CHAPTER 11

A PRIMER ON HAZARD ANALYSIS AND RISK ASSESSMENT: SECTIONS 4.2 AND 5.1.1 OF Z10

Requirements for risk assessment and prioritization within an occupational safety and health management system are introduced in Section 4.2 of Z10: *Processes are to be in place to: assess management system issues and assess the level of risk for identified hazards; establish priorities based on factors such as the level of risk; and identify underlying causes and other contributing factors related to system deficiencies that lead to hazards and risks.*

In the advisory column at E4.2, it is said that the method of assessment should be selected *based on the type of issue, nature of risk, or operations and that various methods may be used in determining the level of risk imposed.* Organizations are advised that priorities are to be set based on several factors, such as *issues requiring immediate attention; opportunities having the greatest potential for improvement or risk reduction; organizational, resource, participation, or accountability issues; and issues with the highest impact or severity.*

E4.2 encourages employers to give consideration not only to hazards that relate to the high probability of incident occurrence but also to hazards that relate to low-probability/serious-consequence events.

It is stated clearly that assessments conducted for Section 4.2 are for the prioritizing of occupational health and safety issues and that they may not be sufficient for the requirements of Section 5.1.1, "Risk Assessments," or to determine the appropriate hazard controls as outlined in Section 5.1.2, "Hierarchy of Controls." Appendix D provides guidance on assessment and prioritization.

Advanced Safety Management: Focusing on Z10 and Serious Injury Prevention, Second Edition. Fred A. Manuele.

An important step forward was taken by adding a provision in the 2012 version of Z10 requiring that risk assessments be made. The requirement is simply stated and the advisory comments are brief. Section 5.1.1 states in its entirety that:

> *The organization shall establish and implement a risk assessment process(es) appropriate to the nature of hazards and level of risk.*

Little is said about risk assessments in the advisory column at E5.1.1. Organizations are informed that:

> *Assessing risks can be done using quantitative (numeric) or qualitative (descriptive) methods. There are many methods of risk assessment. The organization should select methods appropriate to the hazards and type of process.*

Appendix F, "Risk Assessment," has been lengthened considerably and now includes a broader overview of risk assessment processes and data on several risk assessment methods. The bibliography, Appendix O, also lists several risk assessment resources.

Safety professionals can expect that being able to make documented risk assessments will be necessary for their job retention and career enhancement. That premise has acquired weight because of the more frequent inclusion in safety standards and guidelines of provisions requiring that hazards be identified and analyzed and that risk assessments be made. Examples of recently approved examples follow.

- ANSI/ASSE Z590.3-2011: *Prevention Through Design: Guidelines for Addressing Occupational Hazards and Risks in Design and Redesign Processes*
- ANSI/AIHA Z10-2012: *Occupational Health and Safety Management Systems*
- CSA Z1002-12: *Occupational Health and Safety—Hazard Identification and Elimination and Risk Assessment and Control,* issued by the Canadian Standards Association

Other standards and guidelines having such provisions are discussed in Chapter 11, "Provisions for Risk Assessments in Standards and Guidelines".

Since safety professionals are to analyze hazards and assess the risks that derive from them, the question logically follows: What do they need to know? The intent of this chapter is to provide a primer that will serve many of the hazard analysis and risk assessment needs that safety professionals will encounter. In this chapter we:

- Define the terms that must be understood in the hazard analysis and risk assessment process
- Establish the parameters for a hazard analysis
- Indicate how a hazard analysis is extended into a risk assessment
- Establish that the goal is to achieve acceptable risk levels
- Include a hazard analysis and risk assessment guide

- Give examples of the terms used in risk assessment matrices, and their variations
- Present examples of basic two-dimensional risk assessment matrices
- Describe several of the most commonly used hazard analysis and risk assessment techniques

DEFINING HAZARD, HAZARD ANALYSIS, RISK, AND RISK ASSESSMENT

When a safety professional identifies a hazard and its potential for harm or damage and decides on the probability that an injurious or damaging incident can occur, a subjective risk assessment has been made. In doing so, for the simpler and less complex hazards and risks, the assessment may be based entirely on a priori knowledge and experience, without documentation. Making informal risk assessments has been an integral part of the practice of safety and health professionals from time immemorial.

Recent developments take the risk assessment subject to a higher level within the practice of safety. By formalizing the hazard analysis and risk assessment process, a better appreciation of the significance of individual risks is achieved. As risk levels are categorized and prioritized, more intelligent decisions can be made with respect to their elimination or reduction. For the hazard analysis and risk assessment process, it is necessary that agreement be reached on the definitions of hazards, hazards analyses, risks, and risk assessments.

ANSI/AIHA Z10 is an occupational health and safety management systems standard, and its definitions of hazard and risk are, understandably, worker injury and illness related. They do not include considerations for injury to the public, possible damage to the environment or damage to property, or business downtime. This chapter has a broader purpose than Z10, as will be seen.

- A *hazard* is defined as the potential for harm to people, property, or the environment. If there is no potential for harm, injury or damage cannot occur. (In Z10, a hazard is defined as *a condition, set of circumstances, or inherent property that can cause injury, illness, or death.*) The dual nature of hazards must be understood. Hazards encompass all aspects of technology or activity that produce risk. Hazards include the characteristics of things and the actions or inactions of people.
- A hazard analysis is made to estimate the severity of harm or damage that could result from a hazard-related incident or exposure. The hazard analysis process need not include an estimate of incident or exposure probability. Examples of hazards analyses that do not include probability indicators are the estimates made by fire protection engineers of maximum foreseeable loss or maximum probable loss for insurance purposes, and the hazard analysis requirements of *OSHA's Rule For Process Safety Management Of Highly Hazardous Chemicals,* 29 CFR 1910.119.

- Whether hazardous situations are simple or complex, the process for making a hazard analysis will address the following questions:
  1. Is there potential for harm deriving from aspects of the technology or activity, the characteristics of things, or the actions or inactions of people?
  2. Can the potential be realized?
  3. Who and what are exposed to harm or damage?
  4. What is the frequency of endangerment?
  5. What will the consequences be (i.e., the severity of harm or damage) if the potential of a hazard is realized?
- Making a hazard analysis is necessary to and precedes making a risk assessment. William Johnson said this about hazard analysis in *MORT Safety Assurance Systems*: "Hazard analysis is the most important safety process in that, if that fails, all other processes are likely to be ineffective." Johnson's premise is stated soundly.
- *Risk* is defined as an estimate of the probability of a hazards-related incident or exposure occurring and the severity of harm or damage that could result. (Z10 defines risk as *an estimate of the combination of the likelihood of an occurrence of a hazardous event or exposure(s), and the severity of injury or illness that may be caused by the event or exposures.*)
- *Probability* is defined as the likelihood of a hazard's potential being realized and initiating an incident or exposure that could result in harm or damage for a selected unit of time, events, population, items, or activity being considered.
- *Severity* is defined as the extent of harm or damage that could result from a hazard-related incident or exposures.
- *Risk assessment* is a process that begins with hazard identification and analysis, followed by an estimate of the probable extent of severity of harm or damage if an incident or exposure occurs, concluding with an estimate of the probability of the incident or exposure occurring.

In a statement indicating risk level, both probability of occurrence and severity of outcome must be included. After determining the severity of expected damage or harm through a hazard analysis, estimating the probability of an incident or exposure occurring is the additional and necessary step in concluding a risk assessment.

These excerpts from the *Framework for Environmental Health Risk Management* issued by The Presidential/Congressional Commission on Risk Assessment and Risk Management are an indication of the widespread adoption of the foregoing definitions.

What Is "Risk"

Risk is defined as the probability that a substance or situation will produce harm under specified conditions. Risk is a combination of two factors:

- The *probability* that an adverse event will occur;
- The *consequences* of the adverse event.

Risk encompasses impacts on public health and on the environment, and arises from *exposure* and *hazard*. Risk does not exist if exposure to a harmful substance or situation does not or will not occur. Hazard is determined by whether a particular substance or situation has the potential to cause harmful effects.

MAKING A HAZARD ANALYSIS/RISK ASSESSMENT

For many hazards and the risks that derive from them, knowledge gained by safety professionals 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 familiar with the work or process. Reaching group consensus is a highly desirable goal. Sometimes, for what a safety professional considers obvious, achieving consensus is still desirable so that buy-in is obtained for the actions to be taken. A general guide follows on how to make a hazard analysis and how to extend the process into a risk assessment.

This guide is applicable to every phase of the life cycle of facilities, equipment, processes, and materials (e.g., design, construction, operation, maintenance, and disposal).

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

A Hazard Analysis and Risk Assessment Guide.

1. **Select a risk assessment matrix.** A risk assessment matrix provides a method to categorize combinations of probability and severity, thus establishing risk levels. A matrix helps in communicating with decision makers and influencing their decisions on risks and the actions to be taken to ameliorate them. Also, risk assessment matrices can be used to compare and prioritize risks and to effectively allocate mitigation resources.

   Definitions of the levels of probability and severity used in risk assessment matrices vary greatly. That reflects the differences in the perceptions people have of risk. Since a risk assessment matrix is a management decision tool, management personnel at appropriate levels must agree on the definitions of the terms to be used. In so doing, management establishes the levels of risk that require reduction and those that are acceptable.

   Repeating for emphasis: Safety professionals must understand that definitions of terms for incident probability and severity and for risk levels vary greatly. Thus, they should tailor a risk assessment matrix to suit the hazards and risks and the management tolerance for risk with which they deal. Examples of definitions used for incident probability and severity are presented here as well as for risk categories and risk assessment matrices.

They are to provide safety professionals with a broad base of information from which choices can be made in developing the matrix considered appropriate for their clients' needs.

The breadth of possibilities in drafting a risk assessment matrix is extensive. Matrices have been developed that display only one or a combination of several of the following injury or damage classes: employees, members of the public, facilities, equipment, product, operation downtime, and the environment.

For this primer, two-dimensional risk assessment matrices are discussed. They are displays of variations for two categories of terms: the *severity* of harm or damage that could result from a hazards-related incident or exposure, and the *probability* that the incident or exposure could occur. They also show the *risk levels* that derive from the various combinations of severity and probability.

A review of three-and four-dimensional risk assessment systems is given in Chapter 13, "Three and Four Dimensional Numerical Risk Scoring Systems".

2. **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, the environment.
3. **Identify the hazards.** A frame of thinking should be adopted that gets to the bases of causal factors, which are hazards. These questions would be asked: What are the aspects of technology or activity that produces risk? 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 similar systems.
   - Consider the potential for unwanted energy releases.
   - Take into account possible exposures to hazardous environments.
   - Review historical data: industry experience, incident investigation reports, OSHA and National Safety Council data, manufacturers' literature.
   - Brainstorm.

4. **Consider the failure modes.** Define the possible failure modes that would result in realization of the potentials of hazards. Ask: What circumstances can arise that would result in the occurrence of an undesirable event? What controls are in place that mitigate against the occurrence of such an event or exposure? How effective are the controls?

5. **Determine the frequency and duration of exposure.** For each harm or damage category selected for the analysis (people, property, business interruption, etc.), estimate the frequency and duration of exposure to the hazard. This is a very important part of this exercise. For example, in a workplace situation, ask: How often is a task performed, how long is the exposure period, and how many people are exposed? More judgments than one might realize will be made in this process.

6. **Assess the severity of consequences.** The purpose is to determine the magnitude of harm or damage that could result. Informed speculations are made to establish the consequences of an incident or exposure: the number injuries or illnesses and their severity, and fatalities; 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 value as a baseline but should not be treated as the primary or sole determinant. Judgment of knowledgeable and competent personnel should prevail.

   On a subjective basis, the goal is to decide on the worst credible consequences should an incident or exposure occur, not the worst conceivable consequence.

When the severity of the outcome of a hazard-related incident or exposure is determined, a hazard analysis has been completed.

7. **Determine occurrence probability.** Extending the hazard analysis into a risk assessment requires the one additional step of estimating the likelihood, the probability, of a hazardous event or exposure occurring. Unless empirical data are available, and that would be a rarity, the process of selecting incident or exposure probability is subjective. As is the case when determining severity of consequences, historical data can be of value as a baseline but should not be the sole determinant. Judgment of knowledgeable and competent personnel, controls in place and their capability, and lessons learned with respect to similar systems should prevail.

   For the more complex hazardous situations, it should be considered a necessity that brainstorming sessions be held with knowledgeable people and that consensus be reached in determining occurrence probability.

   To be meaningful, 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.

8. **Define the initial risk.** Conclude with a statement that addresses the probability of a hazard-related incident or exposure occurring, the expected severity of

adverse results, and a risk category (e.g., – high, serious, moderate, or low). Using a risk assessment matrix for that purpose assists in communicating on the risk level.

9. **Risk prioritization.** A risk ranking system should be adopted so that priorities can be established. Since the risk assessment exercise is subjective, the risk ranking system would also be subjective. Prioritizing risks gives management the knowledge needed for intelligent allocation of resources with respect to risk avoidance, elimination, or control.
10. **Select and implement risk reduction and control methods.** When the initial risk assessment indicates that elimination or reduction measures are to be taken to achieve acceptable risk levels:
    - Alternative proposals for the design and operational changes necessary would be recommended.
    - In their order of effectiveness, the actions outlined in Chapter 14, "Hierarchy of Controls", would be the basis upon which remedial proposals are made.
    - If informal judgments on costs are considered inadequate for a risk situation, formal action would be taken to establish remediation cost for each proposal and an estimate would be given of its effectiveness in achieving risk reduction to an acceptable risk level.
    - Risk avoidance, elimination, or reduction methods would be selected and implemented.
    - A tracking system should be put in place to assure completion of the actions undertaken.
11. **Assess the residual risk.** *Residual risk* is defined as the risk remaining after preventive measures have been taken. No matter how effective the preventive actions, there will always be residual risk if a facility exists or an activity continues. Attaining zero risk is not possible.
    - If the residual risk is not acceptable, the action outline set forth in this hazard analysis and risk assessment process would be applied again.
    - The risk assessment process is to continue until an acceptable risk level is attained.
    - If an acceptable risk level cannot be achieved, operations should not be continued, except in unusual and emergency circumstances or as a closely monitored and limited exception and with the approval of the person who has the authority to accept the risk.
    - Information on residual risks is to be communicated to relevant downstream stakeholders so that they can use this information in their own risk assessments.

Even though the residual risk may be acceptable, management should consider taking additional risk reduction measures if the cost is reasonable, particularly if so doing resolves concerns of employees.

12. **Risk acceptance decision making.** Risk acceptance decisions shall be made at the appropriate management levels.
    - Temporary acceptance of high and serious risks shall be made at the top management level.
    - Responsibility for moderate or low risks may be assigned to lower management levels.
13. **Documentation.** To the extent appropriate for a given risk situation, documentation should include the:
    - The names and job titles/qualifications of the persons who did the risk assessment
    - The risk assessment method(s) used
    - Hazards identified
    - Risks deriving from the hazards
    - Avoidance, elimination, reduction, and control measures taken to attain acceptable risk levels

    In certain cases, consideration would be given to additional documentation that includes relevant information about the use, effectiveness of design, problems during startup and continued use, and changes to designs over the life cycle of the design.

