Risk Assessment

A review of the fundamental principles

By Bruce W. Main

THE FUNDAMENTALS OF RISK ASSESSMENT are common across the various methods available:

- Identify hazards.
- Assess risk.
- Reduce risk.
- Document results.

The goal of risk assessment is to reduce risks to an acceptable (or tolerable) level. (The terms "acceptable risk" and "tolerable risk" are synonomous in this context. See Main for further discussion.) The risk reduction process is not completed until tolerable risk is achieved. Figure 1 illustrates the overall risk assessment process, which comprises seven steps. This article identifies preparations that need to occur before a risk assessment begins, and presents the basic risk assessment process in a step-by-step approach to help the user achieve the overall goal.

The Value of Risk Assessment

Although risk assessment methods have existed in various forms for many years, interest has increased in recent years because of several factors:

- **Time.** The design cycle is under ever-increasing compressive pressure, which reduces tolerance for late changes or safety fixes.
- **Cost.** Significant opportunities exist for productivity gains and cost efficiencies. (See "Conveyor Design" sidebar on pg. 39.)
- **Competition.** Reducing costs and increasing productivity through risk assessment improvements provides a competitive advantage.
- **International influences.** Through the CE mark, the European Union (EU) explicitly requires a risk assessment. (See "CE Mark" sidebar on pg. 39.)
- **Capturing knowledge.** A completed risk assessment can be used to capture much of the knowledge pertinent to the design being considered that can be applied to similar designs.
- **Product liability.** Risk assessments help reduce exposure to hazards and can support a successful defense against a product liability claim.
- **Lack of standards.** When industry or government standards have only general performance criteria, do not exist or have not kept pace with technological change, risk assessments provide a basis on which to make credible design decisions.
- **Schedule control.** A risk assessment permits a company to make reasoned decisions and move quickly to implement them.
- **Customer requirements.** Some advanced industrial customers are beginning to require that suppliers conduct risk assessments.

Any one of these factors could be a business reason that a SH&E practitioner might use to convince his/her company to allocate resources necessary to conduct a risk assessment. The risk assessment process is quickly gaining momentum because companies are finding value in the results. [A more detailed discussion of these factors is contained in Manuele(b); Main; and Christensen and Manuele.]

Applications of the Risk Assessment Process

The risk assessment process applies to an array of applications. Risk assessments are performed for consumer products, industrial machinery and in occupational settings. Industries such as robotics, machine tooling, packaging machinery, elevators, medical devices, aviation and semiconductors have incorporated the process into standards and guidelines. Risk assessment also appears in cross-industry applications such as process controls, control of hazardous energy (lockout/tagout), environmental and food (Main).

Preparing for the Risk Assessment Effort

Form a Team

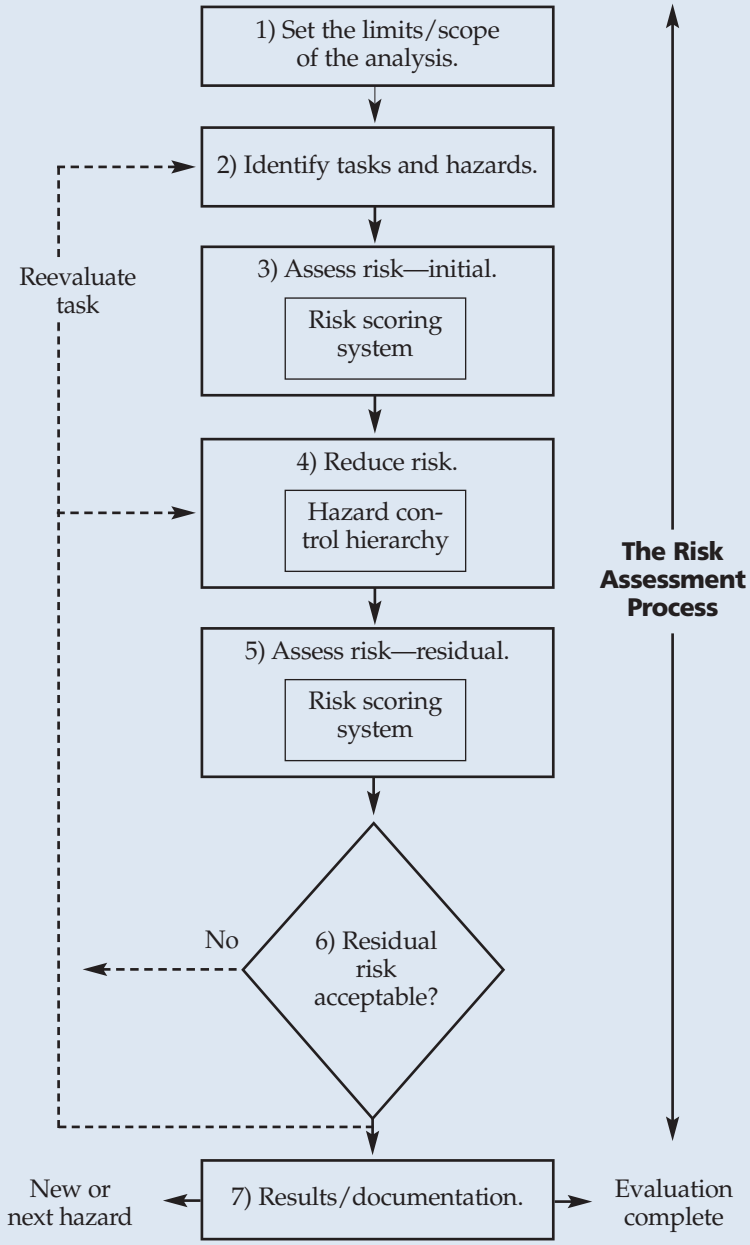
To be most effective, risk assessments should be conducted by a team. The team should include as many affected individuals as reasonably practical. Team members may vary from company to company and industry to industry, but some common elements exist.

