. Such accidents are amenable to behavior modification approaches because the behaviors that give rise to the accident are under the direct control of the individual and are easily predictable. In addition, the nature of the hazard is also usually predictable and hence the behavior required to avoid accidents can be specified explicitly. For example, entry to enclosed spaces, breaking-open process lines, and lifting heavy objects are known to be potentially hazardous activities for which safe methods of work

can be readily prescribed and reinforced by training and motivational campaigns such as posters.

In the case of process safety, however, the situation is much less clear cut. The introduction of computer control increasingly changes the role of the worker to that of a problem solver and decision maker in the event of abnormalities and emergencies. In this role, it is not sufficient that the worker is trained and conditioned to avoid predictable accident inducing behaviors. It is also essential that he or she can respond flexibly to a wide range of situations that cannot necessarily be predicted in advance. This flexibility can only be achieved if the worker receives extensive support from the designers of the system in terms of good process information presentation, high-quality procedures, and comprehensive training.

Where errors occur that lead to process accidents, it is clearly not appropriate to hold the worker responsible for conditions that are outside his or her control and that induce errors. These considerations suggest that behavior-modification-based approaches will not in themselves eliminate many of the types of errors that can cause major process accidents.

Having described the underlying philosophy of the traditional approach to accident prevention, we shall now discuss some of the specific methods that are used to implement it, namely motivational campaigns and disciplinary action and consider the evidence for their success. We shall also discuss another frequently employed strategy, the use of safety audits.

2.4.3. Safety Campaigns

On the assumption that poor motivation or lack of safety awareness have a major contribution to accidents, most companies carry out safety campaigns. A safety campaign may be defined as "an operation or program aimed at influencing people to think or act in a safe manner." Such programs are designed to influence behavior using praise, punishment or fear. In addition, they may also provide specific information as a reinforcement for safety training.

There are at least three different forms of motivational campaigns: posters, films, and incentive schemes.

For posters, there are broadly four distinct types: (1) those appealing to a general awareness of safety issues; (2) those containing a warning or information on specific hazards; (3) pPosters providing general information on, for example, regulatory requirements; and (4) fear-inducing posters.

Films or videos cover the same broad areas as posters. They are typically fairly short (not more than 30 minutes) and are usually intended to be used during training. Instructor's notes are often supplied with the audiovisual material.

Many companies operate incentive schemes, ranging from competitions among departments or factories for an award (e.g., a certificate or trophy) to

elaborate schemes involving inspection and auditing to check for the achievement of certain safety objectives, which are rewarded with prizes.

The question of the effectiveness of motivational campaigns is not easy to answer. The obvious method would be to look at accident rates. However, recorded accident rates vary widely according to the propensity to report or not report events.

A safety campaign may only reduce the willingness of the workforce to report an accident rather than significantly reducing the underlying accident occurrences and hazards.

This is a problem that is not unique to motivational campaigns but is common to all approaches involving the monitoring of accidents or human error, as will be discussed in Chapter 6.

An indirect way to evaluate the effectiveness of safety campaigns is to look at some other observable "performance indicator" such as the use of personal protection equipment (PPE). Many campaigns are targeted at increasing the use of different types of PPE. Monitoring the results of such campaigns is done by establishing a baseline level of use of the equipment prior to the campaign and then looking at the percentage change in this use by the same workforce shortly after the campaign and then after some months have passed. Table 2.2 gives some summary results from a study by Pirani and Reynolds (1976) showing the effects of different types of motivational schemes on the use of PPE for head, hands, eyes, and feet. The first column shows the change from the baseline measurement 2 weeks after the campaign. The second column records the change from the baseline 4 months after the campaign.

In Table 2.2 the results from the use of posters and films are shown in the first three rows. Two points should be noted. First, all three measures show only short term gains. After four months the change in the pattern of use of

TABLE 2.2
Effect of Different Motivational Schemes on Use of PPE (adapted from Pirani and Reynolds, 1976)

MEASURE	PERCENT CHANGE AFTER 2 WEEKS	PERCENT CHANGE AFTER 4 MONTHS
General safety posters	+51%	+11%
Appropriate films	+40%	+11%
Fear posters	+18%	- 2%
Disciplinary measures	+39%	- 7%
Discussion + opinion leaders	+ 9%	+ 2%
Role playing	+71%	+68%

PPE is very similar, if not lower, than the baseline level. This result has been verified by other researchers. Second, the use of fear-inducing posters was not as effective as the use of general safety posters. This is because unpleasant material aimed at producing high levels of fear often affects peoples' *attitudes* but has a varied effect on their *behavior*. Some studies have found that the people for whom the fearful message is least relevant—for example, nonsmokers in the case of anti-smoking propaganda—are often the ones whose attitudes are most affected. Some posters can be so unpleasant that the message itself is not remembered.

