13

COMMENTS ON HAZARDS AND RISKS

INTRODUCTION

All risks to which the practice of safety applies derive from hazards. There are no exceptions. Furthermore, the entirety of purpose of those accountable for safety, in fulfilling their societal responsibilities, is to manage their endeavors with respect to hazards so that the risks deriving from those hazards are at an acceptable level.

Thus, safety professionals must have an understanding of hazards and risks and their relationship to fulfill their responsibilities and to be successful in communicating with those to whom counsel is given.

Hazards and *risks* are not synonymous terms, though some authors use them interchangeably. Also, hazards and risks may be equated in the literature with exposures and perils. Unfortunately, the literature on hazards and risks and exposures and perils can be baffling. We safety professionals, to be effective communicators, seriously need to establish what we mean when we use the terms *hazards* and *risks*. As John V. Grimaldi and Rollin H. Simonds wrote in *Safety Management*:

> Unless there is common understanding about the meaning of terms, it is clear that there cannot be a universal effort to fulfill the objective they define [p. 10].

On the Practice of Safety, Third Edition, By Fred A. Manuele
ISBN 0-471-27275-2

DEFINING HAZARDS: RELATING HAZARDS TO RISKS

Appendix C in *Improving Risk Communication* is titled "Risk: A Guide to Controversy." In that appendix, Baruch Fischhoff wrote:

> By definition, all risk controversies concern the risks associated with some hazard . . . the term "hazard" is used to describe any activity or technology that produces risk [p. 217].

Fischhoff properly relates hazards to risks. A hazard is defined as the potential source of harm. Hazards include the characteristics of things, the technology, and the actions or inactions of persons that have the potential to harm or damage people, property, or the environment.

Hazards must be considered in the broad context of that definition. Every element within the safety management process should serve to avoid, eliminate, or control the aspects of personal activity or inactivity and the aspects of technology that present a potential for harm or damage and produce risk.

SIGNIFICANCE OF HAZARDS WITHIN THE SAFETY PROCESS

Whether the concern of a safety professional is occupational safety, occupational health, product safety, environmental affairs, fire protection, transportation safety, or any other safety-related practice, the generic base for that endeavor is hazards. In every one of those fields of endeavor, all activities should be similarly directed to encompass both the possible actions or inactions of people and the characteristics of properties, equipment, machinery, or materials that present the potential for harm or damage.

Furthermore, whatever the particular safety process — management involvement, safety in the design stages, employee training, hazards communication, incident investigation, use of personal protective equipment, behavior modification, and so on — its fundamental purpose is to avoid, eliminate, or control hazards.

HAZARD IDENTIFICATION

In the definition of hazards given, *potential* is the key word. If a hazard is the potential source of harm, and if a hazard is not avoided, eliminated, or controlled, the potential may be realized.

Two considerations are necessary in determining whether a hazard exists. Do the characteristics of the thing or the actions or inactions of people present the potential for harm or damage? And, can people, property, or the environment be harmed or damaged if the potential is realized?

Many methods are available to identify hazards — from historical data, from codes and standards, from the observations of learned people, and from the use of one of several analytical methods such as the more simple What-If system through to the more complex Fault Tree Analysis. And the literature, of which there is a great deal, speaks extensively of those methods.

DEFINING EXPOSURE

To complete a hazard analysis after a hazard has been identified and evaluated, the exposure must be assessed. An exposure assessment would be a determination of the number of people, the extent of the property, and aspects of the environment in a particular setting that could be affected by the realization of the hazard, as well as the extent of harm or damage that could result. Exposure is not the hazard, nor is it the risk.

DEFINING PERILS

In the insurance-related literature, *peril* is a frequently found term. It may be used synonymously with hazard or risk or exposure. Perils insured against are commonly considered to be fires, explosions, falling aircraft, windstorms, floods, automobile accidents, embezzlements, et cetera. Perils are incidents that occur when hazards are realized. Perils are events; they are not hazards or risks or exposures.

ACQUIRING ADDITIONAL KNOWLEDGE OF HAZARDS

There are two significant thought processes, one built on the other, of which knowledge is a requirement in professional safety practice. They are Haddon's unwanted energy release concept, extended by him to include exposures to hazardous environments, and the concepts on which MORT (management oversight and risk tree) was developed.

I encourage safety professionals to give particular attention to Haddon's concepts and to MORT. Both establish that if there are no unwanted energy releases or exposures to hazardous environments, no hazards-related incidents will occur.

ALL WORK REQUIRES THE EXPENDITURE OF ENERGY

In *The Loss Rate Concept in Safety Engineering*, R. L. Browning wrote:

> Work requires the expenditure of energy, in fact, energy is measured by the work it is capable of performing. It follows that the capability to cause — the key element in the search for valid loss exposures — will be an inventory of potentially destructive energy [p. 17].

Browning's statements are thought-provoking. Certainly, being causal factors oriented is a fundamental in the practice of safety. And, it seems that "potentially destructive energy," the release of which occurs in hazards-related incidents, is directly related to the definition of hazards previously given.

Obviously, the purpose of people in an occupational setting is to work. All work requires the expenditure of energy. If the energy expended is undesired or excessive in relation to human capabilities, that energy expenditure can be an incident causal factor. Safety professionals cannot do a proper job of giving advice on preventing or mitigating harm or damage without extensive knowledge of causal factors that include unwanted releases of "potentially destructive energy." This applies to all types of incidents: material handling incidents, slips and falls, contact with objects or equipment, and so on.

HADDON'S UNWANTED ENERGY RELEASE AND HAZARDOUS ENVIRONMENT CONCEPT

Dr. William Haddon, who was the first Director of the National Highway Safety Bureau, conceived the energy release theory. Its concept is that unwanted transfers of energy can be harmful (and wasteful) and that a systematic approach to limiting their possibility should be taken.

Although Haddon stated in his paper "On the Escape of Tigers: An Ecologic Note" that "the concern here is the reduction of damage produced by energy transfer," he also said that "the type of categorization here is similar to those useful for dealing systematically with other environmental problems and their ecology." Excerpts follow from "On the Escape of Tigers: An Ecologic Note."

> A major class of ecologic phenomena involves the transfer of energy in such ways and amounts, and at such rapid rates, that inanimate or animate structures are damaged.
>
> Several strategies, in one mix or another, are available for reducing the human and economic losses that make this class of phenomena of social concern. In their logical sequence, they are as follows:
>
> - Prevent the marshalling of the form of energy;
> - Reduce the amount of energy marshalled;
> - Prevent the release of the energy;

- Modify the rate or spatial distribution of release of the energy from its source;
- Separate, in space or time, the energy being released from that which is susceptible to harm or damage;
- Separate, by interposing a material barrier, the energy released from that which is susceptible to harm or damage;
- Modify appropriately the contact surface, subsurface, or basic structure, as in eliminating, rounding, and softening corners, edges, and points with which people can, and therefore sooner or later do, come in contact;
- Strengthen the structure, living or non-living, that might otherwise be damaged by the energy transfer;
- Move rapidly in detection and evaluation of damage that has occurred or is occurring, and counter its continuation or extension; and
- After the emergency period following the damaging energy exchange, stabilize the process.

All hazards are not addressed by the unwanted energy release concept. Examples are the potential for asphyxiation from entering a confined space filled with inert gas, or inhalation of asbestos fibers. But all hazards are encompassed within a goal that is to avoid *both* unwanted energy releases *and* exposures to hazardous environments. Many authors have recognized the importance of Haddon's writings.

John V. Grimaldi and Rollin H. Simonds in *Safety Management* recognized Haddon's work (p. 284). Dr. Roger L. Brauer, in *Safety and Health for Engineers* (p. 20), commented on the energy release theory and listed the 10 strategies for preventing or minimizing adverse results as outlined by Dr. Haddon. In *MORT Safety Assurance Systems*, William G. Johnson also listed Dr. Haddon's 10 energy management strategies and made these comments concerning them.

> Haddon systemized a set of 10 energy management strategies in a progressive order, which can be used in various combinations. Haddon points out that the larger the energy, the earlier in the strategy list should control be sought. This author would add, the larger the energy, the greater the need for redundant, successive strategies and barriers. The systematic review of available strategies and the creation of optimum mixes to reduce harm have not been customary in safety. The application of Haddon's concepts was tested in early trials of MORT [p. 28].

As a result of the testing and early trials, Haddon's strategy was introduced into the MORT system with an extended hierarchy of preventive measures, of which there are 12 (p. 29).

Ted Ferry in *Safety and Health Management Planning* wrote about energy transfers and barriers and listed "13 strategies for systematic energy control" as cited by the Department of Energy (p. 244).

Unwanted releases of energy or exposures to hazardous environments contribute as causal factors for all hazards-related incidents. Haddon's 10 energy management strategies are greatly expanded in this book in Chapter 17, "Guidelines: Designing for Safety," under the caption "General Design Requirements: A Generic Thought Process for Hazard Avoidance, Elimination, or Control."

ON THE SIGNIFICANCE OF MORT

I also recommend that safety professionals develop an understanding of the concepts on which the management oversight and risk tree (MORT) is based and the thought process it promotes. In the excerpts that follow, taken from the *Guide to Use of the Management Oversight and Risk Tree*," the relationship of MORT to Haddon's original work will be evident.

> This document is the User's Guide for MORT (Management Oversight and Risk Tree), a logic diagram in the form of a "work sheet" that illustrates a long series of interrelated questions. MORT is a comprehensive analytical procedure that provides a disciplined method for determining the systemic causes and contributing factors of accidents. Alternatively, it serves as a tool to evaluate the quality of an existing system. While similar in many respects to fault tree analysis, MORT is more generalized and presents over 1,500 specific elements of an ideal "universal" management program for optimizing environment, safety and health, and other programs [Abstract].
>
> MORT conceives the accident occurred when an unwanted energy flow or environmental condition that results in adverse consequences reaches persons and/or objects. MORT combines this concept and others into a functional accident definition as follows: An unwanted transfer of energy or environmental condition because of lack of or inadequate barriers and/or controls, producing injury to persons and/or damage to property or the process [p. 2].

After an accident occurs, the first step in the MORT process is to consider the adequacy of the amelioration process, their intent being to limit the severity of the consequences. Then MORT users would determine the unwanted energy flows or hazardous environmental conditions, whether barriers and controls were less than adequate, and whether vulnerable people or property were exposed.

While MORT is based on the fault tree method of system safety analysis, its logic diagram does not require statistical entries and computations for event probabilities. MORT is presented as an incident investigation methodology and as a basis for safety program evaluation.

Its thought process could also serve well the safety professional who participates in design concept discussions. MORT is soundly based on the unwanted energy release and environmental exposure concept, and its use leads to a good understanding of hazards, exposures, and risks.

A first approach to MORT could be intimidating: Its logic diagram presents over 1500 elements. It can seem daunting, but it should not be so judged. Thousands have successfully completed MORT seminars, and have gained considerably from exposure to its thought process.

