A Manager's Guide to

Reducing Human Errors

Improving Human Performance in the Process Industries

API PUBLICATION 770
MARCH 2001

American Petroleum Institute

Helping You Get The Job Done Right.SM

A Manager's Guide to Reducing Human Errors

Improving Human Performance in the Process Industries

Prepared under contract by
D. K. Lorenzo, P.E.,
EQE, International Inc.

February 2001

NOTICE

This Guide was prepared by EQE International, Inc. (EQE), an ABS Group Company, as an account of work sponsored by the Chemical Manufacturers Association (now the American Chemistry Council) and the American Petroleum Institute (API). Neither EQE, the American Chemistry Council, API, nor any of their employees, subcontractors, consultants, or other assigns make any warranty, express or implied, or assume any liability or responsibility for any use, or the results of such use, of any information, product, or process disclosed in this Guide, or represent that its use would not infringe upon privately owned rights.

ACKNOWLEDGMENTS

The following people are recognized for their contributions of time and expertise during this study and in the preparation of this report:

API Staff Contact

William J. Erny, Regulatory and Scientific Affairs Department

Don K. Lorenzo, EQE International, author of the report, appreciates the support given to this project by the American Petroleum Institute and the American Chemistry Council, which published the first edition of this Guide. The author also gratefully acknowledges the contributions of Dr. A. D. Swain who reviewed the first edition and originally developed many of the concepts, principles, and techniques described herein. In the first edition, the author quoted extensively from several of Dr. Swain's works: Design *Techniques for Improving Human Performance in Production* (Reference 3), *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications* (Reference 7), *Comparative Evaluation of Methods for Human Reliability Analysis* (Reference 10), and *Human Reliability in Chemical Processes — Training Course Notes* (Reference 15). We are also indebted to the reviewers of this Guide at EQE International, Inc.: L. N. Vanden Heuvel, J. S. Arendt, L. K. Adair, and P. M. Hafford. And we want to thank S. C. Barnwell, A. L. Nicely, and S. B. Ross for their skill and craftsmanship in preparing this document.

TABLE OF CONTENTS

Section		Page
NOTICE		iii
ACKNOWLEDGMENTS		v
PREFACE		ix
EXECUTIVE SUMMARY		xi
1.	**INTRODUCTION**	1
	1.1 Importance of Improving Human Performance	1
	1.2 Objectives and Organization of This Guide	2
2.	**UNDERSTANDING HUMAN ERROR**	5
	2.1 Definition of Human Error	5
	2.2 Theory of Human Error	6
	2.3 Performance Shaping Factors	8
3.	**STRATEGIES FOR IMPROVING HUMAN PERFORMANCE**	13
	3.1 Examples of Error-likely Situations	13
	3.2 General Approaches to Improving Human Performance	25
4.	**MANAGEMENT USE OF HRA**	29
	4.1 Definition of HRA	29
	4.2 Chartering the Analysis	30
	4.3 Selecting and Applying HRA Techniques	32
	4.4 Understanding the Limitations	36
5.	**CONCLUSIONS**	37
GLOSSARY		39
REFERENCES		45
BIBLIOGRAPHY		46

TABLE OF CONTENTS (con't.)

APPENDIX 1 Self-evaluation Questionnaire for Managers Considering Ways to Improve Human Performance 57

APPENDIX 2 Self-evaluation Survey 65

APPENDIX 3 Example HRA Problem Using the THERP Technique 79

LIST OF TABLES

Table		Page
1	Opportunities for Human Error	2
2	Internal PSFs	9
3	External PSFs	9
4	Stressor PSFs	10
5	Elements of the Work-situation Approach	13
6	HRA Motivations	29
7	Examples of Typical HRA Objectives	31
8	Major Limitations of HRA	36
9	Estimated Decreases in HEPs Resulting from Improvements in the Work Situation	38
10	Events Included in the HRA Event Tree	84
11	HRA Results	84

LIST OF FIGURES

Figure		Page
1	Simple Model of Human Behavior as a System Component	6
2	Random Error	7
3	Systematic Error	7
4	Sporadic Error	8
5	Operator as Essential Element of Overall Process System	8

LIST OF FIGURES (con't.)

6	Relationship of Stress and Performance	11
7	Exit Sign	16
8	Vigilance Effectiveness	23
9	Effects of Practice on Skills	28
10	Elements of an HRA Charter	30
11	Overview of HRA Methods	33
12	HRA Event Tree of Hypothetical Calibration Tasks	35
13	Typical Operator Action Tree	35
14	Propane Condenser Schematic	81
15	HRA Event Tree for Improper Condenser Isolation	83

PREFACE

Human errors have either directly caused or significantly contributed to many major accidents in the process industries. The American Chemistry Council, American Petroleum Institute, and their member companies recognize the importance of reducing human errors to enhance the safety, productivity, and quality of their manufacturing processes. But to improve human performance, managers need specific advice on what can be done to help prevent mistakes and to reduce the likelihood that such mistakes will lead to process upsets or accidents.

This Guide is intended for an audience of middle managers to senior executives who have different levels of knowledge about human factors engineering. It is designed to equip them with a basic understanding of the causes of human errors and to suggest ways for reducing human errors at individual facilities. It also describes how to incorporate human reliability analysis (HRA) into process safety management activities. To convey this information, we use the following steps:

- Establish a basic vocabulary (Glossary) needed to discuss human factors engineering and HRA with experts in the field
- Identify factors affecting human performance, especially those that managers can control
- Suggest ways to reduce human errors
- Describe how HRA can be incorporated in process safety management activities

Section 1 discusses the importance of improving human performance and also discusses the objectives of this Guide. Section 2 defines human error and discusses its most common causes. Section 3 identifies many specific factors in the workplace that increase the likelihood of human errors and discusses ways to improve human performance.

If a manager requires a numerical estimate of the probability of human error, there are several HRA techniques available for that purpose; Section 4 describes how these techniques can be used in conjunction with quantitative risk assessment techniques. Some concluding comments are offered in Section 5. Appendices 1 and 2 contain self-evaluation questionnaires, and Appendix 3 contains an example HRA.

We hope this Guide will help you identify ways to reduce human errors in your own facilities. However, the extent of human factors engineering knowledge that has been accumulated far exceeds what is contained in this Guide. An extensive bibliography has been included to help you find additional information about particular topics. You are strongly encouraged to use these resources in addition to this Guide.

EXECUTIVE SUMMARY

During the past 30 years, the 100 largest accidents at chemical and hydrocarbon processing facilities have severely injured or killed hundreds of people, contaminated the environment, and caused more than $8 billion in property damage losses.[1,2] The actual cost of these accidents was much higher because of the associated business interruption costs, cleanup costs, legal costs, fines, losses of market share, and so forth. Human error was a significant factor in almost all of these accidents. In systems where a high degree of hardware redundancy minimizes the consequences of single component failures, human errors may comprise over 90 percent of the system failure probability.[3]

Any serious attempt to improve process safety must address the fact that human errors in the design, construction, operation, maintenance, and management of facilities are the root causes of almost all quality deficiencies, production losses, and accidents. Too often, managers believe that workers can be selected, trained, and motivated to properly operate any system. Therefore, they believe that human errors are the result of carelessness or stupidity, and that the only way they can reduce human errors is to discipline the guilty parties when errors occur.

Enlightened managers realize that careless or unfit workers account for only a small fraction of the human errors at their facilities; most mistakes are committed by skilled, careful, productive, well-meaning employees. Rather than simply blaming the individual involved, these managers attempt to identify the root causes of the error in the work situation and implement appropriate corrective actions.

Human factors engineering, or ***ergonomics***, is the design of equipment, operations, procedures, and work environments that are compatible with the capabilities, limitations, and needs of the workers. It is a vital complement to other engineering disciplines that primarily seek to optimize hardware performance and/or minimize capital costs with little or no consideration of how the equipment will actually be operated and maintained. For example, a salvaged dial thermometer attached to a nozzle just below the third level platform might be a very inexpensive way to accurately measure temperature in a tower. But from a human factors standpoint, it is a less-than-adequate design if operators must climb up three caged ladders and peer down through the metal grating of the platform in order to read the temperature (which must be controlled within 5 degrees) from a dial graduated in 100-degree increments.

This Guide focuses on techniques that managers can use to improve human performance by identifying and eliminating error-likely situations that may not be as obvious as the one described above. The basic strategy is to reduce the frequency of human errors by applying principles of human factors engineering to the equipment that must be operated and maintained, to the work tasks that must be performed, and to the work environment. In order for this approach to be successful, it is essential that the workers themselves be involved in the design process. From a management standpoint, it would not be cost-effective to ignore the workers' knowledge, which is a valuable resource that already exists within every company. The earlier that workers and human factors specialists are involved in the design process, the more successful and efficient this strategy will be.

Because some human errors will inevitably occur, this Guide also discusses methods that managers can use to reduce the probability that undesirable consequences will result from them. This can be accomplished by designing ways to detect human errors or mitigate their effects. Involving the workers in this activity will also help ensure its success.

One of the tools that managers can use to improve human performance is human reliability analysis (HRA). Like other risk assessment tools (e.g., fault tree analysis), HRA can provide both qualitative and quantitative information. The qualitative results identify the critical actions that a worker must accomplish to successfully perform a task, identify erroneous (unwanted) actions that can degrade the system, identify error-likely situations, and identify any factors that would mitigate errors in the performance of any action. The quantitative results are numerical estimates of the probability that a task will be performed incorrectly or that unwanted actions will be performed. As mentioned in the American Chemistry Council's and Center for Chemical Process Safety's *Evaluating Process Safety in the Chemical Industry: User's Guide to Quantitative Risk Analysis*,[4] these results are a necessary input to comprehensive quantitative risk assessments of process units or facilities. However, managers should realize that the qualitative results of an HRA are as valuable as any quantitative estimates of human error probabilities.

Anticipating and controlling the potentially adverse impacts of human actions or human/system interactions are integral parts of process safety management. Therefore, many process safety management activities are directed toward improving human performance. For example, maintaining current plant procedures will help ensure that workers have correct instructions for the tasks they must perform. Increasing training will help ensure that workers can diagnose process upsets and respond correctly to emergency situations. Scrutinizing designs before they are installed will help eliminate design errors and identify ways to reduce the likelihood of human errors that could adversely affect quality, productivity, or safety.

Ultimately, the term "human error" should connote no more sense of blame or emotion than the term "hardware failure." Rather than seeking to blame or punish a worker when an incident occurs, managers should look for the root causes in the work situation. Only if managers recognize and accept their responsibility to identify and eliminate error-likely situations in the workplace will there be a significant reduction in the frequency and severity of human errors. Directly involving the workers in these efforts is the best way to achieve your goals. Human factors engineering is an important tool that managers can use in their quest for an ever safer and more productive organization.

Section 1
INTRODUCTION

1.1 IMPORTANCE OF IMPROVING HUMAN PERFORMANCE

What caused the last process upset at your facility? The last quality problem? The last unscheduled unit outage? The last accident? Chances are you blamed **human error** as either the direct cause (e.g., an operator opening the wrong valve) or as a significantly contributing cause (e.g., an operator failing to start the spare pump quickly enough) of the process upset. And now that the guilty individual(s) has been counseled, disciplined, or fired, you feel sure that a similar mistake will never happen again.

During the past five years, about 30 major accidents at chemical and hydrocarbon processing facilities have severely injured hundreds of people, contaminated the environment, and caused more than $2 billion in property damage losses.[1,2] The actual cost of these accidents was much higher because of the associated business interruption costs, cleanup costs, legal costs, fines, losses of market share, and so forth. Human error was a significant factor in almost all of these accidents. The total cost (including forced outages and off-specification products, as well as accidents) of human errors in the process industries is incalculable.

Historically, managers have found human errors to be significant factors in almost every quality problem, production outage, or accident at their facilities. One study[5] of 190 accidents in chemical facilities found that the top four causes were insufficient knowledge (34 percent), design errors (32 percent), procedure errors (24 percent), and operator errors (16 percent).* A study[6] of accidents in petrochemical and refining units identified the following causes: equipment and design failures (41 percent), operator and maintenance errors (41 percent), inadequate or improper procedures (11 percent), inadequate or improper inspection (5 percent), and miscellaneous causes (2 percent). In systems where a high degree of hardware redundancy minimizes the consequences of single component failures, human errors may comprise over 90percent of the system failure probability.[3]

Clearly, human errors were considered the cause for an overwhelming fraction of the accidents that were evaluated in these studies. But when you stop and think about these results, they are not really surprising because there is the potential for human error in every aspect of production, refining, or manufacturing, as indicated in Table 1.

The challenge for a manager is to devise effective ways to reduce the frequency of human errors associated with these activities and to reduce the probability that any error that does occur will adversely affect a facility. Managers must also devise ways to learn from the actual and near-miss incidents that do occur and to implement appropriate corrective actions. The reward for creating and implementing such programs will be tangible improvements in process safety, quality, and productivity.

* The percentages total more than 100% because more than one cause could be listed for an accident.

Table 1 Opportunities for Human Error

Research/Development/Exploration	The chemist failed to report that the compound expanded when it froze
Design	The engineer failed to specify heat tracing for a heat exchanger bypass line that subsequently froze and ruptured
Construction/Installation	The contractor failed to install the specified heat tracing on a heat exchanger bypass line that subsequently froze and ruptured
Training/Procedures	The operators did not know where to turn on the heat tracing for a heat exchanger bypass line that subsequently froze and ruptured
Operation	The operators neglected their daily check of the heat tracing, which eventually failed, allowing the heat exchanger bypass line to freeze and rupture
Maintenance/Inspection	The pipefitters failed to replace the heat tracing they pinched while repairing a flange leak, allowing the heat exchanger bypass line to freeze and rupture
Plant Management	The manager delayed activation of the heat tracing system to save energy, but unpredicted cold weather froze and ruptured several pipes and vessels
Corporate Management	The corporate management cut the plant budget, forcing such severe staff reductions that the heat tracing was not all activated when cold weather arrived, resulting in a plant shutdown because of frozen lines

1.2 OBJECTIVES AND ORGANIZATION OF THIS GUIDE

The primary objective of this Guide is to help you understand human factors engineering principles that you can use to improve human performance at your facilities. For simplicity, this Guide focuses on ways to reduce operating and maintenance errors, but many of the ideas could also be applied to research, development, design, construction, training, and management activities.

The first part of this Guide is designed to equip you with a basic understanding of human error and some of the jargon you will encounter in the field of human factors engineering. But the bulk of this Guide is designed to help you recognize some of the causes of human errors, and the errors are illustrated with simple case histories. Integrated with these descriptions are suggestions for eliminating the error-likely situations that you identify. Appendix 1 contains a questionnaire you can use to help critically evaluate the potential for human errors in your facility.

The final portion of this Guide is devoted to explaining how human factors engineering and human reliability analysis (HRA) interrelate with other process safety management activities. In particular, it discusses how HRA can be used in conjunction with any qualitative or quantitative risk assessment techniques you may employ as part of your process safety management program. Appendix 3 shows how HRA can be applied to a practical process problem.

Section 2
UNDERSTANDING HUMAN ERROR

2.1 DEFINITION OF HUMAN ERROR

Every task that must be performed by a human is an opportunity for error. But even though neither two people (nor even one individual) will perform the same task in exactly the same way twice, minor variations in the performance of a task are usually inconsequential. Only when some limit of acceptability is exceeded is a variation considered a human error. Thus, a practical definition of **human error** is any human action (or lack thereof) that exceeds the tolerances defined by the system with which the human interacts.

Any discussion of human error must consider the specific actions and limits involved in a particular task. For example, an operator might be told to add 10 pounds of catalyst after a batch reactor is heated to 200 degrees. The operator can add more or less catalyst; add catalyst sooner or later; add the catalyst quickly or slowly; add a different catalyst; or forget to add any catalyst at all. The operator might also choose a blue or red scoop to measure the catalyst. Any of these variations is inconsequential unless it has the potential to cause a runaway reaction (accident), to extend the processing time (production loss), or to generate off-specification product (quality problem). Only then would the variation be considered a human error. Unfortunately, the limits on human performance are seldom well defined until someone has exceeded them at least once under circumstances that resulted in an actual problem.

In general there are two types of human errors: unintentional and intentional. Unintentional errors are actions committed or omitted with no prior thought. We typically think of these as "accidents": bumping the wrong switch, misreading a gauge, forgetting to open a valve, spilling coffee into the control console, and so forth. If the worker intended the correct action, but simply did it wrong, the error is sometimes called a "slip"; if the worker forgot to perform the action, the error is sometimes called a "lapse."

Intentional deviations (errors) are actions we deliberately commit or omit because we believe, for whatever reason, that our actions are correct or that they will be better (i.e., quicker, easier, safer, etc.) than the prescribed actions. When workers misdiagnose the true cause of an upset, they will intentionally perform erroneous actions as they attempt to respond. For example, operators on other interconnecting oil platforms actually worsened the fire on Piper Alpha in 1988 because they did not understand what was happening and did not respond appropriately. Other intentional deviations are "shortcuts" or "violations" that are not recognized as human errors until circumstances arise in which they exceed the system tolerances. Examples of such errors include failing to electrically ground containers of flammable liquids, attempting to restart a furnace without purging the firebox, adding a little extra catalyst to accelerate the start of a reaction, and so forth.

There is an important distinction between intentional deviations and malevolent behavior: motive. An intentional deviation is not intended to harm the system, but its effect on the system may turn out to be

undesirable. A malevolent act (e.g., sabotage) is not an error at all – it is a deliberate action intended to produce a harmful effect. As used in this Guide, the term human error does not include malevolent acts.

2.2 THEORY OF HUMAN ERROR

Human diversity is both a blessing and a curse: it enables us to learn, adapt, specialize, and fulfill all the different roles in our society, but it also enables us to do things in ways that systems cannot tolerate. At any moment, any individual is able to feel, think, and do any one of countless things. Considering the very large number of things that we could do at any moment, it is amazing that we accomplish so many tasks successfully.

Humans are extremely interactive and adaptable parts of any system. As illustrated in Figure 1, human interactions with a system can be simply modeled as five distinct functions. First, the system hardware or another human in the system must provide some external input. The input may be as obvious as a flashing, ringing alarm, or as subtle as a slight change in the pitch or intensity of background sounds. We must then become actively aware of the input by discriminating it from other inputs that are sensed and recognized. This awareness may be modified by internal feedback, as indicated in the figure, because (1) our mental models and expectations influence our perception of new information and (2) our own responses affect our ability to perceive new information. For example, you are less likely to hear and understand what someone else is saying if you are speaking yourself.

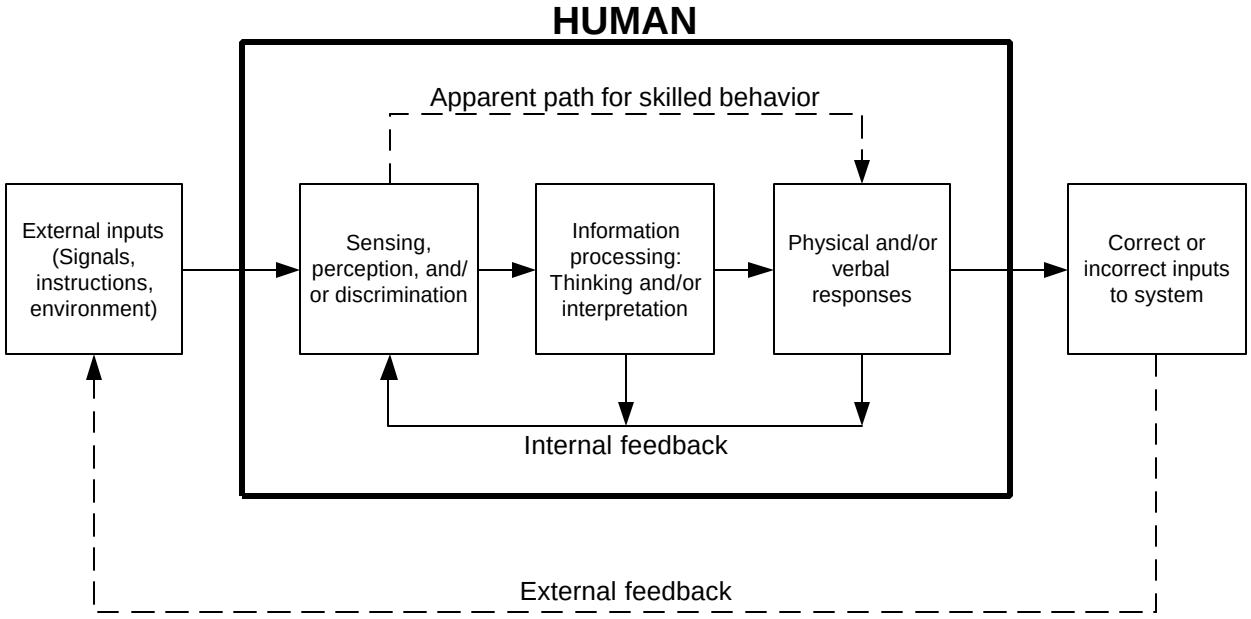


Figure 1 Simple Model of Human Behavior as a System Component (Based on Figure 3-1 in Reference 7)

We then select an appropriate response to the perceived information. This cognitive process is influenced by factors such as training, memory, goals, intentions, personality, attitude, motivation, mood, stress, and knowledge, but the ultimate result is to decide on a course of action. If the response to the perceived information is frequently practiced (such as braking your automobile when you see the brake lights of the vehicle ahead of you), the mental effort required is negligible. In such skill-based behaviors, we appear to leap directly from perception to response with no requirement for conscious thought.