There are exceptions to these comments. In particular, it may be that horrific posters change the behavior of individuals if they can do something immediately to take control of the situation. For example, in one study, fear-inducing posters of falls from stairs, which were placed immediately next to a staircase, led to fewer falls because people could grab a handrail at once. In general, however, it is better to provide simple instructions about how to improve the behavior rather than trying to shock people into behaving more safely. Another option is to link competence and safe behavior together in people's minds. There has been some success in this type of linkage, for example in the oil industry where hard hats and safety boots are promoted as symbols of the professional.

Table 2.2 indicates that the most successful campaign to encourage the use of PPE involved the use of role playing. This is where people are asked to advocate differing views from their own or to act in ways which differed from their usual behavior. In this case, those workers who did not normally wear protective equipment could, for example, be asked to take part in a discussion supporting the wearing of PPE. Such role playing may be effective for two reasons. First, the person will gain greater familiarity with the opposing view. Second, and more importantly, people need to justify why they are doing something and, in this case, advocating the opposite position competently might only be explainable to themselves in terms of partly believing in that position.

Table 2.2 does not include any reference to the effectiveness of incentive schemes. The evidence in this regard is not conclusive. There have often been reports of quite spectacular improvements in accident rates. However, these do not form a controlled evaluation. The main difficulty in trying to establish the effectiveness of incentive schemes is that such campaigns are often only part of a "total safety climate" approach which includes changes in work procedures, job design, etc. In such cases it is difficult to separate out the effects of the incentive scheme alone. However, researchers suggest that simple competitions are not as effective as such "total safety climate" programs, especially when the latter include elaborate setting and monitoring of safety targets.

In summary, the following conclusions can be drawn with regard to motivational campaigns:

- Success is more likely if the appeal is direct and specific rather than diffuse and general. Similarly, the propaganda must be relevant for the workforce at their particular place of work or it will not be accepted.
- Posters on specific hazards are useful as short-term memory joggers if they are aimed at specific topics and are placed in appropriate positions. Fear or anxiety inducing posters must be used with caution. General safety awareness posters have not been shown to be effective
- The safety "campaign" must not be a one-shot exercise because then the effects will be short-lived (not more than 6 months). This makes the use of such campaigns costly in the long run despite the initial appearance of a cheap solution to the problem of human error.
- Motivational campaigns are one way of dealing with routine violations (see Section 2.5.1.1). They are not directly applicable to those human errors which are caused by design errors and mismatches between the human and the task. These categories of errors will be discussed in more detail in later sections.

2.4.4. Disciplinary Action

The approach of introducing punishment for accidents or unsafe acts is closely linked to the philosophy underlying the motivational approach to human error discussed earlier. From a practical perspective, the problem is how to make the chance of being caught and punished high enough to influence behavior. From a philosophical perspective, it appears unjust to blame a person for an accident that is due to factors outside his or her control. If a worker misunderstands badly written procedures, or if a piece of equipment is so badly designed that it is extremely difficult to operate without making mistakes, then punishing the individual will have little effect on influencing the recurrence of the failure.

In addition, investigations of many major disasters have shown that the preconditions for failure can often be traced back to policy failures on the part of the organization. Disciplinary action may be appropriate in situations where other causes have been eliminated, and where an individual has clearly disregarded regulations without good reason. However, the study by Pirani and Reynolds indicates that disciplinary measures were ineffective in the long term in increasing the use of personal protective equipment. In fact, four weeks after the use of disciplinary approaches, the use of the equipment had actually declined. The major argument against the use of disciplinary approaches, apart from their apparent lack of effectiveness, is that they create fear and inhibit the free flow of information about the underlying causes of accidents. As discussed earlier, there is every incentive for workers and line managers to cover up near accidents or minor mishaps if they believe punitive actions will be applied.

2.4.5. Safety Management System Audits

The form of safety audits discussed in this section are the self-contained commercially available generic audit systems such as the International Safety Rating System (ISRS). A different form of audit, designed to identify specific error inducing conditions, will be discussed in Section 2.7. Safety audits are clearly a useful concept and they have a high degree of perceived validity among occupational safety practitioners. They should be useful aids to identify obvious problem areas and hazards within a plant and to indicate where error reduction strategies are needed. They should also support regular monitoring of a workplace and may lead to a more open communication of problem areas to supervisors and managers. The use of safety audits could also indicate to the workforce a greater management commitment to safety.

Some of these factors are among those found by Cohen (1977) to be important indicators of a successful occupational safety program. He found that the two most important factors relating to the organizational climate were evidence of a strong management commitment to safety and frequent, close contacts among workers, supervisors, and management on safety factors. Other critical indicators were workforce stability, early safety training combined with follow-up instruction, special adaptation of conventional safety practices to make them applicable for each workplace, more orderly plant operations and more adequate environmental conditions.

