Prevention Through Design

Addressing occupational risks in the design and redesign processes

By Fred A. Manuele

TRANSFORMATIVE. That's what some have suggested could be the long-term impact of NIOSH's Prevention Through Design (PtD) initiative. Some believe it will lead to a fundamental shift in the practice of safety resulting in greater emphasis being given to the higher and more effective decision-making levels in the hierarchy of controls.

The goal of this initiative, founded on the need to "create a sustainable national strategy for prevention through design," is to "reduce the risk of occupational injury and illness by integrating decisions affecting safety and health in all stages of the design process." To move toward fulfillment of this mission, John Howard, M.D., 2002-08 director of NIOSH, said, "One important area of emphasis will be to examine ways to create a demand for graduates of business, architecture and engineering schools to have basic knowledge in occupational health and safety principles and concepts."

The PtD initiative is based on the premise that "one of the best ways to prevent and control occupational injuries, illnesses and fatalities is to design out or minimize hazards and risks early in the design process" (NIOSH). Notice that this definition limits activity to "early in the design process." At a July 2007 workshop that brought key PtD stakeholders together, many participants called for the concept to be extended to include redesign activities, much as the following definition does:

PtD: Addressing occupational safety and health needs in the design and redesign processes to prevent or minimize the work-related hazards and risks associated with the construction, manufacture, use, maintenance and disposal of facilities, materials, equipment and processes.

Enthusiasm for additional knowledge of PtD principles and practices was significant. Several workshop attendees said it would be helpful if a regulation or a standard were available that sets forth the principles and the methodologies to address hazards and risks in the design and redesign processes. The probability that OSHA could promulgate a regulation or a standard on PtD is unlikely at this time. It is more probable that an ANSI standard could be developed and approved, but that could take several years. For example, ANSI/AIHA Z10-2005 was published 6 years after the secretariat received ANSI approval to begin its work.

Let's assume that the NIOSH initiative, which is a several-year undertaking, is successful. Since hazards analyses and risk assessments are the core of the PtD concept, the impact on the knowledge needs of SH&E practitioners will be significant. As a primer, this article provides guidelines for addressing those needs.

At all levels—management, engineers, safety professionals—it must also be understood that safety standards and guidelines now include more provisions for addressing hazards and risks in the design and redesign processes. Examples of such standards and guidelines include the following:

- ANSI/ASSE Z241.1-2003, Control of Hazardous Energy: Lockout/Tagout and Alternative Methods (ASSE, 2003).
- ANSI/AIHA Z10-2005, Occupational Health and Safety Management Systems (ANSI/AIHA, 2005).
- ANSI/PMMI B155.1-2006, Safety Requirements for Packaging Machinery and Packaging-Related Converting Machinery (ANSI/PMMI, 2006).
- ANSI/RIA R15.06-1999, American National Standard for Industrial Robots and Robot Systems: Safety Requirements (Robotics Industries Association, 1999).
- *Aviation Ground Operation Safety Handbook* (6th ed.) (NSC, 2007).

Fred A. Manuele, P.E., CSP, *is president of Hazards Limited, which he formed after retiring from Marsh & McLennan, for which he was managing director and manager of M&M Protection Consultants. Manuele has published numerous books, including* On the Practice of Safety *and* Advanced Safety Management: Focusing on Z10 and Serious Injury Prevention. *He is an ASSE Fellow and a recipient of the Distinguished Service to Safety Award from National Safety Council. Manuele is a professional member of ASSE's Northeastern Illinois Chapter and a member of the Society's Engineering Practice Specialty.*

•B11.TR3, Risk Assessment and Reduction: A Guideline to Estimate, Evaluate and Reduce Risks Associated With Machine Tools (ANSI/AMT, 2000).

•CSA Z1000-06, Occupational Health and Safety Management (Canadian Standards Association, 2006).

•ISO 14121, Safety of Machinery: Principles for Risk Assessment (ISO, 1999).

•ISO 12100-1, Safety of Machinery: Basic Concepts, General Principles for Design—Part 1 (ISO, 2003).

•SEMI S2-0706, Environmental, Health and Safety Guideline for Semiconductor Manufacturing Equipment (SEMI, 2006).

•SEMI S10-1103, Safety Guideline for Risk Assessment and Risk Evaluation Process (SEMI, 2003).

Promoting the acquisition of knowledge of safety through design/PtD concepts is also in concert with ASSE's position paper on designing for safety. The opening paragraph of that document states:

> Designing for safety (DFS) is a principle for design planning for new facilities, equipment and operations (public and private) to conserve human and natural resources and, thereby, protect people, property and the environment. DFS advocates systematic process to ensure state-of-the-art engineering and management principles are used and incorporated into the design of facilities and overall operations to ensure safety and health of workers, as well as protection of the environment and compliance with current codes and standards (ASSE, 1994).

Scope & Purpose

This article provides guidance on incorporating decisions pertaining to occupational risks into the design and redesign processes, including consideration of the life cycle of facilities, materials, equipment and processes. The goals of applying PtD principles are to:

•achieve safety, which is defined as that state for which the risks are acceptable and tolerable in the setting being considered;

•minimize the occurrence of occupational injuries, illnesses and fatalities.

Since this article is prompted by a NIOSH initiative and since NIOSH is exclusively an occupational safety and health entity, the scope of this article relates principally to the elimination, reduction or control of occupational risks. However, one cannot ignore the fact that the events or exposures which could result in occupational injuries and illnesses can also damage property and the environment, and interrupt business; those additional loss potentials are referred to in several places. In addition, the definition of safety through design—a broader definition than that of PtD—is included in the list of definitions (see sidebar on p. 30).

Application

While these guidelines are applicable to all occupational settings, the focus is on providing assistance to managers, design engineers and safety professionals in smaller organizations (i.e., 1,000 or fewer employees). These guidelines apply to the three major timeframes in the practice of safety:

1) preoperational, in the design process, where the opportunities are greatest and the costs are lower for hazard and risk avoidance, elimination or control;

2) operational mode, where hazards are to be eliminated or controlled and risks reduced before their potentials are realized and hazards-related incidents or exposures occur;

3) postincident, as hazards-related incidents and exposures are investigated to determine causal factors and necessary risk-reduction measures.

Abstract: *Thanks to NIOSH's Prevention Through Design (PtD) initiative, a fundamental shift could occur in the practice of safety that would place greater emphasis on the higher and more effective decision levels in the hierarchy of controls. Since hazards analyses and risk assessments are the core of the PtD concept, the impact on the knowledge needs of SH&E practitioners will be significant. This article provides guidelines addressing those needs.*

Responsibility

Location management must provide the leadership to institute and maintain a policy and procedures affecting the design and redesign processes through which several goals are accomplished:

•Hazards are identified and analyzed.