Regardless of the mental pathway, we eventually make some response that we believe is appropriate. The response may involve movement of our limbs, use of our voice, or no action at all. Our response then becomes an input to the system as we manipulate controls, adjust equipment, or direct the actions of other humans. A well-designed system will feed back some information that will alter the external inputs that prompted our initial action. This will enable us to repeat the cycle as many times as necessary to achieve the desired system conditions, assuming enough time is available.

Human error is a natural and inevitable result of human variability in our interactions with a system. Whatever the task, human error is best understood in terms of human variability that reflects the influences of all pertinent factors at the time the actions are performed. There are three basic types of variability, and knowing which of these types occurs in a given case will help explain why errors occur and what can be done about them. To illustrate these types, let's consider a rifleman firing 10 shots at a target, and let's call any shot off the target an error.

1. Random variability is characterized by a dispersion pattern (Figure 2) centered about a desired norm — the bull's-eye in this example. When the variability is large, some shots will miss the target. Errors due to random variability are called *random errors*. Only reducing the overall variability of performance can reduce these errors. Personnel selection, training, supervision, and quality control programs are ways of controlling random variability. Random errors occur when these programs are deficient, when tolerance limits are too tight, or when workers cannot control key performance factors.

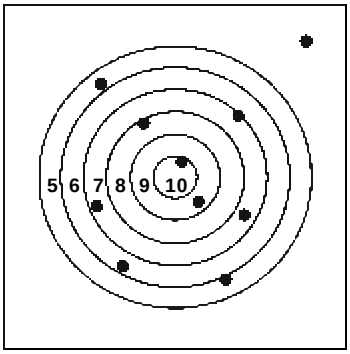


Figure 2 Random Error

2. Systematic variability is characterized by a dispersion pattern (Figure 3) offset from a desired norm. Although the variability may be small, the bias may cause some shots to be off target. Such errors are called *systematic errors*. Bias is often the result of only one or two factors and may be easily correctable. In the example, a gunsight adjustment (or glasses) may put the rifleman right on target. Systematic errors occur, for example, when workers are given only one limit instead of a lower and an upper limit; they may deliberately attempt to be on the apparently safe (unlimited) side. Biases can also exist in tools, equipment, instructions, or the worker's personality, training, or experience. Telling workers how well they are doing with respect to real goals will help reduce systematic errors.

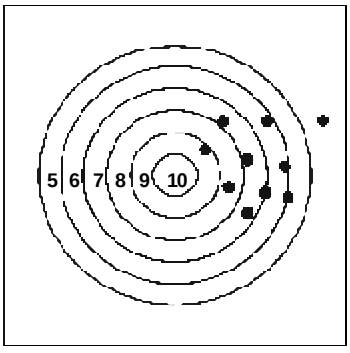


Figure 3 Systematic Error

3. Sporadic variability is characterized by an occasional outlier, such as a tight cluster of shots with one shot way off the mark (Figure 4) for reasons we might readily imagine — a sudden distraction, an involuntary twitch, etc. In work situations, where workers have been well trained and given a reasonable degree of control over major performance factors, most of the errors are due to sporadic variability. Such *sporadic errors* are the most difficult to predict or reduce because they occur infrequently and may not seem correlated to factors in the work situation. They are not correctable by additional training or indoctrination because they are not the result of inadequate knowledge or motivation. To reduce sporadic errors, we must categorize the errors and the conditions under which they occur in such a way that errors can be related to controllable conditions.

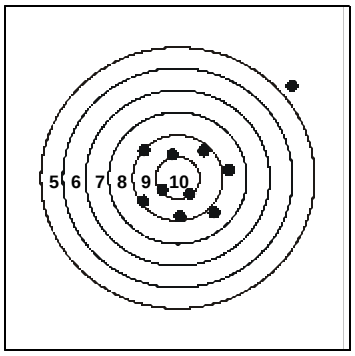


Figure 4 Sporadic Error

2.3 PERFORMANCE SHAPING FACTORS

One can think of the operator as an essential element of the overall process system as illustrated in Figure 5. To minimize human errors, managers must ensure that the operator-machine interface, which includes interactions with other workers as well as with the equipment and environment, is compatible with the capabilities, limitations, and needs of the worker. Anything that affects a worker's performance of a task within the process system is a ***performance-shaping factor*** (PSF). PSFs can be divided into three classes: (1) internal PSFs that act within an individual, (2) external PSFs that act on the individual, and (3) stressors. Table 2 lists some internal PSFs, which are the individual skills, abilities, attitudes, and

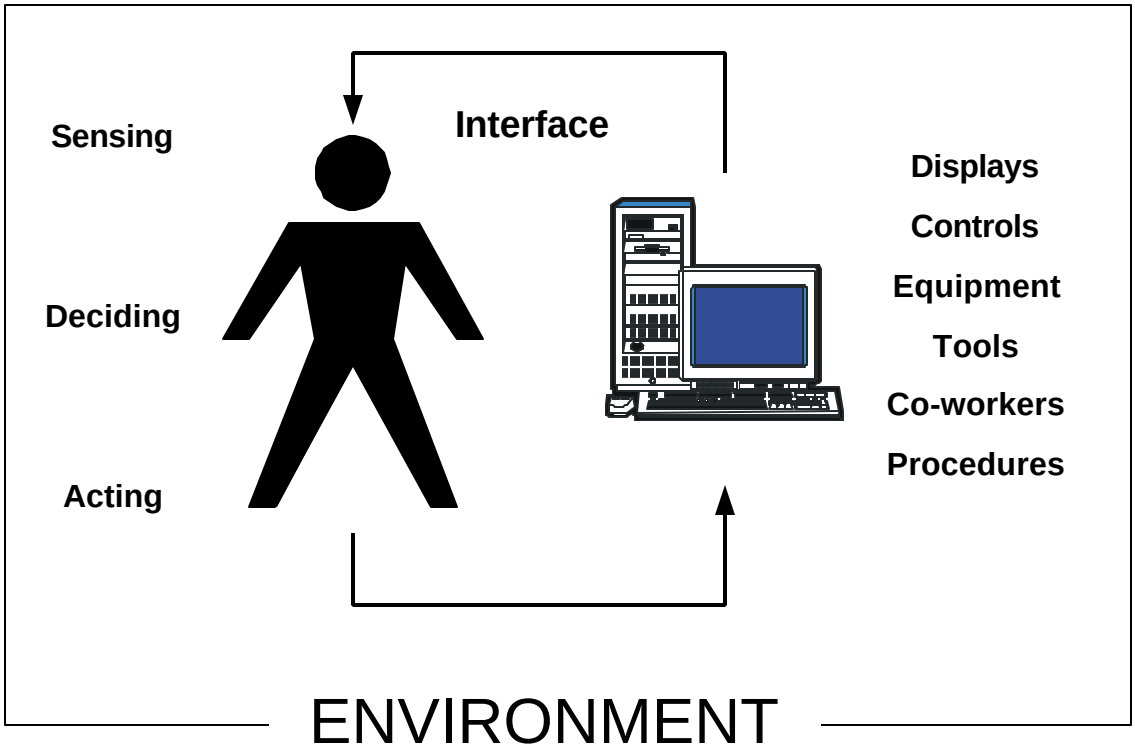


Figure 5 Operator as Essential Element of Overall Process System

other characteristics that a worker brings to any job. Some of these, such as training, can be improved by managers; others, such as a short-term emotional upset triggered by a family crisis, are beyond any practical management control. (However, a manager's style can influence workers' mental/ emotional states, as can counseling programs.)

Table 2 Internal PSFs (Based on Table 3-2 in Reference 7)

Training/Skill
Practice/Experience
Knowledge of Required Performance Standards
Stress (Mental or Bodily Tension)
Intelligence
Motivation/Work Attitude
Personality
Emotional State
Gender
Physical Condition/Health
Influences of Family and Other Outside Persons or Agencies
Group Identifications
Culture

Table 3 lists external PSFs that influence the environment in which tasks are performed. These PSFs are divided into two groups: (1) situational characteristics and (2) task, equipment, and procedural characteristics. Situational characteristics include general PSFs that may affect many different jobs in the plant. Task and equipment characteristics are pertinent to a specific job or a specific task within a job. Job and task instructions are a particularly important part of the task characteristics because they have such a large effect on human performance. ***By emphasizing the importance of preparing and maintaining clear, accurate task instructions, managers can significantly reduce the likelihood of human errors.***

Table 3 External PSFs (Based on Table 3-2 in Reference 7)

SITUATIONAL CHARACTERISTICS	TASK, EQUIPMENT, AND PROCEDURAL CHARACTERISTICS
Architectural Features	Procedures (Written or Not Written)
Environment (Temperature, Humidity, Air Quality, Lighting, Noise, Vibration, General Cleanliness, etc.)	Written or Oral Communications
	Cautions and Warnings
	Work Methods/Shop Practices
Work Hours/Work Breaks	Dynamic vs. Step-by-step Activities
Shift Rotation	Team Structure and Communication
Availability/Adequacy of Special Equipment, Tools, and Supplies	Perceptual Requirements
	Physical Requirements (Speed, Strength, etc.)
Staffing Levels	Anticipatory Requirements
Organizational Structure (Authority, Responsibility, Communication Channels, etc.)	Interpretation Decision Making
	Complexity (Information Load)
	Long- and Short-term Memory Load
Actions by Supervisors, Co-workers, Union Representatives, and Regulatory Personnel	Calculational Requirements
	Feedback (Knowledge of Results)
Plant Policies	Hardware Interface Factors (Design of Control Equipment, Test Equipment, Process Equipment, Job Aids, Tools, Fixtures, etc.)
	Control-display Relationships
	Task Criticality
	Frequency/Repetitiveness

The interaction between internal and external PSFs creates stress in the individual performing the task. Mismatches between our internal and external PSFs result in disruptive stress that degrades our performance. If there is too little stimulation, we will not remain sufficiently alert to do a good job. For example, an operator who passively watches as a computer operates the process is unlikely to be alert enough to take control and continue operation when the computer fails. On the other hand, too much stimulation will quickly overburden us and degrade our performance. In such situations, we tend to (1) focus on the large or most noticeable signals and ignore some information entirely, (2) omit or delay some responses, (3) process information incorrectly and reject information that conflicts with our diagnosis or decision, or (4) mentally and/or physically withdraw. Disruptive psychological and physiological stressors are listed in Table 4.

Table 4 Stressor PSFs (Based on Table 3-2 in Reference 7)

Psychological Stressors	Physiological Stressors
Suddenness of Onset	Long Duration of Stress
High Task Speed	Fatigue
Heavy Task Load	Pain or Discomfort
High Jeopardy Risk	Hunger or Thirst
Threats (of Failure, of Loss of Job, etc.)	Temperature Extremes
Monotonous, Degrading, or Meaningless Work	Radiation
Long, Uneventful Vigilance Periods	Oxygen Deficiency
Conflicting Motives about Job Performance	Chemical Exposure
Negative Reinforcement	Vibration
Sensory Deprivations	Movement Constriction
Distractions (Noise, Glare, Movement, etc.)	Movement Repetition
Inconsistent Cueing	Lack of Physical Exercise
Lack of Rewards, Recognition, and Benefits	Disruption of Circadian Rhythm

Although stress usually has a negative connotation, some stress is actually necessary for humans to function at optimum performance, as illustrated in Figure 6. Facilitative stress is anything that arouses us, alerts us, prods us to action, thrills us, or makes us eager. When there is a good match between our internal and external PSFs, we experience facilitative stress and our performance is at its best.

Managers must recognize that most PSFs (including many internal PSFs) are within their control. By designing work situations that are compatible with human needs, capabilities, and limitations, and carefully matching workers with the job requirements, managers can create conditions that optimize worker performance and minimize human errors.

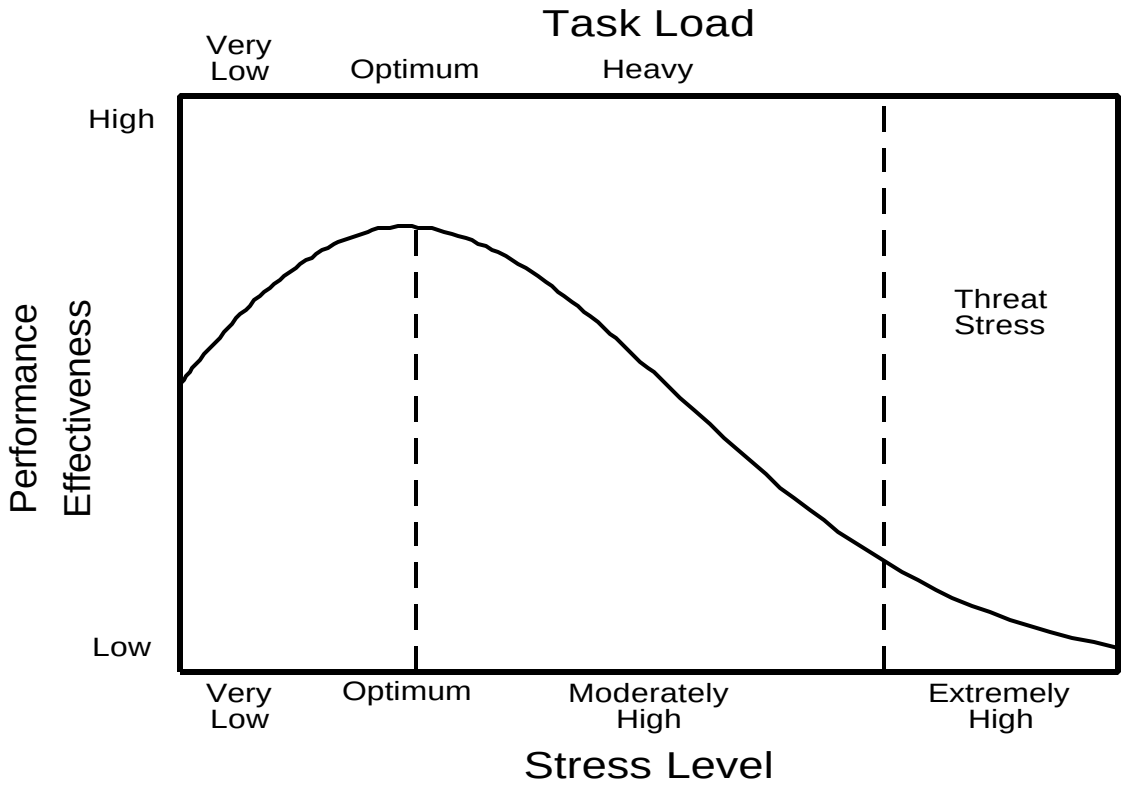


Figure 6 Relationship of Stress and Performance (Based on Figure 17-1 in Reference 7)

Section 3
STRATEGIES FOR IMPROVING HUMAN PERFORMANCE

When contemplating ways to improve human performance, there are two basic types of errors that managers must address: (1) errors whose primary causal factors are individual human characteristics unrelated to the work situation and (2) errors whose primary causal factors are related to the design of the work situation. Hiring and job assignment policies are important ways in which managers can reduce the causes of the first type of error. But on any given day, a worker could be emotionally upset, fatigued, taking medication/drugs, etc., and commit an error. However, human factors specialists estimate that only 15-20percent[3] of workplace errors are primarily caused by such internal human characteristics.

The vast majority (80-85percent)[3] of human errors primarily result from the design of the work situation (the tasks, equipment, and environment), which managers directly control. By providing the resources necessary to identify and eliminate error-likely situations, managers can improve the PSFs and dramatically reduce the frequency of human errors. This strategy is called the work-situation approach, and it involves the elements described in Table 5.

Table 5 Elements of the Work-situation Approach

• Implementing good human factors engineering of control systems, process equipment, and the work environment
• Providing clear, accurate procedures, instructions, and other job aids
• Providing job-relevant training and practice
• Providing ways to detect and correct human errors before an undesired consequence occurs
• Providing avenues for workers to achieve their social and psychological needs

To maximize the benefits of such a strategy, managers should involve the workers themselves at every opportunity. After all, it is the workers who can best identify factors that hinder their performance and who will enthusiastically support such a strategy if they are not penalized for telling the truth.

3.1 EXAMPLES OF ERROR-LIKELY SITUATIONS

This section briefly describes a number of work situations that are likely to lead to human errors. It is intended to serve as a starting point that will help you identify error-likely situations in your own facilities.

3.1.1 Deficient Procedures

Good written procedures help ensure that all qualified operators can correctly and safely operate a system. Procedures should explicitly state the proper actions a worker should take during startup, shutdown, normal operation, and upset/emergency conditions, and the reasons for those actions should be explained during training. Task instructions should be written in simple, understandable language in a format (including appropriate pictures and diagrams) that the workers would use (see items 49 through 57

in the bibliography). To help ensure that procedures are accurate and useful, managers should involve the workers themselves in writing and validating the procedures.

Unfortunately, not all facilities have complete, current procedures that are useful to the workers. Some facilities only have the original procedures drafted by the design engineers and/or startup crew; others have incomplete procedures or none at all. If there have been so many process changes since the written procedures were last updated that they are no longer correct, workers will create their own unofficial procedures that may not adequately address safety issues. Some "procedures" are really checklists that only an expert could follow; others are voluminous training manuals that are not suitable for everyday use. Erroneous, incomplete, nonexistent, or overly complex procedures set the stage for human errors, as the following example illustrates:

- A system designed to circulate a metallic salt solution through a filter was modified so it could occasionally be used to pump a peroxide solution through a filter bypass line. Verbal orders were issued to never pump peroxide through the filter, but the written procedures were not revised. Eventually, a new operator following the written procedures pumped the peroxide through the filter, which exploded when the peroxide contacted the metal contaminants collected on the filter.

3.1.2 Inadequate, Inoperative, or Misleading Instrumentation

Instruments are workers' primary sources of information about a process. If the instruments are inadequate or inoperative, workers must "fill in the blanks" and deduce process conditions from other instruments or indications. This greatly increases the probability of human error. Worse yet, if an instrument is miscalibrated, misleading, or failed (but appears to be working), workers may be tricked into inappropriate actions (or inactions). This is particularly likely to occur when switches are relied upon to activate alarms (high pressure, low level, etc.) but are never tested or repaired unless they fail in such a way that operations are disrupted (i.e., spurious alarms or inadvertent shutdowns). The following incidents resulted from instrument failures:

- The relief valve on a low-pressure separator actuated during apparently normal operations. Operators verified that the separator pressure was normal, and in their haste to stop the release, they blocked in the "bad" relief valve before unblocking the parallel relief valve. The separator immediately ruptured and killed two operators. The pressure transmitter on the separator had failed, closing the normal discharge valve and sending a false signal to the control room.

- Operators relied on a pressure gauge to indicate the level in a concentrated caustic tank because the sight glass tended to plug up. Operators eventually overfilled (and ruptured) the tank because a low-density hydrocarbon layer accumulated on top of the caustic. The pressure gauge was a valid indication of tank level only as long as the density of the tank contents did not change.

- An operator forgot to open an air vent valve before filling the unit with monomer. The operators noticed the unit was filling more slowly than usual, but assumed the filling pump's suction screen was plugging, as it had

in the past. Eventually, as the pump approached its maximum discharge pressure (90 psig), the trapped, compressed air and monomer reacted violently, and the explosion ripped the unit apart. The operators did not notice the pressure buildup in the unit because none of the pressure transmitters were accurate for pressures less than 250 psig. (Normal operating pressure was 750 to 1,000 psig.)