Despite these potential benefits, there are possible problems associated with the use of generic safety audit systems. Questions that need to be considered in the case of such standardized audits include:

- How are the critical factors identified?
- What validation exists for such schemes?
- What does it really mean to do well on such audits i.e. what evaluation criteria are being used?
- What is the likelihood of missing an industry specific hazard when using a general scheme?

Such audits may therefore be useful as a method of increasing safety awareness and management commitment to safety as part of a more general attempt to reduce accidents. They should be treated as first steps and management must be prepared to do more than just carry out a safety audit. The authors of safety audits must be prepared to provide guidance on the next steps in error reduction once the problems have been identified.

Problems can also arise when the results of safety audits are used in a competitive manner, for example, to compare two plants. Such use is obviously closely linked to the operation of incentive schemes. However, as was pointed out earlier, there is no evidence that giving an award to the "best plant" produces any lasting improvement in safety. The problem here is that the competitive aspect may be a diversion from the aim of safety audits, which

is to identify problems. There may also be a tendency to "cover-up" any problems in order to do well on the audit. Additionally, "doing well" in comparison with other plants may lead to unfounded complacency and reluctance to make any attempts to further improve safety.

2.4.6 Training

There is no question that training, particularly where it is task specific, is extremely important in the attempt to reduce human failures. Safety campaigns must always support, not replace safety training. However, all too often, organizations have attacked the problem of human error as simply a matter of training. Training departments have become the dumping grounds for problems created by factors such as bad design and poor management. It must be recognized that even the best-trained worker will experience difficulties if he or she is faced with a complex problem, a poorly designed human–machine interface, unrealistic task and workload demands and a "turbulent" environment with noise, interruptions, and stress. No amount of training can totally compensate for all of these adverse factors. Training should therefore consider the design of the task, equipment, job aids, and similar factors rather than be used instead of them. Training has to be directed at the underlying causes of an error and for this reason, reporting systems need to explicitly identify these root causes. Unfortunately, in many cases, the training approach adopted in response to errors is to provide "more of the same."

2.5. THE HUMAN FACTORS ENGINEERING AND ERGONOMICS APPROACH (HF/E)

Human factors engineering (or ergonomics), is a multidisciplinary subject that is concerned with optimizing the role of the individual in human–machine systems. It came into prominence during and soon after World War II as a result of experience with complex and rapidly evolving weapons systems. At one stage of the war, more planes were being lost through pilot error than through enemy action. It became apparent that the effectiveness of these systems, and subsequently other systems in civilian sectors such as air transportation, required the designer to consider the needs of the human as well as the hardware in order to avoid costly system failures.

The practical needs of military and aerospace systems tended to focus interest on human–machine interfaces (e.g., aircraft cockpits), with particular emphasis on information displays and the design of controls to minimize error. The predominant model of the human prevalent at that time (called *behaviorism*) concentrated exclusively on the inputs and outputs to an individual and ignored any consideration of thinking processes, volition, and other

distinctively human characteristics. However, this model considerably influenced the early workers in HF/E. In fact many of the tasks that were studied in military systems were highly proceduralized and therefore involved little use of higher level skills such as decision making or problem solving. It was therefore possible for early HF/E practitioners to make a contribution to the design of more effective systems even though they only considered a limited subset of human skills and capabilities.

From the 1960s onward, there was a greater interest in psychological issues, dominated by the concept of the human as a single-channel processor of information. This stimulated research into a number of areas. Studies of mental workload were concerned with the ability of humans to cope with extremely high levels of information in situations such as air traffic control. Vigilance studies, which focused on the human's role in situations with very low levels of stimulation such as radar monitoring, represented the other extreme of human performance that was considered.

The conceptualization of the human as a single-channel processor of information was useful in emphasizing the need to design systems to take into account human capabilities and limitations. It did not, however, consider issues such as the meaning that people assign to their work, their intentions, and topics such as problem solving, decision making, and diagnosis. Despite these limitations, the traditional HF/E approach has been the source of many of the practical approaches and techniques which will be described in subsequent chapters. Some of the key concepts used in this approach will therefore be described in this section.

From the traditional HF/E perspective, error is seen as a consequence of a mismatch between the demands of a task and the physical and mental capabilities of an individual or an operating team. An extended version of this perspective was described in Chapter 1, Section 1.7. The basic approach of HF/E is to reduce the likelihood of error by the application of design principles and standards to match human capabilities and task demands. These encompass the physical environment (e.g., heat, lighting, vibration), and the design of the workplace together with display and control elements of the human–machine interface. Examples of the approach are given in Wilson and Corlett (1990) and Salvendy (1987).

2.5.1. The Human–Machine Interface

The human–machine interface (usually abbreviated to interface) is a major focus of interest for the HF/E approach to the reduction of human error. A representation of the interface in a CPI context is provided in Figure 2.2. The interface is the boundary across which information from the process is transduced by sensors and then displayed in a form that can be utilized by the

human process controllers. It also allows control actions to be made to change the state of the system.