- Engineers should be intimately involved in a risk assessment. Since engineers make many design decisions during the course of development, they need to be aware of the impact of their decisions on user safety and risk. Engineers should be involved in developing risk reduction methods, particularly those involving design changes.
- Workers, customers or users should be involved, as these people tend to be most familiar with the tasks and uses to which the design will be submitted. They are best able to help identify hazards associated with their tasks, and can provide valuable insights on practical constraints and opportunities on how to reduce risk.
- SH&E practitioners are often involved. In many cases, the practitioner

Bruce W. Main, P.E., CSP, *is president of Design Safety Engineering Inc., Ann Arbor, MI. He holds mechanical engineering degrees from MIT and the University of Michigan, and an M.B.A., also from the University of Michigan. Main is a member of several national and international standards committees addressing risk assessment. He is also ASSE's primary representative to the B11 Committee (machine tool industry). Main is a member of ASSE's Greater Detroit Chapter.*

Figure 1

The Risk Assessment Process



Source: Main, B.W. Risk Assessment: Basics and Benchmarks.

may lead the risk assessment effort due to his/her ability to identify hazards.

•Management should be involved, particularly in making decisions on risk reduction methods and/or accepting residual risk levels.

•If maintenance tasks will occur, then maintenance personnel should be involved to ensure that these tasks and related hazards are identified.

•The team leader should be familiar with the risk assessment process. This role can be assumed by consultants or knowledgeable internal personnel.

•Risk assessment specialists may also be involved, particularly when quantitative analyses are conducted. The specialist may conduct or facilitate risk assessments, lead risk assessment efforts or provide follow-through on risk reduction methods.

•Other situations may involve legal counsel, insurers and others. For example, if product liability is a significant concern, the risk assessment team should consult with an attorney. This person can bring a legal perspective to the project and may protect documents through the attorney/client privilege.

McNab clearly states that specialists should not be the sole instrument of risk assessments and risk management: "The task of risk management should *not* be limited to a few specialists. The power of risk management will increase if many employees use its basic principles on a daily basis" (emphasis in original) (McNab). Furthermore, the Norwegian offshore industry standard NORSOK Z-013 states that "experience has shown that the users of the analysis results need to be actively involved in the risk evaluation in order for it to be effective" (Norwegian Center for Ecological Agriculture).

Assign Responsibilities

Before beginning a risk assessment effort, the responsibilities of key players need to be clearly defined. Even though the risk assessment concept may be generally considered a favorable idea, responsibility can get quickly passed from person to person because few candidates likely have time to take the lead. In general, the following separation of responsibilities will apply.

•**Senior management.** Allocates appropriate personnel, time and resources to permit the assessment to be successfully completed; holds ultimate responsibility to determine level(s) of acceptable risk.

•**SH&E professional.** Identifies hazards, proposes risk reduction methods, and follows through on implementing risk reduction methods and completing the risk assessment.

•**Project leader.** Leads the risk assessment process and keeps it on schedule; also responsible for overall risk assessment documentation and for ensuring that all risks are reduced to an acceptable level before a product is released to production.

•**Risk assessment team.** Identifies all reasonably foreseeable hazards associated with the design and assigns risk reduction responsibility for particular hazards; this team must develop consensus assessments of individual hazard risk and is responsible for documenting the risk assessment.

•**Design engineers.** Participate on the risk assessment team; also responsible for identifying hazards, ensuring that the risk assessment team is aware of the hazards; and developing risk reduction solutions where appropriate.

Gather Appropriate Information

Before beginning a new assessment, the risk assessment team should identify any existing assess-

ments conducted on previous hardware version(s) or for similar products that might be applicable. Predecessor risk assessments can be templates or starting points to speed the process. In addition, the team should obtain resource information needed to conduct the risk assessment. Such information may include:

- design layout and proposed system(s) integration;
- information on energy sources;
- accident and incident history;
- design limitation;
- lifecycle requirements;
- system drawings, sketches or detailed descriptions;
- information on product materials to be used and potential damage to health.

Once preparations have been made, the team can begin working through the steps of the risk assessment process.

Conveyor Design

Is there really value in the risk assessment process? Consider this example.

A manufacturing process at an auto component supplier includes a large oven to bake a finish on the parts. Occasionally, parts can fall off the conveyor, become jammed or otherwise require unplanned service. The designers did not identify or adequately plan for these unplanned tasks. The time required for the oven to cool sufficiently to permit entry is eight hours, with another four hours needed to reheat, in addition to repair time. A risk assessment identified these maintenance tasks and the associated risks, and enabled engineering changes to be identified that minimize conveyor problems and reduce correction duration if they do occur. In this situation, the value derived from the risk assessment process includes improved production time, reduced costs, increased competitive position and better schedule control.

The Step-by-Step Process

1) Set the Limit/Scope of the Risk Assessment

Before an assessment begins, project parameters should be clearly established. These will be set by management with input from the risk assessment team. The limits can relate to equipment or product design, facility or location, the environment, uses and misuses, exposure interval (time) or particular users. Limits can include specific tasks, locations, operational states (e.g., shutdown) or space constraints. Other limits could include what can be harmed or damaged, such as people (the public, employees), property, equipment, productivity or the environment. The team should document these parameters so that it understands and communicates the nature of its evaluation. A key part of this step is establishing the level(s) of acceptable risk (Manuele and Main).

CE Mark

The European General Product Safety Directive 2001/95/EC requires that consumer products sold in the EU bear the CE mark and meet all relevant EU directives. The CE mark is required on consumer products sold in the EU and indicates conformity to the "common level of safety." Through this demarcation, the EU explicitly requires a risk assessment and analysis of the hazards in accordance with the hazard elimination and control hierarchy. A consumer product manufacturer must declare that its products comply with all relevant CE-marking directives and indicate so by affixing the CE mark. The manufacturer bears the responsibility to determine which EU directives apply to its products.

Identifying the assessment scope helps the team focus efforts to stay on track. It also helps communicate the focus of a particular assessment to those outside the team. Partial assessments that concentrate on certain design aspects or certain high-risk uses are acceptable, provided such limitations are documented with the assessment. A partial assessment that can later be interpreted as being a poorly completed assessment should be avoided.

2) Identify Hazards

How to Identify Hazards

Hazards can be identified through many different approaches, each with specific strengths and weaknesses. For all approaches, hazard identification is the first and critical component of a risk assessment. Hazards not identified during this first stage can create substantial risks. In *MORT Safety Assurance Systems,* Johnson notes, "Hazard analysis is the most important safety process in that, if that fails, all other processes are likely to be ineffective" (Johnson). Similar language appears in AS/NZS 4360:1999, Risk Management [Standards Australia(b)].