☞ The single level monitoring device on a light hydrocarbon storage sphere falsely indicated that the sphere level was low. Operators pumped hydrocarbon into the sphere until it ruptured as a result of being overfilled and overstressed. The vapor cloud ignited, and the ensuing fireball scattered burning debris throughout the plant. Adjacent storage tanks also caught fire and exploded, and eventually the entire tank farm was destroyed.

3.1.3 Insufficient Knowledge

Workers must develop an accurate mental model of the process system so they can diagnose process upsets and understand the consequences of their actions. The only way such mental models can be built is for operators to be thoroughly trained not only in what/how to do something but also in why to do it. Workers should be required to demonstrate their proficiency (via tests, talk-throughs, etc.) before being allowed to work independently. Training must be reinforced with periodic drills so workers can practice and perfect their skills. Inadequate knowledge inevitably results in human errors, such as those described below:

☞ The operator used the column bottoms volume as a surge tank, and he deliberately increased the level in anticipation of reduced feed to the column. The operator did not understand that the relief valve would not work properly when its inlet was flooded by the excess level in the column. When an overpressure occurred, the column ruptured.

☞ The operator did not understand the dangers of combining catalyst and reactants in an uncontrolled manner. When she found the agitator had tripped off, she immediately reset the circuit breaker and restarted the agitator. The sudden mixing of the stratified materials initiated a runaway reaction that blew the reactor head through the building roof.

☞ The supervisor did not realize how quickly wet hydrofluoric acid vapors attacked carbon steel, so he attempted to continue running until the upcoming turnaround rather than shutting down to repair the leaking condenser. The head blew off the badly corroded condenser a few days later, releasing a toxic vapor cloud.

3.1.4 Conflicting Priorities

Decision-making errors often result when workers have conflicting priorities, particularly between safety and production. If the rewards for production are much more tangible than the rewards for safety, many workers will do everything possible to keep a unit productive. If workers fear punishment/ridicule for shutting down a unit "unnecessarily" (even though it was the safe course of action), then workers may fail to shut down a unit in time to prevent a process upset from causing an accident. Managers should ensure that workers have clear criteria for shutting down a unit or discontinuing an activity so that the fear

of being second-guessed will not interfere with workers' decision making. The cases below illustrate how conflicting priorities can worsen emergencies:

- The operator recognized that pressure was rising in the polymerization reactor, but he was reluctant to inject the shortstop solution because it would take days to clear it out of the system. Only after exhausting all other options (stopping feeds, increasing cooling, etc.) did the operator inject the shortstop solution, but it was too late to prevent a runaway reaction.

- Firefighters were deluging a burning spill of pesticide with water. Even though the diked area had been completely filled with water, some secondary fires still burned in the unit. Rather than abandoning the unit and letting the fires burn out, the firefighters continued to apply water. The pesticide-contaminated water overflowed into the plant's storm sewer system and into other areas that were far more expensive to clean up than the value of the equipment saved by continued firefighting.

- The operator realized the mud density was too low, but decided to continue drilling. Before the proper mud density was restored, the drill hit a gas pocket, resulting in a well blowout.

3.1.5 Inadequate Labeling

One of the simplest ways to reduce selection errors is to clearly and unambiguously label all controls and equipment. Labeling is particularly helpful to new workers, to workers who only occasionally interact with a system, and to experienced workers in stressful situations (e.g., responding to an emergency). Even if good labels are installed in new units, they will quickly be torn off, painted over, covered with insulation, or outdated by changes in the equipment or process materials, unless an employee has the responsibility and resources to diligently maintain them. When labels are missing, incorrect, or misleading, workers make mistakes such as the following:

- An unlabeled, high-voltage rectifier for an electrochemical cell had been isolated for routine maintenance. The electrician left the area to get more tools, and upon returning mistook a similar, unlabeled rectifier for the one he had been working on. The electrician was electrocuted when he touched the energized rectifier.

- Truck drivers from the acid supplier were allowed to connect their own hoses to the storage tanks and unload without operator supervision because the same truck drivers made several deliveries daily. The substitute driver was given routine access to the unloading rack, but she hooked her hose to an adjacent rack. The acid reacted with the tank contents, releasing toxic fumes and melting the tank.

- In case of a toxic gas release, the sign (Figure 7) at the end of a hallway was intended to direct people down the right-hand corridor, but to keep them on the left side of it so the

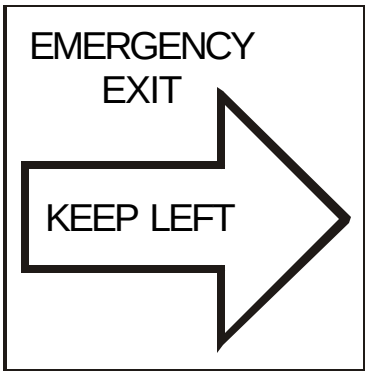


Figure 7 Exit Sign

emergency response team would have a clear path into the building. When an actual release occurred, several workers died trying to escape via the left-hand corridor because the sign required too much information processing when the workers were under time stress.

☞ The crude oil unit had been debottlenecked by squeezing a third feed preheater ("C") in between the two original heat exchangers ("A" and "B"). A new operator was told to isolate the "B" exchanger to stop a tube leak, but she mistakenly assumed the middle exchanger was "B" and blocked in the new "C" exchanger.

When in control rooms and process units, managers should be alert for marks that workers have made on the instruments and equipment to correct labeling deficiencies. You will likely find grease pencil marks on gauge faces to indicate the normal values, masking tape on control panels to relabel controls or mark switch positions, and arrows drawn on three-way valves to indicate the normal flow direction. Rather than accepting such haphazard, temporary markings, you should ensure that clear, accurate, permanent labels are installed wherever they will help the workers.

3.1.6 Inadequate Feedback

Workers require prompt feedback that their actions are eliciting the desired system response. When such feedback is not provided, workers are prone to overreact, as illustrated in the following example:

☞ A computer-based control system was so overloaded by a process upset that it ceased to update the video terminals in the control room. Unaware that the displayed information was inaccurate, operators unknowingly moved valves to their fully open or closed limits while waiting for the display to show some response. The mispositioned valves worsened the upset, eventually causing an emergency shutdown of the unit when some relief valves lifted.

3.1.7 Policy/Practice Discrepancies

Written plant policies and procedures are meaningful only when they are enforced; otherwise, worker practices *are* the policy. Once discrepancies are tolerated, individual workers have to use their own judgment to decide what tasks are necessary and/or acceptable. Eventually, someone's action or omission will violate the system tolerances and result in a serious accident like the ones described below:

☞ Even though procedures called for operators to verify the continuity of all electrical grounds and bonds on process equipment daily, only visual checks were actually performed. A severe fire resulted when a corroded connection was not observed, and a static spark ignited a tank's contents.

☞ To resume production as quickly as possible after a furnace trip, operators were in the habit of relighting one burner and "jumping" the flame to adjacent burners (contrary to the written procedure). Supervisors were aware of the practice and allowed it to continue because it saved time and there had never been any significant problems. However, when one of the burners failed to light promptly, a flammable gas cloud accumulated in the furnace and exploded.

☞ Operators reported that the outboard bearing of a product pump was damaged, but they did not close the suction valve so that flushing flow to the pump seals could be continued. Since the bearing repair did not involve the pump casing, the maintenance crew (in violation of plant policy) decided to proceed without waiting for an operator to isolate and secure the pump. Unfortunately, they could not see that the pump shaft was broken. When the bearing cover was removed, the bearing and stub shaft were forced out of the packing, and a 3-inch stream of 300° F material sprayed the maintenance crew.

Managers should vigorously enforce plant policies/procedures, and ensure that plant policies/procedures and practices are revised as necessary to be consistent.

3.1.8 Disabled Equipment

Workers expect hardware, particularly safety-related hardware, to function when required. However, they will not tolerate such equipment for long if it causes spurious alarms and trips. When such equipment is disabled to maintain production, there is a much greater chance that workers will be unaware of an upset or will not respond quickly enough, as the cases below illustrate:

☞ A level alarm switch had slipped down its support into a sump and was alarming every few minutes as the sump pump cycled on and off. The operator taped down the ACKNOWLEDGE button on the console to stop the incessant alarm, thereby deactivating all audible alarms. The operator later failed to notice a high temperature alarm light, which eventually led to a large toxic vapor release.

☞ Operations continued even though the level control for the column bottoms was malfunctioning and had been bypassed. When feed to the column was lost, the bottoms level quickly drained into the downstream vessel, which ruptured when high-pressure gases from the column flowed into it.

☞ The vendor no longer sold spare parts for the old distributed control system, so some operator consoles were cannibalized for parts. During an upset, the operator could not find a functional keyboard quickly enough to prevent a unit crash.

☞ The maintenance supervisor decided to temporarily use instrument air as a source of breathing air for some maintenance workers, so he disconnected the automatic nitrogen backup system. The nitrogen backup system was never reactivated, so when the instrument air compressor tripped, operators quickly lost control of the pneumatic valves. Had they known the nitrogen backup was disconnected, the operators would have begun a controlled shutdown instead of watching the process crash and ruin the batches in several reactors.

In situations similar to the last example, fatalities have occurred when the inert gas backup was not disconnected before the victim deliberately or accidentally used an instrument air system as a source of breathing air. Other fatalities have occurred when equipment was not properly isolated or de-energized for maintenance, or when workers relied upon malfunctioning instruments for information.

Managers must institute adequate administrative controls to ensure that equipment is properly locked out/tagged out when required for personnel or process safety and to ensure that equipment is properly restored to service as soon as the danger is past or the equipment is repaired.

3.1.9 Poor Communication

Many workers are involved in process operations, and clear communication is essential. Managers must ensure that the workers understand their assignments; a nod or a grunt in response to your instructions is not enough. If verbal instructions are given, the worker should repeat them back to the originator (manager or co-worker) so their accuracy can be verified. Preferably, any departures from normal procedures should be written down so workers do not have to rely on their memories. Logs should be kept that document the status of the equipment and the process, and the departing shift should discuss log entries with the arriving shift. Anyone entering an operating unit for any reason should be required to check in and explain the purpose of their visit (maintenance, construction, inspection, etc.). Workers will then be aware of the activity and can assist (initialing or issuing permits, explaining safety rules, locating equipment, etc.) as required. Human errors are likely to occur whenever communications break down, as illustrated below:

- ☞ Each shift normally made an entire batch of resin, but equipment failures had interrupted the usual schedule. The arriving shift misunderstood the batch status and mixed in a second bag of additives. They realized their error when the agitator motor overloaded. The entire process had to be disassembled so the solidified resin could be removed.

- ☞ Unit operators had practiced responding to an acid vapor leak and devised a system of hand signals to communicate with personnel responding to the release in fully encapsulated suits. Unfortunately, when an actual leak occurred on a calm morning, visibility was restricted throughout the unit by the acid-induced fog. Emergency response personnel could not coordinate their actions with the unit operators, and attempts to isolate the leak were initially unsuccessful, resulting in a much larger release.

- ☞ In preparation for construction work, the plant staff marked the location of an underground electrical bus with flags on the surface. The backhoe operator, believing the flags indicated where he was supposed to dig, cut through the bus and blacked out half the facility.

3.1.10 Poor Layout

Anything that must be monitored or manipulated by workers should be located in convenient, accessible locations that make sense in relation to the tasks that must be performed and their frequency. In control rooms, designers often stick instruments, controls, and annunciator lights wherever there is space, regardless of the position of related devices. In the field, control valves and bypasses may be located in elevated pipe racks, or drain valves may be stuck underneath vessels with insufficient clearance. It is unrealistic to expect humans to reliably use equipment that is inconveniently located, as illustrated in the following three examples:

☞ Because there was no more space on the front of the control panel, the instrument technician installed the new pressure gauge on the backside of the panel. Operators subsequently hung a mirror from the ceiling so they could see the gauge without leaving their normal workstation. During an upset, operators misread the reversed image of the gauge and improperly responded, eventually losing the reactor contents when the rupture disk blew.

☞ A storage tank was equipped with a system for shortstopping runaway reactions, but the only "panic button" was located in the second-story control room. While out on rounds, the operator noticed that the storage tank temperature was abnormally high, and he escaped from the building just as the tank blew up. When asked why he didn't run upstairs to activate the shortstop system, he replied, "It wasn't on my way out!"

☞ Operators had to routinely look out a porthole to see depth marks on each leg of the platform. It was inconvenient to open and close the metal porthole cover for each reading, so the cover was left open. During a storm, waves broke the porthole, and seawater shorted out the ballast control system. The entire crew was lost when the semisubmersible platform capsized and sank.

3.1.11 Violations of Populational Stereotypes

Populational stereotypes are behavior patterns ingrained in a group of people. For example, most people in the United States interpret a red light to mean stop, expect to close a valve by turning the handle clockwise, and tend to dodge any oncoming object by moving to the right. (In the U.K. and Japan, people would dodge to the left.) Anything in the workplace that violates populational stereotypes invites human error, particularly if the worker is under stress. This can lead to accidents like the ones described below:

☞ An explosives plant expanded its capacity and constructed a new control room adjacent to the existing one. The emergency feed shutoff valve was located in a pipe run between the walls of the two control rooms, so the handwheel shaft was simply extended through the wall into the new control room. Unfortunately, this simple modification required that the handwheel in the new control room be turned counter-clockwise to close the valve. The plant was destroyed when an operator in the new control room responded to an upset by turning the valve handle clockwise, which increased the feed flow instead of stopping it.

☞ A British company duplicated a standard control panel when it built its U.S. plant. The process suffered numerous trips when U.S. operators flipped switches up to turn equipment on (like a typical U.S. light switch), but the British designed the switches to be flipped down to turn them on (like a typical U.K. light switch).

☞ The operator increased hydrogen throughput to the unit by closing the recycle hydrogen valve. During an upset requiring her to reduce the hydrogen flow, she instinctively closed the valve instead of opening it, and the increased hydrogen flow caused the unit to trip.

3.1.12 Overly Sensitive Controls

When processes are very sensitive to small changes in the process variables, the system must be designed so workers have a reasonable range of control movements. For example, errors would be very likely if operators attempted to regulate a flow of 57.3 gpm with a control knob that changed the flow by 1,000 gpm for each half turn. Sensitive systems should also be designed to limit the rate at which workers can affect the process variables. These may be programmed limits in the control software or physical limits (orifices, dampers, etc.) in the field. Such limits give the workers time to detect and correct errors like the ones described below:

- ☞ An operator was changing the feed rate from 75 to 100 gpm. She inadvertently typed 1,000 gpm into the computer-based controller, which responded by fully opening the feed valve. The excessive feed caused a rapid pressure rise that was relieved to the flare.

- ☞ An operator was attempting an emergency shutdown, and he stopped the flow of recycled hydrocarbon by setting the flow controller to 0. The 12-inch valve slammed closed, and the resulting hydraulic hammer ripped the line off a distillation column. The hydrocarbon vapor cloud deflagrated, causing moderate damage.

3.1.13 Excessive Mental Tasks

As workers are required to remember or calculate more and more things, their chances of error rise exponentially. For example, an operator is much less likely to forget a step in a long written procedure than to forget one of many oral instructions. Workers may calculate a critical parameter incorrectly or, when responding to an emergency, workers may not have the time to perform calculations. Good work situations provide workers with the information they need instead of relying heavily on their mental capabilities. The following example illustrates the problems that can arise if workers are mentally overburdened:

- ☞ It was crucial that the reactor's contents be kept just below the boiling point during the manufacture of a shock-sensitive compound. Operators monitored the reactor pressure and temperature regularly and referred to a graph in order to control the process. During a process upset, operators miscalculated the process conditions and allowed the reactor contents to boil, which caused the product to detonate.

3.1.14 Opportunities for Error

If we give workers enough opportunities to make a mistake, one will eventually occur, as illustrated in the following example:

- ☞ Workers were required to manipulate valves about 100 times during each 8-hour shift to produce a batch of resin. After about a year of operation, the reactor exploded because a critical valve was left open, leading to a runaway reaction.

This system required over 100,000 valve manipulations during a year of operation. Even though the operators were extremely unlikely to make a mistake positioning any one valve, a mistake was inevitable given the overwhelming number of valve manipulations required. After the accident, the plant automated many of the valves and installed limit switches so the control system could detect mispositioned valves and sound an alarm.

3.1.15 Inadequate Tools

Tools facilitate the workers' interaction with a system, and the proper tools can effectively expand human capabilities and reduce the chances for error. The proper tools are particularly important for maintenance, inspection, testing, and assembly tasks, but they can greatly simplify other tasks as well. Inadequate tools were the root cause of the following problems:

- ☞ Flammable vapor leaks from a high-pressure heat exchanger were common during unit startups because no one was strong enough (even with wrenches, sledgehammers, and cheater bars) to properly torque the head bolts on the exchanger when it was cold. Procurement of a hydraulic bolt tensioner eliminated the problem.

- ☞ Resin batches often failed to meet product specifications until a gas chromatograph was installed in the quality control laboratory. This allowed the staff to identify specific impurities and devise ways to eliminate them.

- ☞ After a fire started in the unit, the operator was unable to reach a critical isolation valve in the elevated pipe rack. Had the valve been equipped with a pneumatic operator, the operator could have closed the valve and greatly reduced the fire damage.

3.1.16 Sloppy Housekeeping

The outward appearance of a facility is often an accurate reflection of management's general attitude. A neat, clean appearance usually indicates that management cares about every detail and wants to maintain a first-class operation; a sloppy, unkempt appearance usually indicates the opposite. Beyond the obvious personnel hazards (slips, trips, etc.), poor housekeeping engenders an uncaring attitude among workers that affects their work performance. Poor housekeeping is seldom the sole cause of an operator error, but it was a primary factor in the accident described below:

- ☞ The side of the mix tank was badly stained by chemicals that had overflowed from time to time. Therefore, the operator assumed the previous shift had caused another small spill when she saw that the side of the insulated tank was wet. When the tank was refilled later that day, the corrosion-weakened seam (which had been leaking earlier) split and dumped the tank contents.

3.1.17 Extended, Uneventful Vigilance

Humans are inherently unable to remain alert for signals that seldom, if ever, occur. Even a sailor whose life is at stake cannot maintain an effective watch for more than 30 minutes or so. (Figure 8 illustrates the rapid decrease of vigilance with time.) It is important that control systems be designed to require regular operator interaction so that the operator will remain attentive. Placing a worker in situations requiring extended, uneventful vigilance may lead to accidents like the ones described below:

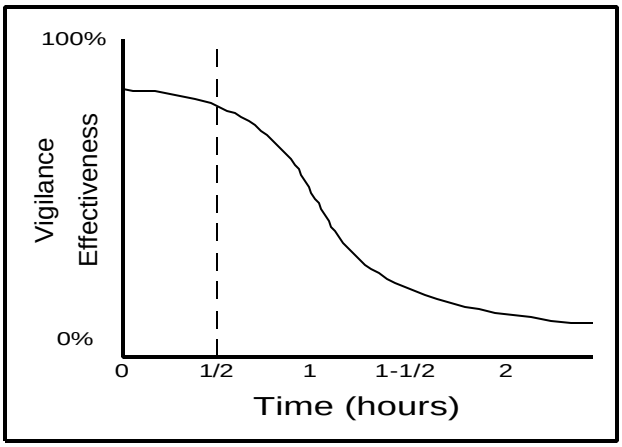


Figure 8 Vigilance Effectiveness (Based on Figure 3-5 in Reference 7)

- The distributed control system was working perfectly, and the control room was quiet. The operator dozed off, only to be awakened by several alarms. One of the control modules had failed, but the operator could not diagnose the situation and regain manual control in time to prevent a severe process upset.

- The relief valve had to be removed for maintenance, so an operator was stationed by the manual vent valve and pressure gauge atop a distillation column. Removing and replacing the relief valve took much longer than expected. When the condenser lost cooling water, the operator did not observe the pressure rise quickly enough to prevent deformation of the column as a result of the excessive pressure.

A similar situation occurs when workers are asked to monitor the progress of some activity and then take some action when the activity is complete. If the activity lasts more than a few minutes, workers are prone to abandon their posts so they can attend to other duties and then return just in time to take the appropriate action. Managers must ensure that workers remain at their posts as long as required and that workers do not use safety devices for control of routine operations. Otherwise, accidents such as the following may occur:

- An operator was procedurally required to be present during railcar unloading and to stop the transfer when the storage tank was filled. However, operators were in the habit of leaving the area as soon as unloading began because the high level interlock on the storage tank would shut down the unloading process. When the high level interlock failed, several thousand gallons of flammable material was spilled from the storage tank before an operator noticed the problem and shut down the system.