Figure 2.2 provides a more detailed description of the human side of the interface. This is based on the information processing model of Wickens (1984). It describes how the information presented at the interface (e.g., a control panel) goes through various stages of processing before a response is eventually made in the form of a control action (e.g., pressing a button to close a valve). The first stage, sensing and perception, involves the information being captured by a sensory channel, for example, vision, after which it will be stored in a limited-capacity store called working memory. The way in which information is acquired will be influenced by the knowledge and experience of the world, which is part of the observer's long-term memory. For example, an operator scanning a control panel for indications of problems will tend to focus on sources of information (e.g., alarms) that have proved to be particularly important in the past.

Interpretation of the information in working memory involves the use of knowledge and experience from long-term memory. For example, on the basis of experience, the panel operator may interpret a rapid rise in temperature as indicative of a dangerous situation. The process of diagnosis and then deciding on and selecting an appropriate response occurs at the next stage of processing (represented by the next box in Figure 2.2). Finally, an appropriate response is initiated (e.g., closing the valve), which will change the state of the system. This, in turn, will be displayed by the interface, thus completing the processing loop.

The Wickens model suggests that there are finite information-processing or attentional resources available, as represented by the box in Figure 2.2. These resources can be distributed in different ways but cannot be increased. Thus, interpretation of complex or unusual information displayed by the interface will leave fewer resources available for handling the response selection and decision making demands. This provides a theoretical basis for the view of human error described in Section 1.7, which described error as a mismatch between demands and capabilities.

A familiar example of limited attentional resources being distributed among different mental and physical processes occurs in car driving. A driver in a foreign country who is required to operate a manual gear change system, and at the same time drive on the opposite side of the road, may find that he or she has little capacity available to navigate or respond to a sudden stop by the car in front.

In the CPI, the most extensively studied human–machine interface is in the central control room in automated plants where plant information is displayed on visual display units (VDUs) and appropriate control actions are made by the operating team. In the case of a highly automated plant, the primary role of the human is to respond to unexpected contingencies such as plant states that have not been anticipated by the designers of the automatic