I would like to repeat the quotation from Baruch Fischhoff's *Risk: A Guide to Controversy* which appeared earlier in this chapter:

> By definition, all risk controversies concern the risks associated with some hazard . . . the term "hazard" is used to describe any activity or technology that produces risk [p. 217].

Risks with which safety professionals deal derive from hazards. We need to know more about risks.

DEFINING RISK AND THE ROLE OF THE SAFETY PROFESSIONAL WITH RESPECT TO RISK

Risk is defined as a combination of the probability of occurrence of harm and the severity of that harm (ISO/IEC Guide 51:1999(E), Safety aspects — Guidelines for their inclusion in standards.) In producing the measure that becomes a statement of risk, it's necessary that determinations be made of the following:

- The existence of a hazard or hazards
- The exposure to the hazard
- The frequency of endangerment of that which is exposed to the hazard
- The severity of the consequences should the hazard be realized (the extent of harm or damage to people, property, or the environment)
- The probability of the hazard being realized

If the exercise is stopped after the severity of possible consequences is determined, the result is a hazard analysis. To determine risk, the probability of an occurrence must also be estimated. Estimating risk requires determining both the probability of a hazard-related incident occurring and the consequences of the incident.

Thus, in fulfilling their responsibilities, safety professionals must consider the two distinct aspects of risk:

- Avoiding, eliminating, or reducing the *probability* of a hazard-related incident occurring
- Minimizing the *severity* of harm or damage that could result

As safety practice further evolves, the required attention will be more often given to the avoidance of hazards in the design and redesign processes. As more safety professionals are successful in establishing themselves as consultants in those processes, they will become more familiar with concepts of risk and how risk reduction is effectively achieved.

Along the way, questions will arise concerning what the content of professional safety practice ought to be and how it is best applied in giving advice that actually attains a significant reduction of risk.

Some safety practitioners are directed by their managements to apply all of their efforts to obtaining compliance with laws, codes, standards, and regulations. Surely, being in compliance is a laudable goal. Unfortunately, merely being in compliance usually means achieving a minimal level of hazards management. It should not be assumed that actions taken to be in compliance with legal requirements address an organization's principal risks or that doing so, by itself, will attain effective hazards management.

A safety director tells the story of convincing his management to spend $1,000,000 to comply with OSHA standards. Later, he was asked what impact the expenditures would have on the types of employee injuries and illnesses that had occurred. Injury and illness records were available for 30 years. Not one of the reported incidents was related to the expenditures for OSHA compliance. Yes, risks of employee injury and illness were reduced through the expenditures to comply with OSHA standards, but by how much?

UNDERSTANDING MANAGEMENT'S VIEW OF RISK

A successful communication with management personnel on risk is not possible until an understanding has been reached on the meaning of the term as it is to be used in those communications. That's important, because risk is a term with far too many meanings.

On any given day, managements may hear the term in a variety of contexts: in examining a financial venture, in considering the possible increase in the price of a commodity, in receiving a phone call from a

stockbroker who proposes a risk management program. It's also important that safety professionals appreciate the culture of an organization and the perception of risk a management staff may have, its fears and logic concerning risk, and its tolerance for risk. Managers are risk takers; so are safety professionals.

ON ACCEPTABLE RISK

Safety was defined as the freedom from unacceptable risk. Conversely, safety may be defined as that state for which the risks are judged to be acceptable. These definitions imply a determination of risk, as well as a judgment of the acceptability of risk. Often, when the term *acceptable risk* is used, the response of the uninformed may be, How dare you suggest that some risk is acceptable.

But consider this: Every safety professional who writes a recommendation to eliminate or control a hazard makes a risk acceptance decision. It cannot be presumed that complying with the recommendation achieves zero risk. No thing or activity is risk-free. Also, in the practical world, all risks will not be eliminated. Even when deciding which risks are to be given priority consideration, a risk acceptance decision is made about those risks to be dealt with later, if only for the short term.

A few safety practitioners object to the idea that they make risk acceptability decisions. They create an atmosphere of being above that sort of thing, of super-righteousness. Perhaps they believe that if all that they propose is favorably acted upon, a risk-free environment will be achieved. Safety professionals know that is not possible. If they want to be a part of the management team, they must share in risk acceptance decisions. Chapter 14, "Acceptable Risk," is devoted to this subject.

RISK REDUCTION ADVICE

Safety professionals must acquire knowledge of risk determination concepts to give validity to the proposals they make to reduce risk. Since there are always resource and scheduling and time constraints, the advice given should ideally include

- Risk categorization and priority indications
- Possible alternative remediation measures
- Expected effectiveness of each alternative in risk reduction
- Remediation costs

RISK MANAGEMENT DECISIONS MAY NOT BE BASED ON LOGIC

Although a safety professional may present logically developed data on risks, it should be understood that risk reduction decisions might not be made on that data alone, particularly when dealing with the perceptions the public or employees may have of risk. Richard F. Griffiths wrote in *Dealing with Risk: The Planning, Management and Acceptability of Technology Risk* that

> The applicability in risk assessment and acceptability is that for low-frequency events the probability estimate is not based on a large number of trials and the public evaluation may well be more conditioned on how bad the outcome might be, with little regard for arguments as to how likely it is [p. 12].

In this one paragraph, Griffiths introduces two important subjects: that probability estimates used for low-frequency/high-consequence incidents may be questionable; and that public concerns may reflect only perceptions of severity of outcomes.

At a symposium on risk sponsored by the National Safety Council and ILSI Risk Science Institute, the theme for which was "Regulating Risk: The Science and Politics of Risk," one speaker expressed the view that public risk concerns would best be considered as public outrage. Even though at times it may be believed that the public outrage is illogical, it will often be a significant factor in risk decision-making. All risk reduction measures may not be based entirely on risk assessment logic. And it may be that in dealing with public outrage, or employee concerns, or perceived risks, facts will not be convincing.

When risk decisions are made, it will not be unusual that the decision process is influenced by elements of fear and dread, and the perceived risks of employees, the immediate community, a larger public, and management personnel.

QUESTIONING THE VALIDITY OF SOME QUANTITATIVE RISK ANALYSES

Since so many subjective judgments are necessary in applying what are otherwise sound statistical quantification systems, I believe that, except when statistical concepts can be applied to the known such as the face markings of dice, or when empirical probability evidence has been produced, all quantitative risk analyses are really qualitative risk analyses.

Vernon L. Grose in *Managing Risk: Systematic Loss Prevention for Executives* appropriately cautioned on several occasions against an over-reliance on numbers in determining risk when the numbers may not be sound. A reasoned skepticism would serve safety professionals well concerning the validity of the numbers used in what appear to be precise determinations of both the probability of an incident occurring and an assessment of its consequences.

Both probability and consequence numbers may be greatly overstated or understated. Grose may have exaggerated only slightly when he wrote the following:

> Because desire overrode reality, the unfortunate gamesmanship that has evolved supposedly to upgrade reliability and safety has come to be called "numerology", defined in the dictionary as follows:
>
> > A system of occultism (hidden, secret, or beyond human understanding) involving divinations (the practice of trying to foretell the future by mysterious means) by numbers [p. 263].

Grose indicates that when there is a demand for numbers and an inventing to fill the need, the numbers eventually appear in print and there is no way to recognize their illegitimacy. Thus a caution: Be wary of the numerologists.

Grose is not alone in expressing concern about the validity of risk quantification systems. These quotes come from *Improved Risk Communications*, a text prepared under the guidance of the Committee on Risk Perception and Communication as a project of the National Research Council:

> Analysts are prone to overlook the ways human errors or deliberate human interventions can effect technological systems [p. 46].
>
> The need to quantify risks as an aid to decision making creates special difficulties because the choice of which numerical measures to use depends on values and not only on science [p. 48].

Emphasis is given here to the phrase "the choice of which numerical measures to use depends on values and not only on science."

I quote again from Griffiths' *Dealing with Risk: The Planning, Management and Acceptability of Technological Risk*:

> If one compares the experts' best estimates of the consequences of an accident with the historical record it is often found that the estimates are greatly in excess of the consequences actually manifested [p. 14].

My experience requires an opposite observation to what Griffiths says about consequence estimates being greatly in excess of the actual consequences. Over many years, I observed that estimates of possible property damage losses developed by fire protection engineers in relation to described hazard scenarios were often notably less than the actual damage when an incident occurred. Nevertheless, the point is this: Estimating consequences of an accident is not an exact science.

I also offer a caution concerning numerical risk scoring systems. For example, I was presented with risk data to which a scoring system was to be applied and risk priority ratings given. An incident with a probability of 1 per 100 plant operating years for which devastating results were calculated, including many fatalities, was given a lower priority than a single disabling back injury with a probability of 1 per plant operating year. Such may not be in the best interest of employees, management, or the public.

Nevertheless, there is a growing demand for risk scoring systems, which are the sort of thing that engineers like because of their preciseness. Chapter 9 in *Innovations in Safety Management: Addressing Career Knowledge Needs* is titled "Risk Scoring Systems," and the following excerpts come from it.

Users of (risk scoring) systems should be inquisitive and cautious concerning their content, the meanings of the terms adopted, the numericals applied to the gradations within elements to be scored, and how they are applied in determining risk levels.

- Risk scorings begin with subjective judgments on the individual elements to be considered, and those subjective judgments are translated into numbers, not followed by any qualifying statements. What starts out as judgmental observations become finite numbers, which then attain an image of preciseness.

  Further, those numbers are multiplied or totaled to produce a risk score, giving the risk assessment process the appearance of having attained the status of science. In reality, the risk assessment process is as much art as science.
- The numbers assigned to the elements to be scored are entirely judgmental, have no basis in fact or good science, and vary for the same subject in different systems. There are no universally applied rules to assign value numbers to elements to be scored. All values in risk scoring systems reflect the experience and views of those who create the system.
- Frequency of exposure has, historically been one of the elements considered in determining event probability. But, giving frequency

of exposure its own multiplier, separate from and in addition to a probability multiplier (as is done in at least one system obtaining notoriety), diminishes the needed emphasis on the severity of harm or damage that could result from an event.

- Meanings of the terms probability, likelihood, frequency of exposure or endangerment, and severity as used in risk scoring systems are not consistent. Also, it may be that within a system: a term may appear more than once and have different usages; and consistency in the meanings of the terms used initially in the system may not be maintained.
- If risk-scoring systems are applied rigidly whereby a higher score indicates a greater risk than a lower score, and the scores are not considered in light of the employee, community, social, and financial concerns of the organization, its best interests may not be well served. This applies especially to low probability events that may have severe consequences, for which risk scores may be low [p. 171].