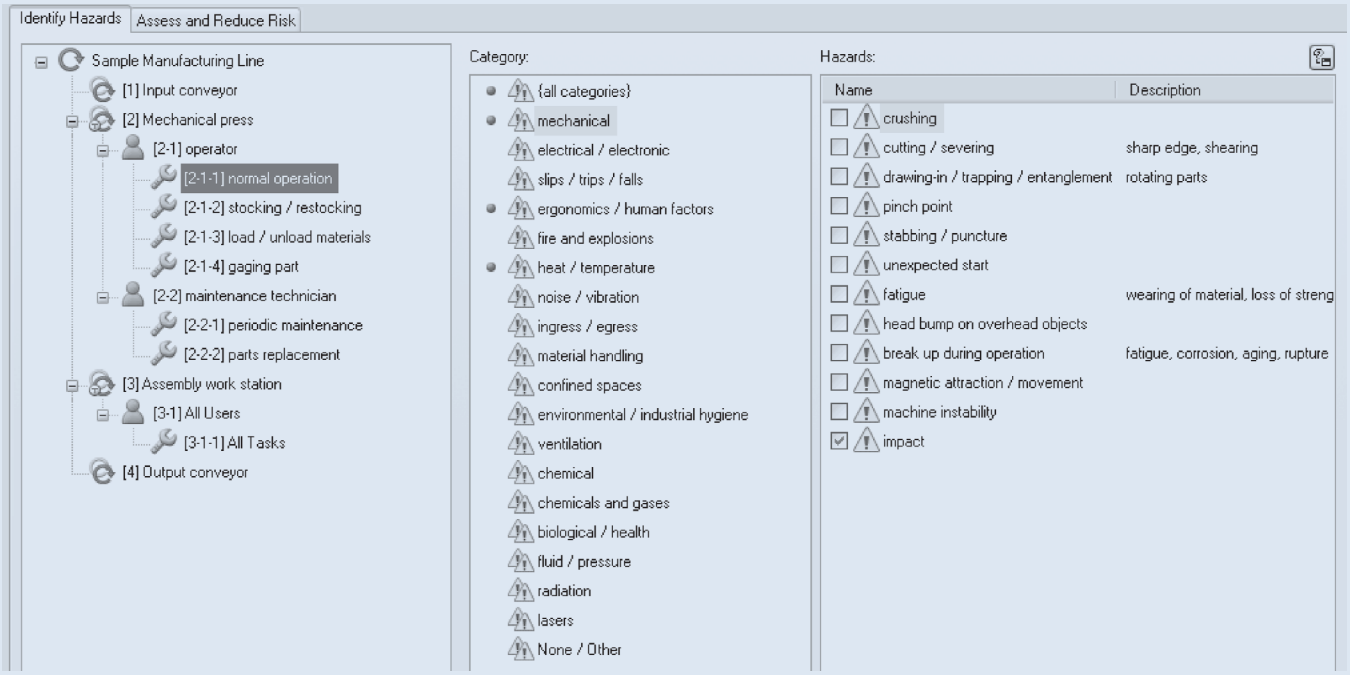
As noted, many methods exist for identifying hazards. Depending on the complexity of the situation, some or all of the following may apply.

- Use intuitive operational and engineering sense; this is paramount throughout the process.
- 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 other similar systems.
- Consider the potential for unwanted energy releases and exposures to hazardous environments.
- Review historical data, such as industry experience, incident investigation reports, OSHA and National Safety Council data, and manufacturer's literature.
- Brainstorm.

Generating a list of hazards is usually a brainstorming activity conducted by the risk assessment team. When developing this list, the basic question is, "How could someone get hurt?" Failure modes should be considered when developing the list.

Figure 2

Example Hazards for Operator: Normal Operation



Manual checklists, database systems or new computer tools can guide and speed this effort.

In some cases, such as nuclear power or environmental waste, a hazard is easily identified, but the conduit for exposure requires effort to evaluate (e.g., how hazardous material could be released). In other cases, this challenge is reversed. Identifying how someone could be harmed is straightforward (e.g., excessive force causes back injury), but identifying the source is difficult (e.g., anticipating maintenance task and conditions that require excessive force). In some situations, both aspects are challenging.

One recent advance in risk assessment methods is a task-based approach to identifying hazards. Although a task-based focus has been used for many years in creating a job safety analysis (or job hazard analysis), General Motors, ANSI B11 TR3 and others have moved the task-based approach further upstream in the design process to be part of the overall risk assessment effort.

The task-based approach has enjoyed success particularly because it helps the team identify more hazards. This approach focuses on what people do, which helps the risk assessment team better identify how someone could be injured. A typical breakdown is to first identify the various users who will interact with a design, examine the tasks they perform, then identify the hazards associated with each task. The result is a listing of task-hazard pairs. For most teams, this approach is recommended. Regardless of the method used, the purpose is to ensure that all reasonably foreseeable hazards are identified.

Identify Users

Users are the people who interact with the design, machine, product, equipment, process or facility that is being assessed. For example, users for an industrial machine such as a mechanical press might include operator; temporary/stand-in operator; set-up person; maintenance technician; electrician/controls technician; materials handler; leader/supervisor; manager; engineer; trainee; installer; remover; cleaning crew; and a passer-by/nonuser. A consumer product might have users identified by age (e.g., adult, youth, child, senior), skill level (novice, intermediate, advanced) or other logical breakdown(s).

Identify Tasks

For each user, the risk assessment team should identify all reasonably foreseeable tasks. A task is an activity that is performed with, on or around the product or equipment. Operator tasks on an industrial machine could include: normal operation, load/unload parts, clear jams, basic troubleshooting, machine cleaning, lubrication, and positioning/fastening parts and components. Youth tasks for a consumer product could include: play, clean, repair, aggressive play, misuse and others.

How minutely the tasks are broken down depends on the application. In some applications, a task might be "service machine," where other applications might require a step-by-step breakdown of the subtasks (e.g., replace pump, change oil). The more detailed and specific the task definition, the more likely hazards associated with the task will be

Table 1

Example Risk Scoring System

Probability of Occurence of Harm	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

Source: ANSI B11 TR3 2000.

identified. However, the further a task is broken down, the more time and effort is required to fully assess the risks. In some cases, too much detail can be counterproductive. Early risk assessments often start with tasks at a fairly general level and later progress to more detail. Striking a balance between task detail and benefit derived therefrom comes with experience in conducting risk assessments.