•Risks deriving from the identified hazards are assessed and prioritized.

•Risks are reduced to an acceptable level through the application of the hierarchy of controls (see discussion starting on p. 37).

These methods are to be applied when new facilities, equipment and processes are acquired; when existing facilities, equipment and processes are altered; and when incidents are investigated.

All who have design responsibilities, as well as the operations personnel who will be affected and SH&E professionals should be involved in the decision-making process. In executing these responsibilities, management may:

•designate qualified in-house personnel to identify and analyze hazards, and assess the risks deriving from them for operations in place;

•employ independent consultants with hazard identification/analysis and risk assessment capabilities to assist with respect to operations in place and in the acquisition of new facilities, equipment, materials or processes;

•enter into arrangements with suppliers of newly acquired facilities, equipment, materials or processes to fulfill these responsibilities.

Relationships With Suppliers

Many organizations do not have design or technical staffs to fulfill the highlighted responsibilities. Thus, to avoid bringing hazards and risks into the workplace when new facilities, equipment, materials and processes are considered, and to ensure that hazards and risks are properly addressed when existing operations are altered, location management should take the following steps:

1) Establish design specifications and objectives.

2) Have an in-depth dialogue with suppliers and contractors on the expected use of the facilities, equipment and processes.

3) Include specifications to minimize bringing hazards and their related risks into the workplace in purchasing agreements and contracts for services.

4) Ask suppliers of services to attest that processes have been applied to identify and analyze hazards and to reduce the risks deriving from those hazards to an acceptable level. [There is precedent for having suppliers attest that risk analyses have been completed. Manufacturers of equipment to be used in the European Union are required by International Organization for Standardization (ISO) standards to certify that they have met applicable standards, including ISO 12100-1 and ISO 14121.]

5) Arrange for staff members (e.g., design engineers, SH&E professionals, maintenance personnel) to visit the supplier of equipment that the staff may consider hazardous, or for which design specifications have been provided to the supplier, before the equipment is shipped to ensure that safety needs have been met.

6) Require that a test run of the equipment is conducted during that visit.

7) Have an additional validation test performed after the equipment has been installed during which safety personnel or others sign off indicating that safety needs have been met.

Safety Through Design Key Terms

Acceptable risk. That risk for which the probability of a hazards-related incident or exposure occurring and the severity of harm or damage that may result are as low as reasonably practicable and tolerable in the setting being considered. (This definition incorporates the ALARP concept.)

ALARP. That level of risk which can be further lowered only by an increment in resource expenditure that cannot be justified by the resulting decrement of risk.

Design. The process of converting an idea or market need into the detailed information from which a product or technical system can be produced.

Hazard. The potential for harm. Hazards include all aspects of technology and activity that produce risk. Hazards include the characteristics of things (e.g., equipment, dusts) and the actions or inactions of people.

Hazard analysis. A process that commences with recognition of a hazard and proceeds into an estimate of the severity of harm or damage that could result if its potential is realized and a hazard-related incident or exposure occurs.

Hierarchy of controls. A systematic way of thinking and acting, considering steps in a ranked and sequential order, to choose the most effective means of eliminating or reducing hazards and the risks that derive from them.

Life cycle. The phases of the facility, equipment, material and processes, including design and construction, operation, maintenance and disposal.

Prevention through design. Addressing occupational safety and health needs in the design and redesign processes to prevent or minimize the work-related hazards and risks associated with the construction, manufacture, use, maintenance, and disposal of facilities, materials, equipment and processes.

Probability. The likelihood of an incident or exposure occurring that could result in harm or damage—for a selected unit of time, events, population, items or activity being considered.

Residual risk. The risk remaining after preventive measures have been taken. No matter how effective the preventive actions, residual risk will always be present if a facility or operation continues to exist.

Risk. An estimate of the probability of a hazards-related incident or exposure occurring and the severity of harm or damage that could result.

Risk assessment. A process that commences with hazard identification and analysis, through which the probable severity of harm or damage is established, and concludes with an estimate of the probability of the incident or exposure occurring.

Safety. That state for which the risks are acceptable and tolerable in the setting being considered.

Safety through design. The integration of hazard analysis and risk assessment methods early in the design and redesign processes and taking the actions necessary so that the risks of injury or damage are at an acceptable level. This concept encompasses facilities, hardware, equipment, tools, materials, layout and configuration, energy controls, environmental concerns and products.

Severity. The extent of harm or damage that could result from a hazards-related incident or exposure.

Conducting Hazards Analyses & Risk Assessments

For many hazards and their associated risks, knowledge gained by management personnel, design engineers and 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 more complex risk situations, however, it is vital to seek the counsel of experienced personnel at all levels who are close to the work or process. Reaching group consensus is a highly desirable goal. Sometimes, for what an SH&E professional considers obvious, achieving consensus is still desirable so that buy-in is obtained for the actions to be taken.

The goal of the risk assessment process, and the subsequent remediation actions, is to achieve acceptable risk levels. The risk assessment and remediation processes are not complete until acceptable risk levels are achieved. Other published standards or guidelines will be considered in the application of these guidelines.

However, applying existing standards may or may not attain acceptable risk levels. Standards offer only minimum requirements or may not contain provisions relating to the hazards in a given situation. Also, as they age, standards may become obsolete and inadequate in relation to more recently developed knowledge.

For example, designing lockout/tagout (LOTO) systems that meet all requirements of the National Electric Code, OSHA standards and ANSI/ASSE Z244.1-2003 may still result in unacceptable risk levels. In the analyses of electrocutions, one causal factor often found is that the LOTO station was inconveniently placed (e.g., 200 ft away, on the floor above), resulting in error-provocative and error-inviting situations. The standards cited do not require that LOTO stations be placed conveniently in the areas where the work is being performed.

A supplementary document to SEMI

S2-0706 is titled "Related Information 1: Equipment/Product Safety Program." This document supports the premise that sometimes one must go beyond issued safety standards in the design process.

> Compliance with design-based safety standards does not necessarily ensure adequate safety in complex or state-of-the-art systems. It often is necessary to perform hazard analyses to identify hazards that are specific with the system, and develop hazard control measures that adequately control the associated risks beyond those that are covered in existing design-based standards (SEMI, 2006).

Although participants in the hazard analysis and risk assessment process will refer to existing standards as resources, the primary goal is to attain acceptable risk levels. A general guide on how to conduct a hazard analysis and how to extend the process into a risk assessment is offered in the following discussion. Whatever the simplicity or complexity of the hazard/risk situation, and whatever analysis method is used (there are many), the thought and action process outlined here is applicable.