- An operator was required to hold open a spring-loaded valve 30 to 45 minutes to drain the heavy tars from the bottom of a flash column into a surge drum. The operator tied open the valve handle so he could complete his inspection of the unit, but he failed to return before all the tars had drained. The column depressurized into the surge drum, which ruptured when the relief line plugged with cold tar.

3.1.17 Computer Control Failure

Computer-based control systems can dramatically improve the quality, productivity, and safety of chemical processes. However, they are not immune to human errors. Programming errors and erroneous operator inputs account for about 40percent of the observed failures of computer-based control systems.[8] To reduce the likelihood of such failures, managers must ensure that workers are properly trained, that software is thoroughly tested, and that programming changes are strictly controlled. The following examples illustrate situations where human errors caused computer control failures:

- The control system had a primary computer controlling the process and a backup computer that would assume control if the primary computer failed. When a process upset occurred, the control software generated invalid output commands because of an abnormal, unanticipated combination of input signals. The backup computer attempted to take over, but because its software was identical, it also failed, resulting in an emergency shutdown and depressurization of the unit.

- The operators had enthusiastically learned all about the new computer control system, and a few operators had even learned how to make program changes. Eventually, they obtained an access key and "fixed" problems as they arose. Unfortunately, the operators failed to restore one of the critical interlocks that had been bypassed to simplify startup, so the computer failed to prevent an explosion of the unstable reactants.

When computer-based control systems are retrofitted to existing processes, managers sometimes try to preserve the old instrumentation as an emergency backup in case the computer fails. (New control rooms usually have multiple computers/terminals that can back each other up.) Even if the old hardware is maintained, the operators' abilities to use the old equipment will quickly deteriorate. As new workers are hired and experienced ones are reassigned, the likelihood of errors will further increase. To ensure that use of the old controls (or the backup computer systems) remains a viable option, managers must require the operators to regularly practice control with the alternate system under conditions that would exist if part or all of the normal control system malfunctioned. Otherwise, an error like the one described below is likely to occur:

- The company was converting all its processes to computer control. The experienced operator had been using one of the new systems for about a year when he was called on to temporarily replace an operator in an old control room just like the one he once used. The operator forgot to verify that the reactor was purged with nitrogen before adding the flammable feed material, and a severe fire resulted. (The computer controller would not have opened the feed valve if the nitrogen valve had not been cycled twice.)

3.1.18 Inadequate Physical Restrictions

Whenever possible, equipment should be physically designed so that it can only be operated in the correct manner. For example, valve handles can be interlocked, hoses and fittings of different diameters can be used, and removable spools can be provided in pipelines that are seldom used. As long as they do

not impede normal operations, physical restrictions can virtually eliminate the possibility of human error on some tasks, such as those illustrated below:

☞ A bagging operation was enclosed to minimize dust emissions. An operator's right hand was crushed when he actuated the door closure mechanism before removing his right hand from the enclosure. The door controls were changed so that the operator had to use both hands to press two widely spaced switches simultaneously to close the door.

☞ A pneumatic diaphragm pump was used to transfer a highly flammable material from drums into a storage tank. The pump's inlet and outlet hoses were attached with identical quick couplings, and they were accidentally reversed. The tank contents were pumped/siphoned back into the drum, spilling into the small curbed area and overflowing to the storage sewer.

3.1.19 Appearance at the Expense of Functionality

Although a design can be both functional and attractive, functionality should always be given precedence. Unfortunately, sometimes the opposite occurs. For example, laying out the instruments and controls for two parallel units as mirror images may look pretty, but it increases the likelihood of error if an operator works on both units. (Could you drive a car from the right-hand seat if the brake and accelerator pedals were reversed?) Making all the valve switches exactly the same color, shape, and size and locating them all in a precise, rectangular grid may look very neat, but it greatly increases the chance that an operator will choose the wrong switch. Although excessive concern for appearance is seldom the sole cause of an accident, it can be a major contributor, as illustrated in the following example:

☞ The supervisor would not allow operators to make any marks (denoting normal levels, pressures, temperatures, etc.) on the few remaining standard instruments and controls in the new, computerized central control room. The supervisor knew a lot of visitors would be touring the new control room, and he thought such marks would look "tacky." While responding to an upset, the operator glanced at the wall-mounted gauges but failed to note that the instrument air pressure had fallen dramatically. This delayed diagnosis of the broken instrument air line that was causing the upset.

Worker modifications usually indicate labeling deficiencies that they are trying to overcome. When managers see such modifications, they should take appropriate actions to remedy both the specific problems and the root causes of labeling deficiencies.

3.2 GENERAL APPROACHES TO IMPROVING HUMAN PERFORMANCE

The examples in the previous section illustrate several error-likely situations. The following paragraphs explain some general principles that managers can apply throughout their facilities to eliminate such situations before they result in an accident. ***Worker involvement is an essential part of any successful program for identifying and eliminating error-likely situations. Human factors specialists should also be employed to provide expert assistance in implementing any changes.***

3.2.1 Hardware Changes

First and foremost, managers should ensure that work situations conform to accepted human factors engineering principles. At the most basic level, this involves providing equipment compatible with fundamental human capabilities: knobs that can be grasped and turned with reasonable force, labels that can be read from a reasonable distance, manways large enough for access, etc. Beyond that, it involves locating equipment where it can conveniently be used in some logical relationship with the other equipment being used to perform a task. It also involves providing an environment (comfortable temperature, adequate lighting, limited noise, etc.) compatible with the physical requirements of the workers using the equipment.

Managers can also implement hardware changes that eliminate opportunities for human error. Such changes might include installing guards around pump switches, making hose couplings unique, or installing three-way valves to switch between parallel relief valves. Controls and displays can be simplified to minimize potential confusion and to directly provide the information workers need. And all equipment can be clearly and accurately labeled.

A third type of hardware modification is the installation of interlocks. When humans cannot perceive, diagnose, and respond to upsets before a serious accident occurs, the design should include appropriate interlocks. However, if the interlocks hinder normal operation or often trigger spuriously, they may create a hazard more severe than the one they are intended to prevent. Alarms and interlocks cause more problems than they solve if they must be disabled routinely so the process can be started up or production can be maintained, or if the alarms and interlocks are seldom tested and maintained.

3.2.2 Procedural Changes

Ensuring that current, accurate procedures are available to workers is the most important action managers can take in this area. The procedures should be written in simple, straightforward language with helpful diagrams and warnings, and be organized into a logical sequence of tasks. Critical procedures should include checkoff provisions and be written so each numbered step requires only one action. Ideally, there should be one current set of procedures kept where all workers can use them; personal copies of the procedures should not be allowed unless there is a rigorous system for controlling and updating them. Managers should require that procedures be regularly reviewed by workers and their supervisor to ensure that the procedures are kept up to date. Managers should also regularly audit worker practices to ensure compliance with the written procedures, so any differences can be resolved.

Managers can also require that procedures specify limiting conditions for system operation. *Such procedures should contain critical equipment lists and critical operating parameters.* If a component (e.g., a level controller) on the critical equipment list fails, the component must be repaired/replaced within a specified time or the feed rate must be reduced or a new batch must not be started. Similarly, if a critical operating parameter is exceeded, the system must be shut down. By clearly defining the system tolerances and identifying situations requiring worker intervention, the chance of worker inaction leading to accidents is greatly reduced.

Managers should look for ways to modify procedures so the likelihood of an undetected human error will be minimized. For example, to help workers detect and correct their own mistakes (as well as other system faults), procedures should state the expected system response to each worker action. Human redundancy can provide additional recovery factors for human errors. For example, procedures can require that a second (and even a third) person verify the performance of critical actions such as calculating the quantities of reactants for a batch. Good procedures and management systems maximize the chance that human errors will be detected before undesirable consequences occur.

3.2.3 Policy Changes

Policy decisions are completely the province of managers, so you can change policies that adversely affect human performance. One fundamental responsibility is to hire suitable workers and to give workers job assignments that match their capabilities, qualifications, and temperament. Management policies that reward workers for self-improvement and accomplishment will motivate superior performance.

Another fundamental management responsibility is to develop a safety culture within your company that discourages unsafe worker behavior. However, you must ensure that plant practices are consistent with your policies. *If "safety first" is your motto but "production first" is your practice, then workers may recklessly disregard safe practices to maintain production.*

Management policies on training have a major impact on worker performance. If workers only receive on-the-job training, they will not be prepared to deal with problems they have not yet seen. Some initial training helps, but as shown in Figure 9, their skill level on jobs they do not routinely perform will deteriorate rapidly. (How long after first learning cardiopulmonary resuscitation could you correctly perform the technique?) A manager who wants to minimize worker errors will implement training and practice programs that regularly challenge the workers' knowledge and let them practice their skills. Such programs (including onsite drills, talk-throughs, what-if challenges, and simulator training) will help workers develop and maintain a high level of skill, especially if they are initiated on a frequent, unpredictable basis by the workers' direct supervisors. As illustrated by the sawtooth curve in Figure 9, practice will not only arrest the rapid loss of a worker's new skills, but will also enhance those skills beyond the initial training. With repeated practice, these skills will become such well-learned behavior that there is very little loss of proficiency between practice sessions.

A third policy area that managers should review is staffing and working hours. When managers reduce staff, more and more tasks must be performed by fewer and fewer people. When workers feel rushed to complete their assignments, they are more apt to take shortcuts, to skip some tasks entirely, and to make more mistakes on the tasks they do perform. Mistakes are less likely to be caught because no one

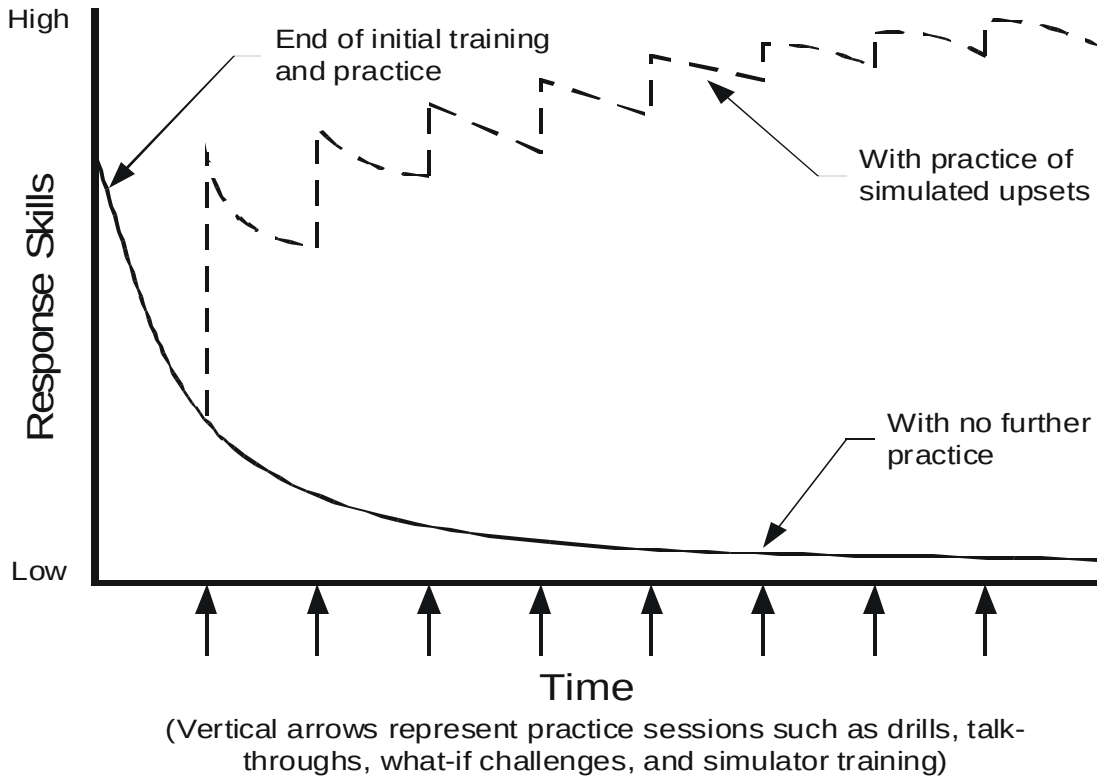


Figure 9 Effects of Practice on Skills (Based on Figure 3-6 in Reference 7)

has time to check another person's work. The problem is exacerbated when long working hours fatigue workers or shift rotation schedules disrupt their circadian rhythms. It is more than coincidence that so many major accidents occur on the graveyard shift and holiday weekends.[9] Managers must ensure that all shifts are staffed with an adequate number of qualified personnel, that working hours are not excessive, and that shift rotations are scheduled to minimize the disruption of workers' circadian rhythms. Managers should also ensure that the same person or crew on the same shift does not perform critical human tasks, such as testing/calibrating redundant instrument and control systems. Otherwise, a single, consistent human error could simultaneously defeat all the redundant systems.

Another policy area that managers should review is incident reporting and investigation. Very few major accidents have occurred without warning; most were preceded by one or more near misses. Therefore, it is critical that all near misses be reported so they can be investigated just as thoroughly as an accident. The investigation of both accidents and near misses must go beyond blaming "operator error" to identifying the true root causes in the work situation. Managers must ensure that the lessons learned from such investigations are applied not only at the site of the specific incident, but also at similar sites throughout the plant and the company.

Remember, your policies directly or indirectly establish all work situations within your facilities. Therefore, within the limits of your resources, you can significantly reduce the likelihood and consequences of human errors.

Section 4
MANAGEMENT USE OF HRA

4.1 DEFINITION OF HRA

Human reliability analysis (HRA) is a general term for methods by which the probability of human errors is estimated for any activity, including research, design, construction, operation, maintenance, management, and so forth. In an HRA, those human actions that can contribute to system failure are evaluated both qualitatively and quantitatively. Managers can often directly employ the qualitative HRA results alone to identify practical ways to reduce human errors such as those described in Section 3. If necessary, managers can extend the HRA to quantify the likelihood of human error and to assess the benefits of proposed changes in procedures, equipment, or other PSFs. Managers should consider using HRA when needs such as those listed in Table 6 arise.

Table 6 HRA Motivations

• The potential human errors associated with specific tasks must be identified so appropriate preventive measures and/or recovery factors can be identified and implemented
• Estimates of human error probabilities are needed as input for cost/benefit studies of alternative designs, procedures, or policies
• Estimates of human error probabilities are needed as input for quantitative risk assessments

When general improvements in human performance are desired, managers should employ human factors specialists to suggest improvements in the overall work situation and PSFs. Qualitative HRA results may be very useful in helping to justify both general and specific human factors engineering improvements. However, it is usually more efficient to correct any general human factors engineering deficiencies before investing in detailed, quantitative HRAs, because such deficiencies would have a major impact on the HRA results.

Once you decide to use HRA to satisfy a particular need, you must devote attention to three key areas that are described in the next three sections:

1. Chartering the analysis
2. Selecting and applying HRA techniques
3. Understanding the limitations

These areas are interrelated, and decisions about one affect the others. The first and third areas involve actions that primarily you, the ultimate user, must take (e.g., carefully defining written objectives for the HRA project team). Other actions in these areas will require your careful interaction and negotiation with the HRA team (e.g., defining analysis scope and available resources) to ensure that their

final product meets your needs. The second area involves decisions that you will influence, but that should be left to the team's discretion (e.g., selection of specific analytical techniques).

Decisions concerning these areas are not simply made once, never to be considered again. You should review each area periodically as intermediate results are developed to ensure that the HRA remains on track. Ignoring any of these areas diminishes the likelihood that your HRA objectives will be satisfied.

4.2 CHARTERING THE ANALYSIS

If an HRA is to efficiently satisfy your requirements, you must specifically define its charter for the analysts. Figure 10 contains the various elements of an HRA charter. Defining these elements requires an understanding of the reasons for the study, a description of the manager's needs, and an outline of the type of information required from the study. Sufficient flexibility must be built into the analysis scope, technical approach, schedule, and resources to accommodate later refinement of any undefined charter element(s) based on knowledge gained during the study. The HRA team must understand and support the analysis charter; otherwise, a useless product may result.

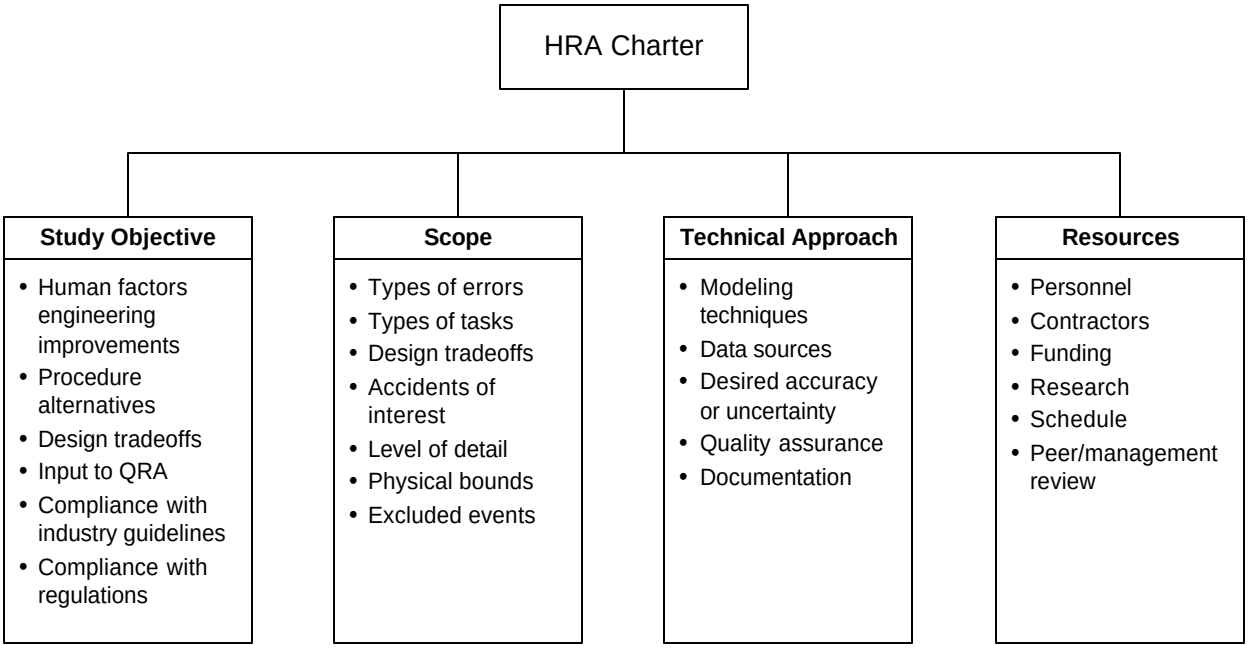


Figure 10 Elements of an HRA Charter

4.2.1. Study Objective

An important and difficult task is concisely translating your requirements into HRA study objectives. For example, if you need to decide between two methods for making a hazardous chemical, you should state the specific objective ("I want to know the relative difference in the human error

probabilities for the two methods"), not the more general objective ("I want to know the chance of human error for the two methods"). And asking your HRA team for more than is necessary to satisfy your particular need is counterproductive. For example, if qualitative results will provide adequate information, you should not waste your resources pursuing quantitative estimates of human error probabilities. For any HRA to efficiently produce the necessary types of results, you must clearly communicate your requirements through well-written objectives. Table 7 gives some examples of practical achievable objectives for HRA.

Table 7 Examples of Typical HRA Objectives

• Identify human factors issues in the process hazard analysis of the startup and shutdown procedures for a furnace
• Determine the probability of a human error causing a toxic chemical release during truck loading
• Identify the most likely human errors that would cause a runaway reaction, and identify the best way to improve safety
• Compare three procedures, and rank them according to their human error probability
• Determine the probability that a spare pump will be unavailable as the result of a maintenance error
• Identify the most cost-effective ways to reduce the probability that human errors will cause process interruptions
• Estimate how much having a second engineer independently verify process parameters would reduce the probability of off-specification products

4.2.2 Scope

Establishing and documenting the physical and analytical boundaries and assumptions for an HRA are also difficult tasks. Even though you will provide input, the HRA project team will largely make the scope definition. Of the items listed in Figure 10, selection of an appropriate level of detail is the scope element that is most crucial to performing an efficient HRA. You should encourage your HRA team to use screening data and gross levels of resolution during the early stages of the HRA, particularly if the HRA results will be used as input to a quantitative risk analysis (QRA). Once the analysts determine the tasks that are significant contributors to risk, they can selectively apply more detailed effort to specific issues as the analysis progresses. This strategy will help conserve analysis resources by focusing only on areas important to developing improved risk understanding. You should review the boundary conditions and assumptions with the HRA team during the course of the study and revise them as more is learned about key sensitivities. *In the end your ability to effectively use HRA estimates will be determined largely by your appreciation of important study assumptions and limitations resulting from scope definition. Therefore, it is critical that the physical and analytical boundaries and assumptions be clearly documented.*

4.2.3 Technical Approach

The HRA project team can select the appropriate technical approach once you specify the study objectives, and together you can define the scope. A variety of modeling techniques (discussed in Section 4.3) and general data sources can be used to produce the desired results. The HRA team must take care to select an HRA technique that will satisfy your study objectives because many techniques are theoretical models with limited practical applicability.