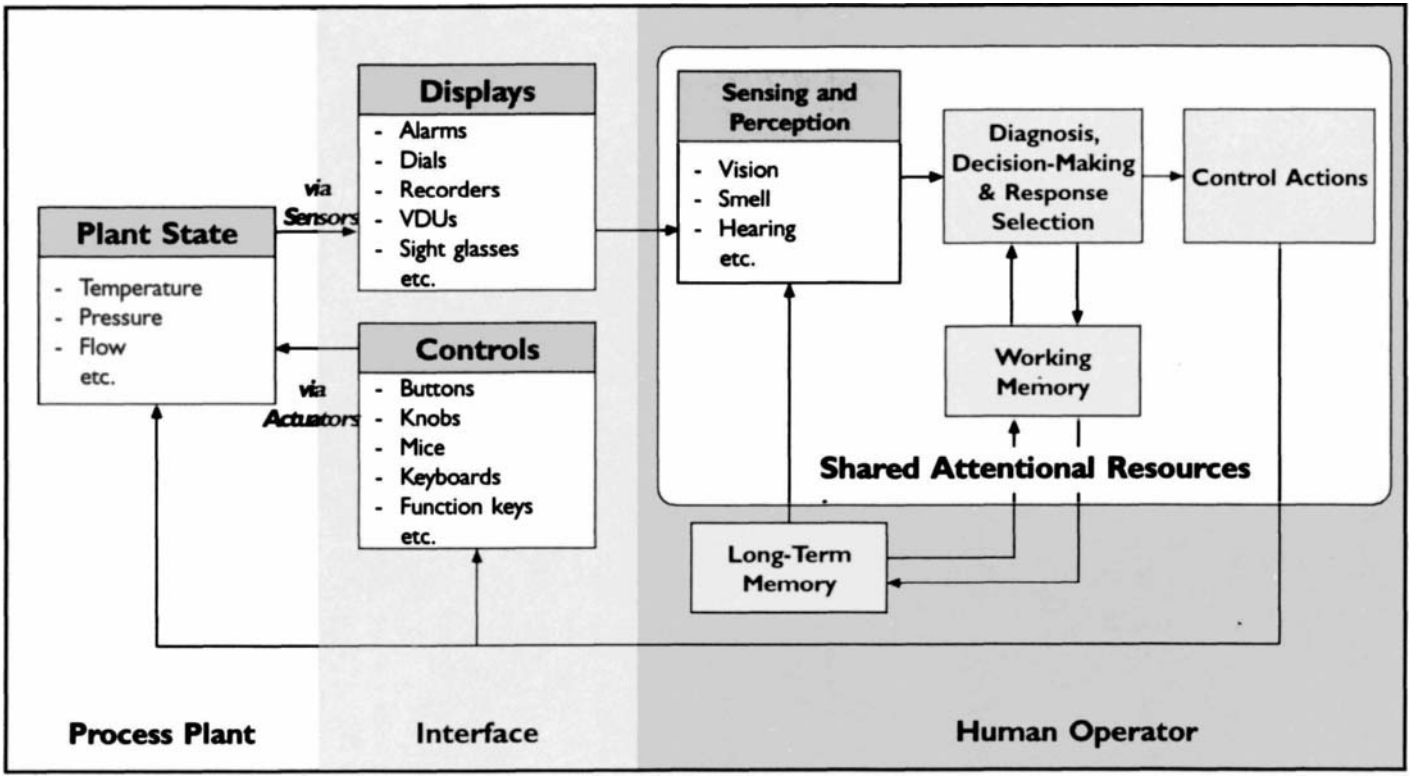

FIGURE 2.2. **The Human–Machine Interface (adapted from Wickens, 1984).**

control and protection systems. Even in the most automated systems such interventions are likely to occur occasionally, due to the difficulty of anticipating every process state in a complex plant. Only extremely simple processes can be completely automated. Although a large number of highly automated plants exist, it is probably true to say that the majority still require considerable human intervention from the control room, together with manual operations on the plant. This is particularly true of batch processes. The issue of whether or not automation is the solution to the problem of human error will be discussed further in Section 2.5.5.

Although most research on human factors in process control has focused on the control room interface, in fact the human–machine interface concept can be applied to all situations where the CPI worker has to take actions based on information acquired directly or indirectly concerning the state of the process. For example, a local indicator situated close to a reactor or a charging vessel is also a process interface. In these cases, the displays may consist of a sight glass or level indicator and the controls may be manually operated valves. It is important to emphasize that the principles of interface design are of equal importance to these situations as in a central control room. In fact, there is a tendency to focus interface design resources in the control room at the expense of equally critical but less prominent interfaces on the plant. Neglect of operability considerations by designers often leads to highly error inducing situations on the plant such as gauges displaying important information being placed in inaccessible positions, and valves or process lines being unlabeled.

Example 2.4: An Error Due to a Poorly Designed Interface

In a resin plant, solvents were directed from storage tanks to a blender by means of solvent charging manifold. Because of the poor panel layout and labeling of the charging manifold, a worker made connections that pumped solvent to blender 21A instead of 12A as directed by the instructions. An earlier error had left the valve open from the charging manifold to blender 21A and hence the misdirected solvent degraded a batch already in the blender (this example will be analyzed in more detail in Chapter 7).

The functions of the interface can be summarized as follows:

- To allow the presentation of process information consistent with the worker's needs and expectations (e.g., monitoring normal operations, responding to abnormalities in emergencies)
- To provide immediate feedback for control actions
- To support diagnosis, decision making and planning
- To facilitate the selection of the correct control actions and minimize accidental activation of controls

A number of design principles exist to achieve these aims, and these are described in detail in handbooks such as those described in the Bibliography at the end of the book. Examples of such principles are given below:

- *Representational layout of control panels.* Where the physical location of items is important, for example, area displays in fire control systems, the layout of the displays on a control panel should reflect the geographical layout of the plant. In other cases a functional arrangement of the elements of the process plant will be appropriate, for example, when monitoring the status of the system via an alarm panel.
- *Sequential design.* When a particular procedure is always executed in sequential order, for example, the start-up of a distillation column, a similar sequential arrangement of the controls will help to ensure that parts of the sequence are not omitted.
- *Design according to frequency of use or importance.* Controls and displays that are frequently used or are of special importance (e.g., critical alarms), should be placed in prominent positions, for example, near the center of the control panel.
- *Hierarchical organization of information.* Information should be provided at a range of different levels of detail from major systems such as reactors, to individual components such as valves, in order to satisfy a range of different process control requirements.

2.5.2. Human Error at the Human–Machine Interface

The following sections discuss how errors can arise at each of the stages of perception, decision-making and control actions. The account given below of how information is processed by the human perceptual system is highly simplified. More technical descriptions are provided in many textbooks, for example, Wickens (1984).

2.5.2.1. Perception

As described earlier, in the first stage of perception, information is acquired via the senses from a number of sources. These may include gauges and chart recorders, VDU screens in a control room, verbal communication with individuals on the plant, or direct observation of process variables. In the short term, this information provides feedback with regard to specific control actions.

For example, if a worker turns on a stirrer in a reactor, he or she may use a local or control room indicator to verify that current is flowing to the agitator motor. Errors may arise at several points in the input process. At the sensory stage, there may be so many sources of information that the worker may be unable to scan them all in the time available. This can be a particular problem when a large number of alarms occur following a major process disturbance.