    The foregoing applies whether the documentation is done directly under the direction of management or by a supplier of services.
14. **Reassess the risk:** follow up on actions taken. This step is a part of all effective problem-solving exercises. Follow-up activity would determine that the:
    - Problem was resolved, only partially resolved, or not resolved, and that acceptable risk levels were or were not achieved.
    - Actions taken did or did not create new hazards.

If acceptable risk levels were not achieved or new hazards were introduced, the risk is to be reevaluated and other countermeasures are to be proposed and taken.

DESCRIPTIONS: PROBABILITY AND SEVERITY

Examples follow in Tables 11.1 to 11.5 to show variations in the terms and their descriptions as used in a variety of applied risk assessment processes for the probability of occurrence and severity of consequence. There is no single correct method of selecting probability and severity categories and their descriptions. Tables 11.4 to 11.6 show how severity of harm or damage categories can be related to several types of adverse consequences and levels of harm or damage.

TABLE 11.1 Example A: Probability Descriptions

Descriptive Word	Probability Descriptions
Frequent	Likely to occur repeatedly
Probable	Likely to occur several times
Occasional	Likely to occur sometime
Remote	Not likely to occur
Improbable	So unlikely that one can assume occurrence will not be experienced

TABLE 11.2 Example B: Probability Descriptions

Descriptive Word	Probability Descriptions
Frequent	Occurs often, experienced continuously
Probable	Occurs several times
Occasional	Occurs sporadically, occurs sometimes
Seldom	Remote chance of occurrence; unlikely but could occur sometime
Unlikely	Can assume that incident will not occur

TABLE 11.3 Example C: Probability Descriptions

Descriptive Word	Probability Descriptions
Frequent	Could occur annually
Likely	Could occur once in two years
Possible	Would occur no more than once in five years
Rare	Would occur no more than once in 10 years
Unlikely	Would occur no more than once in 20 years

TABLE 11.4 Example A: Severity Descriptions for Multiple Harm and Damage Categories

Catastrophic	Death or permanent total disability, system loss, major property damage, and business downtime
Critical	Permanent, partial, or temporary disability in excess of three months, major system damage, significant property damage, and downtime
Marginal	Minor injury, lost-workday accident, minor system damage, minor property damage, and little downtime
Negligible	First aid or minor medical treatment, minor system impairment

TABLE 11.5 Example B: Severity Descriptions for Multiple Harm and Damage Categories

Catastrophic	One or more fatalities, total system loss, chemical release with lasting environmental or public health impact
Critical	Disabling injury or illness, major property damage and business downtime, chemical release with temporary environmental or public health impact
Marginal	Medical treatment or restricted work, minor subsystem loss or damage, chemical release triggering external reporting requirements
Negligible	First aid only, nonserious equipment or facility damage, chemical release requiring only routine cleanup without reporting

TABLE 11.6 Example C: Severity Descriptions for Multiple Harm and Damage Categories

Category: Descriptive Word	Facilities; People: Employees, Public	Product or Equipment Loss	Operations Downtime	Environmental Damage
Catastrophic	Fatality	Exceeds $3 million	Exceeds 6 Months	Major event, requires more than 2 years for full recovery
Critical	Disabling injury or illness	500,000 to $3million	4 weeks to 6 months	Significant event, injury or requires 1 to 2 years for full recovery
Marginal	Minor injury or illness	50,000 to 500,000	2 days to 4 weeks	Recovery time is less than 1 year
Negligible	Injury requires only first aid	Less than 50,000	Less than 2 days	Minor damage, easily repaired, little time for recovery

EXAMPLES OF RISK ASSESSMENT MATRICES

Five examples of risk assessment matrices follow. Shown here in Table 11.7 is an adaptation of the "Risk Assessment Matrix" in MIL-STD-882E, the Department of Defense, *Standard Practice for System Safety*. (p. 11) MIL-STD-882, first issued in 1969, is the grandfather of risk assessment matrices. All of the over 30 variations of matrices that I have collected include the basics found in the 882 standard. They include event probability categories, severity of harm or damage ranges, and risk gradings.

TABLE 11.7 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
Eliminated	This category is used only for identified hazards that are totally removed			

TABLE 11.8 Risk Scoring System: B155.1-2011[a]

Probability Level	Severity Category			
	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	Low	Low

[a]Identified in B155.1-2011 as MIL STD 882: Two-Factor Risk Model [4×5].

The risk scoring system shown in Table 11.8 appears in the ANSI/PMMI B155.1-2011 standard titled *Safety Requirements for Packaging Machinery and Packaging-Related Converting Machinery* (p. 53). It is shown here for two reasons. It is an indication of the validity of the concepts on which the risk assessment matrices in MIL-STD-882 are based and why so many developers of matrices use 882 as a reference.

Table 11.8 is almost identical with the 882 version shown in Table 11.7 except for the addition of an "eliminated" probability category in the 882 model. But there is one other slight difference: People who drafted B155.1 made a change in one risk severity category.

As noted previously, people who develop risk assessment matrices work their own risk perceptions into them. And that's great. Safety professionals should feel free to do so too.

Table 11.9 shows a risk assessment matrix that combines types of severity categories and uses alphabetical risk gradings.

Table 11.10 is close to a risk assessment matrix shown in Annex E of the original version of Z10. Its uniqueness is that it was a broadly published matrix that includes not only probability and severity categories and descriptive data for each category but also advice on decision making and remedial action for each risk category.

As the matrix in Table 11.10 was developed, one of the participants thought that the risk levels presented were one step too high in two places. In the discussion that

TABLE 11.9 Risk Assessment Matrix: Alphabetical Risk-Level Indicators: Probability That Something Will Go Wrong[a]

Severity Categories	Frequent: Likely to occur immediately or soon	Likely: Quite likely to occur often	Occasional: May occur in time	Seldom: Not likely to occur but possible	Unlikely: Unlikely to occur
Catastrophic: death, multiple injuries, severe property or environmental damage	E	E	H	H	M
Critical: serious injuries, significant property or environmental damage	E	H	H	M	L
Marginal: may cause minor injuries, financial loss, negative publicity	H	M	M	L	L
Negligible: minimum threat to persons or damage to property	M	L	L	L	L

[a]E, extremely high risk; H, high risk; M, moderate risk; L, low risk.

followed, it was agreed that changes could be made. What is the significance of this? Risk assessment is more art than science. Since establishing risk levels is largely a matter of judgment, people will come to different conclusions in a given situation. Nevertheless, the ultimate goal needs to be kept in mind, which is to be satisfied that the residual risk that exists after risk reduction measures are implemented is acceptable.

There are no restrictions or rules with respect to the terms used to establish qualitative risk levels. But at a minimum, a matrix should show probability and severity categories and risk gradings. Tables 11.7 through 11.10 and Figure 11.1 show a general acceptance of a group of terms for incident probability and severity and for risk categories. However, safety professionals should draft matrices with which they are comfortable. Since risk assessment matrices are valuable communication tools, the terms used in them must be agreed upon and the education time necessary to achieve an understanding of them must be allocated.

The risk assessment matrix shown in Figure 11.1 is a composite of matrices that include numerical values for probability and severity levels that are transposed into qualitative risk gradings. It was originally developed for people who prefer to deal with numbers rather than qualitative indicators. To provide a one-page tool that could be used by safety professionals who wanted to get shop floor personnel involved in

TABLE 11.10 The Risk Assessment Matrix Example in Z10

Example of a Risk Assessment Matrix				
Likelihood of OCCURRENCE or EXPOSURE For selected Unit of Time or Activity	**Severity of Injury or Illness Consequence and Remedial Action**			
	CATASTROPHIC Death or permanent total disability	**CRITICAL** Disability in excess of 3 months	**MARGINAL** Minor injury, lost workday accident	**NEGLIGIBLE** First Aid or Minor Medical Treatment
Frequent Likely to occur repeatedly	**HIGH** Operation not permissible	**HIGH** Operation not permissible	**SERIOUS** High priority remedial action	**MEDIUM** Take Remedial action at appropriate time
Probable Likely to occur several times	**HIGH** Operation not permissible	**HIGH** Operation not permissible	**SERIOUS** High Priority remedial action	**MEDIUM** Take Remedial action at appropriate time
Occasional Likely to occur sometime	**HIGH** Operation not permissible	**SERIOUS** High Priority Remedial action	**MEDIUM** Take Remedial Action at appropriate time	**LOW** Risk Acceptable: Remedial Action discretionary
Remote Not likely to occur	**SERIOUS** High Priority Remedial action	**MEDIUM** Take Remedial action at appropriate time	**MEDIUM** Take Remedial action at appropriate time	**LOW** Risk Acceptable: Remedial Action Discretionary
Improbable Very unlikely – may assume exposure will not happen	**MEDIUM** Take Remedial action at appropriate time	**LOW** Risk Acceptable: Remedial Action Discretionary	**LOW** Risk Acceptable: Remedial Action Discretionary	**LOW** Risk Acceptable: Remedial Action Discretionary

risk assessments, extensions were made to include severity and probability descriptions and action levels.

In two instances, shop floor personnel said to safety professionals that relating numbers to each other first—such as 6 to 12—was a big help in understanding whether the risk category was moderate or serious. If using a risk assessment matrix in which numbers are used to begin with to establish risk levels makes the process more understandable and acceptable for operating personnel, that should be encouraged.

As noted in Figure 11.1, numbers in the matrix were derived intuitively: They are qualitative, not quantitative. Thus, the numbers have value only in relation to each other. And that is the case for all risk scoring systems that are not based on hard probability and severity numbers, which are rarely available.

On Acceptable Risk

The theoretical goal should always be to eliminate all hazards, but that may not be feasible. When a hazard cannot be eliminated, the associated risk should be reduced to a level as low as reasonably practicable and acceptable, considering cost constraints

Severity levels and values	Occurrence probabilities and values				
	Unlikely (1)	Seldom (2)	Occasional (3)	Likely (4)	Frequent (5)
Catastrophic (5)	5	10	15	20	25
Critical (4)	4	8	12	16	20
Marginal (3)	3	6	9	12	15
Negligible (2)	2	4	6	8	10
Insignificant (1)	1	2	3	4	5

Numbers were intuitively derived. They are qualitative, not quantitative. They have meaning only in relation to each other.

Incident or Exposure Severity Descriptions

Catastrophic: One or more fatalities, total system loss and major business down time, environmental release with lasting impact on others with respect to health, property damage or business interruption.

Critical: Disabling injury or illness, major property damage and business down time, environmental release with temporary impact on others with respect to health, property damage or business interruption.

Marginal: Medical treatment or restricted work, minor subsystem loss or property damage, environmental release triggering external reporting requirements.

Negligible: First aid or minor medical treatment only, non-serious equipment or facility damage, environmental release requiring routine cleanup without reporting.

Insignificant: Inconsequential with respect to injuries or illnesses, system loss or down time, or environmental release.

Incident or Exposure Probability Descriptions

Unlikely: Improbable, unrealistically perceivable.
Seldom: Could occur but hardly ever.
Occasional: Could occur intermittently.
Likely: Probably will occur several times.
Frequent: Likely to occur repeatedly.

Risk Levels

Combining the Severity and Occurrence Probability values yields a risk score in the matrix. The risk levels and the action levels are categorized below.

Risk Categories, Scoring, and Action Levels

Category	Risk Score	Action Level
Low risk	1 to 5	Remedial action discretionary.
Moderate risk	6 to 9	Remedial action to be taken at appropriate time.
Serious risk	10 to 14	Remedial action to be given high priority.
High risk	15 or greater	Immediate action necessary. Operation not permissible except in an unusual circumstance and as a closely monitored and limited exception with approval of the person having authority to accept the risk.

FIGURE 11.1 Risk assessment matrix: numerical gradings.

in relation to the extent of risk reduction to be obtained and performance requirements. In Chapter 2, "Achieving Acceptable Risk Levels: The Operational Goal," it is said that as every element in Z10 is applied, the outcome is to achieve acceptable risk levels so that the risk of harm is as low as reasonably practicable. It is also said that the risk assessment matrices in this chapter and the discussions of risk categories will help in determining acceptable risk levels.

Applying the concept of ALARP—as low as reasonably practicable—is recognized as a valuable tool to assist in determining acceptable risk levels. But a caution was offered indicating that, on occasion, achieving risk levels as low as reasonably

practicable will not achieve acceptable risk levels. Prior to presenting the following definition, it was made clear that a workable and sound definition of acceptable risk must encompass hazards, risks, probability, severity, and economics.

> Acceptable risk is that risk for which the probability of an incident or exposure occurring and the severity of harm or damage that may result are as low as reasonably practicable (ALARP) in the setting being considered.

Thus far in this chapter we have dealt with hazards, risks, probability, and severity. In applying the ALARP concept, economics is brought into the decision making. ALARP is defined as follows: ALARP is that level of risk which can be further lowered only by an increment in resource expenditure that is disproportionate in relation to a resulting decrement of risk.

MANAGEMENT DECISION LEVELS

Remedial action or acceptance levels must be attached to risk categories to permit intelligent management decision making. Examples are given in Tables 11.10 and 11.11. It must be understood that they are examples only and that remedial action and acceptance levels should be developed to suit the needs and exposures in an individual operation. They must be agreed upon, understood, and supported by senior management.

TABLE 11.11 Management Decision Levels

Risk Category	Remedial Action or Acceptance
Low	Risk is acceptable; remedial action discretionary
Medium	Remedial action to be taken within appropriate time
Serious	Remedial action to have high priority
High	Immediate action necessary. Operator not permissable except in an unusual circumstance and as a closely monitored and limited exception with approval of the person having the authority to accept the risk

Going through the exercise of creating and reaching agreement on a risk assessment matrix and the management decision levels adds to a safety professional's effectiveness in communicating about risks and obtaining consideration of the remedial actions recommended.

For the discussion that follows of acceptable risk levels and the management actions to be taken to achieve them, the contents of Tables 11.10 and 11.11 are used as base data. Keep in mind that:

- An acceptable risk level must be tolerable in the situation being considered
- While economic considerations are a part of decision making, the risk level is to be as low as reasonably practicable, and acceptable

- Special consideration should be given to preventing incidents resulting in serious injuries and fatalities
- What follows represents my opinion; others may have different views.

If the risk category for worker injury or illness or environmental damage or other property damage is high, operation is not permissible except in an unusual circumstance and as a closely monitored and limited exception, only with approval of the person having the authority to accept the risk. If it is determined that the cost to reduce the risk to an acceptable level is excessive in relation to the risk reduction benefit to be achieved, the operation should cease in all but rare situations (e.g., society accepts the risks of deep-sea fishing, a high-hazard occupation).