You should consider obtaining internal and external quality assurance reviews of the study (to ferret out errors in modeling, data, etc.). Independent peer reviews of the HRA results can help by presenting alternate viewpoints, and you should include outside experts (either consultants or personnel from another plant) on the HRA review panel. You should also set up a mechanism wherein disputes between HRA team members (e.g., technical arguments about system responses) can surface and be reconciled. All of these factors play an essential role in producing a defendable, high-quality HRA. Once the HRA is complete, you must formally document your response to the project team's final report and any recommendations the report contains.

4.2.4 Resources

Managers can use HRA to study small-scale as well as large-scale enterprises. For example, an HRA can be performed on a single activity, such as a loading procedure.[10] Depending upon the study objectives, a complete HRA (with HRA event trees and human error probability estimates) could require as little as a few days to a few weeks of technical effort. On the other hand, a major study to identify all the human errors contributing to the hazards associated with a large process unit (e.g., a unit with an associated capital investment of $50 million) may require 1 to 3 person-months of effort, and a complete HRA of that same unit may require up to 1 or 2 person-years of effort.

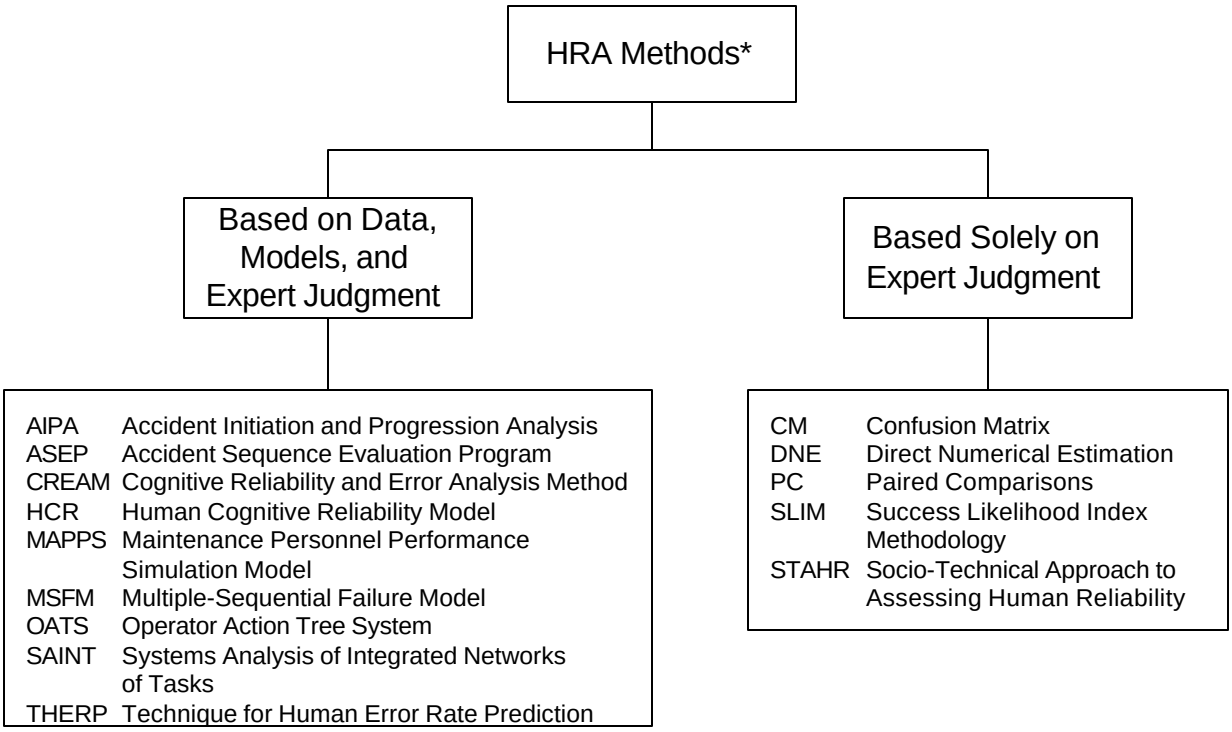
If an HRA is commissioned, you must adequately staff the HRA team in order to successfully perform the work. An appropriate blend of engineering and scientific disciplines must be assigned to the project. If the study involves a production activity, operations and maintenance personnel will play a crucial role in ensuring that the HRA models accurately represent the real system and plant practices. In addition to the HRA analyst(s), a typical team may also require assistance from systems analysts, process engineers, senior operators, design engineers, instrumentation engineers, maintenance supervisors, and/or inspectors who are familiar with the system. Unless your company has significant in-house HRA experience, you may be faced with selecting outside specialists to help perform the larger or more complex analyses. If contractors are used extensively, you should require that cognizant personnel be an integral part of the HRA team.

4.3 SELECTING AND APPLYING HRA TECHNIQUES

Depending upon your objectives, an HRA involves one or more of the following four basic steps:

1. Human factors engineering evaluation
2. Task analysis
3. Quantification
4. Sensitivity and uncertainty analyses

Numerous analysis techniques and models have been developed to aid in performing these four steps (Figure 11). Many references exist for specific methods, and several recent publications give specific advice and "how to" details for the various techniques. You will not have to select specific techniques — your HRA team will do that. But you should verify that the techniques selected are useful, practical, and acceptable. (See Reference 11 for an evaluation of various HRA techniques.)



* Some of these HRA methods have limited applications

Figure 11 Overview of HRA Methods

A useful technique will yield qualitative information that can be used as the basis for recommending safety or operability improvements, regardless of whether any quantitative analysis is performed. But, if quantification is required, a useful technique should yield valid and consistent estimates of human performance characteristics necessary for QRA, such as response times, conditional

human error probabilities, and uncertainties. The selected technique(s) should also be applicable to the range of human tasks being evaluated and flexible enough to address plant-specific conditions.

In addition to being useful, an HRA technique must be practical to apply, given the time, money, and human resources available for the analysis. Some techniques are not practical because they are so complex that only a few experts can apply them, or the required data are simply unavailable for the tasks being evaluated.

Finally, a technique must produce results that will be acceptable for your stated purpose. Although many of the techniques have undergone peer review, very few have been benchmarked with actual data from industrial activities. Several have been used in QRAs that were accepted by government authorities issuing licenses and permits or conducting public hearings.

Regardless of the method selected, the four basic steps listed previously must be accomplished in a complete HRA. The first task involves collecting data, inspecting the facility, and evaluating the general PSFs that will influence the operators as they work. Analysts must then work with the entire HRA team to dissect the worker tasks into specific potential errors of omission or commission that can be quantified.

When the task analysis is complete, the HRA analysts can begin the quantification process. Most analysts begin by constructing event trees such as those illustrated in Figures 12 and 13 and then estimating nominal human error probabilities (HEPs) for each potential error. (A typical HEP would be 0.003 for a specific error of omission or commission, such as skipping an item in a checklist or misreading an analog meter.[7]) The nominal HEPs are modified to account for plant-specific PSFs and the effects of success or failure on preceding tasks (dependence). (Modified HEPs may be factors of 10 or more higher or lower than the nominal HEPs.) Finally, the benefits of any recovery factors are accounted for, and total human error probabilities are calculated. The quantitative results may then be subjected to sensitivity and uncertainty analyses.

Sensitivity analyses are very useful to a manager because they show how changes in the analysts' assumptions or boundary conditions would alter the HRA results. Uncertainty analyses of the variations in the results attributable to data uncertainties are generally less useful. Uncertainties arise from many different causes (model completeness, analyst judgment, etc.), and data uncertainties are often not the most significant. For most decisions involving HRA results, managers can rely on best estimates and sensitivity results, using good judgment and intuition to make some allowance for uncertainty.

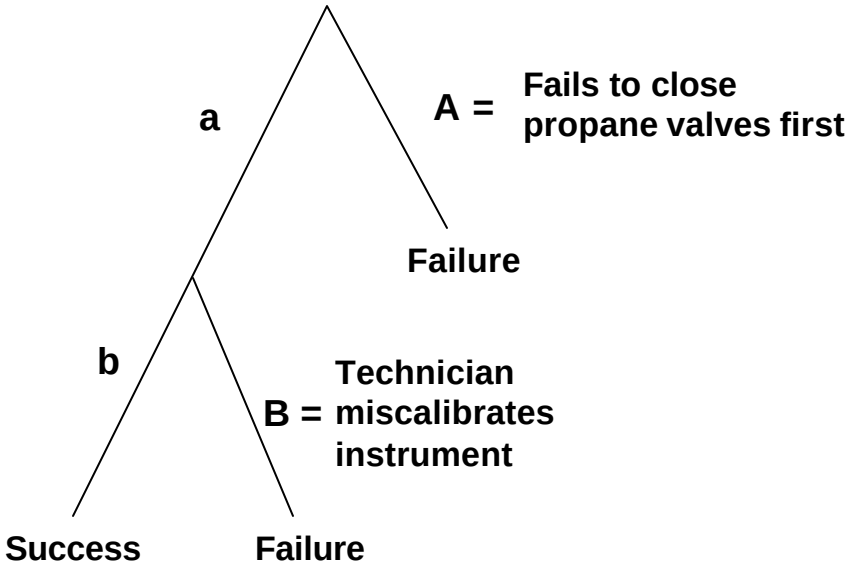


Figure 12 HRA Event Tree of Hypothetical Calibration Tasks

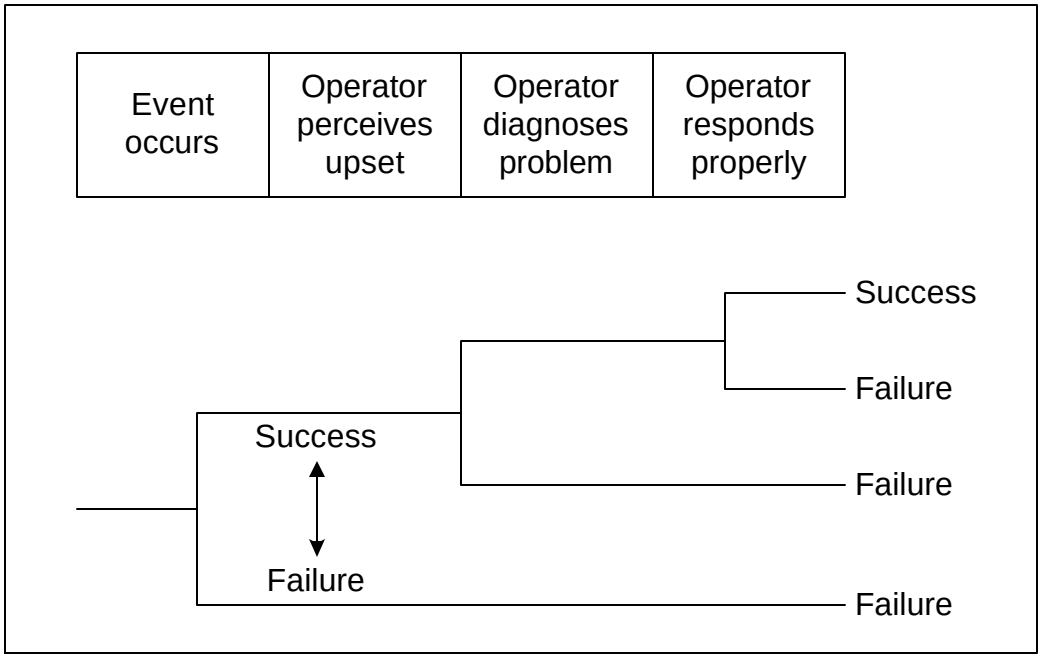


Figure 13 Typical Operator Action Tree

4.4 UNDERSTANDING THE LIMITATIONS

Human reliability analyses suffer from essentially the same limitations as quantitative risk analyses.[4] Table 8 lists five of the major limitations of HRA. Some of these may be relatively unimportant for a specific study, and using qualified analysts with adequate resources may minimize others. However, you must be aware of these limitations when chartering an HRA and when using the results for decision-making purposes. And you must understand that *the assumptions made during an HRA are as important as any results.* Therefore, the assumptions should be as carefully documented as the HRA results. Despite these limitations, HRA is an extremely valuable tool for identifying and evaluating ways to reduce human errors.

Table 8 Major Limitations of HRA

Issue	Description
Completeness	There can never be a guarantee that all human errors, extraneous acts, and recovery factors have been considered, nor that everything affecting human behavior has been considered.
Validity/Specificity	Probabilistic failure models cannot be completely verified. Human behaviors are observed in experiments and used in model correlations, but models are, at best, approximations of specific circumstances. Some HRA models are based on debatable assumptions about human behavior. The HRA may not provide a good representation of specific plant tasks and PSFs.
Accuracy/Uncertainty	The lack of specific data on human error probabilities, PSFs, and accident diagnosis models severely limits accuracy and can produce large uncertainties, especially for prediction of very low-probability human behavior.
Reproducibility/Bias	Various aspects of HRA are highly subjective – the results are very sensitive to the analyst's assumptions. The same problem, using identical data and models, may generate widely varying answers when analyzed by different experts, or by the same expert at different times.
Traceability/Scrutability	Attempting to understand all the detailed documentation of analyses that led to the HRA results can be an overwhelming, tedious task.

Section 5
CONCLUSIONS

People perform critical system functions, and their decisions and actions dictate any system's performance. Even in "automated" processes, people must decide what a system is to do, prepare it to operate, monitor its performance, respond to any upsets, and shut it down at the end of a production run. People are the only responsible agents in a system, and their errors assume an importance commensurate with their responsibilities.

Many process safety management activities are directly or indirectly intended to improve human performance. The *Responsible Care® Process Safety Code of Management Practices*,[12] which was developed to help managers implement the American Chemistry Council's Responsible Care® program, and the *Guidelines for the Technical Management of Chemical Process Safety*,[13] published by the Center for Chemical Process Safety, explicitly address the importance of human factors as an element of process safety. Similarly, the *Recommended Practice for Management of Process Hazards*[14] and the *Recommended Practice for Development of a Safety and Environmental Management Program for Outer Continental Shelf (OCS) Operations and Facilities*,[15] published by the American Petroleum Institute (API), recognize the importance of human factors, as do several government agencies.[16,17,18] Obviously, updating procedures and increasing training will directly reduce the likelihood of errors, as will increasing the process safety information readily available to workers. Process hazard analyses, safety reviews, and inspection programs help detect human errors in the design, construction, installation, modification, and maintenance of process equipment before such errors cause a process upset or accident.

Human factors engineering and human reliability analyses can also make specific contributions to process safety by identifying error-likely situations that should be corrected. As indicated in Table 9, incorporating well-established human factors engineering principles into the design of equipment and procedures will help reduce the frequency of errors and help ensure that any errors that do occur are detected before the system suffers some adverse consequence. Human reliability analyses are uniquely useful to managers because they offer a means to both qualitatively identify error-likely situations and to quantitatively estimate the probability of human errors. Managers can use the quantitative results directly in their decision-making process or as an input to QRAs.

You can use the lists of questions[19, 20] in Appendixes 1 and 2 as a starting point to help identify ways to improve human performance at your facilities. You can also immediately begin to involve workers in the design of their work situations and to develop human factors engineering expertise within your organization. The bibliography identifies many excellent references for further reading. The Center for Chemical Process Safety has also published *Guidelines for Preventing Human Error in Process Safety*.[21]

Table 9 Estimated Decreases in HEPs Resulting from Improvements in the Work Situation (Based on Table 3-8 in Reference 7)

Improvement	Resulting Decrease in HEPs (Factors [a])
Good human factors engineering practices in design of controls, displays, and equipment	2 to 10
Use of well-designed written procedures and checklists to replace typical narrative-style procedures	3 to 10
Redesign of displays or controls that violate strong populational stereotypes	over 10
Redesign of valve labeling to clearly indicate each valve's function and its normal operating status	about 5
Frequent practice of the appropriate responses to potential emergencies or other abnormal situations	2 to 10

[a]These estimated factors are neither directly multiplicative nor additive.

In the end, managers must recognize that most human errors are a consequence of the work situation and not worker carelessness. The term "human error" should connote no more sense of blame or emotion than the term "hardware failure." Rather than seeking to blame or punish a worker when an incident occurs, managers should look for the root causes in the work situation. Only if managers recognize and accept their responsibility to identify and eliminate error-likely situations in the workplace will there be a significant reduction in the frequency and severity of human errors. Directly involving the workers in these efforts is the best way to achieve your goals. Ultimately, improvements in human performance will be reflected as tangible improvements in safety, quality, and productivity throughout the process industries.

GLOSSARY

Administrative controls — Procedural mechanisms, such as lockout/tagout procedures, for directing and/or checking human performance on plant tasks.

Checklist — A written procedure in which each item is marked off (or acknowledged on a computer screen) as its status is verified.

Circadian rhythm — The approximately 24-hour rhythm of sleep and waking hours.

Decision making — (1) Decision making as part of diagnosis: the act of choosing between alternative diagnoses, e.g., to settle on the most probable cause of the pattern or stimuli associated with an abnormal event; (2) postdiagnosis decision making: the act of choosing which actions to carry out after a diagnosis has been made (in many cases, these actions are prescribed by rules or procedures, and decision making is not required).

Dependence (between two tasks) — The situation in which the probability of failure (or success) of one task is affected by success or failure of another task. The tasks may be performed by the same or different persons.

Diagnosis — The mental evaluation of the most likely causes of an abnormal event and the identification of those systems or components whose status can be changed to reduce or eliminate the problem; diagnosis includes interpretation and (when necessary) decision making.

Display — Any instrument or device that presents information to any human sense organ (visual, audible, etc.).

Disruptive stress — The bodily or mental tension resulting from the response to a stressor that threatens, frightens, worries, or angers a person, or increases his/her uncertainty, so that the person performs at a decreased level of effectiveness or efficiency.

Ergonomics — See human factors.

Error-likely situation — A work situation in which the performance shaping factors are not compatible with the capabilities, limitations, or needs of a person to perform a task correctly.

GLOSSARY (contend.)

Facilitative stress	The bodily or mental tension resulting from the internal response to a stressor that stimulates a person to work at optimum performance levels.
HRA event tree	A graphical representation of sequential events in which the tree limbs designate human actions and other events as well as different conditions or influences upon these events. The values assigned to all tree limbs (except those in the first branching) are conditional probabilities. At any branch point in the tree, the sum of the probability values assigned to all of the limbs emanating from that point is 1.0. Typically, the HRA event tree is drawn as a binary tree (i.e., only two limbs at each branch point).
Human error	Any human action (or lack thereof) that exceeds some limit of acceptability (i.e., an out-of-tolerance action) where the limits of human performance are defined by the system.
Human error probability (HEP)	The probability that an error will occur when a given task is performed. Synonyms: human failure probability and task failure probability.
Human factors	A discipline concerned with designing machines, operations, and work environments so that they match human capabilities, limitations, and needs. Among human factors specialists, this general term includes any technical work (engineering, procedure writing, worker training, worker selection, etc.) related to the human factor in operator-machine systems.
Human factors engineering	See human factors. Among human factors specialists, the term is often restricted to design of equipment. In this Guide, the term is used interchangeably with human factors and ergonomics.
Human factors specialist	A person working in the human factors area. Synonyms: ergonomist and engineering psychologist.
Human reliability analysis (HRA)	A method used to determine the probability that system-required human actions, tasks, or jobs will be completed successfully within a required time period, as well as the probability that no extraneous human actions detrimental to the system will be performed.

Intentional deviation (error) — An error that occurs when the worker performs some action that is incorrect but that he/she believes to be correct or to be a superior method of performance. Such errors often occur when the worker misdiagnoses the true cause of an upset or when the worker disregards the written procedure. *This type of error is not malevolent behavior.*

Operator — An individual responsible for monitoring, controlling, and performing tasks as necessary to accomplish the productive activities of a system. Often used in this Guide in a generic sense to include people who perform all kinds of tasks (e.g., reading, calibration, maintenance).

Operator-machine interface — Any point of interaction between people and other people or components in a system (e.g., a display, a manual control, or an oral instruction). Synonyms: man-machine interface, human-machine interface, operator-process interface, and operator-hardware interface.