Hazard Analysis & Risk Assessment Process

Although the focus is on eliminating, reducing and controlling occupational risks, as noted, this process is equally applicable in avoiding injury to the public, property and environmental damage, business interruption and product liability.

Establish Analysis Parameters

Select a manageable task, system, process or product to be analyzed, and establish its boundaries and operating phase (e.g., standard operation, maintenance, startup). 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 (employees, the public); property; equipment; productivity; the environment.

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 aspects of technology or activity produce risk? What characteristics of things (equipment, dusts) or the actions or inactions of people present a potential for harm? Depending on the complexity of the hazardous situation, some or all of the following may apply:

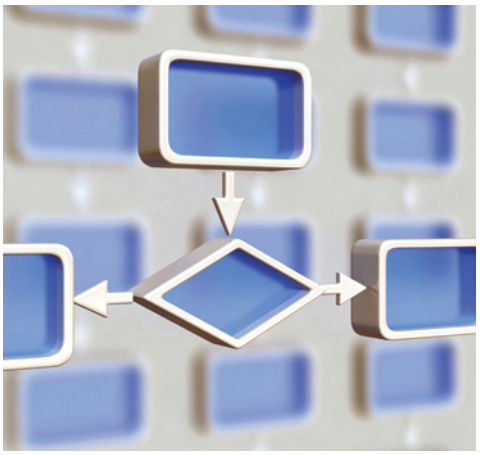
- Use intuitive engineering and operational sense. This is paramount throughout.
- Examine system specifications and expectations.
- Review relevant codes, regulations and consensus standards.
- Interview current or intended system users or operators.
- Consult checklists.
- Review studies from similar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

Consider Failure Modes

Define the possible failure modes that would result in realization of the potentials of the hazards. Consider intentional and foreseeable misuse of facilities, equipment, materials and processes. Ask several questions: What circumstances can arise that would result in the occurrence of an undesirable event? What controls are in place that would mitigate the occurrence of such an event or exposure? How effective are the controls? Can controls be maintained easily? Can controls be defeated easily?

Determine Exposure Frequency & Duration

For each harm or damage category selected for the scope of the analysis (e.g., people, property, business interruption), estimate the frequency and duration of exposure to the hazard. This is an important part of this exercise. For instance, in a workplace situation, more judgments than one might realize will be made in this process. Ask, How often is a task performed? How long is the exposure period? How many people are exposed? What property or aspects of the environment are exposed?



A frame of thinking should be adopted that gets to the bases of causal factors, which are hazards. These questions would be asked: What aspects of technology or activity produce risk? What characteristics of things (equipment, dusts) or the actions or inactions of people present a potential for harm?

Assess the Severity of Consequences

On a subjective basis, the goal is to identify the worst credible consequences should an incident occur, not the worst conceivable consequences. Historical data can be of great value as a baseline. Informed speculations are made to establish the consequences of an incident or exposure. Consider the following:

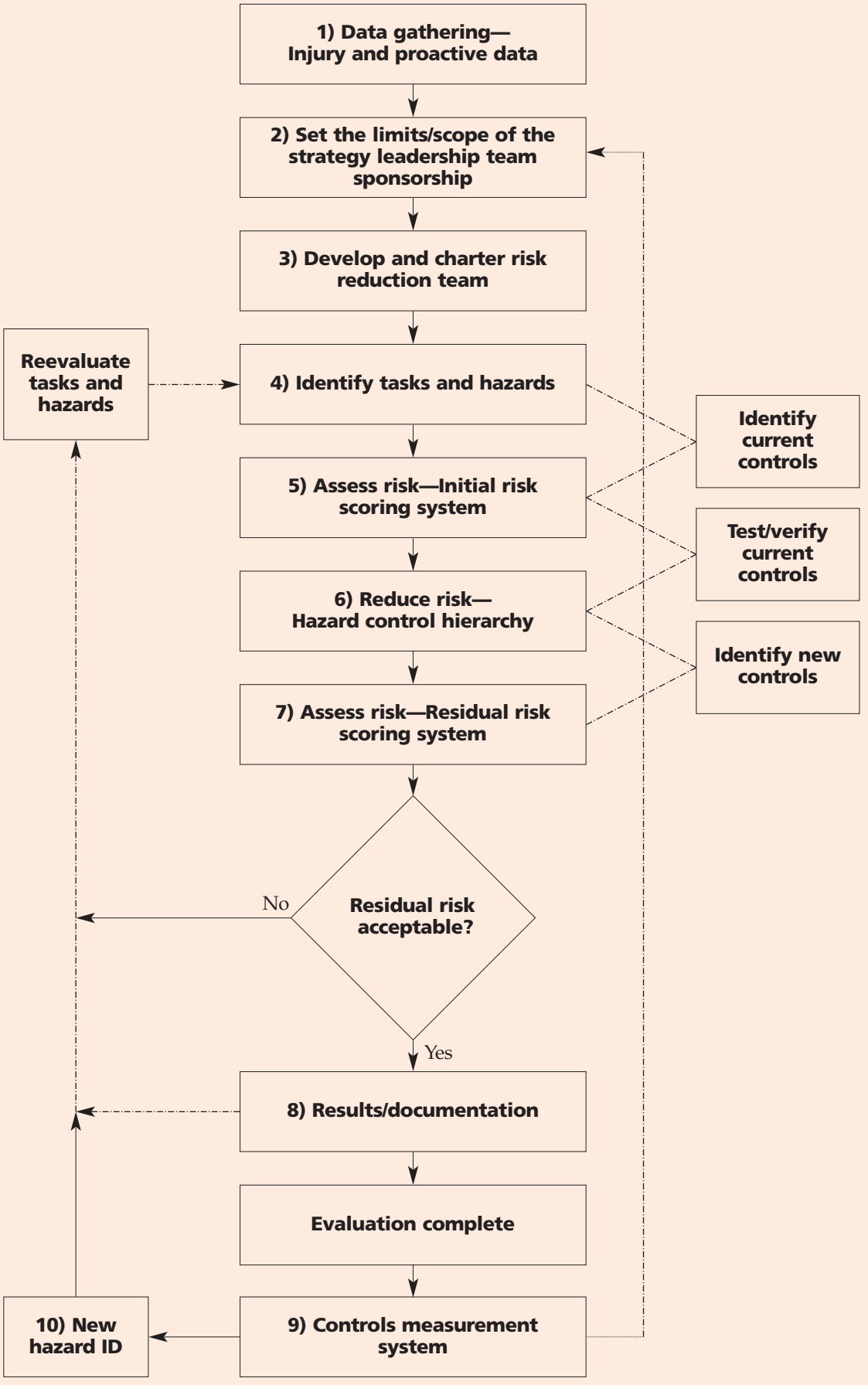
- number of injuries or illnesses and their severity, and fatalities that might occur;
- value of property or equipment that could be damaged;
- time for which the business may be interrupted and productivity lost;
- extent of environmental damage that could occur.