Identify Hazards

The next step is to identify hazards associated with each user and task. Hazards can be equipment-related, energy-related, natural phenomena or other types. ANSI B11 TR3 defines hazard as "a potential source of harm." Example hazards include crushing and pinch points, live electrical parts, excessive noise, inadequate ventilation and chemical exposure. Checklists of hazards appear in several publications, including ANSI B11 TR3, ISO 14121/EN 1050 and SEMI S10. Different methods can be used to identify hazards, and the different industry approaches to hazard identification reflect these variations. Figure 2 shows example hazard categories and related mechanical hazards for the normal operation task.

Identify Hazards Not Related to Tasks

Not all hazards are task-related. Risk assessment teams must identify these hazards as well. Examples include seismic hazards, UV degradation of plastic insulation, and process or system hazards.

3) Assess Initial Risk

The elements of risk can be assessed in many ways. Some documents use different terms to describe these general ideas, such as consequence instead of severity. Different approaches analyze these elements to greater or lesser levels of complexity.

Risk level is assessed both before and after risk reduction measures are implemented. These risk levels are referred to as the initial risk level and the residual risk level. Assessing initial risks should be conducted by assuming that no risk reduction methods are in place (e.g., no barrier guards, no electrical grounding, no warnings). The controls identified for the particular hazard are assumed to be in place when assessing residual risks. Four sub-steps are involved in assessing the initial risk.

Select a Risk Scoring System

Before risks can be assessed, a risk scoring system must be selected. A risk scoring system is simply those factors used to assess risk and how these factors combine to obtain a risk level. The systems attract considerable attention in discussions of the risk assessment process, as they can be contentious and confusing.

Two-factor risk scoring systems have been in use for many years. Table 1 provides a sample risk scoring system from the U.S. machine tool industry. The risk factors used in this system include severity and probability of occurrence of harm, each with four levels. Together, the risk factors in this system are used to derive a risk level shown as high, medium, low and negligible. Table 1 is only one example of a risk scoring system. Many different systems are used in practice. If a three- or four-factor system is used, additional step(s) must be added to assess the additional risk factors to obtain a risk level [Manuele(b); Main].

Once a risk scoring system is selected, the assessment process continues. For simplicity, a two-factor risk scoring system has been selected to illustrate how risks are assessed.

Assess the Severity of Consequences

For each hazard or task/hazard pair, the severity of harm or consequences that could result should be assessed. Historical data can be of great value as a baseline. Severity is often assessed as personal injury, although it can include other elements such as the number of fatalities, injuries or illnesses; the value of property or equipment damaged; the time for which productivity will be lost; or the extent of environmental damage. Severity of harm is also referred to as consequences of exposure in some approaches. In these instances, this step is referred to as a consequence assessment.

Severity can be assessed using various scales. For example, the severity levels in ANSI B11 TR3 are:

- Catastrophic: Death or permanent disabling injury or illness (unable to return to work).
- Serious: Severe debilitating injury or illness (able to return to work at some point).
- Moderate: Significant injury or illness requiring more than first aid (able to return to same job).
- Minor: No injury or slight injury requiring no more than first aid (little or no lost-worktime) (AMT).

Assessing severity usually focuses on the worst-credible consequence rather than the worst-conceivable consequence. Some advanced methods evaluate all severity levels against the associated probability distributions. Analyzing risk distributions is a relatively advanced application.

Figure 3

Initial Risk Level: Normal Operation

Identify Hazards | Assess and Reduce Risk

Item Id	Sub-process	User	Task	Hazard Category	Hazard	Cause/Failure Mode
2-1-1-1	Mechanical press	operator	normal operation	mechanical	impact	dropped parts

	Task	Hazard Category	Hazard	Cause/Failure Mode	Severity	Probability	Risk Level	Reduce Risk
1	<None>	<None>	<None>					
2	normal operation	mechanical	impact	dropped parts	Serious	Very Likely	High	gloves, stand
3	normal operation	ergonomics / human factors	lifting / bending / twisting	some parts weighing >35 lbs	Serious	Likely	High	move incomin twisting, stan tools or fixture
4	normal operation	heat / temperature	severe heat	surface temperatures > 160F	Serious	Likely	High	slow down er longer air cool cooling fans
5	stocking / restocking	ergonomics / human factors	lifting / bending / twisting		Serious	Likely	High	look into addin weight?
6	load / unload materials	mechanical	cutting / severing	sharp edges	Moderate	Unlikely	Low	gloves
7	load / unload materials	slips / trips / falls	impact to / with	dropped parts	Minor	Unlikely	Negligible	
8	load / unload materials	heat / temperature	severe heat		Serious	Likely	High	see air cooling
9	load / unload materials	fluid / pressure	high pressure air		Serious	Very Likely	High	standard proc
10	gaging part	mechanical	cutting / severing		Moderate	Unlikely	Low	
11	gaging part	ergonomics / human factors	lifting / bending / twisting		Moderate	Unlikely	Low	
12	periodic maintenance	mechanical	cutting / severing	getting access to / avoiding work in progress	Serious	Unlikely	Medium	special proce
13	periodic maintenance	heat / temperature	severe heat	surface temperatures >160F	Serious	Unlikely	Medium	gloves, restric
14	parts replacement	<None>	<None>					
15	All Tasks	mechanical	cutting / severing	rotating blade	Moderate	Likely	Medium	interlocked ba

Severity	Probability
☐ Catastrophic	☑ **Very Likely**
☑ **Serious**	☐ Likely
☐ Moderate	☐ Unlikely
☐ Minor	☐ Remote

Assess Probability

Unless empirical data is available (which is rare), the process of selecting the probability of an incident occurring will be subjective. For a complex scenario, brainstorming with knowledgeable people is advantageous. HB 203-2000, Environmental Risk Management: Principles and Process, states:

> Probability is the likelihood of a specific event. . . . Probability is expressed as a number between 0 and 1. By definition, probability is a numerical measure and can be used in quantitative risk approaches. . . . Likelihood is used as a qualitative description of probability or frequency [Standards Australia(a)].