If the risk category is serious, the risk is not acceptable and action should be undertaken on a high-priority basis, meaning very soon, to lower the risk to an acceptable level. While arrangements are made to reduce the risk, an extra-heavy application of the lower levels in the hierarchy of controls (warning systems, blocking off work areas, administrative controls, training, personal protective equipment) is in order. If it is determined that the cost to reduce the risk to an acceptable lower level is excessive in relation to the risk reduction benefit to be achieved, the operation should cease in all but rare situations.

Where the risk category is medium, even though the probability ratings for severe injury or illness are "improbable" or "remote," and the probability rating for minor injury is "occasional," and the probability ratings for negligible injury are "frequent" or "probable," remedial action should be taken, in good time, to reduce the risk in accord with good economics. This is the risk category where the lower levels in the hierarchy of controls, if applied more extensively and effectively, may be sufficient to achieve acceptable risk levels.

Where the risk category is low, the risk is considered acceptable. Nevertheless, there will be times when it is good business management and employee relations to reduce low risks further if they are perceived by employees to be more serious than they actually are. Remember, employee perceptions are their reality.

Some of the risk assessment matrices shown in this chapter combine elements pertaining to personal injury with the financial impact of an incident represented by the amount of property damage, business interruption time, and time to recover from an environmental incident. Safety professionals who have made such combinations in their risk assessment matrices say that they get better management response to their proposals for risk reduction if they tie the severity of injury potential to avoiding operational property damage, downtime, business interruption, and environmental damage. That has also been my experience.

DESCRIPTIONS OF HAZARDS ANALYSES AND RISK ASSESSMENT TECHNIQUES

Over the past 50 years, a large and unwieldy number of hazard analysis and risk assessment techniques have been developed. For example, 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. In ANSI/ASSE Z690.3-2011, *Risk Assessment Techniques*, comparisons and descriptions are given of 31 risk assessment techniques. (Z690.3 is the American National Standard adoption of IEC/ISO 31010:2009.)

Brief descriptions are given here of purposely selected hazard analysis techniques. If a safety professional understands all of them and is capable of bringing them to bear in resolving hazard and risk situations, she or he will be exceptionally well qualified to meet the risk assessment requirements in Z10.

As a practical matter, having knowledge of three risk assessment concepts will be sufficient to address most occupational safety and health risk situations: preliminary hazard analysis, the what-if checklist analysis methods, and failure mode and effects and analysis.

It is important to understand that each of those techniques complement, rather than supplant, the others. Selecting a technique or a combination of techniques to be used to analyze a hazardous situation requires good judgment based on knowledge and experience. Qualitative rather than quantitative judgments will prevail. For all but the complex risks, qualitative judgments will be sufficient.

Sound quantitative data on incident probabilities are seldom available. Colleagues who are skilled in system safety, a field in which making quantitative risk assessments is ordinarily done, are not overly pleased when I say that most quantitative risk assessments are really qualitative risk assessments because so many judgments have to be made in the process to decide on the occurrence probability and the severity of outcome .

PRELIMINARY HAZARD ANALYSIS: HAZARD ANALYSIS AND RISK ASSESSMENT

Originally, the preliminary hazards analysis (PHA) technique was used to identify and evaluate hazards in the early stages of the design process. However, in actual practice the technique has attained much broader use. Principles on which preliminary hazards analyses are based have been adopted for use not only in the initial design process, but also in assessing the risks of existing products or operations.

For example, a standard adopted by the International Organization for Standardization is employed in the European Union, and the standard requires that risk assessments be made for all machinery that is to go into a workplace in member countries. That standard is EN ISO 12100–2010. *Safety of Machinery—General principles for design. Risk assessment and risk reduction.* Those risk assessment requirements have been met in some companies by applying an adaptation of the PHA technique.

In reality, the PHA technique needs a new name, reflecting its broader usage. In one organization, the process is called hazard analysis and risk assessment, a designation that is coming into greater us since it is more descriptive of its purpose.

(Also, take note to avoid confusion: In *OSHA's Rule for Process Safety Management of Highly Hazardous Chemicals* and *EPA's Risk Management*

Program for Chemical Accidental Release Prevention, "PHA" stands for process hazard analysis.)

Headings on preliminary hazard analysis forms include the typical identification data: date, names of evaluators, department, and location. The following information is usually 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.
- The exposures that are to be analyzed: 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 alphabetical indicator for the severity of harm or damage that might result if the hazard's potential is realized.
- A numerical or alphabetical 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 required.

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. A hazard analysis and risk assessment worksheet (formerly called a preliminary hazard analysis worksheet) appears as Addendum A in this chapter. That form, and similar forms, require entry of severity, probability, and risk codes before and after countermeasures are taken. Figure 11.1 is an add-on to Addendum A.

On Developing a Coding System

Assume that there are to be four severity categories, for which numerical codes are to be used: catastrophic, 1; critical, 2; marginal, 3; negligible, 4. Assume that there are to be five categories of occurrence probability, having alphabetical codes: frequent, A; probable, B; occasional, C; remote, D; improbable, E. Table 11.12 displays combinations of numerical and alphabetical indicators and the risk codes that derive from them.

TABLE 11.12 Risk Assessment Matrix, Including Probability and Severity Codes

Occurrence Probability	Severity Categories			
	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Low	Low

Risk codes would then be as follows, taking into account the combinations of the severity and probability codes:

Combinations	Risk Category	Risk Code
A–1, A–2, B–1, B–2, C–1	High	H
A–3, B–3, C–2, D–1	Serious	S
A–4, B–4, C–3, D–2, D–3, E–1, E–2, E–3	Medium	M
C–4, D–4, E–4	Low	L

The foregoing is intended as an example from which suitable adaptations can be made by safety professionals.

WHAT-IF ANALYSIS

For a what-if analysis, a group of people (as few as two, but often several more) use a brainstorming approach to identify hazards, hazard scenarios, how incidents can occur, and what their probable consequences might be. Questions posed during the brainstorming session may begin with "what-if," as in "What if the air-conditioning system 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."

All of the questions are recorded and 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 controls in effect, suggesting additional risk reduction measures if appropriate.

CHECKLIST ANALYSIS

Checklists are primarily adaptations from published standards, codes, and industry practices. There are many such checklists. They consist of lists of questions pertaining to the applicable standards and practices, usually with a "yes" "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 hazards that are customarily recognized. Nevertheless, the quality of checklists is dependent on the experience of the people who develop them. Further, they must be crafted to suit particular needs. If a checklist is not complete, the analysis may not identify some hazardous situations. An example of a checklist for machinery design is provided as Addendum C at the end of this chapter. A checklist for general design purposes appears in Chapter 16. These can serve as resources for those who choose to build their own checklists.

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 a checklist. Combining the 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 during the brainstorming process. Usually, a team experienced in the design, operation, and maintenance of the operation performs the analysis. The number of people required depends, of course, on the operation's complexity.

FAILURE MODES AND EFFECTS ANALYSIS

In several industries, failure mode and effects analysis (FMEA) has been the technique of choice by design engineers for reliability and safety considerations. Such techniques are used to evaluate the ways in which equipment fails and 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.

An FMEA produces qualitative, systematic lists that include 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: 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 do or do not work.

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 is similar.

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

Note that the FMEA process described here requires entry of probability, severity, and risk codes. The risk assessment matrix shown in Table 11.12 and the risk category codes that follow it fulfill the need for traditional FMEA purposes. A failure modes and effects analysis form on which those codes would be entered is provided as Addendum B.

HAZARD AND OPERABILITY ANALYSIS

The hazard and operability analysis (HAZOP) technique was developed to identify both hazards and operability problems in chemical process plants. An interdisciplinary team and an experienced team leader are required. In a HAZOP application, a process or operation is reviewed systematically to identify deviations from desired practices that could lead to adverse consequences. HAZOPs can be used at any stage in the life of a process.

HAZOPs usually require a series of meetings in which the team, using process drawings, systematically evaluates the impact of deviations from the desired practices. The team leader uses a set of guide words to develop discussions. As the team reviews each step in a process, they record any deviations, along with their causes, consequences, safeguards, and required actions, or the need for more information to evaluate the deviation.

FAULT TREE ANALYSIS

A fault tree analysis (FTA) is a top-down, deductive logic model that traces the failure pathways for a predetermined undesirable condition or event called a TOP event. An FTA can be carried out either quantitatively or subjectively.

An FTA generates a fault tree (a symbolic logic model) that enter's failure probabilities for combinations of equipment failures and human errors that can result in accidents. Each immediate causal factor is examined to determine its subordinate causal factors until the root causal factors are identified.

The strength of an FTA is its ability to identify combinations of basic equipment and human failures that can lead to an accident, allowing the analyst to focus preventive measures on significant basic causes. An FTA has a particularly high value when analyzing highly-redundant systems and high-energy systems in which high severity events can occur.

For systems vulnerable to single failures that can lead to accidents, the FMEA and HAZOP techniques are better suited. FTA is often used when another technique has identified a hazardous situation that requires more detailed analysis. Making a fault tree analysis of other than the simplest systems requires the talent of experienced analysts.

MANAGEMENT OVERSIGHT AND RISK TREE

As Pat Clemens wrote in a paper cited previously, the management oversight and risk tree (MORT) technique applies "a pre-designed, systematized logic tree to the identification of total system risks, both those inherent in physical equipment and processes and those which arise from operational/management inadequacies." MORT is an incident investigation and analysis technique. It is discussed here for a particular purpose. There are four major stages in operational risk management:

1. Pre-operational stage: in the initial planning, design, specification, prototyping, and construction processes, where the opportunities are greatest and the costs are lowest for hazard and risk avoidance, elimination, reduction, or control.

2. Operational stage: where hazards and risks are identified and evaluated and mitigation actions are taken through redesign initiatives or changes in work methods before incidents or exposures occur.
3. Post-incident stage: where investigations are made of incidents and exposures to determine the causal factors that will lead to appropriate interventions and acceptable risk levels.
4. Post-operational stage: where demolition, decommissioning, or reusing/rebuilding operations are undertaken.

All of the hazard analysis and risk assessment techniques discussed previously relate *principally* to the design process or achieving risk reduction in the operational mode *before hazards-related incidents occur*. MORT was developed for use *principally* when incident investigations are made—the post-incident stage. In the Introduction to the *NRI MORT User's Manual*, the following comments are made.

> The Management Oversight and Risk Tree (MORT) method is an analytical procedure for inquiring into causes and contributing factors of accidents and incidents. The MORT method is a logical expression of the functions needed by an organization to manage its risks effectively. MORT reflects a philosophy which holds that the most effective way of managing safety is to make it an integral part of business management and operational control. (p. viii)

MORT is a comprehensive analytical procedure that provides a disciplined method for determining the systemic causes and contributing factors of accidents. MORT directs the user to the hazards and risks deriving from both system design and procedural shortcomings. When used properly in the post-incident stage of the practice of safety, MORT provides an excellent resource from which decisions can be made to redesign technical and procedural aspects of operations.

ADDITIONAL RESOURCES

A Risk Assessment Tool made available by the European Agency for Safety and Health at Work can be found at http://hwi.osha.europa.eu/ra_tools_generic/. Parts I and II provide basic information on risk assessment. The subject matter consists of only eight pages. Nevertheless, it takes a reader through a basic hazard identification and risk assessment process. Part III provides checklists for hazard identification and selection of preventive measures for 10 subjects (e.g., moving machinery electrical installations and equipment, fire, etc.). Part IV consists of checklists for seven occupation settings (e.g., office work, food processing, small-scale surface mining, etc.)

In the UK, the Health and Safety Executive recently updated "Five steps to risk assessment." It can be accessed at http://www.hse.gov.uk/risk/fivesteps.htm. It is also a basic, uncomplicated system.

If a safety professional undertakes to inform supervisors and workers on the fundamentals of hazard identification and risk assessment, say at safety meetings, the two foregoing resources will serve well in developing the presentations and the written material.

A particularly valuable reference is the *Guidelines for Hazard Evaluation Procedures, Second Edition With Worked Examples*, issued by the Center for Chemical Process Safety. Although this text is issued by a chemical industry organization, it is largely generic.

The Basics of FMEA, a 75-page 5×7-inch paperback FMEA by McDermott, Mikulak, and Beauregard, is a primer on the FMEA process.

In Chapter 13, "Three and Four Dimensional Numerical Risk Scoring Systems," we comment on an FMEA publication issued for the semiconductor industry by International SEMATECH. It is well done. Its uniqueness is that environmental, safety, and health considerations are vital in the process described.

OSHA has issued a paper on Job Hazards Analysis which has enough guidance points to warrant inclusion of a modified version of it as Addendum C to this chapter. Its definition of a hazard is the same as mine: A hazard is the potential for harm. The paper also says that "Ideally, after you identify uncontrolled hazards, you will take steps to eliminate or reduce them to an acceptable risk level." But the data on eliminating or reducing hazards are a bit shallow.

Should a safety professional want to acquire extensive and valuable texts devoted entirely to applications in risk assessment, it is suggested that he or she consider two books written by Bruce Main, president of design safety engineering.

1. *Risk Assessment: basics and benchmarks* is a 485-page treatise published in 2004.
2. *Risk Assessment: Challenges and Opportunities* is a 364-page text published in 2012.

With respect to risk assessment, Main has been a researcher, writer, consultant, software developer, instructor, and a leader in standards development.

Addendum D provides additional information on types of hazards, hazardous situations, and hazardous events.

AVOIDING UNREALISTIC EXPECTATIONS

Making hazards analyses and risk assessments is both an art and a science. Whatever the methodology—the simplest or the most complex—many judgments will be made in determining the severity potentials of hazards and the probably of occurrence of incidents and exposures.

Even though appliers of the risk assessment methodologies make informed judgments, they may disagree on which hazards are most important because of their severity potential and which risks deserve the highest priority. One way to resolve those differences is to have qualified teams participate when the hazards and risks are considered significant, the intent being to reach consensus.

Some who oppose the use of qualitative risk assessment techniques do so because the outcomes are not stated in absolutely assured, precise numbers. Such accuracy is not attainable because incident probability data are lacking, and the severity of event outcomes is a best estimate. Expecting such results is unrealistic. Fortunately, recognition continues to grow that hazard analysis and risk assessment methods, although largely qualitative, add value to operational risk management decision making.

CONCLUSION

This chapter is simply a primer on hazard analysis and risk assessment. Its purpose is to provide a foundation for those who perceive that having additional knowledge in this aspect of safety and health risk management provides an opportunity for professional growth, accomplishment, and recognition. Having that knowledge adds to one's ability to evaluate hazardous situations and make more convincing presentations to management for resource allocation to accomplish the risk reduction measures proposed.

Looking to the future, safety professionals can expect that having knowledge of hazard analysis and risk assessment techniques will be required for job retention and career enhancement. Fortunately, it is not difficult to acquire the knowledge and skill required to fulfill almost all of their needs.