When the severity of the outcome of a hazards-

If the residual risk is not acceptable, the action outlined presented in the hazard analysis and risk assessment process would be applied again.

Figure 1

The Risk Assessment Process



related incident or exposure is determined, a hazard analysis has been completed.

Determine Occurrence Probability

Extending the hazard analysis into a risk assessment requires an additional step—estimating the likelihood (the probability) of a hazardous event or exposure occurring. Unless empirical data are available, which is rare, this is a subjective process. For more complex hazardous situations, it is necessary to brainstorm with knowledgeable people. To be meaningful, probability must 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 product.

Define the Risk

It is necessary to conclude with a statement that contains the:

- probability of a hazards-related incident or exposure occurring;
- expected severity of adverse results;
- risk category (e.g., high, serious, moderate, low).

A risk assessment matrix should be used to identify risk categories. A matrix helps one communicate risk levels to decision makers (see Table 1 and Tables 2 and 3 on p. 34).

Rank Risks in Priority Order

A risk-ranking system should be adopted so that priorities can be established. Since the risk assessment exercise is subjective, this system would also be subjective. Prioritizing risks gives management the knowledge needed to appropriately allocate resources for their elimination or reduction.

Develop Remediation Proposals

When results of the risk assessment indicate that risk elimination, reduction or control measures are to be taken to achieve acceptable risk levels, several actions are needed:

- Alternate proposals for the design and operational changes necessary to achieve an acceptable risk level would be recommended.
- The actions shown in the hierarchy of controls (see pp. 38-39) would be the base on which remedial proposals are made, in the order of their effectiveness.
- Remediation cost for each proposal would be determined and its effectiveness in achieving risk reduction would be estimated.
- Risk elimination or reduction methods would be selected and implemented to achieve an acceptable risk level.

Follow Up on Actions Taken

Good management requires that the effectiveness of actions taken to attain acceptable risk levels be assessed. Follow-up activity would establish that the:

- hazard/risk problem was resolved, only partially resolved or not resolved, as well as whether the actions taken created new hazards;
- risk should be reevaluated and other countermeasures proposed if the risk level achieved is not acceptable or if new hazards have been introduced.

Table 1

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

Document the Results

Documentation, whether compiled under the direction of site management or by the equipment/service provider, should include comments on the:

- risk assessment method(s) used;
- hazards identified and the risks deriving from those hazards;
- reduction measures taken to attain acceptable risk levels.

Residual Risk

Residual risk is that which remains after preventive measures have been taken. No matter how effective the preventive actions, residual risk will always remain if an activity continues. Attaining zero risk is not possible. If the residual risk is not acceptable, the action outline presented in the hazard analysis and risk assessment process would be applied again. (Figure 1 provides an outline of one company's risk assessment process.)

Risk Assessment Matrixes

A risk assessment matrix provides a method to categorize combinations of probability of occurrence and severity of harm, thus establishing risk levels. A matrix helps one communicate about risk reduction actions with decision makers. Also, a matrix can be used to compare and prioritize risks, and to effectively allocate mitigation resources. It should be understood that definitions of terms used for incident probability and severity and for risk levels vary greatly in the many matrixes in use. Thus, an organization should create and obtain broad approval for a matrix that is suitable to the hazards and risks inherent in its operations.

Three examples of risk assessment matrixes are provided. Table 1 is adapted from a matrix in MIL-STD-882 D, Department of Defense Standard Practice for System Safety. (MIL-STD-882, first issued in 1969, is the grandfather of risk assessment matrixes.)

Table 2 (p. 34) is a composite of matrixes that include numerical values for probability and severi-

Table 2

Risk Assessment Matrix: Numerical Gradings

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

Note. *Numbers are arrived at judgmentally and are qualitative. ≥ 15 = very high risk; 9 to 14 = high risk; 4 to 8 = moderate risk; < 4 = low risk.*

Table 3

Risk Assessment Matrix in ANSI B11.TR3-2000

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

Note. *From "Risk Assessment and Reduction: A Guide to Estimate, Evaluate and Reduce Risks Associated with Machine Tools (B11.TR3-2000)," by ANSI/AMT, 2000, McLean, VA: Authors.*

ty levels that are transposed into risk scorings. It is presented here for those who prefer to deal with numbers rather than qualitative indicators. (A word of caution for Table 2: The numbers are arrived at judgmentally and are qualitative.)

Table 3 is taken from ANSI B11.TR3-2000, the ANSI technical report titled "Risk Assessment and Risk Reduction—A Guide to Estimate, Evaluate and Reduce Risks Associated with Machine Tools." It is the base document used when the risk assessments shown in Figure 2 were conducted.

Management Decision Levels

Remedial action or acceptance levels must be attached to the risk categories to permit intelligent management decision making. Table 4 provides a basis for review and discussion. Others who craft risk assessment matrixes may have differing ideas about acceptable risk levels and the management actions to be taken in a given risk situation.

Selecting Probability & Severity

There is no one right method for selecting probability and severity categories and their descriptions, and many variations are in use. Examples in Tables 5 through 8 (pp. 36-37) show variations in the terms and their descriptions as used in applied risk assessment processes for probability of occurrence and severity of consequence.

Hazards Analysis & Risk Assessment Techniques

Over the past 40 years, a large number of hazard analysis and risk assessment techniques have been developed. Clemens (1982) gives brief descriptions of 25 techniques, while Stephans and Talso (1997) describe 101 methods. Brief descriptions of select hazard analysis techniques are offered here. As a practical matter, having knowledge of three techniques—initial hazard analysis and risk assessment, the what-if/checklist analysis methods, and failure modes and effects analysis—will be sufficient to address most risk situations.

It is important to understand that each of these techniques complements, rather than supplants, the others. Selecting the technique or a combination of techniques 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 and exposure probabilities are seldom available. Many quantitative risk assessments are really qualitative risk assessments because so many judgments have to be made when deciding on the probability levels.