However, many methods use the terms probability and likelihood synonymously. Probability must be related to an interval base of some sort, such as a unit of time or activity; events; units produced; or the lifecycle of a facility, equipment, process or product. In most cases, the unit of time is the useful life of the system.

Occurrence probability is estimated by considering the frequency, duration and extent of exposure, training and awareness, and the characteristics of the hazard. When estimating probability, the highest credible level of probability should be selected.

Estimating probability includes:

- frequency and duration of exposure to a hazard;
- personnel who perform tasks;
- machine/task history;
- workplace environment;
- human factors;
- reliability of safety functions;
- possibility to defeat or circumvent protective measures;
- ability to maintain protective measures.

Similar to severity, many scales are used to assess the probability of occurrence of harm. ANSI B11 TR3 includes these levels:

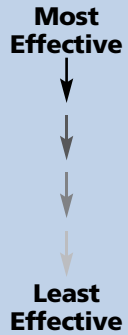
- Very likely: Near certain to occur.
- Likely: May occur.
- Unlikely: Not likely to occur.
- Remote: So unlikely as to be near zero (AMT).

Some risk scoring systems break probability into two components, for example, frequency of exposure and avoidance, or likelihood of the hazard occurring and the likelihood of harm occurring [Manuele(a)]. Regardless of the method used, the risk assessment process continues once the risk factors have been assessed.

Derive Initial Risk Level

Once severity and probability (or other factors)

Hazard Control Hierarchy



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

are assessed, an initial risk level can be derived from the selected risk scoring system. This system maps the risk factors to risk levels either quantitatively or qualitatively as shown in Table 1. This system maps the severity and probability levels to four levels of risk: High, medium, low and negligible. How the risk factors of severity and probability (or subsets of probability) are combined varies with different risk scoring systems. The result of this initial evaluation will typically yield an array of low to high risks. Since the risk assessment process is usually subjective, the risk-ranking system will also be subjective. Figure 3 shows the initial risk for the normal operation task for a mechanical power press.

Once initial risk is estimated, the risk level can be compared to acceptability levels. If the risk is not acceptable, the next step is to reduce the risk. Determining what risks are and are not acceptable is company- and situation-specific. In some cases, industries have provided guidance on levels of acceptable risk. In many instances, this decision is left to the risk assessment team, since the decision is culture-, situation- and time-dependent.

4) Reduce Risk

Set Priorities

Risk reduction activities begin after the initial risk rating is known, as shown in Figure 1. However, not all risks are equal. Higher risks must be addressed first; lesser risks can be subsequently considered. This screening approach makes the process more efficient so that significant risks can be more effectively addressed.

Although higher risks deserve more attention, lower-risk hazards should not be forgotten. In the ongoing process of continuous improvement, these risks can be further reduced or eliminated as time, resources and opportunities allow. The fact that hazards have been identified and assessed as low risk should still be documented.

Use the Hazard Control Hierarchy

Just as not all risks are equal, not all methods of reducing risks are equal either. The hazard control hierarchy (as depicted above) is a prioritized approach to hazard elimination and control. Part of practicing safety through design is identifying situations where hazards exist and developing the best response to the hazard according to this hierarchy. The hierarchy depicts a way of thinking about hazards and risks and establishes an effective order of action for risk elimination or reduction. It should be employed to resolve safety concerns.

Identify Risk Reduction Measures

Identifying risk reduction measures involves an engineering brainstorming effort to first identify a list of potential ideas, evaluate those ideas in terms of feasibility or practicality, and select the best solution(s) using the hazard control hierarchy. Not all potential risk reduction measures are practical or feasible. Many factors determine feasibility or practicality, such as technical, cost, usability and productivity. Cost is sufficiently significant that it is addressed in greater detail later in this article.

The critical piece to completing this feasibility step is the "good-faith" effort. A company or manufacturer that makes a good-faith effort to determine the risk reduction measures that are and are not feasible will have completed this step. Concerning risk treatment (reduction), HB203-2000 notes:

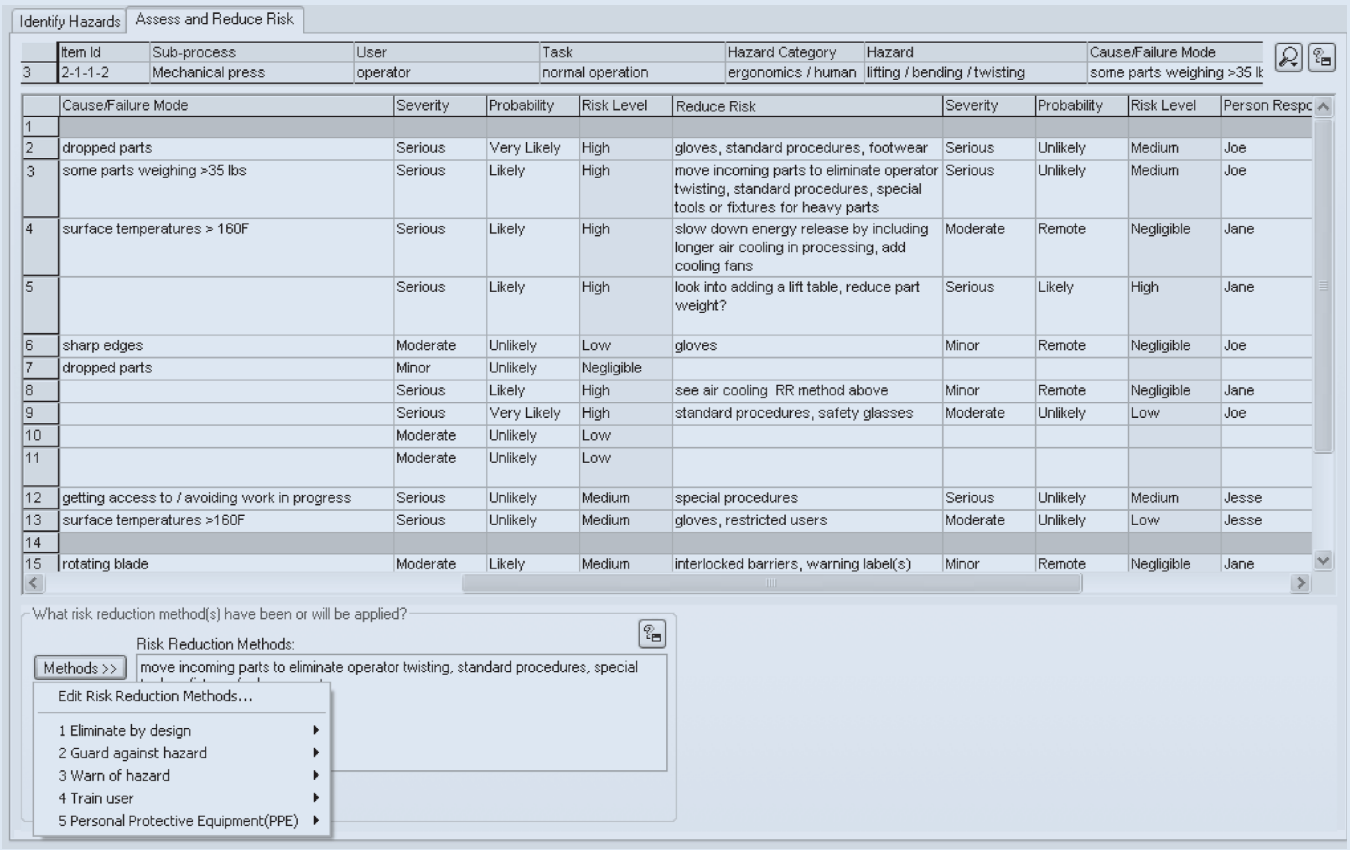
> Options and strategies for treating risk are assessed in terms of:
> - their potential benefits;
> - their effectiveness in reducing losses;
> - the cost to implement the option(s);
> - the impact of control measures on other stakeholder objectives, including the introduction of new risks or issues.
>
> The options preferred will generally optimize the reduction in environmental impact and the costs of achieving this, and create the least adverse side effects [Standards Australia(a)].