As safety and health professionals become more involved in risk assessments, they will come to understand that professional safety practice requires attention to the two distinct aspects of risk:

- Avoiding, eliminating, or reducing the probability of occurrence of a hazard-related incident or exposure
- Having the severity of the potential for harm or damage be as low as reasonably practicable

REFERENCES

"A Risk Assessment Tool." European Agency for Safety and Health at Work. At http://hwi.osha.europa.eu/ra-tools-generic/.

ANSI/AIHA Z10-2012. *Occupational Health and Safety Management Systems*. Fairfax, VA: American Industrial Hygiene Association, 2012. The American Society of Safety Engineers is now the secretariat. Available at https://www.asse.org/cartpage.php?link=z10-2005

ANSI/ASSE Z590.3-2011. *Prevention through Design: Guidelines for Addressing Occupational Hazards and Risks in Design and Redesign Processes*. Des Plaines, IL: American Society of Safety Engineers, 2011.

ANSI/ASSE Z690.3 *Risk Assessment Techniques*. Des Plaines, IL: American Society of Safety Engineers, 2011.

ANSI/PMMI B155.1-2011. *Safety Requirements for Packaging Machinery and Packaging-Related Converting Machinery*. Arlington, VA: Packaging Machinery Manufacturers Institute, 2011.

Clemens, Pat. "A Compendium Of Hazard Identification And Evaluation Techniques for System Safety Application." *Hazard Prevention*, Mar./Apr., 1982.

CSA Z1002-12. *Occupational Health and Safety—Hazard Identification and Elimination and Risk Assessment and Control*. Toronto, Canada: Canadian Standards Association, 2012.

EN ISO 12100–2010. *Safety of Machinery—General principles for Design. Risk Assessment and Risk Reduction*. Geneva, Switzerland: International Organization for Standardization, 2010.

EPA's Risk Management Program for Chemical Accidental Release Prevention. Washington, DC: U.S. Environmental Agency, 1996. Preview at http://www.epa.gov/emergencies/content/lawsregs/rmpover.htm.

Failure Mode and Effects Analysis (FMEA): A Guide for Continuous Improvement for the Semiconductor Equipment Industry. Technology Transfer No.92020963A-ENG. Austin, TX: International SEMATECH, 1992a. Also available at www.sematech.org.

"Five Steps to Risk Assessment." London: Health and Safety Executive, 2008.

Framework for Environmental Health Risk Management, Final Report, Vol 1. Washington, DC: Presidential/Congressional Commission on Risk Assessment and Risk Management, 1997.

Guidelines for Hazard Evaluation Procedures, Second Edition With Worked Examples. New York: Center for Chemical Process Safety of the American Institute of Chemical Engineers, 1992.

Job Hazard Analysis. U.S. Department of Labor, Occupational Safety and Health Administration, OSHA 3071, 2002 (Revised). Available at http://www.osha.gov/Publications/osha3071.html.

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

Main, Bruce W. *Risk Assessment: basics and benchmarks* . Ann Arbor, MI: Design Safety Engineering, Inc., 2004. Information at www.designsafe.com.

Main, Bruce W. *Risk Assessment: Challenges and Opportunities*. Ann Arbor, MI: Design Safety Engineering, Inc., 2012. Information at www.designsafe.com.

McDermott, Robin E., Raymond J. Mikulak, and Michael R. Beauregard. *The Basics of FMEA*. New York: Productivity Press, 1996.

Mil-STD-882E. *Standard Practice for System Safety*. Washington, DC: Department of Defense, 2000. Also at http://www.systemsafetyskeptic.com/yahoo_site_admin/assets/docs/MIL-STD-882E_final.135152939.pdf.

NRI MORT User's Manual. Delft, The Netherlands: Noordwijk Risk Initiative Foundation, 2009. Enter "NRI MORT User's Manual" into a search engine for a free download.

OSHA's Rule for Process Safety Management of Highly Hazardous Chemicals, 29 CFR 1910.119. Washington, DC: Department of Labor, Occupational Safety and Health Administration, 1992.

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

ADDITIONAL READING

Grose, Vernon L. *Managing Risk, Systematic Loss Prevention for Executives*. Originally published by Prentice-Hall, 1987. Now available through Omega Systems Group, Inc., Arlington, VA.

Manuele, Fred A. *On the Practice of Safety*, 4th ed. Hoboken, NJ: Wiley, 2014.

Roland, Harold E. and Brian Moriarty. *System Safety Engineering and Management*, 2nd ed. New York: Wiley, 1990.

Stevens, Richard A. *System Safety for the 21st Century*. Hoboken, NJ: Wiley, 2004. (This is an updated version of *System Safety 2000* by Joe Stephenson.)

ADDENDUM A–1

Preliminary Hazard Analysis and Risk Assessment
Codes are in Addendum A–2

Prepared by _____ Date_____ Location_____ Project No._____ Page No.____ of Pages____
Description of task/operation/process _____

	Risk Before				Risk After		
Hazards Identified	E	S	P	Risk Code	Risk Reduction Measures	S	P	Risk Code

Advanced Safety Management: Focusing on Z10 and Serious Injury Prevention, Second Edition. Fred A. Manuele.

ADDENDUM A–2

Risk Assessment Matrix

Severity Levels and Values	Occurrence Probabilities and Values				
	Unlikely (1)	Seldom (2)	Occasional (3)	Likely (4)	Frequent (5)
Catastrophic (5)	5	10	15	20	25
Critical (4)	4	8	12	16	20
Marginal (3)	3	6	9	12	15
Negligible (2)	2	4	6	8	10
Insignificant (1)	1	2	3	4	5

Numbers were intuitively derived. They are qualitative, not quantitative and have meaning only in relation to each other.

Exposure Codes: P – personnel; E – environment; D – damage – facility, equipment, business interruption; M – material, product

Severity Descriptions

C – Catastrophic: One or more fatalities, total system loss and major business down time, environmental release with lasting impact on others with respect to health, property damage or business interruption.

Cr – Critical: Disabling injury or illness, major property damage and business down time, environmental release with temporary impact on others with respect to health, property damage or business interruption.

M – Marginal: Medical treatment or restricted work, minor subsystem loss or property damage, environmental release triggering external reporting requirements.

N – Negligible: First aid or minor medical treatment only, non-serious equipment or facility damage, environmental release requiring routine cleanup without reporting.

I – Insignificant: Inconsequential with respect to injuries or illnesses, system loss or down time, or environmental release.

Probability Descriptions

U – Unlikely: Could occur but hardly ever.

O – Occasional: Could occur intermittently.

L – Likely: Probably will occur several times.

F – Frequent: Likely to occur repeatedly.

Risk Levels

Combining the Severity and Occurrence Probability values yields a risk score in the matrix. The risks and the action levels are categorized below.

Risk Categories, Scoring, and Action Levels

Category	Risk Score	Action Level
L – Low risk	1 to 5	Remedial action discretionary.
M – Moderate risk	6 to 9	Remedial action to be taken at appropriate time.
S – Serious risk	10 to 14	Remedial action to be given high priority.
H – High risk	15 or greater	Immediate action necessary. Operation not permissible except in an unusual circumstance and as a closely monitored and limited exception only with approval of the person having authority to accept the risk.

ADDENDUM B

Advanced Safety Management: Focusing on Z10 and Serious Injury Prevention, Second Edition. Fred A. Manuele.

FMEA FORM
SYSTEM:
SUBSYSTEM:
REFERENCE DRAWING:

FAILURE MODE AND EFFECTS ANALYSIS (FMEA)
FAULT CODE#

DATE:
SHEET:
PREPARED BY:

Subsystem/ Module &Function	*Potential Failure Mode*	*Potential Local Effect(s) of Failure*	*Potential End Effect(s) of Failure*	SEV	Cr	Potential Cause(s) of Failure	OCC	Current Controls/ Fault Detection	DET	RPN	Recommended Action(s)	Area/ Individual Responsible & Completion Date(s)	Action Taken	SEV	OCC	DET	RPN
Subsystem name and function	"How can this subsystem fail to perform its function?" "What will an operator see?"	The local effect of the subsystem or end user	Downtime # of hours at the system level. 2. Safety 3. Environ-mental 4. Scrap loss			"How can this failure occur?" Describe in terms of something that can be corrected or controlled. 2. Refer to specific errors or malfunctions		"What mechanisms are in place that could detect, prevent, or minimize the impact of this cause?"			"How can we change the design to eliminate the problem?" "How can we detect (fault isolate) this cause for this failure?" "How should we test to ensure the failure has been eliminated?" "What PM procedures should we recommend?" 1. Begin with highest RPN. 2. Could say "no action" or "Further study is required." 3. An idea written here does not imply corrective action.	"Who is going to take responsibility?" "When will it be done?"	"What was done to correct the problem?" Examples: Engineering Change, Software revision, no recommended action at this time due to obsolescence, etc.				

Critical Failure symbol (Cr). Used to identify critical failures that must be addressed (i.e., whenever safety is an issue).

Severity Ranking (1–10) (see Severity Table)

Occurrence Ranking (1–10) (see Occurrence Table)

Detection Ranking (1–10) (see Detection Table)

Risk Priority Number
RPN = Severity*Occurrence *Detection

How did the "Action Taken" change the RPN?

7 1 5 6 210 6 1 1 6

ADDENDUM C

This presentation is an adaption from *Job Hazard Analysis*, U.S. Department of Labor, Occupational Safety and Health Administration, OSHA 3071, 2002 (revised). Available at http://www.osha.gov/Publications/osha3071.html.

What is a Hazard?

A hazard is the potential for harm. In practical terms, a hazard often is associated with a condition or activity that, if left uncontrolled, can result in an injury or illness. Identifying hazards and eliminating or controlling them as early as possible will help prevent injuries and illnesses.

What is a job hazard analysis?

A job hazard analysis is a technique that focuses on job tasks as a way to identify hazards before they occur. It focuses on the relationship between the worker, the task, the tools, and the work environment. Ideally, after you identify uncontrolled hazards, you will take steps to eliminate or reduce them to an acceptable risk level.

Why is Job Hazard Analysis Important?

Many workers are injured and killed at the workplace every day in the United States. Safety and health can add value to your business, your job, and your life. You can help prevent workplace injuries and illnesses by looking at your workplace operations, establishing proper job procedures, and ensuring that all employees are trained properly.

One of the best ways to determine and establish proper work procedures is to conduct a job hazard analysis. A job hazard analysis is one component of the larger commitment of a safety and health management system.

Advanced Safety Management: Focusing on Z10 and Serious Injury Prevention, Second Edition. Fred A. Manuele.

What is the Value of a Job Hazard Analysis?

Supervisors can use the findings of a job hazard analysis to eliminate and prevent hazards in their workplaces. This is likely to result in fewer worker injuries and illnesses; safer, more effective work methods; reduced workers' compensation costs; and increased worker productivity. The analysis also can be a valuable tool for training new employees in the steps required to perform their jobs safely.

For a job hazard analysis to be effective, management must demonstrate its commitment to safety and health and follow through to correct any uncontrolled hazards identified. Otherwise, management will lose credibility and employees may hesitate to go to management when dangerous conditions threaten them.

What Jobs are Appropriate for a Job Hazard Analysis?

A job hazard analysis can be conducted on many jobs in your workplace. Priority should go to the following types of jobs:

- Jobs with the highest injury or illness rates;
- Jobs with the potential to cause severe or disabling injuries or illness, even if there is no history of previous accidents;
- Jobs in which one simple human error could lead to a severe accident or injury;
- Jobs that are new to your operation or have undergone changes in processes and procedures; and
- Jobs complex enough to require written instructions.

Where do I Begin?

Involve your employees. It is very important to involve your employees in the hazard analysis process. They have a unique understanding of the job, and this knowledge is invaluable for finding hazards. Involving employees will help minimize oversights, ensure a quality analysis, and get workers to "buy in" to the solutions because they will share ownership in their safety and health program.

Review your accident history. Review with your employees your worksite's history of accidents and occupational illnesses that needed treatment, losses that required repair or replacement, and any "near misses" — events in which an accident or loss did not occur, but could have. These events are indicators that the existing hazard controls (if any) may not be adequate and deserve more scrutiny.

Conduct a preliminary job review. Discuss with your employees the hazards they know exist in their current work and surroundings. Brainstorm with them for ideas to eliminate or control those hazards.

If any hazards exist that pose an immediate danger to an employee's life or health, take immediate action to protect the worker. Any problems that can be corrected easily should be corrected as soon as possible. Do not wait to complete your job hazard analysis. This will demonstrate your commitment to safety and health and enable you to focus on the hazards and jobs that need more study because of their complexity. For those hazards determined to present unacceptable risks, evaluate types of hazard controls.

List, rank, and set priorities for hazardous jobs. List jobs with hazards that present unacceptable risks, based on those most likely to occur and with the most severe consequences. These jobs should be your first priority for analysis.

Outline the steps or tasks. Nearly every job can be broken down into job tasks or steps. When beginning a job hazard analysis, watch the employee perform the job and list each step as the worker takes it. Be sure to record enough information to describe each job action without getting overly detailed. Avoid making the breakdown of steps so detailed that it becomes unnecessarily long or so broad that it does not include basic steps. You may find it valuable to get input from other workers who have performed the same job.

Later, review the job steps with the employee to make sure that you have not omitted something. Point out that you are evaluating the job itself, not the employee's job performance. Include the employee in all phases of the analysis—from reviewing the job steps and procedures to discussing uncontrolled hazards and recommended solutions.

Sometimes, in conducting a job hazard analysis, it may be helpful to photograph or videotape the worker performing the job. These visual records can be handy references when doing a more detailed analysis of the work.

How do I Identify Workplace Hazards?

A job hazard analysis is an exercise in detective work. Your goal is to discover the following:

- What can go wrong?
- What are the consequences?
- How could it arise?
- What are other contributing factors?
- How likely is it that the hazard will occur?

To make your job hazard analysis useful, document the answers to these questions in a consistent manner. Describing a hazard in this way helps to ensure that your efforts to eliminate the hazard and implement hazard controls help target the most important contributors to the hazard. Good hazard scenarios describe:

- Where it is happening (environment),
- Who or what it is happening to (exposure),
- What precipitates the hazard (trigger),
- The outcome that would occur should it happen (consequence), and
- Any other contributing factors.

Rarely is a hazard a simple case of one singular cause resulting in one singular effect. More frequently, many contributing factors tend to line up in a certain way to create the hazard. Here is an example of a hazard scenario:

In the metal shop (environment), while clearing a snag (trigger), a worker's hand (exposure) comes into contact with a rotating pulley. It pulls his hand into the machine and severs his fingers (consequences) quickly.