Preliminary Hazard Analysis: Initial Hazard Analysis & Risk Assessment

The preliminary hazard analysis technique has its origins in system safety. It is used to identify and evaluate hazards in the very early stages of the design process. In actual practice, however, the tech-

Table 4

Management Decision Levels

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

nique has attained much broader use. The principles on which a preliminary hazard analysis are based are used not only in the initial design process, but also in assessing the risks of existing operations or products. Thus, the technique needs a new name: initial hazard analysis and risk assessment.

Headings on initial hazard analysis forms will include typical identification data such as date, evaluators' names, the department and location. The following information is usually included in an initial hazard analysis process:

- hazard description (also called a hazard scenario);
- description of the task, operation, system, subsystem or product being analyzed;
- exposures to be analyzed: people (employees, the public); facility, product or equipment loss; operation downtime; environmental damage;
- probability interval to be considered: unit of time or activity; events; units produced; life cycle;
- risk assessment code, using the agreed upon risk assessment matrix;
- remedial action to be taken, if risk reduction is needed.

A communication accompanies the analysis, indicating 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 expected completion dates. (Figure 2 presents a sample of an initial hazard analysis and risk assessment worksheet.)

Figure 2

Sample Initial Hazard Analysis & Risk Assessment Worsheet

designsafe Report **Provided by design safety engineering, inc. www.designsafe.com**

Application:	Transfer Line, Machine #334185
Description:	Sample assessment for demonstration
Analyst Name(s):	Steve, Rick, Rob plant operators, Bruce Jones, safety , Tom Woods, engineering
Company:	ABC Company
Facility Location:	Washington, DC
Product Identifier:	Model 89RX-1
Assessment Type:	Detailed
Limits:	This initial risk assessment is for certain Operator tasks
Sources:	on site investigations, discussions w/ plant personnel
Risk Scoring System:	ANSI B11 TR3 Two Factor

Guide sentence: When doing [task], the [user] could be injured by the [hazard] due to the [failure mode].

			Initial Assessment			Final Assessment		
Item Id	User / Task	Hazard / Failure Mode	Severity Probability	Risk Level	Risk Reduction /Comments	Severity Probability	Risk Leve	Status / Responsible / /Reference
1-1-1	operator(s) tool change	mechanical : cutting / severing	Moderate Remote	Negligible	gloves /issue to all new hires	Minor Remote	Negligible	Complete Joe
1-1-2	operator(s) tool change	mechanical : impact dropping heavy tool	Moderate Unlikely	Low	lift assist, standard procedures	Minor Remote	Negligible	Complete
1-1-3	operator(s) tool change	mechanical : pinch points	Minor Remote	Negligible	standard procedures	Minor Remote	Negligible	Complete
1-1-4	operator(s) tool change	mechanical : head bump on overhead objects	Minor Remote	Negligible	other	Minor Remote	Negligible	Complete
1-1-5	operator(s) tool change	ergonomics / human factors : lifting / bending / twisting	Minor Remote	Negligible	look into lift assists or quick release fasteners	Minor Remote	Negligible	Complete Jane
1-1-6	operator(s) tool change	slips / trips / falls : slips	Serious Likely	High	graded floors, non-slip flooring, contain coolant, footwear	Minor Remote	Negligible	In-process Jane
1-2-1	operator(s) remove reject parts	mechanical : cutting / severing	Moderate Remote	Negligible		Minor Remote	Negligible	Complete
1-2-2	operator(s) remove reject parts	mechanical : drawing-in / trapping	Catastrophic Likely	High	interlocked barriers, presence sensing devices, stop line to pull part /requisition submitted	Minor Remote	Negligible	In-process John
1-2-3	operator(s) remove reject parts	mechanical : impact by dropped parts	Moderate Unlikely	Low		Minor Remote	Negligible	Complete
1-2-4	operator(s) remove reject parts	ergonomics / human factors : lifting / bending / twisting	Moderate Remote	Negligible		Minor Remote	Negligible	Complete
1-3-1	operator(s) probe check	Other : None, no hazards						Complete

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, failure modes, how incidents can occur and their probable consequences. Questions posed during this session may commence with what-if, as in "What if the air conditioning fails in the computer room?" or may express general concerns, as in "I worry about the possibility of spillage and chemical contamination during truck off-loading."

All 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 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 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 walkthrough of the area to be surveyed. Checklists are easy to use and provide a cost-effective way to identify customarily recognized hazards.

However, the quality of the checklists depends on the experience of those who develop them. Furthermore, they must be crafted to suit particular facility/operations needs. If a checklist is not complete, the analysis may not identify some hazardous situations.

What-If/Checklist Analysis

The 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 can help the team identify hazards that have the potential to be causal factors for incidents, even though no such incidents have yet occurred. The checklist segment provides a systematic review that can serve as an idea generator during the what-if brainstorming process. Usually, a team experienced in the operation's design, operation and maintenance performs the analysis.

Hazard & Operability Analysis

The hazard and operability analysis (HAZOP) technique was developed to identify both hazards and operability problems in chemical process plants. It has subsequently been applied to a wide range of industry processes and equipment. An interdisciplinary team and an experienced team leader are required. In a HAZOP application, a process or operation is systematically reviewed 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.

A HAZOP usually requires prework in gathering materials and 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 guidewords to develop discussions. As the team reviews each step in a process, several items are documented including:

- deviations and their causal factors;
- consequences should an incident occur;
- safeguards in place;
- required actions or the need for more information to evaluate the deviation.

Table 5

Probability Descriptions: Example A

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

Table 6

Probability Descriptions: Example B

Descriptive word	Probability description
Frequent	Could occur annually
Likely	Could occur once in 2 years
Possible	Not more than once in 5 years
Rare	Not more than once in 10 years
Unlikely	Not more than once in 20 years

Failure Modes & Effects Analysis

In several industries, failure modes and effects analyses (FMEAs) have been the techniques of choice by design engineers for reliability and safety considerations. They are used to evaluate the ways in which equipment fails and the response of the system to those failures. Although an FMEA typically occurs 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 the failure modes, the effects of each failure, safeguards that exist and additional actions that may be necessary. For example, for a pump, the failure modes would include failure 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 documented. Generally, when analyzing impacts the probable worst-case scenario is assumed and analysts would determine whether existing safeguards are adequate. Although an FMEA can be performed by one person, a team is typically appointed

when there is complexity. In either case, the process follows a similar path:

- Identify the item or function to be analyzed.
- Define the failure modes.
- Document the failure causes.
- Determine the failure effects.
- Assign a severity code and a probability code for each effect.
- Assign a risk code.
- Record the actions required to reduce the risk to an acceptable level.