Having considered all of the cautions in the foregoing, a three-dimensional risk scoring system, incorporating severity levels, frequency of exposure, and incident probability was developed. In the text material on the risk scoring system, the fact that subjective judgments are to be made in its use is stressed, terms are clearly defined, and a rigid and unqualified application of it in decision-making is discouraged. As is written in *Innovations in Safety* Management, this risk scoring model:

- Serves the needs of those who are more comfortable with statistics in their risk assessments
- Addresses the strong beliefs of those who want frequency of exposure given separate consideration in the risk assessment process (e.g., having frequency of exposure included as an element in a risk decision matrix was much debated in the meetings out of which the ANSI B11.TR3 report was developed)
- Maintains credibility and efficacy [p. 189].

After running many plausibility and efficacy tests, the following risk scoring formula was developed:

$$\text{Risk score} = (\text{Probability rating} + \text{Frequency of exposure rating}) \times \text{Severity rating}$$

$$\text{RS} = (\text{PR} + \text{FER}) \times \text{SR}$$

Intelligent use of this risk scoring system is proposed, Users of it should recognize that the risk assessment process is as much art as science and that the statistical outcomes derived from its application are to be just one element in the decision-making.

ON RISK ESTIMATES THAT RESULT IN A MONEY NUMBER

Several authors propose that risk be expressed as a precise numerical quantification, in dollars. The computation would derive from a formula through which probability is multiplied by consequence to obtain the expected loss per unit of time or activity. This is a typical formula:

$$\text{Risk (in money terms)} = \text{Probability} \times \text{Consequence}$$

where probability is the event frequency per unit of time or unit of activity, and consequence is the amount of money loss or cost per event.

Similar formulas abound, intended to produce a finite, numerical quantification of risk in money terms. When a hazard analysis is completed, the outcome may sometimes be expressed in a money number representing the value applied to the harm or damage done. In safety management, why that money number must be multiplied by a probability number to obtain a risk cost per unit of time or activity is a mystery. A review of the literature does not give adequate explanation of the soundness of such an exercise for individual risks. The concept has validity in actuarial practice when dealing with large numbers of risks.

CONCLUSION

To be effective, safety professionals must understand hazards, risks, the relationship between hazards and risks, and hazards analysis and risk assessment techniques. In the use of hazard analysis and risk assessment matrices, judgments of incident probability and consequence will often be made on a subjective basis. And such systems can be made to work. They should be considered more art than science.

REFERENCES

Brauer, Roger L. *Safety and Health for Engineers*. New York: John Wiley & Sons, 1990.

Browning, R. L. *The Loss Rate Concept in Safety Engineering*. New York: Marcel Dekker, 1980.

Ferry, Ted. *Safety and Health Management Planning*. New York: John Wiley & Sons, 1990.

Griffiths, Richard F., ed. *Dealing with Risk*. Manchester, UK: Manchester University Press, 1981.

Grimaldi, John V. and Rollin H. Simonds. *Safety Management*. Homewood, IL: Irwin, 1989.

Gross, Vernon L. *Managing Risk—Systematic Loss Prevention for Executives*. Englewood Cliffs, NJ: Prentice-Hall, 1987.

Guide to Use of the Management Oversight and Risk Tree. SSDC—103. Idaho Falls, ID: U.S. Department of Energy, Office of Safety and Quality Assurance, Idaho National Engineering Laboratory, 1994.

Haddon, William J., Jr. "On the Escape of Tigers: An Ecological Note." *Technology Review*, May 1970.

Improving Risk Communication. Washington, DC: National Academy Press, 1989.

ISO/IEC Guide 51:1999(E), Safety Aspects—Guidelines for Their Inclusion in Standards, 2nd edition. Geneva, Switzerland: International Organization for Standardization, 1999.

Johnson, William G. *MORT Safety Assurance Systems*. New York: Marcel Dekker, 1980.

Manuele, Fred A. *Innovations in Safety Management: Addressing Career Knowledge Needs*. New York: John Wiley & Sons, 2001.

14

HAZARD ANALYSIS AND RISK ASSESSMENT

INTRODUCTION

All hazards do not have equal potential for harm or damage. All hazards-related incidents do not have equal probability of occurrence. Nor will the adverse effects from those incidents be equal.

It is the norm that several hazards will be known to exist at the same time. Giving appropriate advice concerning them requires that

- Risk assessments be made, during which
  - hazards are identified, analyzed, and categorized as to the possible severity of harm or damage that could result and
  - estimates are given of the probability of hazards-related incidents occurring.
- Risks are ranked as to their significance and the priority that should be given them.
- Costs are determined of alternate proposals to reduce risks.
- Expected risk reduction benefits are given for each remediation proposal.

WHY EMPHASIZE HAZARD ANALYSIS AND RISK ASSESSMENT

Why make so much of analyzing hazards and assessing risks when dealing with several hazards at the same time? This, typically, is what happens.

On the Practice of Safety, Third Edition, By Fred A. Manuele
ISBN 0-471-27275-2

ADDENDUM A: PRELIMINARY HAZARD ANALYSIS FORM

Sverdrup Technology, Inc. **Preliminary Hazard Analysis**

Brief Descriptive Title (Position of System/Sub-system/Operational Phases covered by this analysis):

Probability Interval: 25 years	Date:	Hazard Target*	Risk Before			Description of Countermeasures	Risk After		
System Number: _____	Analysis: ☐ Initial ☐ Revision ☐ Addition		Severity	Probability	Risk Code	Identify countermeasures by appropriate code letter(s): D = Design Alteration E = Engineered Safety Feature S = Safety Device W = Warning Device P = Procedures/Training	Severity	Probability	Risk Code
Hazard No./Description									

Prepared by/Date: | *Target Codes: P—Personnel E—Equipment T—Downtime R—Product V—Environment | Approved by/Date:

Hazard Analysis and Risk Assessment (Page 118 in *Innovations in Safety Management*)

ADDENDUM B: FAILURE MODES AND EFFECTS ANALYSIS FORM

Project No.: _____
Subsystem: _____
System: _____
Probability Interval: _____
Operational Phase(s): _____

Sverdrup Technology, Inc.
Failure Modes & Effects Analysis
FMEA No.: _____

Sheet _____ of _____
Date: _____
Prep. By: _____
Rev. By: _____
Approved By: _____

IDENT. NO.	ITEM/ FUNCTIONAL IDENT.	FAILURE MODE	FAILURE CAUSE	FAILURE EFFECT	TARGET	RISK ASSESSMENT SEV	RISK ASSESSMENT PROB	RISK ASSESSMENT RISK CODE	ACTION REQUIRED/REMARKS

Sverdrup Technology, Inc. Worksheet

P: Personnel/E: Equipment/T: Downtime/R: Product/V: Environment

Hazard Analysis and Risk Assessment (Page 125 in *Innovations in Safety Management*)

15

ACCEPTABLE RISK

INTRODUCTION

A majority of safety professionals accept the premise that absolute safety, a zero risk state, is not attainable. But, some safety practitioners profess that only a risk-free environment is acceptable. Consider these two examples.

1. At a recent safety conference, a speaker reviewed the hazard analysis and risk assessment methods used in his company and said the outcome to be achieved through the use of those methods was acceptable risk. During the question period, some questioners implied by the nature and tone of their questions that no risk is acceptable. They asked: What do you mean by acceptable risk? Are you suggesting that some risk is acceptable? Acceptable to whom?
   The speaker gave a general response saying that a risk is acceptable if the probability of an incident occurring and the severity of harm that might result are low. Thus, the speaker defined the acceptable risk level for his company.
2. Safety practitioners attending a course on hazard analysis and risk reduction were outspoken in their opposition to the idea that any level of risk is acceptable. They stated their sincere belief that, in the workplace, attaining zero risk is a legitimate goal. The instructor could not convince them otherwise.

On the Practice of Safety, Third Edition, By Fred A. Manuele
ISBN 0-471-27275-2

Individually and collectively we are risk acceptors. And risk acceptance is situational: Variations in the risk levels that individuals and organizations accept in given situations are exceptionally broad. Nevertheless, in an attempt to promote an understanding of the acceptable risk concept, this chapter does the following:

- Establishes that designing and operating to a zero risk level is not attainable.
- Provides definitions of key terms for an ongoing discussion.
- Shows how some entities have, in practice, defined acceptable risk levels.
- Provides examples illustrating the diverse views people have of risk acceptance in certain situations.
- Discusses imposed risks.
- Presents a methodology to achieve an acceptable risk level.

ONLY RELATIVE SAFETY IS ACHIEVABLE

The premise that absolute safety, a zero risk state, is not attainable has become broadly recognized, as evidenced by the following examples.

One of the most significant and influential books on the concept of acceptable risk was written by William W. Lowrance. Its title is *Of Acceptable Risk: Science and the Determination of Safety.* Lowrance notes that:

> Nothing can be absolutely free of risk. One can't think of anything that isn't, under some circumstances, able to cause harm. Because nothing can be absolutely free of risk, nothing can be said to be absolutely safe. There are degrees of risk, and consequently there are degrees of safety [p. 8].
>
> Since the taking of both personal and societal risks is inherent in human activity, there can be no hope of reducing all risks to zero. Rather, as when steering any course, we must continuously adjust our heading so as to enjoy the greatest benefit at the lowest risk cost [p. 11].

Under the caption "The Concept of Safety" (Section 5), this appears in the ISO/IEC Guide 51: Safety Aspects — Guidelines for Their Inclusion in Standards.*

> There can be no absolute safety: some risk will remain, defined in this Guide as residual risk. Therefore a product, process or service can only be relatively safe.

*ISO stands for the International Organization for Standardization. IEC stands for the International Electrotechnical Commission.

> Safety is achieved by reducing risk to a tolerable level, defined in this Guide as tolerable risk.

To repeat the previous quote from ISO/IEC Guide 51, "There can be no absolute safety: some risk will remain, defined in this Guide as residual risk." In the real world, attaining zero risk, whether in the design process or in operations, is not possible. Nevertheless, the residual risk, after risk avoidance, elimination, or control measures are taken, should be acceptable, as judged by the decision makers.

For some situations, the residual risk may be high and still be considered by the participants in an activity to be acceptable. In other situations, no matter how effective the design and control measures, the residual risk will be judged to be unacceptable.

ON THE NATURE OF RISK

Risk is determined by assessing its two components: the severity of harm or damage resulting from a hazard-related event; and the probability that the event could occur. Table 15.1 presents a sample Risk Assessment Matrix, illustrating how these two factors are combined to obtain a risk level. A review of the many published risk assessment matrices appears in chapters titled "A Primer On Hazard Analysis And Risk Assessment" and "Risk Scoring Systems" in this authors book titled *Innovations In Safety Management*.

The purpose of a risk management matrix is to (a) provide a logical framework for hazard analysis and risk assessment and (b) assist risk decision makers in arriving at their risk reduction and risk acceptance or declination conclusions. The implicit goal is to achieve acceptable risk levels. Several standards and guidelines now include the concepts of residual risk and acceptable or tolerable risk (e.g., ANSI/B11 TR3, ISO/IEC Guide 51, SEMI S10—see references for full titles).