In the mechanical press example, the risk reduction methods include: fixed guards, two-hand controls, standard procedures, safety glasses and hearing protection (Figure 4).

Acceptable risk can be achieved by adhering to the principle described as "the good-faith application of the hierarchy of controls" (Taubitz). This principle starts every risk reduction effort at the top of the hierarchy, searching for methods to eliminate hazards by design and working sequentially down through the hierarchy in a good-faith effort to use feasible methods to reduce risk. This principle discourages jumping to lower controls such as warnings, training or PPE that may cost less or require less engineering time, yet provide less-effective risk reduction when higher-level controls such as engineered systems are feasible. This principle also directs engineers to consider the hierarchy for even relatively low-risk hazards because in some instances design improvements can effectively and feasibly further reduce risk. The good-faith portion

Figure 4

Risk Reduction Methods: Normal Operation



of the principle requires an honest evaluation of candidate risk reduction methods. It recognizes that issues of feasibility, practicality and cost be considered and, in many cases, higher-order controls may not be warranted for a specific situation.

What constitutes a good-faith effort? There is no objective answer to this question, as each situation is different. In one situation, such an effort might result in fixed guards to reduce risk, while in another only administrative procedures and PPE may result. In all cases, those who have made a good-faith effort will be able to defend their decisions in the context of the hierarchy of controls and feasible methods to reduce risk. More specifically, they will be able to explain why certain methods were selected rather than others in terms of what was feasible and effective at the time the decision was made.

Check for New Hazards

In some cases, a risk reduction method selected for one hazard may introduce new hazards or impact risks of other tasks or hazards. For example, moving a machine 10 inches away from a wall to make room for maintenance work may expose an operator to forktruck traffic in an aisle. Care should be taken to determine whether new hazards are introduced as a result of risk reduction methods employed. If that occurs, the risk should be reevaluated and other or additional measures proposed.

5) Assess Residual Risk

Once feasible risk reduction methods have been selected, most risk assessment guidelines call for a second assessment of risk factors (Figure 1). This assessment should be conducted to validate that the selected measures effectively reduce the risk. Once again, severity and probability (or other risk factors) are assessed and combined to obtain a new risk level using the selected risk scoring system. This system is typically the same system used in the initial assessment. Risk factors are estimated, assuming that the selected risk reduction measures are in place. Since zero risk is not attainable, some level of residual risk always remains.

6) Decision

Once residual risk is known, those involved must decide whether to accept or further reduce that risk. This decision verifies that the protective measures selected have reduced the risks to an acceptable level. The risk assessment team will make this determination with input from management as necessary.

A general trend has emerged toward using a three-tier framework for determining acceptable or

tolerable risk. The framework is presented by the HSE guideline, "Reducing Risks, Protecting People." The principle presented is that risk should be reduced to a level that is "as low as reasonably practicable (ALARP)" (also termed ALARA: as low as reasonably achievable) [HSE(b)]. The principle divides risk into three regions (Figure 5):

1) an upper-bound limit, above which risks are deemed unacceptably high;

2) a lower-bound limit, below which risks are considered negligible or broadly acceptable;

3) an in-between region, where risks should be reduced to a level that is ALARP.

The principle states that there is a level of risk that is intolerable. Above this level, risk cannot be justified on any grounds. There is also a lower risk level, which is a broadly acceptable region. Below this level, further risk reduction efforts are unwarranted. Between these two levels is the ALARP region. In this region, risk reduction in some form(s) is required. After these efforts, risk levels will presumably be lower although some risk will remain. These residual risk levels are acceptable if further risk reduction is not practicable or feasible.

To increase ease of use and understanding, these three regions are often color-coded with the familiar red-yellow-green color scheme. The unacceptable region is red, interpreted as "stop; design or process cannot proceed until risk is reduced." All involved personnel know that the red region means that the next hurdle, whether it is a design review or a process check, will not be passed until the risk is reduced. The yellow area is a caution zone, where risks need to be examined for opportunities to reduce risk further and implement solutions where feasible. However, a yellow risk is not an automatic fail on the next design or process hurdle. The green area is sometimes interpreted as a "nice to know" zone. Risk reduction does occur when solutions are low cost and easily implemented, but energies and attention are not typically focused in this area.