The FMEA process requires entry of probability, severity and risk codes. Figure 3 presents a sample FMEA form on which those codes would be entered. Good references explaining risk coding for FMEA purposes include *Potential Failure Mode and Effects Analysis* (AIAG, 2001) and *Failure Mode and Effects Analysis: A Guide for Continuous Improvement* (International SEMATECH, 1992).

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 the top event. An FTA can be conducted either quantitatively or subjectively. A subjective (or qualitative) analysis can produce suitable results, especially when quantitative numbers are not available. The FTA generates a fault tree (a symbolic logic model) entering failure probabilities for the combinations of equipment failures and human errors that can result in the accident. 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 incident, allowing the analyst to focus preventive measures on significant basic causes. An FTA has particular 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 a more detailed analysis. Conducting an FTA of other than the simplest systems requires the talent of experienced analysts.

Management Oversight & Risk Tree

All of the hazard analysis and risk assessment techniques previously discussed relate principally to the initial design process in the preoperational mode, and to the redesign process to achieve risk reduction in the operational mode. The management oversight and risk tree (MORT) is relative to the postincident time frame in the practice of safety. MORT was developed principally for incident investigations. U.S. Department of Energy (1994) describes MORT as follows:

> 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* (emphasis added).

MORT provides an excellent resource for postincident investigations. Investigation results may prompt use of the hazard identification and analysis and risk assessment methods described.

Table 7

Severity Descriptions for Multiple Harm & Damage Categories: Example A

Descriptive word	Severity description
Catastrophic	Death or permanent total disability, system loss, major property damage and business downtime
Critical	Permanent, partial, or temporary disability in excess of 3 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 8

Severity Descriptions for Multiple Harm & Damage Categories: Example B

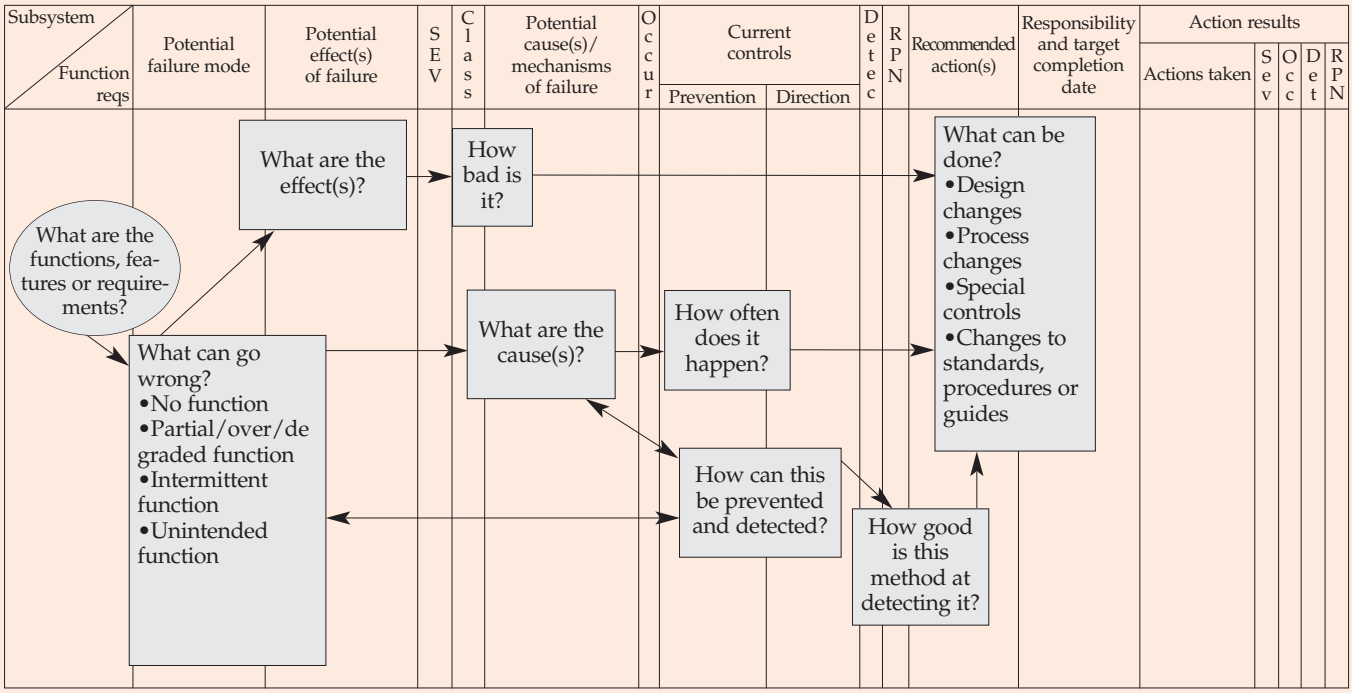
Descriptive word	Severity description
Catastrophic	One or more fatalities, total system loss, chemical release with lasting environmental or public health impact
Critical	Disabling injury or illness, major property damage and business down time, chemical release with temporary environmental or public 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

Hierarchy of Controls

A hierarchy of controls provides a systematic way of thinking, considering steps in a ranked and sequential order, to choose the most effective means of eliminating or reducing hazards and their associated risks. Acknowledging that premise—that risk-reduction measures should be considered and taken in a prescribed order—represents an important step in the evolution of the practice of safety.

Figure 3

Sample FMEA Form



Note. *From* Potential Failure Mode & Effects Analysis *(3rd ed.), by Automotive Industry Action Group (AIAG), 2001, Southfield, MI: Author. Copyright 2001 by AIAG. Reprinted with permission.*

Achieving Acceptable Risk

In applying a hierarchy of controls, the desired outcome of actions taken is to achieve an acceptable risk level. Acceptable risk, as previously defined, is that risk for which the probability of a hazards-related incident or exposure occurring and the severity of harm or damage that could result are as low as reasonably practicable and tolerable in the situation being considered. That definition requires several factors be taken into consideration:

- avoiding, eliminating or reducing the probability of a hazards-related incident or exposure occurring;
- reducing the severity of harm or damage that may result if an incident or exposure occurs;
- the feasibility and effectiveness of risk-reduction measures to be taken, and their costs, in relation to the amount of risk reduction to be achieved.

Six Levels of Action

Decision makers should understand that with respect to the six levels of action shown in the following hierarchy of controls the methods described in the first, second and third action levels are more effective because they:

- are preventive actions that eliminate/reduce risk by design, substitution and engineering measures;
- rely the least on the performance of personnel;
- are less defeatable by supervisors or workers.

Actions described in the fourth, fifth and sixth levels are contingent actions and rely greatly on the performance of personnel for their effectiveness.