Table 15.1. Risk assessment matrix

Occurrence Probability	Severity of Consequences			
	Catastrophic	Critical	Medium	Minimal
Frequent	High	High	Serious	Moderate
Likely	High	High	Serious	Moderate
Occasional	Serious	Serious	Moderate	Low
Remote	Serious	Moderate	Moderate	Low
Improbable	Moderate	Moderate	Low	Low

Achieving understanding of the terms used in risk assessment matrices is vital for their use in a particular organization. For example, in actual practice, a variety of definitions are used of the terms establishing probability and severity levels, as in Table 15.1. Terms applicable to a discussion of acceptable risk are presented in the following definitions.

DEFINITIONS AND COMMENTS

The following is typical of what is becoming universally accepted language with respect to hazards and risks. The section numbers appearing after some definitions refer to the ISO/IEC Guide 51.

- A **hazard** is defined as the potential source of harm (3.5). Hazards include both the characteristics of things and the actions or inactions of people. Identifying hazardous human error potential, as well as the physical aspects of hazards, is an important part of the hazard identification process. All risks with which safety practitioners deal derive from hazards. There are no exceptions. For any particular hazard, the first and best approach is to eliminate the hazard. If there are no potentials for harm, there are no hazards. If there are no hazards, there are no risks. Hazards eliminated result in zero risk from those hazards. But, it is not possible to eliminate all hazards.
- **Probability** is defined as the likelihood of a hazard being realized and initiating an event or series of events that could result in harm or damage—for the selected unit of time, events, population, items or activity.
- **Residual risk** is defined as the risk remaining after protective measures have been taken (3.9).
- **Risk** is defined as a combination of the probability of occurrence of harm and the severity of that harm (3.2).
- **Safety** is defined as freedom from unacceptable risk (3.1).
  An alternate. To avoid the negative, I have defined safety as that state for which the risks are judged to be acceptable.
- **Severity** is defined as the worst credible consequence should a hazard-related incident occur.
- **Tolerable risk** is defined as that risk which is accepted in a given context based on the current values of society (3.7).
  An alternate. For those who prefer to deal in terms of acceptable risk, the definition just given is reversible. Thus, acceptable risk is defined as that risk which is tolerated in a given context based on current values of society.

A MATTER OF SEMANTICS

Meanings variously given to the terms acceptable risk and tolerable risk present a semantics problem. For some people, the terms are synonyms; for others, they have markedly different meanings. Dictionary definitions of acceptable and tolerable differ slightly. Two descriptions for each term follow.

Acceptable:
1. Capable or worthy of being accepted
2. Pleasing to the receiver, satisfactory, agreeable, welcome

Tolerable:
1. Capable of being tolerated, endurable
2. Fairly good, not so bad

In these definitions, tolerable as a term is less demanding: endurable, but only fairly good, not so bad. To be acceptable, the risk level should be satisfactory and agreeable, in accord with the dictionary definition.

Even though these dictionary definitions differ slightly, in daily practice they are commonly used as synonyms. In *Roget's Thesaurus*, tolerable is given as a possible replacement for acceptable, and thus as a synonym. Although there may be a small technical difference between the terms acceptable and tolerable, they can and should be accepted as synonyms. Continued and interchangeable use will lessen the debate over which term should be used. (As I have witnessed, such debates can be vigorous.)

EXAMPLES OF ACCEPTABLE RISK

Real-world descriptions of acceptable risk levels are demonstrated by these examples. They vary considerably.

1. NASA-STD-8719.7, January 1998 defines Acceptable Risk as follows:

> Loss of life as a result of hazards in this facility is unlikely. Hazards may result in no lost workday injuries or no restricted duty cases, loss of facility operational capability of less than 1 day, or damage to equipment or property less than $25,000.

2. In a major manufacturer of heavy mobile equipment, if it can be reasonably assumed that a user of the equipment can lose a day's work, the risk is not acceptable. The risk situation must be dealt with through equipment redesign or through strengthening the operations manual, thus alerting users to the hazard's potential and providing appropriate instructions.

3. In a smaller operation, the design and operation standard requires that if a hazard presents the potential for injury that requires medical treatment beyond first aid, the risk deriving from that hazard must be reduced to a level to avoid such injury to be considered acceptable.

USING RISK DECISION MATRICES TO ACHIEVE ACCEPTABLE RISK LEVELS

Earlier in this chapter, reference was made to a speaker who reviewed the hazard analysis and risk assessment methods used in his company, which relied on typical risk assessment and decision-making matrices, to achieve acceptable risk levels. Use of such matrices is a method some organizations apply to arrive at acceptable risk levels. Table 15.1 is an example of such a risk assessment matrix. Using the results from Table 15.1, levels of remedial action or risk acceptance for individual risk categories can be established, as in Table 15.2.

Table 15.2. Management decision levels

Risk Category	Remedial Action, or Acceptance
High	Operation not permissible
Serious	Remedial action to have high priority
Moderate	Remedial action to be taken in appropriate time
Low	Risk is acceptable: remedial action discretionary

Table 15.2 is a guide: It is not intended to imply that, in all situations, an activity is to proceed only if the risk is in the "low" risk category. Furthermore, while in Table 15.2 the indication given for the "low" risk category is "Risk is acceptable; remedial action discretionary," that does not mean that action would not be taken to reduce the risk if the remedial action could stand a cost–benefit test. Also, remedial action is taken in some such situations for personnel relations purposes to reduce the fear factor when the risk is perceived by workers to be more significant than it is.

DIVERSE VIEWS

A review of several real-world situations follows to provide examples of the diverse views that people have about acceptable risk.

1. Consider these excerpts from an extensive article on auto racing that appeared in the February 14, 2001 issue of the *Chicago Tribune*. Its title is "A risky profession becomes a little safer."

> Mario Andretti is quoted as saying: At the beginning of a season, I would look around at a drivers' meeting and I would think, 'I wonder who's not going to be here at the end.' There were years when we lost as many as six guys.

A history of fatalities in auto racing is given in the article, as well as the notable measures taken over the years to make racing less risky. Nevertheless, the number of driver fatalities in relation to the number of drivers involved would be considered unacceptable in other employment settings.

The article continues with a reference to Richard Petty, who, it says, in his 35 years of NASCAR racing often admonished his wife:

> If I get killed, if you ever sue anybody over it, I will haunt you. I know the risk. I take all the responsibility.

Auto racing is a form of employment. Drivers, auto owners, promoters, television broadcasters, and viewers are aware of the risks, and apparently they accept them. No public outcry has arisen concerning this high-risk activity. To the contrary, it has been reported that the numbers of television viewers for auto racing continues to increase. This suggests that in certain instances relatively high risks are considered acceptable to both individuals and society.

2. The following appears in a paper titled "Spacecraft Human-Rating System Safety — Beyond the Numbers" by D. F. Kip Mikula.

> In the 21st century, new human-rated spacecraft for Earth-to-orbit, on-orbit transfer and work (including space suits), long term on-orbit living, and return from Earth orbit will be appearing on the horizon. Each of these must, as a minimum due to their human-rating, be designed to be safe for those human operators, passengers, and occupants. In particular, these humans must be safe from the risk of death or serious and minor injury (i.e., casualty).
>
> In defining the human-rating requirements for these vehicles, NASA document JSC 28354 Human Rating Requirements has been published. Among other requirements for such things as crew escape, this document has established a Loss of Crew (LOC) probability risk requirement of 1 in 10,000 missions. Stated another way, this requirement equates to a probability of success of 0.9999. This means that over a period of time encompassing 10,000 missions of a specific human-rated space vehicle design that only one casualty will occur. In addition, the document also establishes a Loss of Vehicle (LOV) probability requirement of 1 in 1,000 missions.

Is the risk acceptable? When I asked a group of safety practitioners if the risk of 1 failure resulting in Loss of Crew (LOC) in 10,000 missions was acceptable, their overwhelming response was no. But, they could not reach a consensus to recommend the complete shutdown of space ventures. Those taking part in journeys to outer space are aware of the risks and volunteer for the opportunity to be astronauts, which is a form of employment. So, the managers at NASA and the Congressional Committees that provide oversight to NASA are also aware of the risks. And space ventures will continue.

Understandably, the level of acceptable risk in operations where most safety practitioners have influence is much lower than those tolerated in space ventures. For example, a major equipment failure of 1 in 1000 startups — the NASA design standard for Loss of Vehicle (LOV) probability — would be unacceptable in all but the exceptionally unusual situation.

3. Now to get the discussion down to a more mundane subject, one in which most all safety practitioners participate — motor vehicle operation. According to *Injury Facts, 2001 Edition*, a National Safety Council publication, motor vehicle operation resulted in 43,000 fatalities in the United States in 2000, and 2,300,000 persons sustained disabling injuries (p. 82). Assume a U.S. population of 283,800,000; the probability of a resident, on average, being killed in an auto accident in 2000 was 1 in 6600. The probability of sustaining a disabling injury was 1 in 123.

Those are serious odds, on the negative side. Nevertheless, we continue to drive. Is the risk acceptable? Or are we engaging in a tolerable activity to which the dictionary definition "fairly good; not so bad" applies, and we accept the risks?

Admittedly, we expect a continuing effort to make motor vehicle transportation safer and presume that the risks will be reduced. But, presently, no matter how skilled a person may be as a defensive driver, the risk of fatality or disabling injury is substantial while in traffic. It is never zero. Always, the probability exists of being injured by the actions of another driver.

DESIGNING BEYOND STANDARDS

Many authors have written on the benefits of designing to exceed the requirements of published standards. Achieving an acceptable risk level very often requires doing so. Complying with industry or government standards (e.g., OSHA, ANSI, European Community) will meet the consensus arrived at by the industry or government group that wrote the

standard. However, complying with such standards will not necessarily achieve an acceptable risk level.

To give an example, a learned colleague frequently reminds me that complying with the National Electrical Safety Code or the applicable OSHA lockout/tagout standard will not ensure that electrical disconnects are placed in locations conducive to employee use. All too often, the design of lockout/tagout systems is error-provocative, thus encouraging hazardous human error. Although the design complies with the standards, the residual risk may be unacceptable.

Ergonomic design practices offer another example of how designing to the prevalent norm for the workplace may result in unacceptable residual risk. A common ergonomic design practice is to develop designs that accommodate the 5th to 95th percentile of the target users. Examples of the criteria used are stature, reach, strength, et cetera. Typically, ergonomics design and operations standards that address the dimensions and capabilities of these 90% of the work population are considered acceptable. As a result, there will be some residual ergonomics risks with respect to those in the lower and upper 5% of the population that prove to be excessive.

Furthermore, consider OSHA's permissible exposure limits for hazardous substances or the guidelines in that field issued by the American Conference of Governmental Industrial Hygienists. Although exposure limits are established, it is not presumed that all persons will avoid illness at those levels. Thus, in some companies, say their safety directors, the intent is to achieve operating exposure limits considerably less than generally accepted standards. These companies have set a goal to achieve superior, world-class safety records and have recognized that to do so they must operate at exposure levels lower than the standards. However, they also recognize that even at these improved levels, some small amounts of residual risk remain.