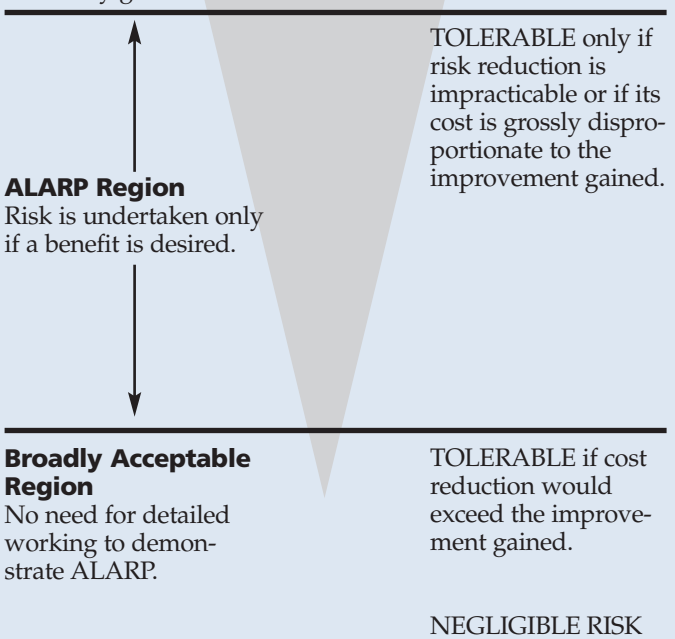
The concept of acceptable risk displaces zero risk as the target for risk assessments. Peeling back the layers further, the ALARP framework suggests that those risk reduction methods which are practicable or feasible should be employed as a method to attain acceptable risk.

Next comes the question, "What is practicable or feasible?" The answer is largely subjective. However, HSE's "The Application of Risk Assessment to Machinery," offers the following guidance:

> For severity levels which are in the ALARP region, the risk is only acceptable if it is reduced as low as is reasonably practicable. Risk evaluation therefore hinges on an assessment of what is reasonably practicable. It is suggested that two approaches are used, and that they are applied in the following order:
>
> a) Assess whether the current machine design complies with the published state-of-the-art for risk reduction for similar types of machine. Current standards on the design of similar machines, particularly European type C standards, provide information on what constitutes the current agreed European state-of-the-art.
>
> b) Apply cost/benefit analysis [HSE(c)].

Figure 5

ALARP Risk Framework



Source: Adapted from the Instrument, Systems and Automation Society (ISA). ©2000. Used with permission. All rights reserved.

In nearly all cases, if the feasible risk reduction measures are applied, then the risk is ALARP by definition [HSE(b); ISA; Main]. If the residual risk is acceptable, then the risk assessment process continues with consideration of other hazards. If no other hazards exist, the process moves to the documentation step.

A practical solution to the tolerable risk question derives from three parts: 1) applying the hierarchy of controls 2) within the risk assessment process and 3) in a good-faith effort. Through the good-faith application of the hierarchy of controls, an ALARP residual risk level will be achieved. In nearly all cases, the residual risk level will be acceptable. If it remains unacceptable, then additional risk reduction is required.

In the extreme case, applying feasible risk reduction measures may not yield an acceptable risk. This could occur if the initial risk level was near the unacceptably high level and feasible measures did not lower that risk. If residual risk is deemed unacceptable, then the process stops. The risk is too high, which requires either fundamental design changes to eliminate the task or hazard, or abandonment of the design.

The good-faith application of the hierarchy of controls can be applied to every level within the ALARP framework.

In the mechanical press example, risk reduction methods identified for the normal operation are considered to yield an acceptable risk.

7) Results/Documentation

The final step in the risk assessment process involves documenting the results. Every risk assessment standard and guideline requires or recommends this step. For example, the Ontario Ministry of Agriculture Food and Rural Affairs states:

> It is important to document the justification of risk control actions. This includes documenting any analyses that were undertaken, and how stakeholder considerations were taken into account. Such documentation is invaluable for monitoring progress in risk management and for due diligence defence if something goes wrong in the process (McNab).

The risk assessment process should document the tasks, hazards and risk reduction methods employed to reduce risks to an acceptable level. The results have several uses.

- **Identified hazards/risks.** Tasks, hazards and risks are explicitly identified; with this information, constructive discussions can take place between design engineers, managers, maintenance personnel and SH&E practitioners about various risk reduction methods, funding priorities, schedules and other related issues.
- **New design criteria.** Emergence of new design criteria will likely occur as a result of the risk assessment process. New hazards or unacceptably high risks of known hazards become new design criteria, and hazards and risks can (and should) be provided back to the product, equipment or facility designers/engineers. The designers may be able to make modifications that can reduce the risk. The further along a design progresses to production before a risk assessment is completed jeopardizes the smooth transition to production or market. Therefore, risk assessment activities should occur relatively early in the design process so that new design criteria can be incorporated easily into the design.
- **High-risk tasks.** If a task-based approach is used, then a result from the risk assessment process is a list of high-risk tasks. This list can then be used to heighten the necessary attention on those administrative controls and to modify future designs through engineering controls to reduce the residual risks.
- **Hazard checklist.** Identified hazards can be recorded on a machine-specific checklist that can be posted on or near the equipment or included with the product instructions.
- **Job safety (or hazard) analysis.** Another result is a job safety (or job hazard) analysis. Tasks can be ordered to show an assessment of hazards and the risk reduction methods necessary to avoid harm. This information would be pertinent to users such as operators or maintenance personnel.
- **Documented risk assessment.** A documented risk assessment is required by all industry standards, guidelines and technical reports that describe risk assessment procedures. The documentation can be used to build a technical file that supports external validations (e.g., CE mark or quality certification) or internal process requirements.

Discussion: Some Examples

The good-faith application of the hierarchy of controls can be applied to every level within the ALARP framework. The following examples illustrate this process.