To perform a job hazard analysis, you would ask:

- What can go wrong? The worker's hand could come into contact with a rotating object that "catches" it and pulls it into the machine.
- What are the consequences? The worker could receive a severe injury and lose fingers and hands.
- How could it happen? The accident could happen as a result of the worker trying to clear a snag during operations or as part of a maintenance activity while the pulley is operating. Obviously, this hazard scenario could not occur if the pulley is not rotating.
- What are other contributing factors? This hazard occurs very quickly. It does not give the worker much opportunity to recover or prevent it once his hand comes into contact with the pulley. This is an important factor, because it helps you determine the severity and likelihood of an accident when selecting appropriate hazard controls.

  Unfortunately, experience has shown that training is not very effective in hazard control when triggering events happen quickly because humans can react only so quickly.
- How likely is it that the hazard will occur? This determination requires some judgment. If there have been "near-misses" or actual cases, then the likelihood of a recurrence would be considered high. If the pulley is exposed and easily accessible, that also is a consideration.

In the example, the likelihood that the hazard will occur is high because there is no guard preventing contact, and the operation is performed while the machine is running. By following the steps in this example, you can organize your hazard analysis activities.

HOW DO I CORRECT OR PREVENT HAZARDS?

After reviewing your list of hazards with the employee, consider what control methods will eliminate or reduce them. The most effective controls are engineering controls that physically change a machine or work environment to prevent employee exposure to the hazard. The more reliable or less likely a hazard control can be circumvented, the better. If this is not feasible, administrative controls may be appropriate. This may involve changing how employees do their jobs.

Discuss your recommendations with all employees who perform the job and consider their responses carefully. If you plan to introduce new or modified job procedures, be sure they understand what they are required to do and the reasons for the changes.

ADDENDUM D

EXAMPLES OF HAZARDS, HAZARDOUS SITUATIONS, AND HAZARDOUS EVENTS

This checklist is an adaptation from a standard issued by the International Organization for Standardization titled *Safety of machinery. General Principles for Design. Risk assessment and risk reduction*, EN ISO 12100-2012. The checklist is a guide for companies located throughout the world that design and manufacture machinery and equipment that would go into workplaces. Although the checklist pertains to a broad range of equipment, those who use it as a reference must understand that it could not possibly include all hazards and all hazardous situations.

Mechanical Hazards

Due to machine parts or work pieces: e.g.,

- Shape
- Relative motion
- Mass and stability (potential energy of elements which may move under the effect of gravity)
- Mass and velocity (kinetic energy of elements in controlled and uncontrolled motion)
- Inadequacy of mechanical strength

Advanced Safety Management: Focusing on Z10 and Serious Injury Prevention, Second Edition. Fred A. Manuele.

Due to accumulation of energy inside the machinery: e.g.,

- Elastic elements (springs)
- Liquids and gases under pressure
- The effect of vacuum

Mechanical Hazards Due to the Potential for

- Crushing
- Shearing
- Cutting or severing
- Entanglement
- Drawing-in or trapping
- Impact
- Stabbing or puncture
- Friction or abrasion
- High-pressure fluid injection or ejection

Electrical Hazards Due to

- Contact of persons with live parts (direct contact)
- Contact of persons with parts which have become live under faulty conditions (indirect contact)
- Approach to live parts under high voltage
- Electrostatic phenomena
- Thermal radiation or other phenomena, such as the projection of molten particles and chemical effects from short circuits, overloads, etc.

Thermal Hazards, Resulting in

- Burns, scalds, and other injuries by a possible contact of persons with objects or materials with an extreme high or low temperature, by flames or explosions, and also by the radiation of heat sources
- Damage to health by hot or cold working environment

Hazards Generated by Noise, Resulting in

- Hearing loss (deafness), other physiological disorders (e.g., loss of balance, loss of awareness)
- Interference with speech communication, acoustic signals, etc.

Hazards Generated by Vibration

- Use of handheld machines resulting in a variety of neurological and vascular disorders
- Whole body vibration, particularly when combined with poor postures

Hazards Generated By Radiation

- Low-frequency, radio-frequency radiation; microwaves
- Infrared, visible, and ultraviolet light
- X- and gamma rays
- Alpha and beta rays, electron or ion beams, neutrons
- Lasers

Hazards Generated by Materials and Substances (and their Constituent Elements) Processed or Used by the Machinery

- Hazards from contact with or inhalation of harmful fluids, gases, mists, fumes, and dusts
- Fire or explosion hazards
- Biological or microbiological (viral or bacterial) hazards

Hazards Generated By Neglecting Ergonomic Principles In Machinery Design; A E.G.,

- Unhealthy postures or excessive effort
- Hazardous situations due to lifting
- Inadequate consideration of hand–arm or foot–leg anatomy
- Neglected use of personal protection equipment
- Inadequate local lighting
- Mental overload and underload, stress
- Human error, human behavior
- Inadequate design, location, or identification of manual controls
- Inadequate design or location of visual display units

Hazards Deriving from Unexpected Startup, Unexpected Overrun/Overspeed (or any Similar Malfunction) from

- Failure/disorder of the control system
- Restoration of energy supply after an interruption
- External influences on electrical equipment
- Other external influences (gravity, wind, etc.)
- Errors in the software
- Errors made by the operator (due to mismatch of machinery with human characteristics and abilities)
- Impossibility of stopping a machine under the best possible conditions
- Variations in the rotational speed of tools
- Failure of the power supply

- Failure of the control circuit
- Errors of fitting
- Breakup during operation
- Falling or ejected objects or fluids
- Loss of stability/overturning machinery
- Slip, trip, and fall of persons, related to machinery

Hazards, Hazardous Situation and Hazardous Events Due to Mobility:

Relating to the traveling function

- Movement when starting an engine
- Movement without a driver in the driving position
- Movement without all parts in a safe position
- Excessive speed of pedestrian-controlled machinery
- Excessive oscillation when moving

Linked to the work position (including driving station) on a machine

- Fall of persons during access (or at/from) the work position
- Exhaust gases/lack of oxygen at the work position
- Fire (flammability of the cab, lack of means extinguish to
- Mechanical hazards at the work position:
  1. Contact with the wheels
  2. Rollover
  3. Fall of objects, penetration by objects
  4. Breakup of parts
  5. Contact of persons with machine parts or tools (pedestrian-controlled machines)
- Insufficient visibility from the work position
- Inadequate lighting
- Inadequate seating
- Noise at the work position
- Vibration at the work position
- Insufficient means for evacuation/emergency

Due to the power source and to the transmission of power

- Hazards from an engine and batteries
- Hazards from transmission of power between machines
- Hazards from coupling and towing

From/to third persons

- Unauthorized startup/use
- Drift of a part away from its stopping position
- Lack of or inadequacy of means of visual or acoustic warning of

Hazards, Hazardous Situations, and Hazardous Events Due to Lifting

Mechanical hazards and hazardous events

- From load falls, collisions, machine tipping caused by:
  1. Lack of stability
  2. Uncontrolled loading, overloading, overturning moments exceeded
  3. Uncontrolled amplitude of movements
  4. Unexpected/unintended movement of loads
  5. Inadequate holding devices/accessories
  6. Collision of more than one machine
- From access of persons to load support
- From insufficient mechanical strength of parts
- From inadequate design of pulleys, drums

CHAPTER 12

PROVISIONS FOR RISK ASSESSMENTS IN STANDARDS AND GUIDELINES: SECTIONS 4.2 AND 5.1.1 OF Z10

As stated in Chapter 11, trends indicate that having the ability to make risk assessments will be expected of safety professionals. That premise has acquired considerable weight because of the more frequent inclusion of provisions in safety standards and guidelines requiring or recommending that risk assessments be made. This trend will have an impact on the knowledge and skills that safety professionals are expected to have. It will also provide career opportunities for them.

Addendum A in this chapter is a partial list of standards, guidelines, and initiatives that require or promote making risk assessments. To avoid having the list become overly lengthy, 2005 was selected as the year to begin recordings in the list. That is the year that the first version of Z10 was adopted as a national standard. Although there are 35 items in the list, it is probably not complete.

To provide guidance for safety professionals on trends throughout the world regarding requirements for risk assessments, we comment in this chapter on selected entries in the list to demonstrate:

- The variations in content for risk assessments in the standards and guidelines
- Specificity or lack thereof in their content
- The pace and importance of recent activity

There are similarities and differences in the approaches taken by the drafters of these standards and guidelines. Some are industry specific whereas others apply across

Advanced Safety Management: Focusing on Z10 and Serious Injury Prevention, Second Edition. Fred A. Manuele.

all industries. The message they give is clear: Safety professionals will be expected to have knowledge of a variety of hazard analysis and risk assessment methods and how to apply them.

EN ISO 12100–2010: *SAFETY OF MACHINERY—GENERAL PRINCIPLES FOR DESIGN. RISK ASSESSMENT AND RISK REDUCTION.*

This standard, issued in 2010 by the International Organization for Standardization (ISO), has had an interesting history. The standard combines and replaces three previously issued ISO standards. Note that "Risk assessment and risk reduction" are included in the title. That's significant, as it displays the significance that risk assessment has attained in designing for the safety of machinery. The impact of this standard worldwide has been substantial.

ISO 12100–1, Safety of machinery—Basic Concepts, General Principles for Design—Part 1, presented general design guidelines and required that risk assessments be made of machinery going into a workplace. ISO 12100–2, Safety of Machinery—Basic concepts, general principles for design—Part 2: Technical Principles, gave extensive details on design specifications for the "safety of machinery." ISO 14121, Safety of machinery—Principles of risk assessment, set forth the risk assessment concepts to be applied. EN ISO 12100–2010 combines these three standards and retains their content.

EN ISO 12100–2010 is truly an international standard and has had considerable influence worldwide. Its existence implies that a huge majority of countries agree on the principle that hazards should be identified and analyzed and their accompanying risks should be assessed in the design processes for machinery.

The "EN" that precedes "ISO" in the title indicates that the origins of the standard were in the European Community (later, the European Union). Several standards that were applicable in the European Union and had titles beginning with the EN designation became ISO standards. Some of the relative EN standards were written in the 1990s.

The European Union standards have had considerable influence on manufacturers throughout the world. An example follows. Suppliers of products that are to go into a country that is a member of the European Union are required to place a "CE" mark on products to indicate that all operable European Union directives have been met. Risk assessment provisions in EN ISO 12100–2010 are among those requirements.

Additional European Influence

Other developments originating in Europe have also had a noteworthy impact throughout the world. Comments on two of them follow.

BS OHSAS 18001:2007 is the designation for a guideline titled *Occupational health and safety management systems—requirements*, a British Standards Institution publication. In some contract situations, particularly in Asian countries, the bidder is required to establish that its safety management system has been "certified." Among other things, the British Standards Institution has attained prominence as a certifying

entity, and 18001 is the base upon which certification is granted or withheld. In a 2007 revision, requirements for risk assessments became more explicit.

The guidelines now say in Section 4.3.1: "The organization shall establish, implement and maintain a procedure(s) for the ongoing hazard identification, risk assessment, and determination of necessary controls." As an indication of how broadly this guideline is known and used, Singapore adopted it fully as law in 2009.

In August 2008, the European Union (EU) launched a two-year health and safety campaign focusing on risk assessment. Their bulletin states:

> Risk assessment is the cornerstone of the European approach to prevent occupational accidents and ill health. If the risk assessment process—the start of the health and safety management approach—is not done well or not at all, the appropriate preventive measures are unlikely to be identified or put in place.

That statement of the EU is seminal. It states boldly: "Risk assessment is the start of the health and safety management approach; if it is not done well or not at all, safety efforts will be misdirected." It is noteworthy that several European countries have continued with innovation on risk assessment since 2010, the year in which the campaign ended.

B11.TR3-2000: *RISK ASSESSMENT AND REDUCTION—A GUIDELINE TO ESTIMATE, EVALUATE AND REDUCE RISKS ASSOCIATED WITH MACHINE TOOLS*

"TR" stands for "Technical Report." "TR3" is the acronym for a report issued by the B11. TR3 Subcommittee formed by the Machine Tool Safety Standards Committee (B11) of the American National Standards Institute. The secretariat for this work is the Association for Manufacturing Technology.

TR3 became a registered document at ANSI in November 2000, the year immediately following the approval of the robotic standard. Its historic value and its influence are recognized here. Principles set by the TR3 subcommittee follow.

- A simple, practical, and generic hazard analysis and risk assessment process is to be developed that has the potential to be incorporated in all B11 standards.
- The process must apply to both suppliers and users.
- To the extent possible, the technical report is to be harmonized with European standards.

The document produced matches the principles. TR3 is a guideline, not a standard. However, the content of the guideline has been incorporated into almost all of the B11 ANSI standards, of which there are 24.

Over 90% of the guideline is generic. Thus, it is a basic document on hazard analysis and risk assessment that provides guidance on reducing risks according to a prioritized

procedure and on the selection of appropriate design and protective measures. When the process is complete, an acceptable risk level is to be achieved.

As an indication of its influence, almost all of its provisions are now included in the 2010 version of B11.0, the American National Standard entitled *Safety of Machinery—General Requirements and Risk Assessment.*

A Standard of Major Consequence

Because of the breadth of its coverage, ANSI B11.0-2010, *Safety of Machinery—General Safety Requirements and Risk Assessment*, has major consequences. This is its stated purpose: "This standard describes procedures for identifying hazards, assessing risks, and reducing risks to an acceptable level over the life cycle of machinery."

Note that its Scope, as follows, has only one exclusion—portable hand tools: "This standard applies to new, modified or rebuilt power driven machines, not portable by hand, used to shape and/or form metal or other materials by cutting, impact, pressure, electrical or other processing techniques, or a combination of these processes."

The standard includes an explicit requirement that machinery suppliers, reconstructors, modifiers, and users achieve acceptable risk levels. ANSI B11.0 is the most comprehensive standard outlining the risk assessment process currently available for all of the operational categories just mentioned.

The ANSI B11.0 standard is built on standards that preceded it, including EN 1050, ANSI B11 TR3, ANSI/RIA R15.06 (robotics), ANSI B155.1 (packaging machinery), ISO 12100 (safety of machinery), SEMI S10 (semiconductors), and several others. As with most standard development efforts, the writing committee started, with the work completed by others, and then advanced the work to improve the content as part of continuous improvement.

The Foreword from B11.0 includes the following: "The concepts and principles contained in this standard can be applied very broadly to a wide variety of systems and applications." Documented risk assessments were first introduced to:

- The machine tool industry in 2000 with the publication of ANSI B11.TR3, *Risk Assessment and Risk Reduction—A Guide to Estimate, Evaluate and Reduce Risks Associated with Machine Tools*
- The robot industry in 1999 with the publication of ANSI/RIA R15.06, *Requirements for Industrial Robots and Robot Systems*
- The packaging and related machinery industry in 2006 with the publication of ANSI/PMMI B155.1, *Safety Requirements for Packaging Machinery and Packaging-Related Converting Machinery*

The Foreword also states: "Prevention through Design or PtD is a recent term in the industry; the objectives of risk assessment, risk reduction and elimination of hazards as early as possible are integral to and not new to this standard." This objective is also taken from the Foreword:

The objective of the B11 standards is to eliminate injuries to personnel from machinery or machinery systems by establishing requirements for the design, construction, reconstruction, modification, installation, set–up, operation and maintenance of machinery or machine systems. This standard should be used by suppliers and users, as well as by the appropriate authority having jurisdiction. Responsibilities have been assigned to the supplier (i.e., manufacturer, the reconstructor, and the modifier), the user, and the user personnel to implement this standard. This standard is not intended to replace good judgment and personal responsibility. Personnel skill, attitude, training and experience are safety factors that must be considered by the user.