The information may not be readily distinguishable either because it is too faint or because it may not be easily separated from other similar information. For example, a critical measurement on a multipoint temperature recorder may be lost in the surrounding clutter of irrelevant information. As discussed in the cognitive engineering approach described in Section 2.6, the worker may also ignore sources of information because of preconceptions that lead him or her to believe they are not significant.

The sensory input information is interpreted according to the worker's **mental model** of the process. The mental model is stored in long-term memory and is an internal representation of the process and its dynamics, which is used as a basis for decision making. This model is built up on the basis of the worker's experience in operating the plant and gaining an intuitive "feel" of the effects of various control actions. The model may be quite different from a chemical engineering model of the plant process but may be perfectly adequate as a basis for controlling the plant. However, if the model is based only on the worker's experience of the plant under normal operating conditions, errors could occur if actions are made in unusual situations for which the model does not apply.

This implies that plant controllers need frequent exposure to problem-solving training and evaluation to ensure that their mental model is kept up to date. A more detailed consideration of mental models is contained in Lucas (1987).

2.5.2.2. Decision Making

During the decision-making stage, evidence acquired from the system is used in an individual's working memory in conjunction with information from long-term memory to decide on an appropriate course of action. The long-term store contains the "mental model" mentioned earlier. The compatibility of the mental model to the actual state of the system and the process dynamics has an important bearing on the likelihood of an error being made. The translation between the actual state of the system and the mental model is facilitated by the use of displays such as schematic diagrams and the availability of hierarchically organized display systems. These have the effect of reducing the information-processing load involved in translating the plant display into an internal mental representation of the process.

Decision making may involve calculations, reference to procedures and past experience, and other demands on long-term memory. This contributes further to the overall mental workload. From the HF/E perspective, many errors are likely to arise from information processing overload, essentially from the mismatch between demands and capabilities. Information-processing demands can be reduced by the provision of information in the form of job aids such as flow charts or decision trees.

2.5.2.3. Control Actions

The final stage of the information-processing chain involves the selection and execution of a particular control action or response, on the basis of the decisions made in the preceding stage. The complexity of the selection process is influenced by the number of alternative control strategies the worker has to choose from, the physical characteristics of the control to be operated and the familiarity of the control action. For example, if the shutdown button for a distillation column is clearly and unambiguously marked, very little searching or information processing is necessary. If controls are ambiguous, or closely crowded together, the likelihood of accidental activation increases, as do the processing demands on the worker. Ergonomics textbooks, such as those described in the general bibliography, contain extensive guidelines for the use of different control types depending on the application.

2.5.3. Information Processing and Mental Workload

As discussed in the last section, attentional resources (see Figure 2.2) are taken up whenever the worker takes in data via the sensory channels such as vision or hearing, and when carrying out processes such as decision making, and making control actions. Since there are limitations on these resources, information processing overload is a common cause of errors. If, for example, a person is trying to perform a complex fault diagnosis, he or she may not have any spare capacity to deal effectively with an unexpected process deviation. The total information-processing load on the individual from inputs, central processing, and outputs, is known as the mental workload. Comprehensive accounts of research in this area are provided by Moray (1979, 1988). Techniques for measuring mental workload are reviewed in Hockey et al. (1989) and Wierwille and Eggemeier (1993).

In order to minimize errors, it is important that the mental workload is within a person's capabilities. If the workload exceeds these capabilities by a moderate amount, the individual may be able to utilize short-term "coping strategies," to maintain performance. However, in addition to the fact that such strategies may involve elements of risk taking, they often lead to some physical or psychological cost. Experiments have shown that experienced workers such as air traffic controllers can maintain their performance even if they are asked to cope with increasing numbers of flights. However, they often exhibit chronic stress symptoms if they are required to maintain this performance over long periods of time. If the worker is forced to use coping strategies as a regular part of his or her work, it is likely that feelings of physical or mental strain will ensue. This may lead to long term problems such as stress illnesses and absenteeism. At very high levels of mental workload, even coping strategies will be inadequate and errors will start to increase rapidly. There has been a considerable amount of research carried out in the area of mental workload,

particularly in the aerospace industry. This has been partly driven by the desire to reduce staffing levels on flight decks.

In the case of the CPI, there are relatively few situations where control room workers are likely to face continuous periods of overload. However, when overload does occur it is likely to be associated with situations when the plant is in an unusual or abnormal state for which the workers may not have any rules or procedures available. In these situations, knowledge-based processing (see Section 2.6.2), which needs considerable mental resources, will be required and errors of diagnosis are likely to occur.