- **Table saw.** An open saw blade on a table saw has an initial risk level that is unacceptable. Applying the risk assessment process identifies potential design changes and guarding systems. The feasible/practical risk reduction measures likely include blade guards, warnings and instructions, as well as training. In this instance, a manufacturer applying only warnings without the guards is not sufficient. Although a professional carpenter may choose to remove the guard and accept the risk, a manufacturer not providing a guard for the table saw blade results in an unacceptable residual risk.
- **Facility aisle.** A wide aisle in a facility has primarily slow-moving forktruck traffic but also the occasional pedestrian. Based on the initial risk level, no further risk reduction is necessary as the risk falls into the broadly acceptable region. By applying the process, it is found that barriers separating the traffic are technically feasible but neither practical nor cost-effective. Feasible risk reduction measures include painting aisle markings, providing signing and training forktruck operators. These measures provide additional risk reduction at minimal cost.
- **Troubleshooting a live electrical panel.** Troubleshooting equipment with a live 440V electrical panel involves risk in the ALARP region. The initial risk level is unacceptable without risk reduction measures. The process identifies a potential risk reduction measure: lockout/tagout of the electrical source. However, power must be on to perform the task, so this is not feasible. Feasible measures could include the following:
  - well-trained and knowledgeable personnel working without time pressures;
  - restricting the area to authorized personnel;
  - limiting system movements in speed or space;
  - providing PPE such as insulated gloves;
  - limiting authorized work procedures to diagnosis only and performing any repairs with power off.

  Applying these measures will still yield a residual risk above the broadly acceptable region. However, it will be lower than the initial risk.

These examples illustrate that good-faith application of the hierarchy of controls will yield an acceptable risk level and can be applied with any initial risk level. The process works equally well with high or low initial risk levels. In some cases, the residual risk will remain relatively high yet still be deemed acceptable.

Cost: A Factor of Feasibility

One of the greatest benefits of conducting a risk assessment is that the real-world constraints of cost, technical feasibility and residual risks must be recognized. The risk assessment process filters out risk reduction methods that are either technically or financially infeasible. When technological ideas have not yet been reduced to practical products or solutions, a risk assessment can be used to evaluate whether applying the new and unproven system lowers risk to an acceptable level. Similarly, if financial resources do not allow for specific risk reduction methods to be deployed, other financially feasible methods must be substituted to reduce the risk to an acceptable level. Although the alternate method may not be the optimal or most desired solution, the substituted risk reduction methods can yield an acceptable result.

Cost is always a factor in engineering design and also in risk assessment. Pretending that risk assessments can be performed divorced of cost concerns is unrealistic. Resources are always limited. Not every desired or technically possible risk reduction strategy can be implemented. Companies only have so many dollars to spend and they must use those funds wisely to obtain the greatest improvements.

Management typically determines what risk level is acceptable through its direct decisions and indirect actions or inactions. Although subjective judgment is required to determine when risk is reduced to an acceptable level, the good news is that manufacturers are currently making these decisions if only informally. At a more-detailed level, risk assessment teams make decisions on whether a given risk is acceptable or whether additional risk reduction is needed. Risk assessments permit hazards and risks to be more carefully identified and decisions on risk acceptability, costs and feasibility to be more clearly made.

Updating an Assessment

When should a risk assessment be updated? When a design is changed or a risk reduction method is modified, the risk assessment should be reviewed and updated. Once an assessment has been documented, updating it is a relatively quick process.

What about Cheaters?

Skeptics will contend that "cheaters" can easily warp this guide to meet specific agendas and not incorporate sufficient risk reduction methods, resulting in residual risk that is too high. This is a valid concern. However, the risk assessment process requires no small amount of resources, time and effort. Those not interested in a good-faith effort to reduce risks will not likely have the energy and patience to complete the process. Even if they do, their documentation may be a greater liability than a benefit.

Conclusion

Although many different risk assessment methods are available, all share the common fundamental elements: identify hazards, assess risk, reduce risk and document the results. The goal of risk assessment is to achieve acceptable risk. Cost, feasibility and the ALARP framework are important elements of achieving acceptable risk. With the increasing adoption in many industries of risk assessment as the means to demonstrate that designs are safe, SH&E professionals need to become familiar with the risk assessment process. ■

The risk assessment process filters out risk reduction methods that are either technically or financially infeasible.

References

Assn. for Manufacturing Technology (AMT). "Risk Assessment: A Guideline to Estimate, Evaluate and Reduce Risks Associated with Machine Tools." ANSI B11 Technical Report #3. McLean, VA: AMT, 2000.

Christensen, W. and F. Manuele. *Safety Through Design.* Itasca, IL: NSC Press, 1999.

Health and Safety Executive (HSE)(a). "Manual Handling Assessment Charts: A Practical Workplace Risk Assessment Tool." News Release. London: HSE, 1992. <http://www.ergonomics.org.uk/resources/newsinfo/hsenews.htm>.

HSE(b). "Reducing Risks, Protecting People: HSE's Decision-Making Process." London: HSE, 2001.

HSE(c). "The Application of Risk Assessment to Machinery." London, HSE, Health & Safety Laboratory Div., 1997.

Instrumentation, Systems and Automation Society (ISA). Application of Safety Instrumented Systems for the Process Industries. ANSI/ISA S84-1996. Research Triangle Park, NC: ISA, 1996.

International Organization for Standardization (ISO). ISO 14121/EN 1050-1999. Safety of Machinery: Risk Assessment. Geneva: ISO, 1999.

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

Main, B.W. *Risk Assessment: Basics and Benchmarks.* Ann Arbor, MI: Design Safety Engineering Inc., 2004.

Manuele, F.A. and B.W. Main. "On Acceptable Risk." *Occupational Hazards.* Jan. 2002: 57.

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

Manuele, F.A.(b). *On the Practice of Safety.* 3rd ed. New York: Van Nostrand Reinhold, 2003.

McNab, B. "Inspection, Investigation and Enforcement Risk Management Through Assessment and Control: A Framework for the Ministry of Agriculture Food and Rural Affairs." Draft document. Toronto, Ontario: Ministry of Agriculture and Food, Aug. 7, 2001.

Norwegian Center for Ecological Agriculture. Risk and Emergency Preparedness Analysis. NORSOK Standard Z-013. Tingvoll, Norway: Norwegian Center for Ecological Agriculture, Rev. 1, March 1998, and Rev. 2, 2001-09-01.

Semiconductor Equipment and Materials International (SEMI). Safety Guideline for Risk Assessment. SEMI S10 1103. San Jose, CA: SEMI, 2003.

Standards Australia (a). Environmetal Risk Management: Principles and Process. HB 203-2000. Sydney: Standards Australia, 2000.

Standards Australia-(b). Risk Management. AS/NZS 4360-1999. Sydney: Standards Australia, 1999.

Taubitz, M. Personal correspondence. 2003.

This article is based on a chapter from B.W. Main's Risk Assessment: Basics and Benchmarks.