Performance influencing factor (PIF), or performance shaping factor (PSF) — Any factor that influences human performance. PSFs include factors intrinsic to an individual (personality, skills, etc.) and factors in the work situation (task demands, plant policies, hardware design, etc.).

Populational stereotype — The way in which an identifiable group of people expect other people or equipment to behave (e.g., turning a valve handle clockwise to close the valve).

Quantitative risk analysis (QRA) — The systematic development of numerical estimates of the expected frequency and/or consequence of potential accidents associated with a facility or operation.

Recovery factors — Factors that limit or prevent the undesirable consequences of a human error.

Responses — The actions carried out after the worker has received and processed information related to his/her tasks. These responses constitute the human outputs in operator-machine systems and serve as inputs to the systems.

Stress — Bodily or mental tension, ranging from a minimal state of arousal through an optimal level of stimulation to a feeling of threat to one's well being. Stress is the human response to a stressor (an unexpected pay raise, a supervisor's criticism, a loud noise, etc.), and it may be either facilitative or disruptive to reliable human performance.

Talk-through — A task analysis method in which workers describe the actions required in a task and explain what they are doing and their mental processes during each action in actual or simulated performance of a task. If the performance is simulated, the workers touch the manual controls they would operate and describe the control action required, point to displays and state what readings they would expect, describe any time delays and feedback signals, and explain the effects of their actions on the process. Synonym: walk-through.

Task — Any unit of action that contributes to the accomplishment of some system goal or function. Tasks are often divided into smaller elements called steps.

Task analysis — An analytical process for determining the specific behaviors required of humans in operator-machine systems. It involves determining the detailed performance required of people and equipment and determining the effects of environmental conditions, malfunctions, and other unexpected events on both. Within each task to be performed by people, behavioral steps are analyzed in terms of (1) information presented to, and received by, the workers; (2) their processing of that information (and previously stored information, goals, intentions, etc.) to interpret the system status and to decide what action, if any, to take; and (3) required worker inputs to the system (which include other workers as well as the equipment).

Task load — The amount of work a person has to do in some time period. A very low task load does not provide sufficient arousal to keep a person alert. An optimum task load matches the worker's capacity and facilitates optimum performance. A heavy task load exceeds a person's normal capacity and is moderately disruptive of performance.

Work-situation approach A strategy for improving human performance based on the premise that most human errors arise from factors primarily related to the design of the work situation. The work-situation approach focuses on identifying and eliminating error-likely situations, not blaming the worker.

REFERENCES

1. J. C. Coco, ed., *Large Property Damage Losses in the Hydrocarbon-Chemical Industries: A Thirty Year Review*, Eighteenth Edition, Marsh and McLennan Protection Consultants, Chicago, IL, 1998.

2. *The Phillips 66 Company Houston Chemical Complex Explosion and Fire*, Occupational Safety and Health Administration, U.S. Department of Labor, Washington, DC, April 1990.

3. A. D. Swain, *Design Techniques for Improving Human Performance in Production*, A. D. Swain, 712 Sundown Place SE, Albuquerque, NM, 87108, January 1986 (Revised).

4. J. S. Arendt and D. K. Lorenzo, *Evaluating Process Safety in the Chemical Industry: User's Guide to Quantitative Risk Analysis*, Center for Chemical Process Safety and American Chemistry Council, Washington, DC, September 2000.

5. B. Rasmussen, "Chemical Process Hazard Identification," *Reliability Engineering and System Safety*, Vol. 24, Elsevier Science Publishers Ltd., Great Britain, 1989, pp 11-20.

6. R. E. Butikofer, *Safety Digest of Lessons Learned*, API Publication 758, American Petroleum Institute, Washington, DC, 1986.

7. A. D. Swain and H. E. Guttmann, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*, NUREG/CR-1278, U.S. Nuclear Regulatory Commission, Washington, DC, August 1983, with *Addendum #1 to NUREG/CR-1278, August 1983*, September 1, 1985, by A. D. Swain.

8. H. M. Paula and R. E. Battle, "Reliability Performance of Fault-Tolerant Digital Control Systems," presented at the *1990 Loss Prevention Symposium of the American Institute of Chemical Engineers*, San Diego, CA, August 19-22, 1990.

9. G. Mapes, "Beating the Clock: Was It an Accident that Chernobyl Exploded at 1:23 in the Morning?," *The Wall Street Journal*, Vol. CCXV, No. 70, April 20, 1990.

10. W. Bridges, J. Kirkman, and D. Lorenzo, "Include Human Errors in Process Hazard Analysis," *Plant Safety*, 1996.

11. A. D. Swain, *Comparative Evaluation of Methods for Human Reliability Analysis*, GRS-71 (ISBN 3-923875-21-5), Gesellschaft für Reaktorsicherheit (GRS) mbH, Garching, Federal Republic of Germany, April 1989 (in English).

12. *Responsible Care®: Process Safety Code of Management Practices*, Chemical Manufacturers Association, Washington, DC, 1990.

13. *Guidelines for the Technical Management of Chemical Process Safety*, Center for Chemical Process Safety of the American Institute of Chemical Engineers, New York, NY, 1989.

14. *Recommended Practice for Management of Process Hazards, API-RP-750*, American Petroleum Institute, Washington, DC, 1990.

15. *Recommended Practice for Development of a Safety and Environmental Management Program for Outer Continental Shelf (OCS) Operations and Facilities*, *API-RP-75*, American Petroleum Institute, Washington, DC, 1998.

16. *Process Safety Management of Highly Hazardous Chemicals, 29 CFR 1910.119,* Occupational Safety and Health Administration, Washington, DC.

17. *Risk Management Program, 40 CFR 68*, Environmental Protection Agency, Washington, DC.

18. *Contra Costa County Safety Program Guidance Document (for Implementing Section 450-8.016(B) of County Ordinance 98-48)*, Contra Costa Health Services, Hazardous Materials Programs, Contra Costa County, CA, 2000.

19. *Human Factors in Industrial Safety*, HS(G)48 (ISBN 011 8854860), Health and Safety Executive, Her Majesty's Stationery Office, London, U.K., 1989.

20. *Improving Human Performance Systems in the Petroleum Industry – Phase I, Data Collection & Feasibility Assessment,* prepared for the American Petroleum Institute, Safety and Fire Protection Subcommittee, by EQE International, Inc., Oakland, CA, April 1999.

21. *Guidelines for Preventing Human Error in Process Safety*, Center for Chemical Process Safety of the American Institute of Chemical Engineers, New York, NY, 1994.

BIBLIOGRAPHY

General Information

1. Ball, P., "The Guide to Reducing Human Error in Process Operation," Report No. SRF R484. Safety and Reliability Directorate, AEA Technology, Warrington, England, 1991.

2. Brown, S. C. and J. N. T. Martin (eds.), *Human Aspects of Man-Made Systems*, Great Britain, Open University Press, 1977.

3. Drury, C. G. and J. G. Fox (eds.), *Human Reliability in Quality Control*, London, Taylor & Francis, 1975.

4. Edwards, E. and F. P. Lees (eds.), *Man and Computer in Process Control*, London, The Institution of Chemical Engineers, 1973.

5. Edwards, E. and F. P. Lees (eds.), *The Human Operator in Process Control*, London, Taylor & Francis, 1974.

6. Embrey, D. E., *Human Reliability in Complex Systems: An Overview*, NCSR.R10, National Centre of Systems Reliability, United Kingdom Atomic Energy Authority, Warrington, England, July 1976.

7. Kletz, T. A. and G. D. Whitaker, "The Man in the Middle," *Safety Newsletter*, No. 123, May 1979.

8. Kletz, T. A. and G. D. Whitaker, *Human Error and Plant Operation*, EDN 4099, Safety and Loss Prevention Group, Petrochemicals Division, Imperial Chemical Industries, Ltd., Billingham, England, 1973.

9. Rasmussen, J. and W. B. Rouse (eds.), *Human Detection and Diagnosis of System Failures*, New York, Plenum Press, 1981.

10. Reason, J., *Human Error*, Cambridge, University Press, 1990.

11. Rook, L. W., *Reduction of Human Error in Industrial Production*, SCTM-93-62(14), Sandia National Laboratories, Albuquerque, NM, June 1962.

12. Smith, H. T. and T. R. G. Green (eds.), *Human Interaction with Computers*, New York, Academic Press, 1980.

13. Swain, A. D., "A Work Situation Approach to Improving Job Safety," *Proceedings, 1969 Professional Conference*, American Society of Safety Engineers, Chicago, August 1969, pp 233-257 (also pp 371-386 in J. T. Widner [ed.], *Selected Readings in Safety*, Macon, GA, Academy Press, 1973).

14. Swain, A. D., "Design of Industrial Jobs a Worker Can and Will Do," *Human Factors*, 1973, Vol. 15, pp 129-136.

15. Woodward, J. L. (ed.), *Proceedings of the International Symposium on Preventing Major Chemical Accidents*, Center for Chemical Process Safety of the American Institute of Chemical Engineers, Washington, DC, February 3-5, 1987.

Human Factors Engineering

16. Banks, W. W., D. I. Gertman, and R. J. Petersen, *Human Engineering Design Consideration for Cathode Ray Tube-Generated Displays*, EG&G Idaho, Inc., NUREG/CR-2496, U.S. Nuclear Regulatory Commission, Washington, DC, April 1982.

17. Chapanis, A., *Man-Machine Engineering*, Belmont, CA, Wadsworth Publishing Co., 1965.

18. Eastman Kodak Company, *Ergonomic Design for People at Work*, Vols. 1 & 2 , New York, Van Nostrand Reinhold, 1986.

19. *Ergonomic Checkpoints: Practical and Easy-To-Implement Solutions for Improving Safety, Health, and Working Conditions*, International Labor Organization, 1996.

20. *Guidance Notes on the Application of Ergonomics to Marine Systems*, American Bureau of Shipping, New York, NY, January 1998.

21. Kantowitz, B. H. and R. D. Sorkin, *Human Factors: Understanding People-System Relationships*, New York, John Wiley and Sons, 1982.

22. Kinkade, R. G. and J. Anderson, *Human Factors Guide for Nuclear Power Plant Control Room Development*, EPRI NP-3659, Electric Power Research Institute, Palo Alto, CA, 1984.

23. McCafferty, Denise, "Successful System Design Through Integrating Engineering and Human Factors," *Plant Safety*, 1996.

24. MIL-STD1472C, *Military Standard, Human Engineering Design Criteria for Military Systems, Equipment and Facilities*, U.S. Department of Defense, Washington, DC, May 2, 1981.

25. NUREG-0700, *Guidelines for Control Room Reviews*, U.S. Nuclear Regulatory Commission, Washington, DC, September 1981.

26. NUREG-0801, *Evaluation Criteria for the Detailed Control Room Design Review*, U.S. Nuclear Regulatory Commission, Washington, DC, October 1981.

27. Pheasant, S., *Body Space: Anthropometry, Ergonomics and Design*, Philadelphia, Taylor & Francis, 1986.

28. Salvendy, G., *Handbook of Human Factors*, New York, John Wiley and Sons, 1987.

29. Sanders, M. S. and E. J. McCormick, *Human Factors in Engineering and Design*, Hightstown, NJ, McGraw-Hill Book Company, 1987.

30. Seminara, J. L., S. K. Eckert, S. Seidenstein, W. R. Gonzalez, R. L. Stempson, and S. O. Parsons, *Human Factors Methods for Control Room Design*, EPRI NP-1118-SY, Electric Power Research Institute, Palo Alto, CA, June 1979.

31. Seminara, J. L. and D. L. Smith, "Remedial Human Factors Engineering–Part I," *Applied Ergonomics*, 1983, Vol. 14, No. 4, pp 253-264.

32. Seminara, J. L. and D. L. Smith, "Remedial Human Factors Engineering–Part II," *Applied Ergonomics*, 1984, Vol. 15, No. 1, pp 31-44.

33. Swain, A. D., *Design Techniques for Improving Human Performance in Production*, A. D. Swain, 712 Sundown Place SE, Albuquerque, NM 87108, January 1986 (Revised).

34. Van Cott, H. P. and R. G. Kinkade (eds.), *Human Engineering Guide to Equipment Design*, Washington, DC, U.S. Government Printing Office, 1972 (Revised).

35. Woodson, W. E., *Human Factors Design Handbook*, New York, McGraw-Hill, 1981.

Performance Shaping Factors

36. Buckner, D. N. and J. J. McGrath (eds.), *Vigilance: A Symposium*, New York, McGraw-Hill, 1963.

37. Colquhoun, W. P. and J. Rutenfranz (eds.), *Studies of Shiftwork*, London, Taylor & Francis, 1980.

38. Colquhoun, W. P., "Circadian Rhythms, Mental Efficiency, and Shift work," *Ergonomics*, 1970, Vol. 13, pp 558-560.

39. Fokard, S., T. H. Monk, and M. C. Lobban, "Towards a Predictive Test of Adjustment to Shift Work," *Ergonomics*, 1979, Vol. 22, pp 79-91.

40. Goodstein, L. P., H. B. Andersen, and S. E. Olsen (eds.), *Mental Models, Tasks and Errors*, London, Taylor & Francis, 1988.

41. Grinker, R. R. and J. P. Spiegel, *Men Under Stress,* New York, McGraw-Hill, 1963 (Reprinted from 1945).

42. Janis, I. L. and L. Mann, *Decision Making: A Psychological Analysis of Conflict, Choice, and Commitment,* New York, The Free Press, 1977.

43. Kaplan, M. F. and S. Schwartz (eds.), *Human Judgment and Decision Processes*, New York, Academic Press, 1975.

44. Kelly, R. J., P. J. Kelly, R. Lajoie, K. M. Raven, and M. F. Schneider, *Final Report on the 12-Hour Shift Task Group*, Ontario Hydro, Toronto, Ontario, Canada, July 1982.

45. Moray, N. (ed.), *Mental Workload, Its Theory and Measurement,* New York, Plenum Press, 1979.

46. Rook, L. W., *Motivation and Human Error*, SC-TM-65-135, Sandia National Laboratories, Albuquerque, NM, September 1965.

47. Schneider, M. F., J. D. Brooke, and N. Moray, *Human Error Rates for 12-Hour vs. 8-Hour Shifts in Bruce Heavy Water Plant Operation*, Ontario Hydro, Toronto, Ontario, Canada, June 1982.

48. Tilley, A. J., R. T. Wilkinson, P. S. G. Warren, B. Watson, and M. Drud, "The Sleep and Performance of Shift Workers," *Human Factors*, 1982, Vol. 24, pp 629-641.

Procedures

49. Bridges, William, "Create Effective Safety Procedures and Operating Manuals," *Chemical Engineering Progress*, December 1997.

50. Brune, R. L. and M. Weinstein, *Procedures Evaluation Checklist for Maintenance, Test, and Calibration Procedures Used in Nuclear Power Plants*, Human Performance Technologies, Inc. and Sandia National Laboratories, NUREG/CR-1369, Revision 1, U.S. Nuclear Regulatory Commission, Washington,DC, September 1982.

51. Brune, R. L. and M. Weinstein, *Checklist for Evaluating Emergency Operating Procedures Used in Nuclear Power Plants*, Human Performance Technologies, Inc. and Sandia National Laboratories, NUREG/CR-2005, Revision 1, U.S. Nuclear Regulatory Commission, Washington, DC, April 1983.

52. *Guidelines for Effective Operating and Maintenance Procedures*, Center for Chemical Process Safety, 1996.

53 INPO 82-017, *Emergency Operating Procedures Writing Guideline*, Institute of Nuclear Power Operations, Atlanta, GA, July 1982.

54 INPO 83-004, *Emergency Operating Procedures Verification Guideline*, Institute of Nuclear Power Operations, Atlanta, GA, March 1983.

55. NUREG-0899, *Guidelines for the Preparation of Emergency Operating Procedures: Resolution of Comments on NUREG-0799*, U.S. Nuclear Regulatory Commission, Washington, DC, August 1982.

56. vonHerrmann, J. L., *Methods for Review and Evaluation of Emergency Procedure Guidelines, Volume I: Methodologies*, Wood-Leaver and Associates, Inc., and EG&G Idaho, Inc., NUREG/CR-3177, U.S. Nuclear Regulatory Commission, Washington, DC, March 1983.

57. Williams and Gromacki, "Eliminating Error-Likely Situations During Procedure Updates," presented at AIChE 32nd Loss Prevention Symposium, 1998.

Task Analysis

58. Beare, A. N., R. E. Dorris, C. R. Bovell, D. S. Crowe, and E. J. Kozinsky, *A Simulator-Based Study of Human Errors in Nuclear Power Plant Control Room Tasks*, General Physics Corporation and Sandia National Laboratories, NUREG/CR-3309, U.S. Nuclear Regulatory Commission, Washington, DC, January 1984.

59. Flanagan, J. C., "The Critical Incident Technique," *Psychological Bulletin*, 1954, Vol, 51, pp 327-358.

60. Grandjean, E., *Fitting the Task to the Man*, Philadelphia, PA, Taylor & Francis, 1988.

61. Kurke, M. I., "Operational Sequence Diagrams in System Design," *Human Factors*, 1961, Vol. 3, pp 66-73.

62. Miller, R. B., *A Method for Man-Machine Task Analysis*, WADC TR 53-137, Wright Air Development Center, Wright-Patterson Air Force Base, OH, June 1953.

63. Mills, R. G. and S. A. Hatfield, "Sequential Task Performance: Task Module Relationships, Reliabilities, and Times," *Human Factors*, 1974, Vol. 16, pp 117-128.

64. Swain, A. D., *System and Task Analysis, A Major Tool for Designing the Personnel Subsystem*, SCR-457, Sandia National Laboratories, Albuquerque, NM, January 1962.

HRA Methods and Evaluations

65. Bell, B. J. and A. D. Swain, *A Procedure for Conducting a Human Reliability Analysis for Nuclear Power Plants*, NUREG/CR-2254, U.S. Nuclear Regulatory Commission, Washington, DC, May 1983.

66. Bell, B. J., S. E. Rose, D. J. Hesse, L. A. Minton, L. N. Haney, H. S. Blackman, and J. P. Jenkins, *Comparison and Application of Quantitative Human Reliability Analysis Methods for the Risk Methods Integration and Evaluation Program (RMIEP)*, NUREG/CR-4835, U.S. Nuclear Regulatory Commission, Washington, DC, March 1988.

67. Comer, M. K., D. A. Seaver, W. G. Stillwell, and C. D. Gaddy, *Generating Human Reliability Estimates Using Expert Judgment*, NUREG/CR-3688, Vols. 1 & 2, U.S. Nuclear Regulatory Commission, Washington, DC, November 1984.

68. Dougherty, Jr., E. M. and J. R. Fragola, *Human Reliability Analysis: A Systems Engineering Approach with Nuclear Power Plant Applications*, New York, John Wiley and Sons, 1988.

69. Embrey, D. E., P. Humphreys, E. A. Rosa, B. Kirwan, and K. Rea, *SLIM-MAUD: An Approach to Assessing Human Error Probabilities Using Structured Expert Judgment*, NUREG/CR-3518, Vols. 1 & 2, U.S. Nuclear Regulatory Commission, Washington, DC, March 1984.

70. Fleming, K. N., P. H. Raabe, G. W. Hannaman, W. J. Houghton, R. D. Pfremmer, and F. S. Dombek, *HTGR Accident Initiation and Progression Analysis Status Report, Volume II, AIPA Risk Assessment Methodology*, GA/A13617, UG-77, General Atomic Co., San Diego, CA, October 1975.

71. Hannaman, G. W. and A. J. Spurgin, *Systematic Human Action Reliability Procedure (SHARP)*, EPRI NP-3583, Electric Power Research Institute, Palo Alto, CA, June 1984.

72. Hannaman, G. W., A. J. Spurgin, and Y. D. Lukic, *Human Cognitive Reliability Model for PRA Analysis*, Draft NUS-4531, NUS Corporation, San Diego, CA, December 1984 (Revision 3).

73. Hannaman, G. W., F. S. Dombek, B. O. Y. Lydell, P. Thurmond, and F. Kopstein, *Application of Selected HRA Methods in an International Benchmark Exercise: A Summary Report*, NUS-5099, San Diego, CA, March 1988.

74. Hollnagel, Erik, *Cognitive Reliability and Error Analysis Method: Cream*, Elsevier Science, January 1998.

75. Kopstein, F. F. and J. J. Wolf, *Maintenance Personnel Performance Simulation (MAPPS) Model: User's Manual*, NUREG/CR-3634, U.S. Nuclear Regulatory Commission, Washington, DC, September 1985.