2.5.4. Automation and Allocation of Function

A commonly suggested solution to the problem of human error is to automate the plant process. The aim of automation is to replace human manual control, planning, and problem solving by automatic devices and computers. The topic of allocation of function is becoming increasingly important with the use of computer-based process control systems, which tend to change the role of the control process operator from that of a direct controller to a system monitor. Allocation of function is concerned with which functions to assign to human control and which to delegate to automatic systems such as computers. The engineering approach is normally to automate all functions for which it is technically feasible to develop an automatic system. In practice there are a number of problems associated with this approach. For example, operating conditions (e.g., the characteristics of feed stocks, the reliability of automatic controllers) are often more variable than the designer is able to take into account. This means that the automated system actually has to be controlled manually during a proportion of its operating range.

This form of unplanned manual operation is unsatisfactory on a number of counts. The fact that the operator may normally be insulated from the process by the automatic control systems means that he or she will probably not be able to develop the knowledge of process dynamics ("process feel") necessary to control the system manually, particularly in extreme conditions. Also, the fact that manual control was not "designed into" the systems at the outset may mean that the display of process information and the facilities for direct control are inadequate. A number of techniques are available to assist designers in the allocation of function process. Some of these are described in Meister (1985). In a paper entitled "Ironies of Automation" Bainbridge (1987) notes four areas where the changed role of the human in relation to an automated system can lead to potential problems. These will be discussed below.

2.5.4.1. The Deterioration of Skills

With automatic systems the worker is required to monitor and, if necessary, take over control. However, manual skills deteriorate when they are not used.

Previously competent workers may become inexperienced and therefore more subject to error when their skills are not kept up to date through regular practice. In addition, the automation may "capture" the thought processes of the worker to such an extent that the option of switching to manual control is not considered. This has occurred with cockpit automation where an alarming tendency was noted when crews tried to program their way out of trouble using the automatic devices rather than shutting them off and flying by traditional means.

Cognitive skills (i.e., the higher-level aspects of human performance such as problem solving and decision making), like manual skills, need regular practice to maintain the knowledge in memory. Such knowledge is also best learned through hands-on experience rather than classroom teaching methods. Relevant knowledge needs to be maintained such that, having detected a fault in the automatic system, the worker can diagnose it and take appropriate action. One approach is to design-in some capability for occasional hands-on operation.

2.5.4.2. The Need to Monitor the Automatic Process

An automatic control system is often introduced because it appears to do a job better than the human. However, the human is still asked to monitor its effectiveness. It is difficult to see how the worker can be expected to check in real time that the automatic control system is, for example, using the correct rules when making decisions. It is well known that humans are very poor at passive monitoring tasks where they are required to detect and respond to infrequent signals. These situations, called vigilance tasks, have been studied extensively by applied psychologists (see Warm, 1984). On the basis of this research, it is unlikely that people will be effective in the role of purely monitoring an automated system.

2.5.4.3. The Need to Hold an Accurate and Up-to-Date Mental Model of the Plant Processes

As discussed earlier, the successful diagnosis of faults in automated control systems is highly dependent on the mental model the worker has built up of the current state of the plant processes. Such a model takes time to construct. An individual who has to act quickly may not be able to make the necessary diagnoses without time to build up and consult his or her mental model. Even in a highly automated plant, provision needs to be made to display major process deviations quickly.

Example 2.5: Failure of Automated Process System Because Critical Information Was Not Displayed

In a highly automated plant, a violent exothermic reaction occurred because of an unanticipated interaction between a chemical process and

a by-product. The symptoms of the problem, a sudden temperature rise, went unnoticed because the process plant VDU display page for alarms was not being displayed, and there was no alarm algorithm to detect rapid temperature changes.

2.5.4.4. The Possibility of Introducing Errors

Automation may eliminate some human errors at the expense of introducing others. One authority, writing about increasing automation in aviation, concluded that "automated devices, while preventing many errors, seem to invite other errors. In fact, as a generalization, it appears that automation tunes out small errors and creates opportunities for large ones" (Wiener, 1985). In the aviation context, a considerable amount of concern has been expressed about the dangerous design concept of "Let's just add one more computer" and alternative approaches have been proposed where pilots are not always taken "out of the loop" but are instead allowed to exercise their considerable skills.

Example 2.6: An Error Due to Overreliance on Technology (Wiener, 1985)

Overreliance on technology was a feature of an accident involving a China Airlines B747-SP that occurred approximately 300 miles northwest of San Francisco in 1989. Toward the end of the flight, the aircraft suffered an in-flight disturbance at 41,000 feet following the loss of its number 4 engine. The aircraft, which was flying on autopilot at the time, rolled to the right during attempts by the crew to relight the engine, following which it entered into an uncontrolled descent. The crew were unable to restore stable flight until the aircraft reached 9500 feet, by which time the aircraft had exceeded its maximum operating speed and sustained considerable damage. In conducting its inquiry, the National Transportation Safety Board concluded that the major contributory factor underlying the incident occurrence was the crew's overdependence on the autopilot during attempts to relight the malfunctioning engine. The correctly functioning autopilot effectively masked the onset of loss of control of the aircraft.