IMPOSED RISKS

Literature is abundant on the opposition people have to risks they believe to be imposed on them. For some safety practitioners, their resistance to the acceptable risk concept derives from their view that imposed risks are objectionable and are to be rebelled against. Conversely, they accept the risks of activities in which they choose to engage — for example, skiing, bicycle riding, driving an automobile.

In the occupational setting, risks are mostly imposed. Joe Stephenson got it right when he wrote this in *System Safety 2000*.

> The safety of an operation is determined long before the people, procedures, and plant and hardware come together at the work site to perform a given task [p. 10].

Start from the beginning: Consider, first, a site survey for ecological considerations, and move into the construction and fitting out of a facility. Thousands of safety-related decisions are made in the design process that result in an imposed level of risk. Usually, those decisions meet (or exceed) applicable safety-related codes and standards with respect to such as (to name but a few): the contour of exterior grounds; sidewalks and parking lots; building foundations; facility layout and configuration; floor materials; roof supports; process selection and design; determination of the work methods; aisle spacing; traffic flow; hardware; equipment; tooling; materials to be used; energy choices and controls; lighting, heating, and ventilation; fire protection; and environmental concerns.

Designers and engineers make decisions on the foregoing in the original design process. Those decisions establish what the designers implicitly believe to be acceptable risk levels. Thus, the risk levels are largely imposed, once a facility is in place and operating. Some may accept that realization only reluctantly, but that's the real world. Safety practitioners, and others, can rail about the undesirability of risks being imposed in the occupational setting if they choose, but the energy expended in so doing is largely a waste.

W. Edwards Deming's 85–15 Rule has a bearing on this discussion. Mary Walton, a Deming colleague, cites the rule in *The Deming Management Method*:

> The Rule holds that 85 percent of the problems in any operation are within the system and are the responsibly of management, while only 15 percent lie with the worker" [p. 242].

Although the 85–15 Rule pertains to quality, the concept also applies to safety. Quality, safety, and risk problems in a system derive from the decisions made in creating or redesigning the system. Thus, the work system, for both quality and safety, is largely imposed through the design process. (For further discussion of quality management and safety management similarities, see Chapter 20, "On Quality Management and the Practice of Safety.")

THE ILLUSIVENESS OF A UNIVERSAL DEFINITION OF ACCEPTABLE RISK

When commencing this chapter, one intent was to develop a definition of acceptable risk that was universally applicable in all risk situations — one

that was more specific than the prevailing general definitions, such as previously given here. Unfortunately, the original intent proved to be illusive.

Although the concept of acceptable risk is becoming more commonly adopted throughout the world, definitions of the term acceptable risk can only be generally written. While it can be said that safety is that state for which the risks are judged to be acceptable, and that tolerable risk is defined as that risk which is accepted in a given context based on the current values of society, applications of those premises in individual situations result in great variations.

Acceptable risk is a function of many factors, and it varies considerably across industries—for example, mining versus medical devices versus farming. Even within a single global company, the acceptable risk levels can vary. The culture dominant in a company and the culture of a country in which a facility is domiciled play an important role in risk acceptability as has been experienced by safety colleagues working in global companies. Training, experience, and resources can also influence acceptable risk levels. Risk acceptability is also time-dependent, in that what is acceptable today may not be acceptable tomorrow, next year, or the next decade.

I believe that developing a distinct and numerically explicit definition of an acceptable risk level that is universally applicable is not possible. There are so many variables.

A METHODOLOGY TO ACHIEVE AN ACCEPTABLE RISK LEVEL

If the residual risk for a task or operation is never zero, for what risk level does one strive? At best, we can say that the concept of designing and operating to attain risk levels as low as reasonably achievable or practicable should be applied to the situation being considered.

ALARA and ALARP are commonly used acronyms in risk assessment and reduction activities. ALARA stands for *as low as reasonably achievable*; ALARP is short for *as low as reasonably practicable*. Although now broadly used, ALARA originated in the atomic energy field. This is taken from the Reference Library, Glossary of Terms at www.nrc.gov.

> ALARA: Acronym for "As Low As Reasonably Achievable," means making every reasonable effort to maintain exposures to ionizing radiation as far below the dose limits as practical, consistent with the purpose for which the licensed activity is undertaken, taking into account the state of technology, the economics of improvements in relation to benefits to the public health and safety, and other societal and socioeconomic considerations, and in relation to utilization of nuclear energy and licensed materials in the public interest (see 10/CFR 20.1003).

The concepts inherent in the terms ALARA and ALARP serve as guidelines in determining whether a risk is acceptable, but cannot be used as absolutes in decision-making. It should be understood that in an exceptional situation, even though the risk level attained is as low as reasonably achievable or practicable, a decision will be made that the residual risk is not acceptable and that the operation should not proceed.

The concept embodied in the terms ALARA and ALARP applies to the design of products, facilities, equipment, and the work environment. (If there is a substantive difference between the intent of ALARA and ALARP, it's difficult to establish.)

Determining whether a risk is acceptable requires consideration of many variables. An additional excerpt from ISO/IEC Guide 51, Section 5, helps in understanding the concept of designing and operating for risk levels as low as reasonably practicable.

> Tolerable risk is determined by the search for an optimal balance between the ideal of absolute safety and the demands to be met by a product, process or service, and factors such as benefit to the user, suitability for purpose, cost effectiveness, and conventions of the society concerned.

In the real world of decision-making, benefits represented by the amount of risk reduction to be obtained, and the costs to achieve those reductions, become important factors. Trade-offs are frequent and necessary. An appropriate goal in those deliberations is to have the residual risk be as low as reasonably achievable.

Ensuring that a high level of risk avoidance, elimination, or control is achieved in new or altered facilities and equipment requires considerable effort. Ideally, safety practitioners should be a part of, and influential in, the design processes; the earlier, the better. More specifically, organizations need to work toward

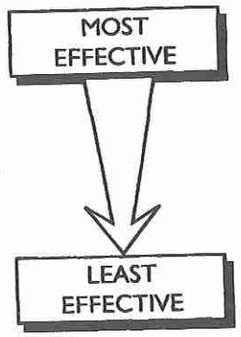
- Having effective design safety standards in place
- Establishing and rigidly applying safety specifications for equipment and materials to be followed by suppliers
- Requiring documented risk assessments
- Implementing and supporting design safety review systems that impact decision-making

To assist those who are to decide if a risk is acceptable, a guide follows, in Figure 15.1, captioned "The Safety Decision Hierarchy." It

A. Problem Identification and Analysis

1. Identify and analyze hazards
2. Assess the risks

B. Consider These Actions, in Their Order of Effectiveness



1. Eliminate hazards and risks through system design and redesign
2. Reduce risks by substituting less hazardous methods or materials
3. Incorporate safety devices
4. Provide warning systems
5. Apply administrative controls (work methods, training, etc.)
6. Provide personal protective equipment

C. Decide and Take Action

D. Measure for Effectiveness: Re-Analyze as Needed

Figure 15.1. The safety decision hierarchy.

is taken from the book *Innovations in Safety Management*. This hierarchy encompasses hazard identification and analysis and risk assessment, the appropriate risk reduction actions, applied in an order of effectiveness — within a sound problem-solving methodology.

As in any sound problem-solving technique, the process commences with identifying and analyzing the problem — that is, identifying and analyzing hazards and assessing the risks. Having done so, risk reduction actions are then taken, in accord with a hierarchy of effectiveness.

In the use of this hierarchy, the terms contained in the definition previously given of ALARA are relevant:

- Making every reasonable effort
- Consistent with the purpose undertaken
- The state of technology
- The economics of improvements in relation to benefits

Comments follow in support of the logic for the risk reduction actions and the significance of their order of effectiveness. They are excerpted from the chapter "The Safety Decision Hierarchy" in *Innovations in Safety Management.* In all but the rare situation, application of this hierarchy will result in attaining an acceptable risk level.

LOGIC IN SUPPORT OF THE SAFETY DECISION HIERARCHY

1. If the hazards are eliminated in the design and redesign processes, risks that derive from those hazards are also eliminated. If there are no hazards, there is no potential for harm and, thereby, no risk. Obviously, hazard elimination is the most effective way to eliminate risk.

2. By substituting less hazardous methods or materials (e.g., using automated material handling equipment rather than manual material handling, using a less hazardous degreasing material), risks can be substantively reduced in the operations or product design and redesign process, and reliance on the performance of people is minimized.

3. When safety devices are incorporated in the system or product in the form of engineering controls, risk reduction can markedly be achieved and reliance on the worker or product user is further reduced.

4. Warning signs, labels, and instructions have been partially effective. Warning systems are reactionary. They alert persons only after the development of a situation for which a hazard's potential is in the process of being realized (e.g., the smoke alarm in a house). Warning system effectiveness relies considerably on training, the quality of maintenance, and people reactions.

5. Administrative controls, only some of which are included here, rely entirely on the performance of people, for whom to err is human. Some administrative controls are: development of appropriate work methods and procedures, personnel selection, training, supervision, motivation, work scheduling, job rotation, scheduled rest periods, maintenance, management of change, investigations, inspections, and behavior modification.

6. The proper use of personal protective equipment relies on an extensive series of supervisory and personnel actions, such as the identification of the equipment needed, its selection, fitting, training, inspection, maintenance, et cetera.

In accord with good problem-solving techniques, the subsequent steps are to (a) decide upon and take action and (b) measure for the effectiveness of the actions taken, reanalyzing as needed.

CONCLUSIONS

Comments follow, based on the study made of the concept of acceptable risk.

1. We must accept that a state of zero risk cannot exist where hazards have not been eliminated.

2. Where hazards cannot be eliminated, the goal should be to reduce risks so that the residual risks are acceptable.
3. It should be recognized that application of The Safety Decision Hierarchy will, in all but the exceptional situations, attain an acceptable risk level.
4. The safety community should debate and consider accepting the proposed definitions for the terms defined herein.
5. The terms acceptable risk and tolerable risk should be considered synonyms rather than as having distinct and different meanings.
6. Risk assessments and the risk decision process should become more structured and documented in accordance with recent guidelines and standards, such as B11.TR3, SEMI S10, ANSI/RIA R15.06–1999, and ISO 14 121 (previously identified as EN 1050).
7. We should recognize that a universally applicable definition of an acceptable risk level cannot be attained, other than in broad general terms, because of the many variables in individual risk situations.

As has been noted here, some safety standards and guidelines issued in recent years include provisions for hazard analysis and risk assessment. That progression will continue, and its impact will be extensively felt. Those standards and guidelines recognize that, even though hazard avoidance, elimination, and control measures are taken, there will always be residual risk, and that such risk should be acceptable — or tolerable, if you prefer.

Having knowledge of hazard analysis and risk assessment methods and the concept of acceptable risk has become a necessity for the professional practice of safety.