Machines typically have long life spans and ANSI B11.0 addresses the life cycle of machinery. Once a supplier sells a machine, it usually has limited control over it. The user owns the machine and determines where it is to be installed, how it is used, and if, how, and who maintains it. Additionally, machinery is often modified—sometimes for the better or less so.

Comments made here on ANSI B11.0 were written, largely, by Bruce Main, president of design safety engineering. He was the chair of the committee that wrote the standard.

ANSI/AIHA Z10-2012: THE STANDARD FOR *OCCUPATIONAL HEALTH AND SAFETY MANAGEMENT SYSTEMS*

The first version of Z10, approved in 2005, required that processes be in place "to identify and take appropriate steps to prevent or otherwise control hazards and reduce risks associated with new processes or operations at the design stage." Its Annex E was captioned "Assessment and Prioritization". That annex commented on assessing the level of risk and included a hazard analysis and risk assessment guide. But a specific requirement that risk assessments be made was not included in the standard.

Thinking changed. The 2012 version of Z10 has a "shall" provision on risk assessment in Section 5.1.1. It says: "The organization shall establish and implement a risk assessment process(es) appropriate to the nature of hazards and level of risk." Annex F, "Risk Assessment." provides extended guidance.

ANSI/PMMI B155.1-2011: *SAFETY REQUIREMENTS FOR PACKAGING MACHINERY AND PACKAGING-RELATED CONVERTING MACHINERY*

The history of B155.1 dates back to 1972. A revision of the standard was approved by ANSI in 2006, one of several revisions in the intervening 34 years. The secretariat for the standard is the Packaging Machinery Manufacturers Institute.

The major revisions in the 2006 version are indicative of the progress in the 1990s toward acceptance of the premise that hazard analysis and risk assessment provisions should be included in ANSI safety standards.

In the following list of the major steps in the risk assessment process, all were included in the 2006 version except Section 6.8, which was added in the 2011 version. These are the key elements in Section 6:

Section 6.0: The Risk Assessment Process
- 6.1 General
- 6.2 Prepare for/set limits of the assessment
- 6.3 Identify hazards
- 6.4 Assess initial risk
- 6.5 Reduce risk
- 6.6 Assess residual risk
- 6.7 Achieve acceptable risk
- 6.8 Validate risk reduction measures
- 6.9 Document the results

A review made of Section 6, which covers nearly eight pages in small print, indicates that the guidelines are largely generic. Note that in the risk assessment process, risk reduction measures are to be taken, if necessary, after the initial risk assessment and that the resulting residual risk is also to be assessed. The goal of all this is to attain acceptable risk levels through a continual application of the process. That's a sound methodology.

In Section 6.4.1, this requirement is stated: "Risks shall be assessed using a risk scoring system." The example risk scoring system shown in the standard's Table 1 is taken from TR3.

Annex D of the standard is a risk assessment matrix. Several scoring systems are shown, one of which, taken from MIL-STD-882, is given in Table 12.1.

TABLE 12.1 Risk Assessment Matrix

Occurrence Probability	Severity of Harm			
	Catastrophic	Serious	Moderate	Minor
Very likely	High	High	High	Medium
Likely	High	High	Medium	Medium
Unlikely	Medium	Medium	Low	Negligible
Remote	Low	Low	Negligible	Negligible

A MAJOR CONCEPT CHANGE

The following sentence appears in the Foreword for both the 2006 and 2011 versions of B155.1 (and in ANSI B11.0-2010):

> This version of the standard has been harmonized with the international (ISO) and European (EN) standards by the introduction of hazard identification and

risk assessment as the principal method for analyzing hazards to personnel and achieving a level of acceptable risk.

That language presents an interesting and weighty concept. It is a good match with the statement in an EU publication indicating that risk assessment is the cornerstone of the European approach to prevent occupational accidents and ill health.

If all safety professionals accept that hazard identification and risk assessment are the first steps in preventing injuries to personnel, a major concept change in the practice of safety will have been achieved. Adopting that premise takes the focus away from what have been called the unsafe acts of workers and redirects it to work system causal factors. This is sound thinking.

CERTAIN GOVERNMENTAL VIEWS

In a July 19, 2010 letter to the OSHA staff, the assistant secretary David Michaels wrote on several subjects, one of which follows: "Ensuring that American workplaces are safe will require a paradigm shift, with employers going beyond simply attempting to meet OSHA standards, to implementing risk-based workplace injury and illness prevention programs."

If elements in injury and illness prevention programs are to be risk-based, activity will be necessary to identify and assess the risks. That starts with hazard identification and analysis and, then, taking the next step to establish the risk level.

OSHA has not shown that it is adopting the concept of risk-based decision making. This statement by Michaels is noteworthy because it demonstrates that the head of a major governmental entity involved in occupational safety and health has recognized that injury and illness prevention programs should be risk-based. As will be seen, heads of other governmental agencies have reached similar conclusions.

In the December 8, 2010 *Federal Register*, the Federal Railroad Administration issued an advance notice of proposed rulemaking for certain railroads to have a risk reduction program. The *Federal Registry* entry stated: "It is proposed that the Risk Reduction Program be supported by a risk analysis and a Risk Reduction Plan." Enter "Federal Railroad Administration Risk Reduction Program" into a search engine and the following appears.

Risk Reduction Program

The primary mission of the Risk Reduction Program Division is ensuring the safety of the nation's railroads by evaluating safety risks and managing those risks in order to reduce the numbers and rates of accidents, incidents, injuries and fatalities.

Our mission is accomplished by:

- Identifying, collecting and analyzing precursor accident data to identify risks
- Developing voluntary pilot programs in cooperation with stakeholders that are designed to mitigate identified and potential risks

- Propagating and institutionalizing best practices and lessons learned to the entire rail industry
- Providing analytical support, data, and recommendations needed by stakeholders to develop strategies, plans and processes to improve safety and promote positive organizational change
- Developing and enforcing regulations promulgated in response to the Rail Safety Improvement Act of 2008

On March 11, 2011, the Pipeline and Hazardous Materials Safety Administration announced that hazardous materials regulations are to be modified to require that risk assessments be made of loading and unloading operations.

If http://primis.phmsa.dot.gov/meetings/MtgHome.mtg?mtg=70 is entered into an address bar, a report will be found on a meeting held in July 2011 to provide an opportunity for stakeholders to comment. Data-gathering activity continues. The report says, among other things:

> This event is to provide an open forum for exchanging information on identifying threats, improving risk assessments and record keeping for onshore pipelines. Specifically it will:
>
> - Provide a U.S. and International Regulatory perspective on pipeline integrity risk assessments.
> - Provide an operator overview of the challenging factors with conducting risk assessments, canvassing effective approaches, and case studies.
> - Identify options with addressing interactive threats, legacy pipelines and approaches for dealing with recordkeeping gaps.

On October 15, 2010, the Bureau of Ocean Energy Management Regulation and Enforcement (BOEMRE) published the Final Rule for 30 CFR Part 250 Subpart S, Safety and Environmental Management Systems, in the *Federal Register* (75 FR 63610). The Final Rule incorporates by reference, and makes mandatory, the American Petroleum Institute's Recommended Practice for Development of a Safety and Environmental Management Program for Offshore Operations and Facilities (API RP 75), 3rd edition, May 2004, reaffirmed May 2008. This recommended practice, including its appendices, constitutes a complete Safety and Environmental Management System (SEMS).

BOEMRE mandated that by November 15, 2011, all operators and lessees working in the Gulf of Mexico had to submit a comprehensive SEMS plan to the regulator that was required to address the following 13 elements of API RP 75:

1. General Management Program Principles
2. Safety & Environmental Information
3. Hazards Analysis
4. Management of Change
5. Operating Procedures

6. Safe Work Practice
7. Training
8. Quality Assurance/Mechanical Integrity
9. Pre-Startup Review
10. Emergency Response & Control
11. Incident Investigation
12. SEMS Element Audit
13. Documentation and Recordkeeping

This development is of particular interest for two reasons. Operators and lessees affected are required by regulation to make hazards analyses (the first step in making a risk assessment). Also, the plan required is a combination that includes occupational safety, public safety, and environmental safety in one instrument. That combination is a development that needs continual observation. I polled safety directors to determine what proportion of the safety professionals at their locations have responsibilities for both occupational safety and environmental concerns. The range was from 50 to 90%.

Risk assessments have been made for many years in the branches of the military; the National Aeronautics and Space Administration; some chemical operations; the atomic energy field; pharmaceutical companies operating under the rules of the Food and Drug Administration; research activities pertaining to public health; traffic control studies; and other fields.

That additional federal governmental entities have become risk conscious and are requiring that risk assessments be made is an indication of the trend—the subject of this chapter.

ANSI-ASSE Z590.3: *PREVENTION THROUGH DESIGN—GUIDELINES FOR ADDRESSING OCCUPATIONAL HAZARDS AND RISKS IN DESIGN AND REDESIGN PROCESSES*

This standard was approved by the American National Standards Institute on September 1, 2011. Extensive comments are made on the standard in Chapter 16, "Prevention through Design". It is mentioned in this chapter because it is another indication of the trend to have provisions for risk assessments in standards and guidelines. The core of Z590.3 is risk assessment.

MIL-STD-882E-2012: THE U.S. *DEPARTMENT OF DEFENSE STANDARD PRACTICE FOR SYSTEM SAFETY*

As is said in its Foreword: "This Standard is approved for use by all Military Departments and Defense Agencies within the Department of Defense." Certain contractors engaged by those departments and agencies are required to meet the requirements of the standard. This version was approved May 11, 2012. It is

available at http://www.system-safety.org/. Scroll down and click on MIL-STD-882E in the right-hand column for a free copy. I strongly recommend that safety professionals obtain a copy of this standard for informative purposes.

The base document for the *Standard Practice for System Safety, MIL-STD-882*, was issued in 1969. It was a seminal document at that time and has continued to be an important reference. Four revisions of this standard have been issued over a span of 43 years. MIL-STD-882 has had considerable influence on the development of hazard identification and analysis, risk assessment, risk elimination, and risk control concepts and methods throughout the world. Much of the wording on risk assessments and hierarchies of control in safety standards and guidelines issued throughout the world relate to that in the several versions of 882.

MIL-STD-882E extends the previous issue—882D—considerably. For example, the 882D version, including addenda, had 26 numbered pages; the 882E version has 98 numbered pages. It replaces some of what was in 882C that was not included in 882D.

In 882E, achieving and maintaining acceptable risk levels dominates; revisions are made in the system safety process that give additional emphasis to hazard analysis and risk assessment; the use of a risk assessment matrix is required; noteworthy revisions are made in the design order of preference; appropriate emphasis is given to managing High and Serious risk levels; and a major section is devoted to software and software assessments. Excerpts follow, some of which are modified to avoid governmental terminology.

Section 4 in 882E, "General Requirements," sets forth the "requirements for an acceptable system safety effort." Section 4.3 and its subsections, outline and comment on the eight elements in the system safety process, as follows.

Element 1: Document the System Safety Approach. Describe the risk management effort and how the program is integrated into the overall business process.

Element 2: Identify and Document the Hazards. Hazards are identified through a systematic analysis process that includes the system hardware and software, system interfaces (to include human interfaces) and the intended use or application and operational environment.

Element 3: Assess and Document Risk. For each identified hazard, across all system modes, the mishap severity and probability are established in accord with the definitions given. A mishap risk assessment matrix is used to assess and display the risks.

Element 4: Identify and Document Risk Mitigation Measures. Potential risk mitigation(s) shall be identified, and the expected risk reduction(s) of the alternative(s) shall be estimated and documented. The goal should always be to eliminate the hazard if practicable. When a hazard cannot be eliminated, the associated risk should always be reduced to the lowest practicable acceptable risk level within the constraints of cost, schedule, and performance by applying the following system safety design order of precedence in their order of effectiveness.

a. Eliminate hazards through design selection. Ideally, the hazard should be eliminated by selecting a design or material alternative that removes the

hazard altogether. (This is comparable to the "Avoidance" element in Chapter 16, "Prevention through Design".)

b. Reduce risk through design alteration. If adopting an alternative design change or material to eliminate the hazard is not feasible, consider design changes that reduce the severity and/or the probability of the mishap potential caused by the hazard(s).
c. Incorporate engineered features or devices. If mitigation of the risk through design alteration is not feasible, reduce the severity or the probability of the mishap potential caused by the hazard(s) using engineered features or devices. In general, engineered features actively interrupt the mishap sequence and devices reduce the risk of a mishap.
d. Provide warning devices. If engineered features and devices are not feasible or do not adequately lower the severity or probability of the mishap potential caused by the hazard, include detection and warning systems to alert personnel to the presence of a hazardous condition or occurrence of a hazardous event.
e. Incorporate signage, procedures, training, and personal protective equipment (PPE). Where design alternatives, design changes, and engineered features and devices are not feasible and warning devices cannot adequately mitigate the severity or probability of the mishap potential caused by the hazard, incorporate signage, procedures, training, and PPE. Signage includes placards, labels, signs, and other visual graphics. Procedures and training should include appropriate warnings and cautions. Procedures may prescribe the use of PPE. For hazards assigned Catastrophic or Critical mishap severity categories, the use of signage, procedures, training, and PPE as the only risk reduction method should be avoided.

Element 5: Reduce Risk. Mitigation measures are selected and implemented to achieve an acceptable risk level. Consider and evaluate the cost, feasibility, and effectiveness of candidate mitigation methods as a part of the overall operation process.

Element 6: Verify, Validate and Document Risk Reduction. Verify the implementation and validate the effectiveness of all selected risk mitigation measures through appropriate analysis, testing, demonstration, or inspection. Document the verification and validation.

Element 7: Accept risk and Document. Before exposing people, equipment, or the environment to known system-related hazards, the risks shall be accepted by the appropriate authority in accord with established acceptance authority levels. Definitions (in Tables and Matrices in this standard) shall be used to define the risks at the time of the acceptance decision, unless tailored alternative definitions and/or a tailored matrix are formally approved. The user representative shall be a part of this process and shall provide formal concurrence before all Serious and High risk acceptance decisions are made.

TABLE 12.2 Risk Assessment Matrix

Occurrence Probability	Severity of Concequence			
	Catastrophic(1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	This category is used only for identified hazards that are totally removed.			

Element 8: Manage Life-Cycle Risk. After the system is fielded, the system program office uses the system safety process to identify hazards, assess the risks and maintain acceptable risk levels throughout the system's life cycle.