The following hierarchy of controls is considered state-of-the-art, and it is compatible with the hierarchy in ANSI/AIHA Z10-2005:

1) Eliminate or reduce risks in the design and redesign processes.
2) Reduce risks by substituting less hazardous methods or materials.
3) Incorporate safety devices.
4) Provide warning systems
5) Apply administrative controls (e.g., work methods, training, work scheduling).
6) Provide PPE.

The Logic of Taking Action in the Order Given

The following discussion addresses each action element in the hierarchy of controls, including providing a rationale for listing actions to be taken in the order given. Taking actions in the prescribed order, as feasible and practicable, is the most effective means to achieve risk reduction.

Eliminate or Reduce Risk in the Design & Redesign Processes

The theory is plainly stated. If hazards are eliminated in the design and redesign processes, risks that derive from those hazards are also eliminated. But, elimination of hazards completely by modifying the design may not always be practicable. In such cases, the goal is to modify the design, within practicable limits, so that the 1) probability of personnel making human errors because of design inadequacies is at a minimum; and 2) ability of personnel to defeat the work system and the work methods prescribed, as designed, is at a minimum. Examples would include designing to eliminate or reduce the risk from hazards related to falls, ergonomics, confined space entry, electricity, noise and chemicals.

Substitute Less-Hazardous Method/Material

Substitution of a less-hazardous method or material may also reduce the risks. However, substitution may or may not result in equivalent risk reduction as

might occur if the hazards and risks were addressed through system design or redesign.

Consider this example. A mixing process for chemicals involves considerable manual materials handling. A reaction occurs and an employee sustains serious chemical burns. Identical operations are performed at two of the company's locations. At one, the operation is redesigned so that it is completely enclosed, automatically fed and operated by computer from a control panel, thus greatly eliminating operator exposure.

At the other location, redesign funds are not available. To reduce the risk, the supplier agrees to premix the chemicals before shipment (substitution). Some mechanical feed equipment for the chemicals is also installed. The risk reduction achieved by substitution is not equivalent to that attained by redesigning the operation, so additional administrative controls are required.

Methods that illustrate substituting a less-hazardous method, material or process include using automated materials handling equipment; providing an automatic feed system to reduce machine hazards; using a less-hazardous cleaning material; reducing speed, force or amperage; reducing pressure or temperature; replacing a dated steam heating system and its boiler explosion hazards with a hot-air system.

Incorporate Safety Devices

When safety devices are incorporated into the system in the form of engineering controls, substantial risk reduction can be achieved. Engineered safety devices are intended to prevent access to the hazard by workers—to separate hazardous energy from the worker and deter worker error. Examples include machine guards, interlock systems, circuit breakers, start-up alarms, presence-sensing devices, safety nets, ventilation systems, sound enclosures, fall prevention systems, and lift tables, conveyors and balancers.

Install Warning Systems

Warning system effectiveness relies considerably on administrative controls, such as training, drills, the quality of maintenance and the reactions of people. Although vital in many situations, warning systems may be reactionary in that they alert people only after a hazard's potential is in the process of being realized (e.g., a smoke alarm). Examples of warning systems include smoke detectors, alarm systems, backup alarms, chemical detection systems, signs and alerts in operating procedures or manuals.

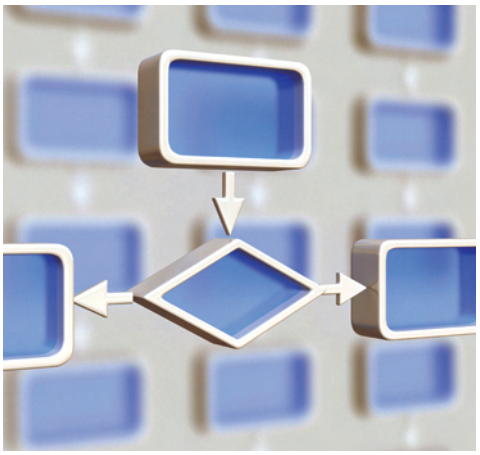
Institute Administrative Controls

Administrative controls rely on the methods chosen being appropriate in relation to needs, the capabilities of those responsible for their delivery and application, the quality of supervision and the expected performance of the workers. Administrative controls include personnel selection, developing and applying appropriate work methods and procedures, training, supervision, motivation, behavior modification, work scheduling, job rotation, scheduled rest periods, maintenance, management of change, investigations and inspections.

Achieving a superior level of effectiveness in all of these administrative methods is difficult and not often accomplished.

Provide Personal Protective Equipment

The proper use of PPE relies on an extensive series of supervisory and personnel actions, such as identifying and selecting the type of equipment needed, proper fitting and training, inspecting and maintaining. Although PPE is necessary in many occupational situations, it is the least effective way to deal with hazards and risks because systems put in place for their use can be easily defeated. One goal of the design processes should be to reduce reliance on PPE to a practical minimum, applying the ALARP concept. PPE examples include safety glasses, face shields, respirators, welding screens, safety shoes, gloves and hearing protection.



In any risk situation assessed, the expectation is that each step will be considered in descending order and that reasonable attempts will be made to eliminate or reduce hazards and their associated risks through steps higher in the hierarchy before lower steps are considered.

The Descending Order of Controls

For many risk situations, a combination of the risk management methods in the hierarchy of controls is necessary to achieve acceptable risk levels. However, the expectation is that each step will be considered in descending order and that reasonable attempts will be made to eliminate or reduce hazards and their associated risks through steps higher in the hierarchy before lower steps are considered. A lower step in the hierarchy of controls is not to be chosen until practical applications of the preceding level or levels are exhausted.

A yet-to-be published document, MIL-STD-882E, includes provisions that further explain the governing thought processes when the hierarchy of controls is applied. Excerpts from this standard follow.

> System safety mitigation order of precedence as in 882E: In reducing risk, the cost, feasibility, and effectiveness of candidate mitigation methods should be considered. In evaluating mitigation effectiveness, an order of precedence generally applies as follows.
>
> a) Eliminate hazard through design selection: Ideally, the risk of a hazard should be eliminated. This is often done by selecting a

design alternative that removes the hazard altogether.

b) Reduce mishap risk through design alteration: If the risk of a hazard cannot be eliminated by adopting an alternative design, design changes should be considered that reduce the severity and/or the probability of a harmful outcome.

c) Incorporate engineered safety features (ESF): If unable to eliminate or adequately mitigate the risk of a hazard through a design alteration, reduce the risk using an ESF that actively interrupts the mishap sequence.

d) Incorporate safety devices: If unable to eliminate or adequately mitigate the hazard through design or ESFs, reduce mishap risk by using protective safety features or devices.

e) Provide warning devices: If design selection, ESFs, or safety devices do not adequately mitigate the risk of a hazard, include a detection and warning system to alert personnel to the presence of a hazardous condition or occurrence of a hazardous event.

f) Develop procedures and training: Where other risk reduction methods cannot adequately mitigate the risk from a hazard, incorporate special procedures and training. Procedures may prescribe the use of personal protective equipment (U.S. Department of Defense, 2005).