Note: A brief version of this chapter appeared as an article in the January 2002 issue of *Occupational Hazards*. Bruce Main, PE, CSP, President of Design Safety Engineering, was a contributor.

REFERENCES

ALARA, Reference Library. *Glossary of Nuclear Terms*, Nuclear Regulatory Commission, www.nrc.gov.

ANSI B11.TR3-2000. *Risk Assessment and Risk Reduction — A Guide to Estimate, Evaluate and Reduce Risks Associated with Machine Tools*. McLean, VA: AMT (Association For Manufacturing Technology), 2000. www.mfgtech.org.

ANSI/RIA R15.06-1999. *Safety Requirements for Industrial Robots and Robot Systems*. Ann Arbor, MI: Robotics Industries Association, 1999 www.robotics.org.

"A Risky Profession Becomes a Little Safer." Section 4, *Chicago Tribune*, February 14, 2001.

Injury Facts, 2001 Edition. Itasca, IL: National Safety Council, 2001. www.nsc.org.

ISO/IEC Guide 51:1999(E), 2nd edition. Geneva, Switzerland: International Organization for Standardization, 1999.

Lewis, Norman. *The New Roget's Thesaurus in Dictionary Form*. New York: G. P. Putnam's Sons, 1978.

Lowrance, William F. *Of Acceptable Risk: Science and the Determination of Safety*. Los Altos, CA: William Kaufman, 1976.

Manuele, Fred A. *Innovations in Safety Management: Addressing Career Knowledge Needs*. New York: John Wiley & Sons, 2001.

Mikula, D. F. Kip. "Spacecraft Human-Rating System Safety — Beyond the Numbers." A paper presented at the American Institute of Aeronautics and Astronautics Space 2000 Conference and Exposition. Long Beach, CA: September 2000.

NASA-STD-8719.7, January 1998. *Facilities System Safety Handbook — NASA Standard*. Washington, DC: NASA.

SEMI S10-1996. *Safety Guideline for Risk Assessment*. Mountain View, CA: Semiconductor Equipment and Materials International, 1996 www.semi.org.

Stephenson, Joseph. *System Safety 2000*. New York: John Wiley & Sons, 1991.

Walton, Mary. *The Deming Management Method*. New York: The Putnam Publishing Group, 1986.

A hazard is identified, and it is assumed that injury or illness or damage can result if the potential of the hazard is realized. Or a hazard may be considered a violation of a standard or regulation. Almost automatically, the safety practitioner presents a recommendation addressing the hazard to the decision-makers.

In that process, little thought is given to the significance of the hazard in relation to other hazards, to the priority it deserves, or to the possible effectiveness of the measures proposed to achieve risk reduction. That doesn't speak well of real accomplishment or effective resource utilization.

In the real world, the safety professional has to recognize that:

- Some risks are more significant than others.
- Resources will always be limited, and staffing and money are never adequate to attend to all risks.
- The greatest good to employees, to employers, and to society is attained if available resources are applied to effectively and economically obtain risk reduction.

A safety professional implicitly has a responsibly to give the advice that results in

- Efficient use of resources, *on a priority basis*, to avoid, eliminate, or control hazards.
- Attaining a state for which the risks are judged to be acceptable.

GIVING PRIORITY TO SEVERITY POTENTIAL

Since resources are always limited, and since some risks are more significant than others, safety professionals must be capable of distinguishing the more important from the lesser important. They would, then, allocate the necessary time to those risks that have the greatest potential for severe harm or damage.

We can learn from what is known as Pareto's law. Pareto observed from analyses of monetary patterns that the significant items in a group will usually constitute a relatively small portion of the total. Those in financial fields often refer to Pareto's findings as the 80–20 rule, with 20% of the statistical body representing 80% of the total impact.

I have observed over the years, but not through scientific study, that Pareto's principle applies generally to employee injuries and illnesses, fires, auto incidents, product liability incidents, and environmental incidents.

A study known as "The Vital Few" made by Employer's of Wausau, an insurance company, indicates that

- 86% of total workers compensation injuries represent only 6% of the total cost;
- 14% of total injuries represent 94% of total costs; and
- 2% of total injuries (a part of the 14%) represent 70% of total costs.

This study included several hundred thousand cases. It supports Pareto's premise. Obviously, the 14% of total injuries representing 94% of the total costs include the most severe injuries.

Experiences of individual organizations will not fit that distribution precisely. But many safety directors with rather large statistical bases have also observed that the principle applies, generally. For example, just previous to this writing, discussions were held with a safety director who had produced his own analysis of severity potential. His results showed that 15% of worker injuries represented 85% of total costs. These differences do not contradict the 80–20 rule; they support it. Whether the percentage of severe cases moves up or down a bit from the preciseness of the 80–20 rule is not significant. The premise holds: A relatively small percentage of total incidents represent a very large part of the financial impact.

Assume that resources are limited and that a safety professional assumes a shared responsibility for having resources effectively applied. When giving hazards management advice, priorities of the employee, the employer, and society in general would be considered. From all viewpoints, it is obvious that hazards presenting the potential for the most severe harm or damage, those for which consequences are most costly, should be given the highest priority.

Whatever the field of endeavor — occupational safety, occupational health, product safety, transportation safety, fire protection engineering, et cetera — Pareto's law applies. And it prompts some interesting questions about whether we spend far too much time on the insignificant.

Chapter 8 is devoted to addressing severe injury potential. It makes the case that safety professionals must undertake separate and distinct activity to seek those hazards that present the most severe injury or damage potential so that they can be given priority consideration. To do that effectively, they must be capable of making hazards analyses and risk assessments.

SUBJECTIVITY IN HAZARDS ANALYSIS AND RISK ASSESSMENT

In Chapter 13, "Comments on Hazards and Risks," I discussed the unlikelihood of having accurate numbers representing the probability of incident occurrence and the severity of their consequences in making hazards analyses and risk assessments. I suggested that safety professionals be wary of numerologists, and of scoring systems whose creators suggest that they are to be the ultimate factor on which decisions are based.

Through my personal experiences, I developed an awareness of the folly of making elaborate computations based on subjective assumptions. While making those elaborate computations may create the appearance of being scientific, the activity is unprofessional when the work being done is based on many subjective judgments.

Fire protection engineers on my staff made many computations of property damage and business interruption loss estimates for their clients. A reasonable-worst-case hazard and exposure scenario — a modeling of an event — would be written. It would include assumptions about hazards being realized, where on the property the incident would most likely occur, the value of the facilities and equipment in that area, and the monetary value of the damage to property that could occur. Clients provided the values of properties used in the computations, and they were often inaccurate.

If a chemical was involved and its release could produce a vapor cloud, assumptions were made about the quantity of material released, its characteristics, the point of release, the shape of the vapor cloud that would develop, wind direction and speed, the barometric pressure, et cetera.

Following a long-used concept, the energy potential of the released material was converted into an equivalency for TNT. Computations would be made and circles drawn on maps indicating blast overpressures in pounds per square inch. Damage levels were reduced as the distance from the blast point increased.

Forgetting the subjectivity of the original assumptions, infinite and excruciating computations expressed as dollar loss estimates were made for a variety of blast overpressure circles. That was done even though it was understood that if one of the assumptions originally made — the variables — was slightly changed, the outcome could be substantively different.

Client personnel would participate in developing hazard and exposure scenarios. They understood the impact of making changes in the variables for which assumptions had been made and that loss estimates at best would be largely subjective.

I made the decision that, for the purposes of producing such property loss estimates, we would make computations to define only the 3-psi damage circle and assume that the value of the salvage within that circle would equal the value of the damage outside the circle. That greatly limited the calculations and avoided the appearance of being overly scientific. Thus, the property damage loss estimate would be the equivalent of 100% of the value within the 3-psi circle. That became known, initially in jest, as the Manuele Theory of Loss Estimating. And it was applied by many.

Charles A. Pacella, then Vice President and National Coordinator for Property Services at M&M Protection Consultants, made a comparative study that included a loss estimating system used extensively in the United States, two such systems commonly used in Europe, and the Manuele Theory of Loss Estimating. He wrote that

> The conclusion from this comparison is that the simplified method requires the least time and effort, has the fewest assumptions, and yields credible, realistic results.

Why should that history be relevant? It indicates that where subjective judgments prevail at the outset, little is gained in making laborious computations as the hazard analysis proceeds.

MAKING A HAZARD ANALYSIS PRECEDES AND IS NECESSARY TO CONCLUDING A RISK ASSESSMENT

Results of the loss estimate studies made by fire protection engineers represented the first part of a risk assessment. They began with hazard identification and, presuming that the hazard's potential was realized, considered that which was exposed to determine the possible consequences. *What was produced was a hazard analysis, always assuming the reasonable worst case.*

Risk is expressed as a combination of the probability of a hazards-related incident occurring and the severity of harm or damage that could result. A hazard analysis concludes with an estimate of the severity of the consequences of a hazard being realized. A hazard analysis does not require that the probability of an incident occurring be determined. Estimating incident probability is the additional and following step necessary in concluding a risk assessment.

DEVELOPING A HAZARD ANALYSIS AND RISK ASSESSMENT MATRIX

While the literature speaks of many hazards analyses and risk assessment techniques, I propose that a safety professional develop a matrix and a thought process that suits client needs.

Several texts include hazard analysis and risk assessment decision matrices. Every matrix I found has been adopted from those included in what was originally known as *Military Standard—System Safety Program Requirements, MIL-STD-882*. Its most recent version is now named *Standard Practice for System Safety, MIL-STD-882D, 2000*. Influence of that standard will be obvious in the remainder of this chapter.

In considering the development of a matrix and a thought process for its application, an awareness of reality will help.

- Because of staffing and time constraints, it is not possible to know of or to analyze all hazards. Since all hazards are not equal, subjective but learned judgments will be necessary concerning which hazards to study.
- Be aware that some situations defy statistical analysis.
- Keep it simple: You don't have to complicate things.
- Making hazards analyses and risk assessments is an art. It is not a science. Achieving absolute certainty in determining incident probability or consequence is not possible. A variation of a thought attributed to Descartes applies: If you can't know the truth, you ought to seek the most probable.
- To communicate with decision makers, terms must have been defined and agreed upon. While identical terms may be used in the several hazard analysis methods described in the literature, those terms may be given different meanings in the text material describing them.
- Also, in communicating with decision makers, it would be well to understand their perceptions and tolerance of risk, and appreciate that perceived risks as well as elements of employee and public fear and dread, along with client interests, may impact on risk decisions.
- Implementing a logical hazard analysis and risk assessment model is more important than which model is chosen.

HAZARD SEVERITY

Hazard severity categories displayed in Tables 14.1 and 14.2 are to provide guidance in developing a hazard analysis/risk assessment matrix. As will be evident, severity categories can be applied to the many subsets of the practice of safety. Table 14.1 is a composite reflecting several sources, my own views, and particularly MIL-STD-882D. Table 14.2 is more specific in designating severity levels. It is an adaptation from MIL-STD-882D and Sverdrup Technology publications (with permission).