An instruction in Element 7 says that "Definitions (in Tables and Matrices in this standard) shall be used to define the risks at the time of the acceptance decision, unless tailored alternative definitions and/or a tailored matrix are formally approved."

Table I presents severity categories, Table II contains probability levels, and Table III in MIL-STD-882, shown here as Table 12.2, is a risk assessment matrix that combines the severity and probability categories and includes numerical and alphabetical indicators.

Numerical and alphabetical indicators are the base for expressing assessed risks in a risk assessment code (RAC), which is a combination of one severity category and one probability level. For example, a RAC of 1A is the combination of a catastrophic severity category and a frequent probability level.

For emphasis: MIL-STD-882E is an excellent resource document. Its base is hazard identification and analysis and risk assessment.

THE CANADIANS

CSA Standard Z1000-2006, *Occupational health and safety management*, was issued in the year following the first edition of Z10 and has a close relationship with respect to the content and order in the American standard. Section 4.3.4 reads as follows: "The organization shall establish and maintain a process to identify and assess hazards and risks on an ongoing basis. The results of this process shall be used to set objectives and targets and to develop preventive and protective methods." (CSA is the designation for the Canadian Standards Association.) The excerpt above is all that is said in the standard about hazard analysis and risk assessment. The subject is dealt with further in Annex A, which is informative. But the intent of the hazard analysis and risk assessment provision is amplified in the "shall" provision in Section 4.4.7, "Management of Change."

The organization shall establish and maintain procedures to identify, assess, and eliminate or control occupational health and safety hazards and risks associated with

(a) new processes or operations at the design stage
(b) significant changes to its work procedures, equipment, or organizational structure et al.

In September 2012, CSA Z1002-12, *Occupational health and safety—Hazard identification and elimination and risk Assessment and control* was issued. This was a major undertaking. It supports the purpose of Section 4.3.4 in Z1000-2006. The content relates entirely to hazards and risks in the workplace. Its issuance is another indication of the trend throughout the world whereby organizations are encouraged to have processes in place to identify and analyze hazards, to assess their accompanying risks, and to achieve acceptable risk levels.

ADVANCES IN FIRE PROTECTION

There are four entries in Addendum A of this chapter pertaining to activities of the National Fire Protection Association (NFPA) and the Society of Fire Protection Engineers (SFPE). In 2007, NFPA issued "Guidance Document for Incorporating Risk Concepts into NFPA Codes and Standards." This is an impressive, thought-provoking risk assessment–related document that will have a long-term affect in the fire protection field. It is available at http://www.nfpa.org/assets/files/PDF/Research/Risk-Based_Codes_and_Stds.pdf.

As an example of how risk concepts are being incorporated into NFPA standards, the 2112 edition of NFPA 70E, the *Standard for Electrical Safety in the Workplace*, has a new section on risk assessment.

SFPE developed an interesting course entitled "Introduction to Fire Risk Assessment," which is available on the Internet. (No publication date is shown, but it probably was 2006.) A paraphrased and brief version of what is said about the course on the Internet follows:

> This five hour equivalent course is presented free of charge by the Society of Fire Protection Engineers. Although the course was developed primarily for fire service and fire prevention officers, it may be of value to engineers and students who would like to understand fire risk assessment. The full course consists of 19 lecture sessions each of which can be viewed in about 15 minutes.

This course is largely generic and deserves a look. Additional information, including the titles of the lecture sessions and how to access them, can be found at: http://www.sfpe.org/SharpenYourExpertise/Education/SFPEOnlineLearning/FireRiskAssessment.aspx.

In 2006, SFPE also issued the *Engineering Guide to Fire Risk Assessment*. This is a highly technical book that would be of particular interest to engineers. Nevertheless, its issuance demonstrates leadership by SFPE with respect to risk assessment.

DEVELOPMENTS IN AVIATION GROUND SAFETY

One of the most interesting innovations regarding hazard analysis and risk assessment can be found in the *Safety Handbook: Aviation Ground Operation* developed by the International Air Transport Section of the National Safety Council. The Air Transport Section is truly international, having representation from all the populated continents.

A sixth edition was published in July 2007. The following text is taken from Chapter 2, "Risk Management."

> Risk management takes aviation safety to the next level. It is a six-step logic-based approach to making calculated decisions on human, material, and environmental factors before, during and after operations.
>
> Risk management enables senior leaders, functional managers, supervisors and others to maximize opportunities for success while minimizing risks. Failure to successfully implement a risk management process will have a financial, legal and social impact. (p. 9)

The air transport group has outlined a way of thinking about and dealing with hazards and risks, applying a logical and sequential methodology. They have developed a "process to detect, assess, and control risk."

The captions in their six-step logic-based commonsense approach are shown in the *Handbook*'s Table 1. (p. 11) The process is shown here as Table 12.3.

Discussions of each step in the text are extensive. Comments will be made here on the first two only. The remaining steps are addressed in Chapter 14, "Hierarchy of Controls". For the first step—identify the hazards—the hazard analysis and risk assessment methodologies listed in Table 12.4, as in the *Handbook*'s Table 2, are discussed. (p. 10)

For Step 2—Assess the Risks—the text says: "The assessment is the application of quantitative or qualitative measures to determine the level of risk associated with a specific hazard. This process defines the probability and severity of an undesirable event that could result from the hazard. The Risk Assessment Matrix is a very useful tool in categorizing the effects of probability and severity as they relate to risk levels." (p. 12)

TABLE 12.3 The Risk Management Process

1. Identify the hazard.
2. Assess the risk.
3. Analyze risk control measures.
4. Make control decisions.
5. Implement risk controls.
6. Supervise and review.

TABLE 12.4 Hazard Analysis and Risk Assessment Methodologies

1. Operations analysis: Purpose—To understand the flow of events.
2. Hazard analysis: Purpose—To get a quick survey of all phases of an operation. In low-hazard situations, the preliminary hazard analysis may be the final hazard identification tool.
3. "What-if" analysis: Purpose—To capture the input of personnel in a brainstorming-like environment.
4. Scenario process tool: Purpose—To use imagination and visualizations to capture unusual hazards.
5. Change analysis: Purpose—To detect the hazard implications of both planned and unplanned change.

TABLE 12.5 Risk Assessment Matrix: Alphabetical Risk-Level Indicators[a]

	Probability That Something Will Go Wrong				
Severity Categories	Frequent: Likely to occur immediately or soon: often	Likely: Quite likely to occur in time	Occasional: May occur in time	Seldom: Not likely to occur, but possible	Unlikely: Unlikely to occur
Catastrophic: death, multiple injuries, severe property or environmental damage	**E**	**E**	**H**	**H**	**M**
Critical: serious injuries, significant property or environmental damage	**E**	**H**	**H**	**M**	**L**
Marginal: may cause minor injuries, financial loss, negative publicity	**H**	**M**	**M**	**L**	**L**
Negligible: minimum threat to persons or damage to property	**M**	**L**	**L**	**L**	**L**

[a]**E, extremely high risk; H, high risk; M, moderate risk; L, low risk.**

A Risk Assessment Matrix is provided. Its configuration is unusual and it does not duplicate well. The terminology used in the matrix for probability and severity and for the risk gradings are identical with those in Table 11.9, "A Primer on Hazard Analysis and Risk Assessment," with one exception. In the *Handbook*, "M" is the designation for medium risk rather than for moderate risk. The version in Table 11.9 is shown here as Table 12.5.

The National Safety Council's *Safety Handbook: Aviation Ground Operation* is a good, thought-provoking, not overly complex resource document. It is an example of what trade groups can do as a service to their members.

SEMI 02-0712A AND SEMI S10-307E

Safety-related guidelines issued by the semiconductor industry are another indication of recognition by a trade group of the value of using hazard analysis and risk assessment techniques to eliminate or control hazards and to attain acceptable risk levels.

Manufacturers of machinery and equipment used in making semiconductors, and their customers (Intel, IBM, et al.), realized that they had mutual interests that would be better served if that equipment was designed to meet agreed-upon safety guidelines. Their trade association, SEMI (Semiconductor Equipment and Materials International), which has global participation, has issued several safety-related guidelines. Two of them are of interest here: SEMI S2-0712a and SEMI S10-307E.

SEMI S2-0712a, *Environmental, Health, and Safety Guideline for Semiconductor Manufacturing Equipment*, issued in July 2006, updated a 2003 version. The *Guideline* sets forth provisions for manufacturers of equipment to be used in the semiconductor industry. Certain aspects of the *Guideline's* Safety Philosophy (Section 6) are pertinent to this chapter.

> 6.2 The assumption is made that operators, maintenance personnel, and service personnel are trained in the tasks that they are intended to perform.
> 6.4 This guideline should be applied during the design, construction, and evaluation of semiconductor equipment, in order to reduce the expense and disruptive effects of redesign and retrofit.
> 6.8 A hazard analysis should be performed to identify and evaluate hazards. The hazard analysis should be initiated early in the design phase, and updated as the design matures.
> 6.8.1 The hazard analysis should include consideration of:
> - the application or process
> - the hazards associated with each task
> - anticipated failure modes
> - the probability of occurrence and severity of harm
> - the level of expertise of exposed personnel and the frequency of exposure
> - the frequency and complexity of operating, servicing and maintenance tasks
> - safety critical parts

If the equipment is designed in accord with the *Guideline* and the hazard analyses prescribed are conducted, the responsibilities of users (employers) to meet the design review provision in Z10 are accomplished more easily. The hazard analysis is really a risk assessment since both occurrence probability and severity of harm are to be identified.

This *Guideline* also gives employers assistance in meeting the procurement provisions in Z10 that require including safety specifications in purchasing documents. This is item 7.1 in the General Provisions: "This guideline should be incorporated by reference in equipment purchase specifications."

Section 6.8.2 states: "The risks associated with hazards should be characterized using SEMI S10-307E, the title of which is *Safety Guideline for Risk Assessment and Risk Evaluation Process*. This is the purpose of S10.

> The purpose of this guideline is to establish general principles for risk assessment to enable identification of hazards, risk estimation and risk evaluation in a consistent and practical manner. The document provides a framework for carrying out risk assessments on equipment in the semiconductor and similar industries and is intended for use by supplier and purchaser as a reference for EHS considerations.

The hazard identification and analysis processes shown in SEMI S10 duplicate those in SEMI S2. In the risk assessment process, severity of outcome and likelihood of occurrence are to be identified and categorized. In appendices, recommended categories for likelihood and severity are given as well as matrices showing risk categories. The exhibits are comparable to those shown in Chapter 11, "A Primer on Hazard Analysis and Risk Assessment".

ANSI/ASSE Z244.1-2009

In July 2003, approval was given by ANSI for the reissuance of a standard entitled *Control of Hazardous Energy—Lockout/Tagout and Alternative Methods*. It was reaffirmed without change in 2009. This standard will have a broad impact because it affects a huge number of locations. Alternative methods of control are discussed in Section 5.4, which can be paraphrased as follows:

> When lockout/tagout is not used for tasks that are routine, repetitive, and integral to the production process, or traditional lockout/tagout prohibits the completion of those tasks, an alternative method of control shall be used. Selection of an alternative control method by the user shall be based on a risk assessment of the machine, equipment, or process.

The foregoing is significant because a risk assessment is required prior to selecting an alternative risk control method.

THE CHEMICAL INDUSTRY: OSHA REQUIREMENTS

OSHA's Rule for Process Safety Management of Highly Hazardous Chemicals 29 CFR 1910.119, issued in 1992, applies to employers at about 50,000 locations, many of which are not considered chemical companies. With respect to requirements for

hazard analyses being included in standards, this OSHA standard merits a review by safety practitioners. The standard requires that:

> The employer shall perform an initial hazard analysis (hazard evaluation) on processes covered by this standard. The process hazard analysis shall be appropriate to the complexity of the process and shall identify, evaluate, and control the hazards involved in the process. The employer shall use one or more of the following methodologies that are appropriate to determine and evaluate the hazards of the process being analyzed:
>
> - What-If;
> - Checklist;
> - What-If/Checklist;
> - Hazard and Operability Study (HAZOP);
> - Failure Mode and Effects Analysis (FMEA);
> - Fault Tree Analysis; or
> - An appropriate equivalent methodology.
>
> Also, the hazard analysis shall address:
>
> - The hazards of the process;
> - The identification of any previous incident which had a likely potential for catastrophic consequences in the workplace;
> - Engineering and administrative controls applicable to the hazards and their interrelationships;
> - Consequences of failure of engineering and administrative controls;
> - Facility citing;
> - Human factors; and
> - A qualitative evaluation of a range of the possible safety and health effects of failure of controls on employees in the workplace.

Under the requirements for pre-startup safety review for new facilities and for significant modifications, the employer is required to provide a process hazard analysis—among other considerations. In no place in the standard is there mention of occurrence probability. This appears in the preamble to the standard:

> OSHA has modified the paragraph [editorial note: paragraph on consequence analysis] to indicate that it did not intend employers to conduct probabilistic risk assessments to satisfy the requirement to perform a consequence analysis.

However, all risks are not equal. And managements do consider incident probability in their decision making when determining the priority levels that individual projects are to have when allocating resources.

THE CHEMICAL INDUSTRY: EPA REQUIREMENTS

The U.S. Environmental Protection Agency (EPA) and OSHA have different legal authority with respect to accidental releases of harmful substances. The concerns at EPA center on off-site consequences: that is, harm to the public and the environment. At OSHA, the legal authority pertains to on-site consequences.

On August 19, 1996, EPA issued rule 40 CFR Part 68, *Risk Management Programs for Chemical Accidental Release Prevention*. Risk Management Plans required of location managements by the rule were due by June 21, 1999. Although the provisions of the rule are extensive, only the specifications for hazards analyses are addressed here.

Processes subject to this rule are divided into three groups, labeled by the EPA as programs 1, 2, and 3. Program levels relate to the quantities and extent of exposure to toxic and flammable chemicals. For locations qualifying for program levels 1 and 2, those with less exposure, EPA will accept hazard reviews done by qualified personnel using suitable checklists.

Hazard reviews must be documented and show that problems have been addressed. In its literature, EPA comments on the desirability of using the "what-if" hazard identification and analysis process. EPA also proposes the use of more involved analytical techniques if findings suggest that to be desirable.

Hazard review requirement for program level 3 locations are more specific and extensive. But those locations that are compliant with the OSHA rule for process safety management of highly hazardous chemicals will need to do little that is new, although they do need to extend their hazard analyses to consider the probability of harm to the public or to the environment. As with OSHA, a team must complete the process hazard analyses required by EPA. One member of the team, at least, is to have experience with the process.

As would be expected at locations with more significant exposures, the process hazard analysis requirements are more extensive. They must be documented and include:

- Hazards of the process
- Identification of previous, potentially catastrophic incidents
- Engineering and administrative controls applicable to the hazards
- Siting
- Human factors
- Qualitative evaluation of health and safety impacts of control failure

For American industry, EPA has obviously extended knowledge and skill requirements regarding hazard analysis techniques.