Conclusion

SH&E professionals cannot ignore the favorable impact of the PtD movement. It is becoming evident that the primary focus is risk—identifying and analyzing hazards, and assessing the risks deriving from them. The entirety of purpose of those responsible for safety is to manage their endeavors with respect to hazards so that their associated risks are acceptable. ■

References

ANSI/AIHA. (2005). Occupational health and safety management systems (ANSI/Z10-2005). Fairfax, VA: Authors.

ANSI/ASSE. (2003). Control of hazardous energy: Lockout/tagout and alternative methods (ANSI/ASSE Z241.1-2003). Des Plaines, IL: Authors.

ANSI/Association for Manufacturing Technology (AMT). (2000). Risk assessment and reduction: A guide to estimate, evaluate and reduce risks associated with machine tools (B11.TR3-2000). McLean, VA: Authors.

ANSI/Packaging Machinery Manufacturers Institute (PMMI). (2006). Safety requirements for packaging machinery and packaging-related converting machinery (B155.1-2006). Arlington, VA: Authors.

ANSI/Robotics Industries Association (RIA). (1999). American national standard for industrial robots and robot systems: Safety requirements (ANSI/RIA R15.06-1999). Ann Arbor, MI: Authors.

ASSE. (1994). Position paper on designing for safety. Des Plaines, IL: Author.

Automotive Industry Action Group (AIAG). (2001). *Potential failure mode and effects analysis: FMEA* (3rd ed.). Southfield, MI: Author.

Canadian Standards Association (CSA). (2006). Occupational health and safety management (CSA Z1000-06). Ottawa, Ontario: Author.

Center for Chemical Process Safety. (1992). *Guidelines for hazard evaluation procedures* (2nd ed. with worked examples). Hoboken, NJ: John Wiley & Sons.

Christensen, W.C. (2003, March). Safety through design: Helping design engineers answer 10 key questions. *Professional Safety, 48*(3), 32-39.

Christensen, W.C. (2007, May). Retrofitting for safety: Career implications for SH&E personnel. *Professional Safety, 52*(5), 36-44.

Christensen, W.C. & Manuele, F.A. (2000). *Safety through design.* Itasca, IL: National Safety Council.

Clemens, P. (1982, March/April). A compendium of hazard identification and evaluation techniques for system safety application. *Hazard Prevention, 2*(2), 11-18.

Flamberg, S., Leverenz, F., Rose, S., et al. (2007). Guidance document for incorporating risk concepts into NFPA codes and standards. Quincy, MA: The Fire Protection Research Foundation. Retrieved Sept. 2, 2008, from http://www.nfpa.org/assets/files//PDF/Research/Risk-base_Codes_and_Stds-Appendices.pdf.

International Organization for Standardization (ISO). (1999). Safety of machinery: Principles for risk assessment (ISO 14121). Geneva, Switzerland: Author.

ISO. (2003). Safety of machinery: Basic concepts, general principles for design—Part 1: Basic terminology, methodology (ISO 12100-1). Geneva, Switzerland: Author.

International SEMATECH. (1992). *Failure mode and effects analysis (FMEA): A guide for continuous improvement for the semiconductor equipment industry* (Technology Transfer No. 92020963A -ENG). Austin, TX: Author. Retrieved Sept. 2, 2008, from http://www.fmeainfocentre.com/handbooks/sematechsemiconductorfmeahandbook.pdf.

Main, B. (2002, July). Risk assessment is coming. Are you ready? *Professional Safety, 47*(7), 32-37.

Main, B. (2004). *Risk assessment: Basics and benchmarks.* Ann Arbor, MI: design safety engineering inc.

Main, B. (2004, Dec.). Risk assessment: A review of the fundamental principles. *Professional Safety, 49*(12), 37-47.

Manuele, F.A. (2003). *On the practice of safety* (3rd ed.). Hoboken, NJ: John Wiley & Sons.

Manuele, F.A. (2005, May). Risk assessments and hierarchies of control. *Professional Safety, 50*(5), 33-39.

Manuele, F.A. (2006, Feb.). ANSI/AIHA Z10-2005: The new benchmark for safety management systems. *Professional Safety, 51*(2), 25-33.

Manuele, F.A. (2007). *Advanced safety management: Focusing on Z10 and serious injury prevention.* Hoboken, NJ: John Wiley & Sons.

National Safety Council. (2007). *Aviation ground operation safety handbook* (6th ed.). Itasca, IL: Author.

NIOSH. Prevention through design (NIOSH Safety and Health Topic). Washington, DC: U.S. Department of Health and Human Services, Centers for Disease Control and Prevention, Author. Retrieved Sept. 3, 2008, from http://www.cdc.gov/niosh/topics/ptd.

Semiconductor Equipment and Materials International (SEMI). (2006). Environmental, health and safety guideline for semiconductor manufacturing equipment (SEMI S2-0706). San Jose, CA: Author.

Society of Fire Protection Engineers (SFPE). (2006). *SFPE engineering guide to fire risk assessment.* Bethesda, MD: Author.

Stephans, R. (2004). *System safety for the 21st century.* Hoboken, NJ: John Wiley & Sons.

Stephans, R. & Talso, W.W. (Eds.). (1997). *System safety analysis handbook: A sourcebook for safety practitioners.* Albuquerque, NM: System Safety Society, New Mexico Chapter.

Swain, A.D. (1963). *Work situation approach to improving job safety* (Report SC-R-69-1320). Albuquerque, NM: Sandia Laboratories.

U.S. Department of Defense. (2000). Standard practice for system safety (MIL-STD-882D). Washington, DC: Author. Retrieved Sept. 2, 2008, from http://www.safetycenter.navy.mil/instructions/osh/milstd882d.pdf#search='MILSTD882D.

U.S. Department of Defense. (2005). Draft standard practice for system safety (MIL-STD-882E). Washington, DC: Author. Retrieved Sept. 3, 2008, from http://www.system-safety.org/~casacramento/Standards.htm.

U.S. Department of Energy. (1994). *Guide to use of the management oversight and risk tree* (SSDC-103). Washington, DC: Author.

Vincoli, J.W. (1993). *Basic guide to system safety.* Hoboken, NJ: John Wiley & Sons.