Table 14.1. Hazard severity categories

Description	Category	Definition
Catastrophic	I	Death, permanent disability, system loss, devastating property damage or environmental damage
Critical	II	Severe injury or occupational illness, or major system, property, or environmental damage
Marginal	III	Minor injury or occupational illness, or minor system, property, or environmental damage
Negligible	IV	No occupational injury or illness, or system, property or environmental damage

Table 14.2. Hazard severity categories, adapted from MIL-STD-882D and Sverdrup Technology Publications

Category: Descriptive Word	People, Employees, Public	Facilities, Product, or Equipment Loss	Operations Down Time	Environmental Damage
Catastrophic	Fatality	Exceeds $1M	Exceeds 4 months	Major event, requiring several years for recovery
Critical	Disabling injury or illness	250K to $1M	2 weeks to 4 months	Event requires 1–5 years for recovery
Marginal	Minor injury or illness	1K to 250K	1 day to 2 weeks	Recovery time is less than 1 year
Negligible	No injury or illness	Less than 1K	Less than 1 day	Minor damage, easily repaired

Adapting a variation of Tables 14.1 and 14.2 will require developing an understanding of what the terms selected are to mean in an individual operation. Particularly, definitions are necessary of the ranges of consequence to which the terms such as *system loss or property damage, major or minor system or environmental damage*, and *severe and minor injury* and *occupational illness* apply if comparable terms are to be used.

HAZARD PROBABILITY

The probability that a hazards-related incident will occur is to be described in probable occurrences per unit of time, events, population, items, or

activity. A qualitative probability may be derived from research, analysis, and evaluations of the historical safety data on similar systems, as well as from a composite of opinions of knowledgeable people. Supporting rationale for assigning a hazard probability should be documented. Table 14.3 is an example of a qualitative hazard probability ranking. It is my composite, but borrows from MIL-STD-882D and the *Air Force System Safety Handbook.*

Table 14.3. Hazard probability rankings[a]

Probability Level	Category	Parameters
Frequent	A	Likely to occur repeatedly
Probable	B	Likely to occur several times
Occasional	C	Likely to occur sometime
Remote	D	Unlikely but possible to occur
Improbable	E	So unlikely, it can be assumed occurrence may not be experienced

[a]Definitions apply for the selected unit of time, events, population, items, or activity.

ACHIEVING ACCEPTABLE RISK LEVELS

Use of a combination of the hazard severity and hazard probability tables given allow a qualitative assessment of risk from which determinations can be made that risks are acceptable, or not acceptable, and from which priorities can be set for actions to be taken.

It must be understood that the charts on hazard severity and probability are to serve only as guides and that definitions of terms within them must be refined to suit the needs of a particular operation.

For further guidance, three examples are given in Tables 14.4, 14.5 and 14.6 indicating how a combination of the hazard severity and probability charts can be used to develop qualitative risk assessments. Table 14.4 is a Risk Assessment Matrix. Table 14.5 sets forth Management Decision Levels pertaining to the risk categories in Table 14.4. Remedial action or acceptance levels must be attached to the risk categories to permit intelligent management decision-making. Possibilities set forth in Table 14.4 are to serve as a base of reflection for those who craft a risk assessment matrix.

Table 14.6 is a Hazard/Risk Assessment Matrix that also includes suggested action levels. It is an adaptation of one of two examples

Table 14.4. Risk assessment matrix

Occurrence Probability	Severity of Consequence			
	Catastrophic	Critical	Marginal	Negligible
Frequent	High	High	Serious	Medium
Probable	High	High	Serious	Medium
Occasional	High	Serious	Medium	Low
Remote	Serious	Medium	Medium	Low
Improbable	Medium	Medium	Medium	Low

Table 14.5. Management decision levels

Risk Category	Remedial Action or Acceptance
High	Operation not permissible
Serious	Remedial action to have high priority
Medium	Remedial action to be taken in appropriate time
Low	Risk is acceptable: remedial action discretionary

Table 14.6. Hazard/risk assessment matrix[a]

Occurrence Probability	Severity of Consequences			
	Catastrophic—1	Critical—2	Marginal—3	Negligible—4
A—Frequent	1-A	2-A	3-A	4-A
B—Probable	1-B	2-B	3-B	4-B
C—Occasional	1-C	2-C	3-C	4-C
D—Remote	1-D	2-D	3-D	4-D
E—Improbable	1-E	2-E	3-E	4-E

Hazard Risk Index	Suggested Category
1-A, 1-B, 1-C, 2-A, 2-B, 3-A	Unacceptable: risk reduction action is necessary
1-D, 2-C, 2-D, 3-B, 3-C	Undesirable, written management decision required as to the corrective action to be taken, and when
1-E, 2-E, 3-D, 3-E, 4-A, 4-B	Acceptable, with management review
4-C, 4-D, 4-E	Acceptable, without management review

[a]It must not be assumed that for the two "acceptable" categories, action is not to be taken to eliminate or control the hazards.

of "Mishap Risk Assessment Values" in the *Air Force System Safety Handbook* (p. 24).

While the indication given in Table 14.5 for the "Low" risk category is "Risk is acceptable: remedial action discretionary," that does not mean that action would not be taken to reduce risk if the remedial action could stand a cost–benefit test. Also, remedial action is taken in some such situations for personnel relations purposes to reduce the fear factor when the risk is perceived by workers to be more significant than it is.

Going through the exercise of creating and reaching agreement on a risk assessment matrix adds immensely to a safety practitioner's effectiveness in communicating about risks and obtaining serious consideration of the remedial actions being recommended. That applies, whatever hazard analysis and risk assessment technique is used.

RISK IMPACT

To discriminate between hazards having the same hazard risk index, a risk impact determination is necessary. An impact determination consists of a review of the effect of an event economically, socially and politically. (*Example*: Release of a small amount of chemical into a stream may not cause measurable physical damage, but extreme political and social damage could result.)

RESIDUAL RISKS

No matter what actions are taken to avoid, eliminate, or control hazards, some residual risks will still exist. If the safety process meets its goal, none of the residual risks will be unacceptable for those operations undertaken or continued.

CONDUCTING A HAZARD ANALYSIS AND A RISK ASSESSMENT

For many hazards and the risks that derive from them, knowledge gained by safety practitioners through education and experience will lead to proper conclusions on how to attain an acceptable risk level, without bringing teams of people together for discussion. For the more complex situations, it is vital to seek the counsel of experienced personnel who are close to the work or process.

Reaching group consensus on the judgments made would be the goal. Sometimes, for what the safety practitioner considers obvious, having discussion and achieving consensus is still desirable so that buy-in is obtained for the actions to be taken and the expenditures to be made.

A general guide follows on how to make a hazard analysis, and then concluding with a risk assessment.

Whatever the simplicity or complexity of the hazard/risk situation, and whatever the analysis method used, the following thought and action process is applicable.

1. Establish the Analysis Parameters

Select a manageable task, system, process, or product to be analyzed, establish its boundaries and operating phase (standard operation, maintenance, startup), and define its interface with other tasks or systems, if appropriate.

Determine the scope of the analysis in terms of what can be harmed or damaged: people (the public, employees); property; equipment; productivity; and the environment.

2. Identify the Hazards

A frame of thinking should be adopted that gets to the bases of causal factors, which are hazards. This question would be asked: What are the characteristics of things or the actions or inactions of people that present a potential for harm.

Depending on the complexity of the hazardous situation, some or all of the following may apply.

- Use intuitive engineering and operational sense: This is paramount, throughout.
- Examine system specifications and expectations.
- Review codes, regulations, and consensus standards.
- Interview current or intended system users or operators.
- Consult checklists.
- Review studies from other similar systems.
- Consider the potential for unwanted energy releases and exposures to hazardous environments.
- Review historical data: industry experience, incident investigation reports, OSHA and National Safety Council data, manufacturer's literature.
- Brainstorm.

3. Consider the Failure Modes

Define the possible failure modes that would result in realization of the potentials of hazards. Ask the question, How could the undesirable event happen?

4. Determine the Frequency and Duration of Exposure, and What is Exposed to Harm or Damage

For each harm or damage category selected in step 1 for the scope of the analysis (people, property, etc.), estimate the frequency and duration of exposure to the hazard (the frequency and duration of endangerment) and the number of people and the extent of the property that is exposed to harm or damage. This is a very important part of this exercise. More judgments than one might realize will be made in this process.

5. Assess the Severity of Consequences

Learned speculations are to be made on the consequences of an occurrence: the number of fatalities, injuries, or illnesses; the value of property or equipment damaged; the time for which productivity will be lost; and the extent of environmental damage. Historical data can be of great value as a baseline. On a subjective basis, the goal would be to decide on the worst credible consequences should an incident occur, not the worst conceivable consequence. When the severity of consequence is determined, a hazard analysis will have been completed.

6. Determine Occurrence Probability

Unless empirical data are available, and that would be a rarity, the process of selecting the probability of an incident occurring will again be subjective. For the more complex hazard scenario, brainstorming with knowledgeable people is advantageous.

Probability has to be related to an interval base of some sort, such as a unit of time or activity, events, units produced, or the life cycle of a facility, equipment, process, or a product.

7. Define the Risk

Conclude with a statement that addresses both the probability of an incident occurring and the expected severity of adverse results. Categorize each risk as acceptable or unacceptable.

8. Rank Risks in Priority Order

To properly communicate with decision makers, a risk ranking system should be adopted so that priorities can be established. Since the hazard analysis and risk assessment exercise is subjective, the risk ranking system would also be subjective.

9. Develop Remediation Proposals

When required by the results of the risk assessment, alternate proposals for the design and operational changes necessary to achieve an acceptable risk level would be recommended. In their order of effectiveness, the action listing shown in "The Safety Decision Hierarchy" mentioned in Chapter 15, "Acceptable Risk," would be the base upon which remedial proposals are made. For each proposal, remediation cost would be determined and an estimate of its effectiveness in achieving risk reduction would be given.

Care should be taken that remedial actions do not introduce new hazards. If that occurs, the risk is to be reevaluated and other countermeasures proposed.

Having an accepted and well-understood risk assessment matrix makes reaching consensus easier to assess the severity of consequences, determine event probability, define the risk, and rank risks in priority order.

Although a hazard analysis and a risk assessment would result from applying the preceding outline, good management requires that the remaining steps in "The Safety Decision Hierarchy" be taken, which are—decide and take action, and measure for effectiveness.

For a more thorough discussion of hazard analysis and risk assessment, I refer the reader to the chapter titled "A Primer on Hazard Analysis and Risk Assessment" in the book *Innovations in Safety Management: Addressing Career Knowledge Needs*.

RISK ASSESSMENT TECHNIQUES

How many risk assessment techniques are there? Pat Clemens gave brief descriptions of 25 techniques in "A Compendium of Hazard Identification & Evaluation Techniques for System Safety Applications"; in the *System Safety Analysis Handbook*, 101 methods are described.