76. Kozinsky, E. J., L. H. Gray, A. N. Beare, D. B. Barks, and F. E. Gomer, *Safety-Related Operator Actions: Methodology for Developing Criteria*, NUREG/CR-3515, U.S. Nuclear Regulatory Commission, Washington, DC, March 1984.

77. Meister, D., "A Critical Review of Human Performance Predictive Methods," *IEEE Transactions on Reliability*, Vol. R-22, No. 3, August 1973, pp 116-123.

78. Meister D., "Alternative Approaches to Human Reliability Analysis," V. T. Covello and R. A. Waller (eds.), *Low-Probability/High-Consequence Risk Analysis*, New York, Plenum Press, 1984.

79. Park, K. S., *Human Reliability–Analysis, Prediction, and Prevention of Human Errors*, New York, Elsevier Science Publishing Company, Inc., 1987.

80. Pew, R. W., C. E. Feehrer, and S. Baron, *Critical Review and Analysis of Performance Models Applicable to Man-Machine Systems Evaluation*, AFOSR-TR-77-0520, Air Force Office of Scientific Research, Bolling AFB, Washington, DC, March 1977.

81. Phillips, L. D., P. Humphreys, D. E. Embrey, and D. L. Selby, "A Socio-Technical Approach to Assessing Human Reliability (STAHR)," Appendix C, *Pressurized Thermal Shock Evaluation of the H. B. Robinson Unit 2 Nuclear Power Plant*, NUREG/CR-4183, U.S. Nuclear Regulatory Commission, Washington, DC, September 1985.

82. Phillips, L. D., P. Humphreys, D. E. Embrey, and D. L. Selby, "A Socio-Technical Approach to Assessing Human Reliability (STAHR)," Appendix D, *Pressurized Thermal Shock Evaluation of the Calvert Cliffs Unit 1 Nuclear Power Plant*, NUREG/CR-4022, U.S. Nuclear Regulatory Commission, Washington, DC, September 1985.

83. Potash, L. M., M. Stewart, P. E. Dietz, C. M. Lewis, and E. M. Dougherty, Jr., "Experience in Integrating the Operator Contributions in the PRA in Actual Operating Plants," *Proceedings of the International ANS/ENS Topical Meeting on Probabilistic Risk Assessment, Port Chester, NY September 1981*, American Nuclear Society, LaGrange Park, IL, 1982, pp 1054-1063.

84. Samanta, P. K., J. N. O'Brien, and H. W. Morrison, *Multiple-Sequential Failure Model: Evaluation of and Procedures for Human Error Dependency*, NUREG/CR-3837, U.S. Nuclear Regulatory Commission, Washington, DC, May 1985.

85. Seaver, D. A. and W. G. Stillwell, *Procedures for Using Expert Judgment to Estimate Human Error Probabilities in Nuclear Power Plant Operations*, NUREG/CR-2743, U.S. Nuclear Regulatory Commission, Washington, DC, March 1983.

86. Sharit, J., "A Critical Review of Approaches to Human Reliability Analysis," *International Journal of Industrial Ergonomics*, Vol. 2, Amsterdam, Elsevier Science Publishers, 1988, pp 111-130.

87. Siegel, A. I., J. J. Wolf, W. D. Bartter, E. G. Madden, F. F. Kopstein, and H. E. Knee, *Maintenance Personnel Performance Simulation (MAPPS) Model: Field Evaluation/Validation*, NUREG/CR-4104, U.S. Nuclear Regulatory Commission, Washington, DC, August 1985.

88. Stillwell, W. G., D. A. Seaver, and J. P. Schwartz, *Expert Estimation of Human Error Problems in Nuclear Power Plant Operations: A Review of Probability Assessment and Scaling*, NUREG/CR-2255, U.S. Nuclear Regulatory Commission, Washington, DC, May 1982.

89. Swain, A. D. and H. E. Guttmann, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*, NUREG/CR-1278, U.S. Nuclear Regulatory Commission, Washington, DC, August 1983, with *Addendum #1 to NUREG/CR-1278, August 1983*, September 1, 1985, by A. D. Swain.

90. Swain, A. D., *Accident Sequence Evaluation Program Human Reliability Analysis Procedure*, NUREG/CR-4772, U.S. Nuclear Regulatory Commission, Washington, DC, February 1987.

91. Swain, A. D., *Comparative Evaluation of Methods for Human Reliability Analysis*, GRS-71 (ISBN 3-923875-21-5) Gesellschaft für Reaktorsicherheit (GRS) mbH, Garching, Federal Republic of Germany, April 1989 (in English).

92. Wreathall, J., *Operator Action Trees, An Approach to Quantifying Operator Error Probability During Accident Sequences*, NUS-4159, NUS Corporation, Gaithersburg, MD, July 1982.

Data

93. German, D. I. and H. S. Blackman, *Human Reliability & Safety Analysis Data Handbook*, New York, John Wiley and Sons, October 1993.

94. Irwin, I. A., J. J. Levitz, and A. M. Freed, *Human Reliability in the Performance of Maintenance*, Report LRP 317/TDR-63-218, Aerojet-General Corp. Sacramento, CA, May 1964.

95. Meister, D., "Subjective Data in Human Reliability Estimates," *Proceedings: 1978 Annual Reliability and Maintainability Symposium*, Institute of Electrical and Electronics Engineers, New York, January 1978, pp 380-384.

96. Munger, S. J., R. W. Smith, and D. Payne, *An Index of Electronic Equipment Operability: Data Store*, AIR-C43-1/62-RP(1), American Institutes for Research, Pittsburgh, PA, January 1962.

97. Oswald, A. J., C. D. Gentillon, S. D. Matthews, and T. R. Meachum, "Generic Data Base for Data and Models" in *National Reliability Evaluation Programs (NREP) Guide*, EGG-EA-5887, Idaho National Engineering Laboratory, Idaho Falls, ID, June 1982.

98. Rigby, L. V., "The Sandia Human Error Rate Bank (SHERB)," R. E. Blanchard and D. H. Harris (eds.), *Man-Machine Effectiveness Analysis: A Symposium of the Human Factors Society, Los Angeles Chapter*, Los Angeles, CA, June 1967, pp 5-1 to 5-13.

99. Speaker, D. M., S. R. Thompson, and W. J. Luckas, Jr., *Identification and Analysis of Human Errors Underlying Pump and Valve Related Events Reported by Nuclear Power Plant Licensees*, Brookhaven National Laboratory, NUREG/CR-2417, U.S. Nuclear Regulatory Commission, Washington, DC, February 1982.

100. Swain, A. D., *System and Task Analysis, A Major Tool for Designing the Personnel Subsystem*, SCR-457, Sandia National Laboratories, Albuquerque, NM, January 1962.

101. Swain, A. D. and H. E. Guttmann, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*, NUREG/CR-1278, U.S. Nuclear Regulatory Commission, Washington, DC, August 1983, with *Addendum #1 to NUREG/CR-1278, August 1983*, September 1, 1985, by A. D. Swain.

102. Topmiller, D. A., J. S. Eckel, and E. J. Kozinsky, *Human Reliability Data Bank for Nuclear Power Plant Operations, Volume 1: A Review of Existing Human Reliability Data Banks*, General Physics Corporation and Sandia National Laboratories, NUREG/CR-2744, U.S. Nuclear Regulatory Commission, Washington, DC, December 1982.

Management/Organization

103. *Human Factors Engineering Program Review Model*, NUREG-0711, U.S. Nuclear Regulatory Commission, 1998.

104. *Management of Safety and Health During Organizational Change*, Chemical Manufacturers Association, 1998.

105. Reason, J., *Managing the Risks of Organizational Accidents*, 1998.

106. "Short Guide to Reducing Human Error in Process Operations," Warrington, UK: United Kingdom Atomic Energy Authority, AEA Technology Ltd., 1987.

107. Wagenaar, W. A., “Influencing Human Behavior: Toward a Practical Approach for E&P,” *Journal of Petroleum Technology*, November 1992.

APPENDIX 1

Self-evaluation Questionnaire for Managers Considering Ways to Improve Human Performance

Self-evaluation Questionnaire for Managers Considering Ways to Improve Human Performance

This appendix contains a list of questions that you can use to help review the status of human factors engineering as an element of process safety management in your organization and facilities. The list is not exhaustive, and all questions are not pertinent to all companies. Ideally, you should be able to answer "YES" to the initial part of all of the questions and then be able to locate documentation explaining or supporting your answer(s) to the follow-up question(s). Any "NO," "I DON'T KNOW," or "I CAN'T FIND IT" answers indicate human factors issues that you should consider investigating further, depending on the potential hazards involved.

Policy Issues

1. Is upper management's commitment to employee health and safety clear? What policy statements communicate this commitment to employees? Do workers understand these policies, and are they convinced of upper management's sincerity?

2. Do supervisors and workers believe that safety has higher (or at least equal) status with other business objectives in the organization? How does the company promote a "safety first" approach?

3. Have supervisors and workers been specifically told to err on the safe side whenever they perceive a conflict between safety and production? Will such decisions be supported throughout the management chain?

4. Is management of worker health and safety an essential part of a manager's daily activities? How are managers held accountable for their health and safety record, and how do the rewards and penalties compare to those for production performance?

5. Are health and safety regularly discussed in management meetings at all levels? Do such discussions involve more than a review of injury statistics? What actions are taken if an injury occurs? Are near misses discussed, and is any action taken to prevent recurrence?

6. Has upper management established human factors engineering policies? How are human factors engineering standards monitored to ensure implementation throughout the organization? Do these standards apply to vendors and subcontractors? How is noncompliance identified and resolved? Who has the authority to remedy human factors engineering deficiencies?

7. In the areas of research, design, construction, procurement, operations, maintenance, management, and so forth, are there clearly defined procedures for evaluating the human factors engineering aspects of:

   – New and modified processes?
   – New and modified equipment?

- New and modified procedures?
- Special, abnormal, and one-of-a-kind procedures?

8. Are human factors engineering resources available in the organization, and are they readily available to help resolve design and procedural issues? Did human factors specialists help establish the company's design standards for human factors engineering? Do they periodically review the adequacy of the standards in conjunction with other groups (engineering, operations, maintenance, etc.)?

9. Are adequate time and resources allocated to human factors engineering? How is human factors engineering integrated with the design process and the procedure-writing process? Is human factors engineering different for new designs/procedures and modified designs/procedures? If so, are the differences justified?

10. Do workers help identify error-likely situations in existing designs/procedures? Are they also involved in the review of new designs/procedures? How is worker input used? Are worker suggestions implemented?

11. Are workers encouraged to discuss potential human errors and near misses with their supervisors? Are such worker disclosures treated as evidence of worker incompetence, as unwarranted criticism of management, or as valuable lessons to be shared and acted upon? What criteria and procedures exist for reporting and investigating accidents and near misses? Are they followed consistently? Do the investigations go into enough depth to identify the root causes of worker errors? How are the human factors engineering deficiencies identified during the investigation of an incident corrected at (1) the site of the original incident, (2) similar sites at the same facility, and (3) similar sites at other facilities? How is the design process modified to prevent similar deficiencies in future designs?

12. Are supervisors trained and encouraged to identify error-likely situations, unsafe behaviors, and personal problems that may adversely affect a worker's performance? What actions are taken if a problem is identified?

13. Are data on human errors collected and made available to managers? Have the data been used as the basis for any management decisions? Are the data collected routinely, or are they only collected after an accident?

Job and Task Issues

14. Have critical jobs and tasks been identified? Have the mental and physical aspects of such jobs been analyzed for both routine and emergency activities? What has been done to reduce the likelihood and/or consequences of potential human errors in the performance of these jobs?

15. Have jobs and tasks been designed to maintain worker interest and involvement? Are assignments rotated to even out workloads and increase worker experience? How have activities with safety implications been emphasized?

16. Are tasks requiring intense activity, repetitive activity, or uneventful monitoring assigned to machines when possible? How are the problems associated with excessive or inadequate workloads handled? Is support from other personnel available when needed?

17. Are the worker's individual responsibilities clearly defined? How do these relate to team responsibilities? How is worker performance monitored and measured?

Human-machine Interface Issues

18. Has the human-machine interface ever undergone a human factors engineering review? Is the whole workplace arranged so the workers can maintain a good working posture and perform a variety of movements?

19. Is adequate information about normal and upset process conditions displayed in the control room? Is the information displayed in ways the workers understand? Do separate displays present information in a consistent manner? What kinds of calculations must workers perform, and how are they checked? Does the computer software check for out-of-range inputs?

20. Are workers provided with enough information to diagnose an upset when an alarm sounds? Are the displays adequately visible from all relevant working positions? Do the displays provide adequate feedback on worker actions?

21. Do control panel layouts reflect the functional aspects of the process or equipment? Are related displays and controls grouped together? Does the control arrangement logically follow the normal sequence of operation? Can the worker override the computer if it, or one of its inputs, fails? What are the consequences of worker intervention in computer-controlled processes?

22. Are all controls accessible and easy to distinguish? Are the controls easy to use correctly and difficult to use incorrectly? Do any controls violate strong populational stereotypes (color, direction of movement, etc.)? Are any process variables difficult to control with the existing equipment? How many manual adjustments must a worker perform during normal and emergency operations?

23. Is there a formal mechanism for correcting human engineering deficiencies identified by the worker? Have workers made any modifications to the displays, controls, or equipment to better suit their needs? How are designers made aware of the problems so they can improve future designs?

24. Are automatic safety features provided when either a rapid response or complex information processing is required to cope with a process upset?

25. Are instruments, displays, and controls promptly repaired after a malfunction? Are any instruments, displays, or controls deliberately disabled during any phase of operation? How are alarm setpoints and computer software protected from unauthorized changes?

26. Is the work environment (temperature, noise, lighting, general cleanliness, etc.) maintained within comfortable bounds?

27. Are the right tools available and used when needed? Are special tools required to perform any tasks safely or efficiently? What steps are taken to identify and provide special tools?

28. Is there adequate access for routine operation and maintenance of all equipment?

29. If protective clothing and equipment are required for the performance of some tasks, have the worker performance limitations imposed by the protective gear been evaluated for both routine and emergency tasks? Are adequate supplies of the protective gear readily available for routine and emergency use?

30. Is all-important equipment (vessels, pipes, valves, instruments, controls, etc.) clearly and unambiguously labeled? Does your labeling program include components (e.g., small valves) that are mentioned in the procedures even if they are not assigned an equipment number? Are the labels accurate? Who is responsible for maintaining and updating the labels?

31. Were the needs for communication and teamwork considered in the workplace design? How do different shifts communicate the process status (batch conditions, process abnormalities, equipment out of service, active work permits, etc.) to each other? What is the procedure for communication between departments? Is it followed?

32. Are there clear procedures during emergencies for communications between workers and emergency response personnel, plant management, corporate management, and public authorities? Are they regularly practiced?

33. Are workers encouraged to ask supervisors for assistance? Do workers know when to seek assistance? Are workers penalized for "unnecessary" shutdowns when they truly believe there is an emergency?

34. Is there adequate supervision of the workers? How do supervisors interact with the workers? What is the supervisor's role in detecting and correcting human errors?

35. Are shift rotation schedules set to minimize the disruption of workers' circadian rhythms? How are problems with worker fatigue resolved? Is there a plan for rotating workers during extended emergencies?

Procedural Issues

36. Is a complete, current set of procedures available for workers to use? How are specific, up-to-date procedures maintained? Do the workers themselves help review/revise the procedures? How often? Are known errors allowed to remain uncorrected?

37. Are procedures written for the right level of knowledge and understanding by the workers, considering their education, background, experience, native language, etc.? Is a step-by-step format used? Are diagrams, photographs, drawings, etc., used to clarify the written text? Are cautions and warnings clearly stated in prominent locations? Does procedure nomenclature match equipment labels? Are there too many abbreviations and references to other procedures?

38. Do worker practices always comply with written procedures? How are differences detected and resolved? Who can authorize changes and deviations from the written procedures? Does such authorization include a review of the safety implications of the change or deviation? Do cautions always precede action steps in the procedures?

39. Are work permit systems correctly used? How are contractors included in such systems?

40. Are the emergency procedures clearly written? Are they practiced regularly? How many "immediate" actions are required? Are the procedures designed so workers can crosscheck each other's performance of the necessary tasks?

41. Are checklists used for critical procedures? Is only one action specified per numbered step? Are any instructions embedded in explanatory notes? Are the steps in the correct sequence? Do steps requiring control actions also specify the correct system response?

Worker Issues

42. Did a human factors specialist help develop worker hiring and assignment policies? How are the results of job and task analyses converted into appropriate criteria for worker selection based on physical abilities, aptitudes, experience, etc.?

43. Is there a written training policy applicable to all workers, including contractors? What safety objectives are established and how is attainment of such objectives monitored?

44. Are training records kept? How are retraining needs identified? How are workers trained on new processes, equipment, and procedures? What training is given to workers changing jobs or taking on additional responsibilities? What training is given to new workers? How is training effectiveness assessed? Are only trained and qualified workers assigned to tasks? How do supervisors know which workers have appropriate qualifications for an assignment?

45. Are pre-employment and periodic health assessments performed for workers who must meet and maintain defined medical standards? Is a worker's health evaluated before he/she is allowed to return to work after an illness?

46. Are there programs for identifying and helping workers with substance abuse or mental health problems? What counseling, support, and professional advice are available to workers during periods of ill health or stress? What is the company policy on reassigning or terminating workers who are unable/unfit to perform their jobs?

Now that you have asked yourself these questions, go out into your facilities and ask the workers. Their knowledge, opinions, and attitudes will help you develop an effective strategy for improving human performance within your company.

APPENDIX 2

Self-evaluation Survey

Self-evaluation Survey

Dear [survey respondent][*]:

Introduction

OSHA 1910.119, *The Process Safety Management of Highly Hazardous Chemicals*, requires that human factors be "addressed" as part of the overall process hazards analyses [(e)(3)(vi)]. To help address this requirement, companies are using a wide variety of tools and techniques that help identify and evaluate human factors concerns.

The [CEO] would like to better understand the techniques and practices that we are currently using to improve human performance systems. A survey form has been prepared for this purpose. The intent is to circulate a survey that will be useful to participating facilities as a self-assessment tool, and provide information for evaluation of our entire organization.

Definitions

"Human factors" is a broadly used term for describing the technology devoted to reducing the potential for human error. For the purposes of this survey, the following definitions will be used:

- Human error. Any human action (or lack thereof) that exceeds some limit of acceptability (i.e., an out-of-tolerance action) where limits of human performance are defined by the system. [Definition per the American Chemistry Council and API document *A Manager's Guide to Reducing Human Errors, Second Edition*]

- Human factors. A discipline concerned with designing machines, operations, and work environments so that they match human capabilities, limitations, and needs. Among human factors specialists, this general term includes any technical work (engineering, procedure writing, worker training, worker selection, etc.) related to the human factor in operator-machine systems. [Definition per the American Chemistry Council and API document *A Manager's Guide to Reducing Human Errors, Second Edition*]

- Human performance systems. The job-related components of work environment, man-machine interface, work processes, management, organizational and cultural influences, and human variability, interacting together in such a way as to affect an increase or decrease in the likelihood of human error.

[*] Note: Items that need to be modified to make the survey company-specific are enclosed by square brackets ([ ]).

Why Should Your [site] Support This Project?

The need for improved human performance tools is generally recognized. Thorough investigation of most process plant incidents identifies human error among the root causes. In many accidents, human error may be the primary contributor to the event. Most process safety experts view improving human performance systems as a key to further reducing the potential for major accidents.

Organizations have found that they can sharply reduce such accidents by applying methods directed at improving human performance systems. Some of the benefits include:

- Finding and reducing situations in the workplace (e.g., repetitive stress, confusing signals, awkward positioning, hard-to-operate equipment) that contribute to accidents and injuries

- Identifying and changing confusing or conflicting work processes (e.g. permit-to-work systems, safe work practices) that can lead directly to serious accidents if there is human error

- Identifying and changing *behaviors* that can lead to accidents and injuries – both at the hourly and managerial levels

Some "first quartile" petrochemical companies in Canada believe that their success is due, in large part, to an ambitious human performance improvement process. Typically, the human performance process they employ goes beyond traditional reward/punishment and human/machine interface engineering principles. Root cause analysis is aimed at addressing improvements in both technical and *social* systems.