2.5.5. System Reliability Assessment and Human Error

The main thrust of the HF/E approach is to provide the conditions that will optimize human performance and implicitly minimize human error. However, there is rarely any attempt to predict the nature and likelihood of *specific* human errors and their consequences. By contrast, the study of human error in the context of systems reliability is concerned almost exclusively with these latter issues. It is appropriate to introduce the systems reliability assessment approach to human error at this stage because, until recently, it was largely

based on the mechanistic view of the human in traditional HF/E which was described at the beginning of Section 2.5.

Interest in human error in **system reliability** originated in work on military missile systems in the 1950s, when it became apparent that a large proportion of system failures could be traced to errors in design, manufacturing, and assembly. The application of formal techniques such as fault tree analysis in nuclear safety and the occurrence of the Three Mile Island accident also emphasized the need for predictive analyses of human error. Human reliability assessment originated from a very specific engineering requirement: the need to insert human error probabilities in fault trees for assessing the likelihood that predefined procedures involving human actions would be successfully carried out. For this reason human reliability assessment in the context of safety analysis is very mechanistic in its philosophy and is based on a simplified version of the HF/E approach described in earlier sections. In the CPI, human reliability assessment forms an integral part of chemical process quantitative risk analysis (CPQRA). A comprehensive description of this application is given in a companion volume in this series, *Guidelines for Chemical Process Quantitative Risk Analysis* (1989b) published by CCPS. More detailed descriptions of specific quantification techniques are provided in Chapter 5 of this book and in Swain (1989), Miller and Swain (1987), Kirwan, Embrey, and Rea (1988), and Kirwan (1990).

In this mechanistic approach to human reliability, the individual is modeled as being analogous to a hardware component that provides a function when required. A definition of human reliability from this perspective is as follows:

Human reliability is the probability that a job or task will be successfully completed by personnel at any required stage in system operation within a required minimum time (if a time requirement exists) (Meister, 1966).

This has close affinities with definitions of system reliability from a hardware perspective, for example, "the probability of performing a function under specified conditions for a specific period of time" (Zorger, 1966).

When performing human reliability assessment in CPQRA, a qualitative analysis to specify the various ways in which human error can occur in the situation of interest is necessary as the first stage of the procedure. A comprehensive and systematic method is essential for this. If, for example, an error with critical consequences for the system is not identified, then the analysis may produce a spurious impression that the level of risk is acceptably low. Errors with less serious consequences, but with greater likelihood of occurrence, may also not be considered if the modeling approach is inadequate. In the usual approach to human reliability assessment, there is little assistance for the analyst with regard to searching for potential errors. Often, only omissions of actions in proceduralized task steps are considered.

Since this approach to human reliability has its roots in the traditional HF/E perspective, it does not include any systematic means for identifying errors due to failures in higher level human functions such as diagnosis. Nevertheless, such diagnostic errors can give rise to particularly serious failures, where they lead to an erroneous series of actions being initiated based on the mistaken diagnosis. The Three Mile Island accident was a typical result of these types of errors. In order to address cognitive errors of this type, a comprehensive model of human error is required, as is discussed in detail in Section 2.6.5 of this chapter. Techniques for systematically identifying human error in safety analyses are described in Chapter 5.

2.5.6. Summary and Evaluation of the HF/E Perspective on Human Error in the CPI

The traditional HF/E approach provides techniques and data relevant to optimizing human performance and minimizing certain categories of error in chemical process industry operations. The main application of human factors and ergonomics methods is in the design of new systems. However, audit checklists are available for evaluating HF/E deficiencies that could give rise to errors in existing systems. These are considered in Chapters 3 and 4. As part of this design process, many of the performance-influencing factors described in Chapter 3 are taken into account. Some of the techniques described in Chapter 4—for example, task analysis—are also employed during the design process.

The disadvantages of the classical HF/E perspective as a basis for human error prediction have been reviewed earlier. The approach focuses mainly on the external aspects of human performance and does not provide any systematic methods for error identification or for addressing underlying causes of errors. In addition, the HF/E approach does not provide a systematic framework for addressing and eliminating cognitive errors in areas such as diagnosis and problem solving.

2.6. THE COGNITIVE ENGINEERING PERSPECTIVE

The classical human factors engineering/ergonomics approach to human error was essentially based on a "black box" model of human behavior that focused primarily on information inputs and control action outputs. In this section a more modern perspective, based on approaches from cognitive psychology, is introduced. At one level, the cognitive perspective is still concerned with information processing, in that it addresses how people acquire information, represent it internally and use it to guide their behavior. The key difference from the HF/E approach is that the cognitive approach emphasizes the role of intentions, goals, and meaning as a central aspect of

Next Page