As a beginning, a safety practitioner should be learned in at least three of those techniques. They are *preliminary hazard analysis, what-if analysis*, and *failure modes and effects analysis*. Comments follow on

those techniques, taken from the previously mention chapter titled "A Primer on Hazard Analysis and Risk Assessment" in *Innovations in Safety Management.*

Preliminary Hazard Analysis (PHA)

The original intent of the preliminary hazard analysis technique was to serve as the initial effort to identify and evaluate hazards in the early stages of the design process. But, in actual practice the technique has attained broader use. The principles on which preliminary hazard analyses are based are used not only in the initial design process, but also in reassessing the safety of existing products or operations.

For example, the hazard analysis and risk assessment requirements of the European Standard ISO 14121, *Safety of Machinery—Principles for risk assessment* (formerly EN 1050), have been adequately met in some companies in the design or redesign stages by applying an adaptation of the preliminary hazard analysis technique.

Furthermore, when simpler techniques (i.e., what-if analyses, checklist analyses) reveal hazardous situations needing additional review, the substance of the preliminary hazard analysis technique may be used. In reality, the technique needs a new name because it has achieved broader use than the original intent, which was as a preliminary assessment system to be used in early concept and design stages for a product or system.

Headings on preliminary hazard analysis forms will include the typical identification data: date, names of evaluators, department, and location. The following information is typically included in a preliminary hazard analysis form.

- A hazard description, sometimes called a hazard scenario.
- A description of the task, operation, system, or product being analyzed.
- Which exposures are the subject of the analysis: people (employees, the public); facility, product or equipment loss; operation downtime; environmental damage.
- The probability interval to be considered: unit of time or activity; events; units produced; life cycle.
- A numerical or alpha indicator for the severity of harm or damage that might result if the hazard's potential is realized.
- A numerical or alpha indicator for the occurrence probability.
- A risk assessment code, using the agreed-upon risk assessment matrix.
- Remedial action to be taken, if risk reduction is needed.

A communication accompanies the analysis, explaining the assumptions made and the rationale for them. Comment would be made on the assignment of responsibilities for the remedial actions to be taken, and when. An example of a preliminary hazard analysis worksheet appears as Addendum A in this chapter, courtesy of Sverdrup Technologies, Inc. This form requires entry of severity, probability, and risks codes before and after countermeasures are taken.

What-If Analysis

For a what-if analysis, a group of people (as few as two, but often several more) would use a brainstorming approach to identify hazards, hazard scenarios, how incidents can occur, and what their probable consequences might be.

Questions posed in the brainstorming session may commence with What-if, as in "What if the air conditioning fails in the computer room?," or may be expressions of more general concern, as in "I worry about the possibly of spillage and chemical contamination during truck offloading."

In a typical procedure, all of the questions are recorded and then assigned for investigation. Each subject of concern is then addressed by one or more team members. They would consider the potential of the hazardous situation and the adequacy or inadequacy of risk management controls in effect, suggesting additional risk reduction measures if appropriate.

Checklist Analysis

Checklists are primarily used when published standards, codes, and commonly accepted industry practices exist. There are many such checklists. They consist of lists of questions pertaining to the applicable standards and practices—usually with a yes or no or not applicable response. Their purpose is to identify deviations from the expected, and thereby possible hazards. A checklist analysis requires a walk-through of the area to be surveyed.

Checklists are easy to use and provide a cost-effective way to identify customarily recognized hazards. Nevertheless, the quality of checklists is dependent on the experience of the people who develop them. Furthermore, they must be crafted to suit particular needs. If a checklist is not complete, the analysis may not identify some hazardous situations.

What-If/Checklist Analysis

A what-if/checklist hazard analysis technique combines the creative, brainstorming aspects of the what-if method with the systematic approach of the

checklist. The combination of techniques can compensate for the weaknesses of each. The what-if part of the process, using a brainstorming method, can help the team identify hazards that have the potential to be the causal factors for incidents, even though no such incidents have yet occurred. The checklist provides a systematic approach for review that can serve as an idea generator in the brainstorming process. Usually, a team experienced in the design, operation, and maintenance of the operation performs the technique. The number of people required depends, of course, on the operation's complexity.

Failure Modes and Effects Analysis (FMEA)

In several industries (automobiles, semiconductors), failure modes and effects analysis has been the technique of choice by design engineers for reliability and safety considerations. They are used to evaluate (a) the ways in which equipment fails and (b) the response of the system to those failures. Although an FMEA is typically made early in the design process, the technique can also serve well as an analysis tool throughout the life of equipment or a process.

For each item of equipment, an FMEA produces qualitative, systematic lists that include the failure modes, the effects of each failure, safeguards that exist, and additional actions that may be necessary. For example, for a pump, the failure modes would include the following: fails to stop when required; stops when required to run; seal leaks or ruptures; and pump case leaks or ruptures. Both the immediate effects and the impact on other equipment would be recorded. Generally, when analyzing impacts, the probable worst case is assumed and analysts would conclude that existing safeguards are or are not sufficient.

Although an FMEA can be made by one person, it's typical for a team to be appointed when there is complexity. In either case, the traditional process, as follows, is similar.

1. Identify the item or function to be analyzed.
2. Define the failure modes.
3. Record the failure causes.
4. Determine the failure effects.
5. Enter a severity code and a probability code for each effect.
6. Enter a risk code.
7. Record the actions required to reduce the risk to an acceptable level.

Note that the FMEA process described here requires entry of probability, severity, and risk codes. A typical FMEA form in which such entries would be made is provided as Addendum B, courtesy of Sverdrup Technology, Inc.

The FMEA technique is principally a design and redesign analysis tool. Safety practitioners who become involved in the design aspects of safety would benefit greatly by having knowledge of the technique.

INFLUENCE OF ORGANIZATIONAL CULTURE

Incidents for which consequences are graded as catastrophic and critical must be addressed. Most such incidents would have low occurrence probabilities. In the decision-making for those events, an organization's culture would be determinant — its values, its concern for its employees and the public, its sense of responsibility, and its assumptions with respect to the risk it can bear.

This sort of question, considered from many views, would be typically asked in the decision process: If it happens, can we stand it? Aspects of an organization's culture cannot be fitted into a risk assessment system.

INITIATING A HAZARD ANALYSIS AND RISK ASSESSMENT SYSTEM

If a safety professional initiates a more formal procedure for hazard analysis and risk assessment, thought should be given to how those measures might succeed. It may be that what is being proposed requires a significant change in management practice. Thus, the concepts applicable in successfully achieving change would apply. Too much at one time may be disruptive.

A planned effort will be necessary to convince decision makers that the safety professional's counsel on hazard analysis and risk assessment can be of value. Small steps forward, proving value, are recommended. In preparing for such an endeavor, I suggest that safety professionals:

- Develop an awareness of the risk tolerance beliefs held by decision makers.
- Study the approach to be made to decision makers; consider history, risk tolerance, their needs, and how decision makers could be influenced to conclude that what is being proposed is of value in their achieving their goals.
- Work with a team of knowledgeable people and obtain agreement on the benefits to be obtained from the use of an additional hazard analysis and risk assessment system, the methodologies to be used,

and the meanings of terms in the hazard analysis/risk assessment decision matrix developed.

- Determine which risks deserve priority consideration.
- Select one or two higher category hazard/risk situations.
- Follow the outline under "Conducting a Hazard Analysis/Risk Assessment."
- Continue to try, assess, modify, and try again.

RESOURCES ON HAZARD ANALYSIS AND RISK ASSESSMENT

Many hazard analysis and risk assessment techniques have been developed. These are just a few of the methodologies mentioned in the literature: *preliminary hazard analysis; gross hazard analysis; hazard criticality ranking; catastrophe analysis; change analysis; energy flow/barrier analysis; energy transfer analysis; event tree analysis; human factors review; the hazard totem pole*; and *double failure analysis*. There are many other hazard analysis systems.

For an education in hazard analysis and risk assessment, these references are suggested.

- "A Compendium of Hazard Identification and Evaluation Techniques for System Safety Applications" by P. L. Clemens
- *System Safety Engineering and Management* by Harold E. Rowland and Brian Moriarty
- *System Safety 2000* by Joe Stephenson
- *System Safety Analysis Handbook, a Sourcebook for Safety Practitioners* by Richard Stephan and Warner W. Talso
- *MORT Safety Assurance Systems* by William G. Johnson
- *Safety and Health For Engineers* by Roger L. Brauer
- *Managing Risk: Systematic Loss Prevention For Executives* by Vernon L. Grose
- *Standard Practice for System Safety*, MIL-STD-882D, Department of Defense
- *Air Force System Safety Handbook*

CONCLUSION

Professional safety practice requires that hazards be analyzed, that the risks deriving from those hazards be assessed, and that a risk ranking system be utilized. Also, it must be understood that hazard analysis is the first step in the safety process, and that the quality of all other safety initiatives follows the quality of hazards analyses.

REFERENCES

Air Force System Safety Handbook. Kirtland AFB, NM: Air Force Safety Agency, 2000.

Brauer, Roger L. *Safety and Health for Engineers*. New York: John Wiley & Sons, 1990.

Clemens, Pat. "A Compendium of Hazard Identification and Evaluation Techniques for System Safety Applications." *Hazard Prevention*, March/April 1982.

Failure Mode and Effects Analysis (FMEA): A Guide for Continuous Improvement for the Semiconductor Equipment Industry. Sematech. 1992. At http://www.sematech.org.

Grose, Vernon L. *Managing Risk: Systematic Loss Prevention for Executives*. Englewood Cliffs, NJ: Prentice-Hall, 1987.

Johnson, William G. *MORT Safety Assurance Systems*. New York: Marcel Dekker, 1980.

Manuele, Fred A. *Innovations in Safety Management: Addressing Career Knowledge Needs*. New York: John Wiley & Sons, 2001.

Pareto's Law and the "Vital Few." Wausau, WI: Employers of Wausau, undated.

Potential Failure Mode and Effects Analysis (FMEA). Detroit, MI: Automotive Industry Action Group.

Rowland, Harold E. and Brian Moriarty. *System Safety Engineering and Management*. New York: John Wiley & Sons, 1991.

Safety of Machinery—Principles for risk assessment, International Standard ISO 14121 (formerly EN 1050). Geneva, Switzerland: International Organization for Standardization, 1999.

Standard Practice For System Safety, MIL-STD-882D. Washington: DC: Department of Defense, 2000.

Stephans, R. A. and W. W. Talso. *System Safety Analysis Handbook*, 2nd edition. Albuquerque, NM: New Mexico Chapter of the System Safety Society, 1997.

Stephenson, Joe. *System Safety 2000*. New York: John Wiley & Sons, 1991.

Sverdrup Technologies, Inc. Safety Literature at http://www.sverdrup.com/safety.