Several projects have emerged reflecting a growing interest on the part of both industry and government in improving human performance systems. For example, in addition to the American Chemistry Council and API document *A Manager's Guide to Reducing Human Errors, Second Edition,* the American Institute of Chemical Engineers' Center for Chemical Process Safety has published *Guidelines for Preventing Human Error in Process Safety*, a comprehensive top-level treatment of the subject. The U.S. Minerals Management Service (MMS) has also completed a project titled *Human Factors in Offshore Operations*. One of the MMS project objectives was to develop simple, practical tools that could be used by plant/platform personnel to analyze job tasks.

Most recently, at least one local government agency (in concert with representatives of local industry and the International Oil, Chemical and Atomic Workers Union) has drafted a proposed ordinance that details the inclusion of human factors in process safety management efforts. This proposed ordinance includes requirements for covered facilities to:

- Develop a written human factors program, with employee participation, that includes but is not limited to staffing, shift work, and overtime
- Include human factors in process hazards analyses (per OSHA 1910.119)
- Consider human systems as factors in the incident investigation process

- Train employees in the human factors program
- Address human factors in operating procedures
- Conduct management of change, with employee participation, for changes in permanent staffing levels/organization, operations, and emergency response
- Provide a written description of the human factors plan

Given the wide-ranging activities taking place in the field of human performance, it is an appropriate time for us to capitalize on previous work, while at the same time expanding the science and helping us address this important issue efficiently, effectively, and consistently.

Survey Content

The attached survey identifies three general areas of human activity where information would be useful to operating facility management, as well as to the overall organization. Specifically:

1. Individual activities. These include human performance concerns associated with the human-machine interface, job tasks, work environment, and other issues related to the individual and the direct performance of work.

2. Work processes. These include human performance concerns associated with key process safety activities such as conducting incident investigations, performing hazards analyses, writing/updating operating procedures, training, and safe work practices.

3. Management, organizational, and cultural influences. These include management, organizational, and cultural factors that may have an adverse or beneficial effect on process safety such as might be reflected in policy, attitudes, paradigms, communications, interfaces and responsibilities, and the way things really get done.

The survey is intended to be a useful assessment tool for the facility and is designed so that multiple levels within the organization can complete it. We believe that a multilevel response will provide a more accurate and thorough assessment, increasing the utility of the survey for both the site/division and the organization. The four suggested response levels (categories) include (1) manager, (2) first line supervisor, (3) wage/hourly, and (4) technical/professional. By requesting both hourly and management personnel to answer the same questions, we are better able to identify perceptions at each level and prepare a balanced composite finding. For this reason, we suggest the survey be distributed across the organizational spectrum.

The number of persons to be involved in the survey is at the location's discretion. For large facilities, a minimum of 10percent to 15percent sampling size is recommended, across all four job categories. Smaller facilities should consider larger samples, up to 100percent participation. We request all individual questionnaires be returned to [sponsor], grouped in the four job categories. We will analyze the data and return the results to the locations, depending upon the group's desire. While awaiting the corporate

analysis, some locations may choose to evaluate their own data in order to obtain immediate feedback of the survey information.

The completed survey aggregate results will be used to identify state-of-the-art activities being used by our organization, as well as major concerns or problem areas**.** Moreover, by understanding what is currently being done, we can help ensure that any future management system changes are compatible with our existing programs.

The results of the survey will be summarized and forwarded to participating locations.

Survey Logistics

When completing the survey, please note the following:

- Division, Location, and Contact Identification. The results of the survey will be returned to the contact person identified.

- Survey Structure. The survey is comprised of the following two sections:

    1. *Section 1*, which consists of a three-page, multiple-choice questionnaire to be filled out by all four groups within the facility as indicated.
    2. *Section 2*, which consists of a series of general questions. These are to be filled out by the survey lead (the person at the facility who is coordinating the survey) after reviewing the completed multiple-choice questionnaires.

- Due Date. Please complete and return the survey by [Date].

- Questions about the survey administration should be directed to [sponsor] at [xxx-xxx-xxxx]. An electronic copy of this survey is available at: [**www/XXXXXXXXX].**

- Return Survey. Please send completed surveys to:

    [sponsor]

Follow-on Visits

The task force would like to conduct follow-on visits with selected groups that have sophisticated or otherwise illustrative human performance systems efforts in place. The purpose of the follow-on visit would be to provide more detailed information to the task force than can be obtained from the survey. If your location is amenable to a 1-day visit or teleconference, please indicate this on the survey.

Survey on Human Performance

Division:

Location:

Number of Employees:

Contact Name:

Section 1
Three-page Questionnaire

(Job Function) ____ ***Manager*** ____ ***Supervisor*** ____ ***Wage/Hourly*** ____ ***Technical/Professional***

Individual Activities and Human Performance

Please indicate if you agree or disagree with the following statements.

Questions 1-12 deal with the impact of individual activities on human performance.	**Strongly Agree**	**Agree**	**Strongly Disagree**	**Disagree**	**Do Not Know**
1. Critical operating steps that have a high potential for injury or process upset have been analyzed to identify ways to reduce error. Examples include job safety analyses (JSA) and human error analyses.					
2. Work group reassignments are reviewed to provide a balance of operator experience and knowledge and to promote safety and reliability.					
3. Design standards are employed for new projects to help field operators perform jobs safely. These standards incorporate requirements for equipment layout, spacing, and access to critical valves and controls.					
4. Control rooms are designed with human factors considered. This includes panel layout, lighting, and access to emergency controls.					
5. Panel alarms have been evaluated and implemented to reduce the potential of operator confusion and overload during upset conditions. (Hierarchy of alarms)					
6. Uncomfortable work environments (dirt, noise, heat, cold, etc.) have been evaluated and changes made to reduce the potential for unsafe conditions leading to error.					
7. Operator actions during startup, shutdown, and unusual or emergency upset conditions have been reviewed and implemented to identify the potential for errors.					
8. Requirements for additional staffing during unusual operations have been evaluated and addressed.					
9. Checklists are used for high-risk procedures and abnormal operations.					
10. Human factors resources (e.g., job task analysis and root cause analysis, etc.) are available in the company and are utilized.					
11. Programs are in place to deal with people bringing external stress to the workplace.					
12. Communication between shifts and between operations and maintenance is well executed.					

Work Processes and Human Performance

Questions 13-20 deal with the impact of work processes on human performance.	Strongly Agree	Agree	Strongly Disagree	Disagree	Do Not Know
13. Compliance auditing is performed on high-risk activity checklists (such as lockout/tagout and furnace light-off).					
14. All human error-related incidents are encouraged to be reported even when there are no serious consequences.					
15. Human performance is considered during process safety-related incident investigations.					
16. Procedures are in place for evaluating staffing changes (hourly, supervisor, technical/professional, managerial) to help ensure appropriate staffing levels and experience.					
17. Training programs are established, and learning environments are created where employees are willing to ask questions.					
18. Recommendations from hazard analyses (e.g., HAZOP) studies that address improvements in human performance are taken seriously and implemented or resolved.					
19. Additional training and time to adapt are given when hourly personnel are transferred from one operating unit to another or when computerization/downsizing occurs.					
20. People who actually perform the jobs are involved in procedure writing.					

Organizational Activities and Human Performance

Questions 21-29 deal with the impact of organizational activities on human performance.	**Strongly Agree**	**Agree**	**Strongly Disagree**	**Disagree**	**Do Not Know**
21. Written requirements addressing the need to include human performance in management of change (MOC) have been established.					
22. Human factors standards have been established that apply to all company and contractor facilities and activities.					
23. All practices and procedures reinforce the concept that anyone has the right, and responsibility, to stop production without repercussion in the event of an emergency or safety hazard.					
24. Employees are encouraged to report near misses (process and personnel safety) without fear of reprisal.					
25. Discipline is administered equally at all levels (management, professional, and hourly) when incidents involving human performance occur.					
26. Employees are involved and their recommendations considered in efforts to reduce human error.					
27. Incident investigations emphasize finding root or basic causes rather than placing blame.					
28. Compliance with high risk activity checklists (such as lockout/tagout and furnace light-off) is "expected" by management even at the expense of production.					
29. Employees are encouraged to question the acceptance of additional process risks and are treated constructively when they do so.					

Any comments on the above:

_____

_____

_____

General comments. (Please describe any specific human factors concerns. Use the back of the page, if necessary.)

_____

_____

_____

Section 2 – General Questions
(To be completed by survey leader after reviewing the results of the survey)

1. What tools does your site/facility use for identifying human factors/error issues?

2. Describe your site's overall human performance improvement efforts.

3. When it comes to reducing human error, what should your site do?

4. How are violations of safety-critical procedures, such as furnace light-offs, permit-to-work systems, or lockout/tagout, handled?

5. Is your site concerned with information overload for panel operators during times when the process is upset? If no, should it be? If yes, what is being done?

6. Has there been consideration for developing clear and unambiguous equipment displays, control panels, and layouts? If no, should there be? If yes, is it working adequately?

7. Are process-related incidents thoroughly investigated for root causes when human error is initially found or suspected to be a major contributing factor to the incident?

APPENDIX 3

Example HRA Problem Using the THERP Technique

EXAMPLE HRA PROBLEM USING THE THERP TECHNIQUE

This appendix illustrates how an HRA of a simple, practical problem might be performed. The THERP technique, as described in the *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications (Handbook)*,[7] was used to solve this problem. Readers who want to fully understand the THERP technique and the logic behind the data selected for this example must read the *Handbook*.

Assume that the system described below exists in a process unit recently purchased by your company. As the manager, the safety of this unit is now your responsibility. You are concerned because your process hazard analysis team identified the potential for an operator error to result in a rupture of the propane condenser. You have chartered an HRA to estimate the likelihood of the condenser rupturing as the result of such an error and to identify ways to reduce the expected frequency of such ruptures.

SYSTEM DESCRIPTION

Four parallel propane condensers, one of which is illustrated in Figure 14, are designed with a 450-psig shell pressure rating and a 125-psig tube pressure rating. The propane vapor pressure is controlled at 400 psig; the cooling water flowing through the condenser tubes is normally maintained at 75 psig. Liquid propane flows out of the condenser as soon as it condenses; there is no significant inventory of liquid propane in the condenser. The two propane isolation valves for each condenser are rising-stem gate valves with no labels. The two water isolation valves for each condenser are butterfly valves with no labels. Their handwheel actuators have position indicators.

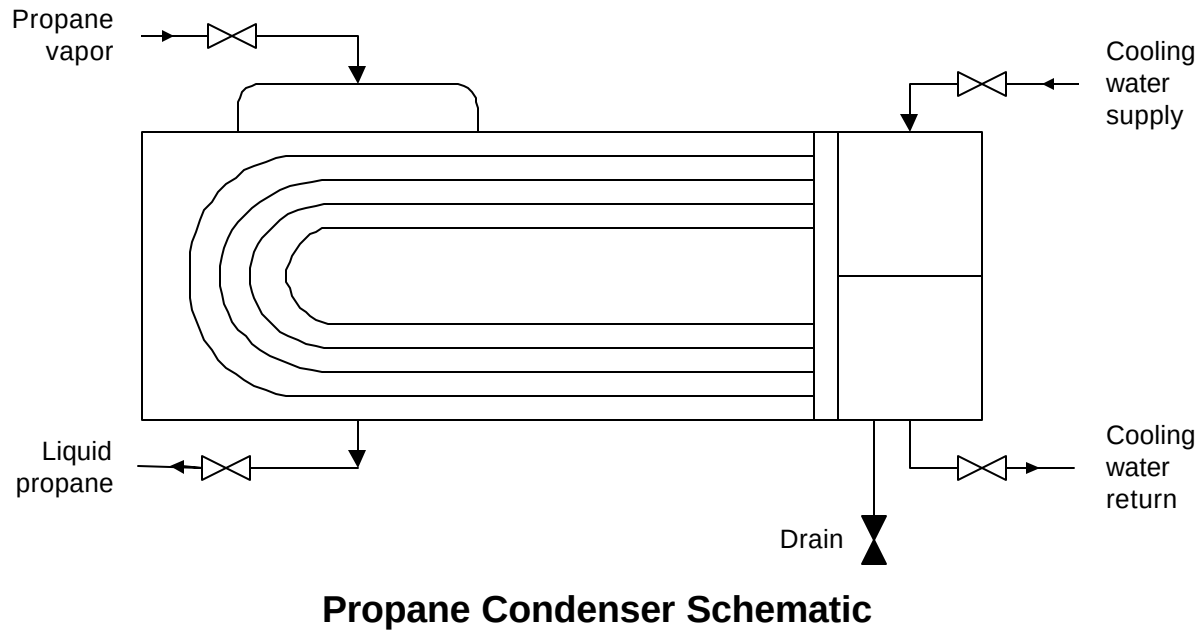


Figure 14 Propane Condenser Schematic

A tube has failed in one of the four condensers about once every 3 years. If a condenser tube fails, the affected condenser can be removed from service by closing four isolation valves (propane vapor inlet valve, liquid propane outlet valve, cooling water supply valve, and cooling water return valve). However, if a tube fails, it is essential that the operator close the two propane isolation valves before closing the two water isolation valves. Closing the two water valves first would allow pressure to build on the tube side of the condenser and rupture the tube head.

ANALYZED SYSTEM CONDITIONS

- A tube has failed in the condenser.
- The low depropanizer pressure alarm has sounded in the control room.
- The experienced field operator has observed water and gas spewing from the hydrocarbon vent at the cooling tower. The field operator shouts over the radio that a propane vapor cloud appears to be forming and moving toward the control room.
- The control room operator has directed the field operator to isolate the failed condenser as quickly as possible so that a unit shutdown will not be necessary.
- The operator must close the valves by hand. If a valve sticks, there is no time to go get tools to help close the valve – the process must be shut down.
- The field operator has correctly identified the condenser with the failed tube by the sound of the expanding propane and the visible condensation/frost on the shell.

QUALITATIVE HRA RESULTS

The first step of the analysis is to identify the human actions and equipment failures that can lead to the failure of interest. An HRA event tree (Figure 15) is then constructed to depict the potential human errors (represented by capital English letters) and the potential equipment failures (represented by capital Greek letters.) The series of events that will lead to the failure of interest is identified by a F_i at the end of the last branch of the event tree. All other outcomes are considered successes even though the propane release is not isolated in outcomes S_2 and S_3, so the process must be shut down.

Inspection of the HRA event tree reveals that the dominant human error is Error A: the operator failing to isolate the propane valves first. The other potential human errors are factors only if a propane isolation valve sticks open. Based on these qualitative results alone, a manager might decide to periodically train operators on the proper procedure for isolating a failed condenser and to ensure that operators are aware of the potential hazards. The manager might also decide to require regular preventive maintenance on the propane isolation valves to help ensure that they will properly close when required.

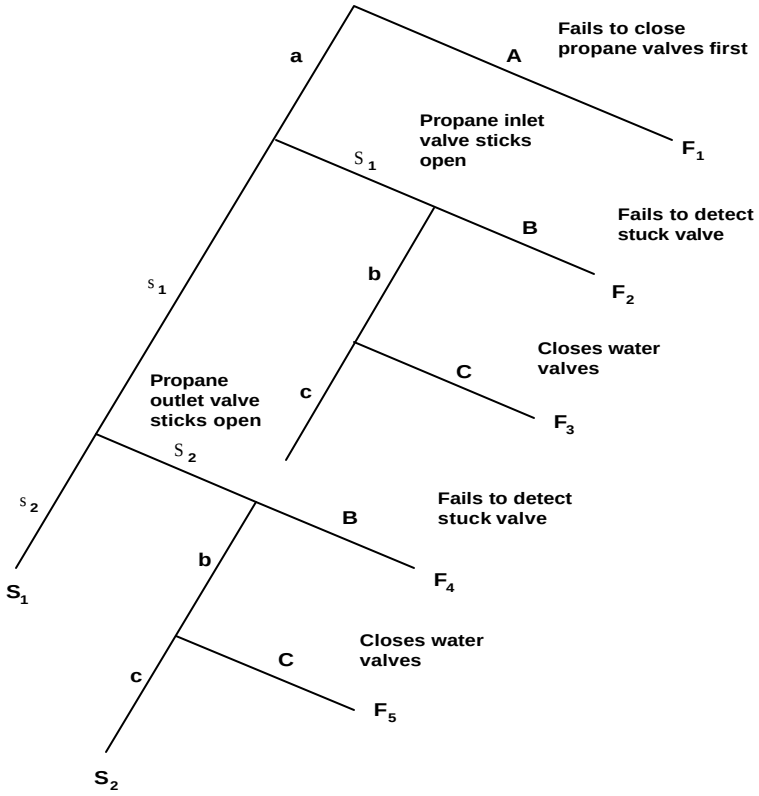


Figure 15 HRA Event Tree for Improper Condenser Isolation

QUANTITATIVE HRA RESULTS

This manager requested quantitative results, so the analyst must estimate the probability of each failure or error included in the event tree. Data for all the failures and errors in this particular problem are available in tables in the *Handbook*. The analyst must modify these data as necessary to account for specific characteristics of the work situation, such as stress levels, equipment design features, and inter-operator dependencies. Table 10 summarizes the data used in this problem.

There is a written procedure for condenser isolation, but it is normally a simple step-by-step task that is second nature to the operator and is performed from memory. However, under the threat of a potential vapor cloud explosion, the operator may forget to close the propane valves first (Error A). The HEP in *Handbook* Table 20-7 #5 footnote (.01) is increased by a factor of 5 per *Handbook* Table 20-16 #6a to account for stress.

Table 10 Events Included in the HRA Event Tree

Failure Symbol	Failure Description	Estimated Probability	Data Source
A	Operator fails to close the propane valves first	0.05	T20-7 #5 footnote × 5, per T20-16 #6a
Σ_1	Propane inlet valve sticks open	0.001	T20-14 footnote
Σ_2	Propane outlet valve sticks open	0.001	T20-14 footnote
B	Operator fails to detect a stuck valve	0.025	T20-14 #3 × 5, per T20-16 #6a
C	Operator chooses to close the cooling water valves to stop the propane release	0.25	T20-16 #7a

The probability of a valve sticking open is unaffected by the operator's stress level (despite Murphy's law), but the probability of the operator failing to detect the stuck valve (Error B) is increased. The HEP in *Handbook* Table 20-14 #3 is increased by a factor of 5 per *Handbook* Table 20-16 #6a.

The third potential human error (Error C) is that the operator will decide to close the cooling water valves even though he/she diagnoses that the propane valve is not closed. The likelihood of such an error (a dynamic decision in a threatening situation) is listed as 0.25 in *Handbook* Table 20-16 #7a.

The analyst can then calculate the total probability of failure (F_T) by summing the probability of all failure paths (F_{1-5}). The probability of a specific path is calculated by multiplying the probabilities of each success and failure limb in that path. (Note: The probabilities of success and failure sum to 1.0 for each branch point. For example, the probability of Error B is 0.025, and the probability of Success b is 0.975.) Table 11 summarizes the calculations of the HRA results, which are normally rounded to one significant digit after the intermediate calculations are completed.

Table 11 HRA Results

$F1 = A$	$= 5.0 \times 10^{-2}$
$F2 = a\Sigma_1 B$	$= 2.4 \times 10^{-5}$
$F3 = a\Sigma_1 bC$	$= 2.3 \times 10^{-4}$
$F4 = a\sigma_1\Sigma_2 B$	$= 2.4 \times 10^{-5}$
$F5 = a\sigma_1\Sigma_2 bC$	$= 2.3 \times 10^{-4}$
$FT = F1 + \ldots + F5$	≈ 0.05

Finally, the HRA analyst would calculate the expected frequency of condenser ruptures as a result of improper isolation. The frequency of condenser tube failures is 0.33 per year (one every 3 years), and the calculated probability of improper isolation is 0.05. Multiplying these two numbers shows the expected frequency of improper isolation of a failed condenser is 0.017/y, or about once every 60 years. The manager can use this number to help compare the costs and benefits of improvements proposed as a result of the HRA or other studies.

For example, the same process hazards review team that spurred the manager's original concern might have suggested (1) installing a pressure relief device on the tube side of the exchanger or (2) removing the propane isolation valves (which would require that the unit be shut down in the event of a condenser tube failure). In addition, the HRA team may have suggested (3) increasing operator training and (4) more frequent maintenance of the propane isolation valves. Based on the quantitative HRA results and estimates of the consequences of a condenser rupture, the manager can decide whether the benefits of the proposed changes outweigh their costs. The manager can then choose the best way to apply available loss prevention resources.

Additional copies are available through Global Engineering Documents at (800) 854-7179 or (303) 397-7956

Information about API Publications, Programs and Services is available on the World Wide Web at: http://www.api.org

American Petroleum Institute
1220 L Street, Northwest
Washington, D.C. 20005-4070
202-682-8000

Product No. K77001