THE CHEMICAL INDUSTRY: THE EXTENSIVE BODY OF INFORMATION

Completing hazard analyses was a common practice in the chemical industry many years before requirements for them were established by OSHA and EPA. Although that practice is not of recent origin, it is mentioned here because of its extensive

knowledge requirements. The body of information in the chemical industry on hazard analysis is extensive. But reference will be made here to only one publication because of its particular significance.

The Center for Chemical Process Safety is a part of the American Institute of Chemical Engineers. One of its several books is entitled *Guidelines For Hazard Evaluation Procedures, Second Edition With Worked Examples*. Publication of the text by a chemically oriented group should not dissuade those who want an education in the following evaluation techniques. Their descriptions are generic.

- Safety Review
- Checklist Analysis
- Relative Ranking
- Preliminary Hazard Analysis
- What-If analysis
- What-If Checklist Analysis
- Hazard and Operability Analysis
- Fault Tree Analysis
- Event Tree Analysis
- Cause-Consequence Analysis
- Human Reliability Analysis

These techniques are dealt with broadly in the *Guidelines* in chapters entitled "Overview of Hazard Evaluation Techniques" and "Using Hazard Evaluation Techniques." Brief descriptions of some of those techniques were given in Chapter 11.

CONCLUSION

The message is clear. Including provisions requiring hazard analyses and risk assessments in safety standards and guidelines is becoming ordinary. It is logical to assume that this trend will continue and that safety professionals will be expected to have the knowledge and skill necessary to give counsel on applying those provisions.

REFERENCES

ANSI/AIHA Z10-2012. *Occupational Health and Safety Management Systems*. Fairfax, VA: American Industrial Hygiene Association, 2012. ASSE is now the secretariat. Available at https://www.asse.org/cartpage.php?link=z10_2005.

ANSI/ASSE Z241.1-2009. *Control of Hazardous Energy: Lockout/Tagout and Alternative Methods*. Des Plaines, IL: American Society of Safety Engineers, 2009.

ANSI/ASSE Z690.3, *Risk Assessment Techniques*. Des Plaines, IL: American Society of Safety Engineers, 2011.

ANSI B11.0. *Safety of Machinery—General Safety Requirements and Risk Assessments.* Leesburg, VA: B11 Standards, Inc., 2010.

ANSI/PMMI B155.1-2011. *Safety Requirements for Packaging Machinery and Packaging-Related Converting Machinery.* Arlington, VA: Packaging Machinery Manufacturers Institute, 2011.

API RP 75 (R2008). *Recommended Practice for Development of a Safety and Environmental Management Program for Offshore Operations and Facilities*, 3rd ed. American Petroleum Institute. Go to http://www.techstreet.com/standards/api/rp_75_r2008_?product_id=1157045.

B11.TR3. *Risk Assessment and Reduction—A Guideline to Estimate, Evaluate and Reduce Risks Associated with Machine Tools.* McLean, VA: Association for Manufacturing Technology, 2000.

BOEMRE (Bureau of Ocean Energy Management Regulation and Enforcement). Requirements for SEMS: Safety and Environmental Management Systems, at www.boemre.gov/semp.

BS OHSAS 18001:2007. *Occupational Health and Safety Management Systems—Requirements.* London: British Standards Institution, 2007.

CSA Standard Z1000-06. *Occupational Health and Safety Management.* Mississauga, Ontario, Canada: Canadian Standards Association, 2006.

CSA Standard Z1002-12. *Occupational Health and Safety—Hazard Identification and Elimination and Risk Assessment and Control.* Mississauga, Ontario, Canada: Canadian Standards Association, 2012.

EN ISO 12100–2010. *Safety of Machinery—General Principles for Design. Risk Assessment and Risk Reduction.* Geneva, Switzerland: International Organization for Standardization, 2010.

EPA. *Risk Management Programs for Chemical Accidental Release Prevention.* http://www.epa.gov/emergencies/content/lawsregs/rmpover.htm.

European Union,. Risk Assessment 2008. http://osha.europa.eu/en/topics/riskassessment.

Federal Railroad Administration Risk Reduction Program. Enter the title into a search engine to bring up information; or go to http://www.fra.dot.gov/Page/P0049.

Guidance Document for Incorporating Risk Concepts into NFPA Codes and Standards. National Fire Protection Association, 2007. Available at http://www.nfpa.org/assets/files/PDF/Research/Risk-Based_Codes_and_Stds.pdf.

Guidelines for Hazard Evaluation Procedures, Second Edition with Worked Examples. New York: Center for Chemical Process Safety of the American Institute of Chemical Engineers, 1992.

ISO 10218:1992. *Manipulating Industrial Robots—Safety.* Geneva, Switzerland: International Organization for Standardization, 1992. http://www.iso.ch/iso/en/aboutiso/introduction/index.html.

ISO 12100–1. *Safety of Machinery—Basic concepts, general principles for design; Part 1. Basic terminology, methodology.* Geneva, Switzerland: International Organization for Standardization, 2003.

ISO 12100–2. *Safety of machinery – Basic concepts, general principles for design; Part 2. Technical principles and specifications.* Geneva, Switzerland: International Organization for Standardization, 2003.

ISO 14121. *Safety of Machinery—Principles for risk assessment.* Geneva, Switzerland: International Organization for Standardization, 1999.

Michaels, David. Assistant Secretary at OSHA, July 9, 2010 letter to the OSHA. At http://orc-dc.com/?q=node/3649.

MIL-STD-882E. *Standard Practice for System Safety*. Washington, DC: Department of Defense, 2012 Available at http://www.system-safety.org/. Scroll down and click on MIL-STD-882E in the right-hand column for a free copy.

NFPA 70E, Standard for Electrical Safety in the Workplace, 2112 ed. Begin inquiry at http://us.yhs4.search.yahoo.com/yhs/search;_ylt=A0oG7psAQy1R2CoAgLVXNyoA?p=32.%09NFPA%2070E%2C%20Standard%20for%20Electrical%20Safety%20in%20the%20Workplace%2C%202112%20Edition&fr2=sb-top&hspart=att&hsimp=yhs-att_001& type=att_lego_portal_home&type_param=att_lego_portal_home.

OSHA's Rule for Process Safety Management of Highly Hazardous Chemicals, 29 CFR 1910.119. Washington, DC: Department of Labor, Occupational Safety and Health Administration, 1992.

Pipeline and Hazardous Materials Safety Administration announced their hazardous materials Regulations. See comments at http://primis.phmsa.dot.gov/meetings/MtgHome.mtg?mtg=70.

Risk Management Programs for Chemical Accidental Release Prevention, 40 CFR Part 68. Washington, DC: Environmental Protection Agency, 1996.

Safety Handbook: Aviation Ground Operation, 6th ed. Itasca, IL: National Safety Council, 2007.

SEMI S2-0712a. *Environmental, Health, and Safety Guideline for Semiconductor Manufacturing Equipment*. San Jose, CA: SEMI (Semiconductor Equipment and Materials International), 2006.

SEMI S10-307E. *Safety Guideline for Risk Assessment and Risk Evaluation Process*. San Jose, CA: SEMI (Semiconductor Equipment and Materials International), 2007.

Society of Fire Protection Engineers. *Engineering Guide to Fire Assessment*, 2006. Available at http://findpdf.net/documents/SFPE-engineering-guide-to-fire-risk-assessment.html.

Society of Fire Protection Engineers. *Introduction to Fire Risk Assessment*, 2006b. Enter the title in a search engine for information on the course. Or go to http://www.sfpe.org/SharpenYourExpertise/Education/SFPEOnlineLearning/FireRiskAssessment.aspx.

ADDENDUM A

PARTIAL LIST OF STANDARDS, GUIDELINES, AND INITIATIVES THAT REQUIRE OR PROMOTE MAKING RISK ASSESSMENTS BEGINNING IN 2005

1. ANSI/AIHA Z10-2005, *Occupational Health and Safety Management Systems* standard.

   Z10 sets a benchmark provision requiring that processes be in place: To identify and take appropriate steps to prevent or otherwise control hazards and reduce risks associated with new processes or operations at the design stage.

2. *Guidance On The Principles Of Safe Design For Work.* Australian Safety and Compensation Council, Australian government, 2006.
3. In 2006, NIOSH announced a major national initiative on Prevention through Design.
4. SFPE, *Engineering Guide to Fire Assessment*, 2006. This is a technical book that would be of particular interest to engineers.
5. SFPE, *Introduction to Fire Risk Assessment* [Believe release date was 2006.]

   Enter the title in a search engine for course modules on fire risk assessment.

6. CSA Z1000-2006, the *Occupational Health and Safety Management Standard*, issued by the Canadian Standards Association.

Advanced Safety Management: Focusing on Z10 and Serious Injury Prevention, Second Edition. Fred A. Manuele.

7. The Industrial Safety and Health Act of Japan was revised: effective in April 2006. It stipulates—without penalty—that employers should make efforts to implement risk assessment.
8. ISO 14121–1, *Safety of Machinery—Principles for risk assessment.* 2007.
9. In 2007, the OSHA Alliance Construction Roundtable developed a video training program entitled "Design for Construction Safety."
10. NFPA, *Guidance Document for Incorporating Risk Concepts into NFPA Codes and Standards*, 2007.
11. BS OHSAS 18001:2007, *Occupational health and safety management systems—requirements*, a British Standards Institution publication.

    In the 2007 revision, requirements for risk assessments are more explicit. The guidelines now say: "The organization shall establish, implement and maintain a procedure(s) for the ongoing hazard identification, risk assessment, and determination of necessary controls."

12. The Nano Risk Framework, issued in June 2007 through the combined efforts of the Environmental Defense Fund and DuPont, includes a six-step guidance framework for "the responsible development of nanoscale materials."

    They are: 1. Describe the material and its application; 2. Profile life cycle(s); 3. Evaluate risks; 4. Assess risk management; 5. Decide, document, and act; 6. Review and adapt.

13. ANSI B11.TR7 2007: *ANSI Technical Report for Machines – A Guide on Integrating Safety and Lean Manufacturing principles in the use of Machinery.*
14. China's State Administration of Work Safety published provisional regulations on risk assessment in 2008.
15. The Health and Safety Executive in the UK issued "Five steps to risk Assessment" in 2008.
16. All employers in the UK must conduct a risk assessment. An HSE bulletin says: "The law does not expect you to eliminate all risk, but you are required to protect people as far as is 'reasonably practicable'."
17. In August 2008, the European Union launched a two-year health and safety campaign focusing on risk assessment. Their bulletin states:

    Risk assessment is the cornerstone of the European approach to prevent occupational accidents and ill health. If the risk assessment process—the start of the health and safety management approach—is not done well or not at all, the appropriate preventive measures are unlikely to be identified or put in place.

18. *Machine Safety: Prevention of mechanical hazards.* Issued by The Institute for research for safety and security at work and The Commission for safety and security at work in Quebec, 2009.

19. ASSE Technical Report Z790.001: *Prevention Through Design: Guidelines for Addressing Occupational Risks in the Design and Redesign Processes*, 2009.
20. Singapore Standard SS 506: *Occupational Safety and Health (OSH) Management Systems; Part 1: Requirements*, 2009.
21. ANSI-ITAA GEIA-STD-0010-2009: *Standard Best Practices for System Safety Program Development and Execution.*

    Foreword: Coupled with use of the system safety risk mitigation order of precedence, functional hazard analysis lets a program identify early in the life cycle those risks which can be eliminated by design, and those which must undergo mitigation by other controls in order to reduce risk to an acceptable level.

22. ExxonMobil issued its *Operations Integrity Management System* in July 2009. It pertains to safety, health, the environment and product safety. The first four of 11 elements in this management system are:
    1. Management leadership, commitment, and accountability
    2. Risk assessment and management
    3. Facilities design and construction
    4. Information and documentation
23. ISO/IEC 31000–2009: *Risk Management—Principles and guidelines* and ISO/IEC 31010–2009: *Risk assessment techniques.*
24. EN ISO 12100–2010: *Safety of Machinery—General principles for design. Risk assessment and risk reduction.*

    This standard combines three previously issued ISO standards (including item 8 in this list) and replaces them. Risk assessments are explicitly required.

25. In a July 19, 2010 letter to the OSHA staff, assistant secretary David Michaels wrote on several subjects, one of which follows.

    Ensuring that American workplaces are safe will require a paradigm shift, with employers going beyond simply attempting to meet OSHA standards, to implementing risk-based workplace injury and illness prevention programs.

26. ANSI B11.0: *Safety of Machinery—General Safety Requirements and Risk Assessments*, December 2010.

    Purpose: This standard describes procedures for identifying hazards, assessing risks, and reducing risks to an acceptable level over the life cycle of machinery.

27. In the December 8, 2010 *Federal Register*, the Federal Railroad Administration issued an advance notice of proposed rulemaking for certain railroads to have a risk reduction program.

It is proposed that the Risk Reduction Program be supported by a risk analysis and a Risk Reduction Plan.

28. ANSI/PMMI B155.1—March 2, 2011: *Safety Requirements for Packaging Machinery and Packaging-Related Converting Machinery.*

    Foreword: This version of the standard has been harmonized with international (ISO) and European (EN) standards by the introduction of hazard identification and risk assessment as the principal method for analyzing hazards to personnel and achieving a level of acceptable risk.

29. Pipeline and Hazardous Materials Safety Administration, March 11, 2011.

    Hazardous materials regulations are to be modified to require that risk assessments be made of loading and unloading operations.

30. *OSH Management System: A tool for continual improvement* – issued by the International Labour Organization, Geneva. April 28, 2011.

    Hazard and risk assessments have to be carried out to identify what could cause harm to workers as well as property so that appropriate preventive and protective measures can be developed and implemented.

31. ANSI-ASSE Z590.3—September 1, 2011: *Prevention through Design: Guidelines for Addressing Occupational Hazards and Risks in Design and Redesign Processes.*

    This is an American National Standard. The core of Z590.3 is risk assessment, to be performed as a continuum in the design and redesign processes.

32. NFPA 70E: *Standard for Electrical Safety in the Workplace*, 2112 ed., has a new section on risk assessment.
33. MIL-STD-882E. *Department of Defense Standard Practice for System Safety*, approved May 11, 2012. It is available at http://www.system-safety.org/links/; click on Home. Click on 882E for a free download.
34. ANSI/AIHA Z10-2012: *Occupational Health and Safety Management Systems* standard. The second version of Z10, approved in June 2012, now contains a specific requirement for a risk assessment process to be in place.

    5.1.1 Risk Assessment

    The organization shall establish and implement a risk assessment process(es) appropriate to the nature of hazards and level of risk.

35. CSA Z1002-12: *Occupational Health and Safety—Hazard Identification and Elimination and Risk Assessment and Control.* Canadian Standards Association, 2012.