by Douglas Nix, C.E.T.

Don't gamble with safety

Choose the right risk-assessment strategy for your plant

Risk is a fact of life. We live in a world full of things that can harm us, from the mosquitoes in the back yard to the inattentive driver behind the wheel of the car next to you on the way to work.

Everyone makes risk assessments every day, whether they realize it or not. When you back your car out of a parking space, you check for other cars, people, pets and obstacles before you start moving the vehicle. Before you cross the street you look both ways.

In the same way, we must make decisions about risk related to machinery and processes in the workplace. The formal methods of risk assessment explained in this article will give readers the tools to make rational decisions.

The most common mistake made in this process is to leave risk assessment to the end of the manufacturing cycle. The cost of implementation is inversely proportional to the point in the design cycle where the work takes place.

If the design process incorporates both risk assessment and risk reduction, design can eliminate hazards, reducing the need for guarding and other safety management methods. Also, the safer design reduces the manufacturer's liability, helping to control insurance costs and potential civil damages.

What is risk?

Risk is the product of two entities: potential harm and probability. To understand risk, we need to know more about both harm and probability.

In order to have a risk, the ability to do harm must exist. Harm exists as a result of a hazard.

A hazard is something that could hurt a person, animal or the environment, if the two interact. Hazards may be mechanical such as a rotating saw blade, an electrical shock hazard, or some other machine.

Harm is damage done to a person, animal or the environment by the hazard.

Severity is the degree of harm done by the hazard. If we are considering a skin burn, is it a first-degree burn or a third-degree burn?

So, harm is possible when a hazard exists and there is interaction between an exposed person and the hazard. Analysts sometimes call such an incident a harm event.

Since we have a hazard and a harm event, we must have a risk, right? Not necessarily. Until we understand the likelihood or the probability of the harm event occurring, we can't assess the risk. Let's look at the relationship in a couple of ways.

As you can see from Figure 1, risk is a result of harm (shown as severity) and the probability of encountering the hazard (the harm event) and avoiding or limiting the resulting harm.

This diagram shows three elements of probability: duration, occurrence and avoidance. As an example, a hazard that presents a low severity may be a high risk if the exposure is constant, while a relatively high severity hazard may present the same level of risk if the exposure is less frequent.

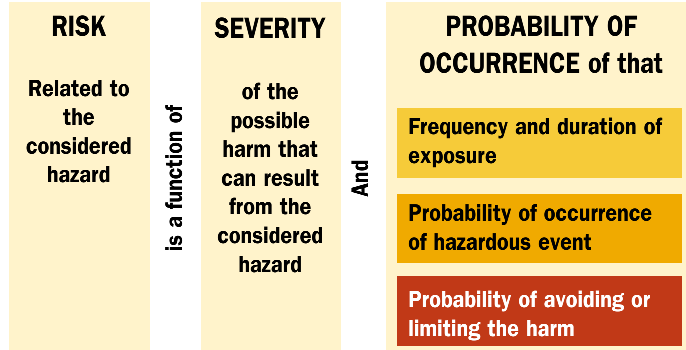


FIGURE 1 — Elements of risk

Another way to look at this is in the form of a simple formula.

$$R=S_h\ x\ P_h$$

WHERE

R represents the risk

S_h represents the severity of harm

P_h represents the probability of harm

Pretty simple really. But, there are a few more wrinkles for us to look at before we get the whole picture.

Two case studies explain how to apply the risk assessment methods

CASE 1: Robotic assembly cell

A robot assembly cell with two robots is installed in a plant. Robot 1 takes the incoming assembly from the feed conveyor and places it into a fixture, then removes it when robot 2 is done and places the finished assembly onto the exit conveyor. Robot 1 places two components onto the assembly and welds them in place.

The initial assessment shows that the perimeter fencing around the cell is too close to robot 2. This causes some trapping points (anyplace where the robot could trap a person) between robot 2 and the fence. Additionally, robot 1 is too close to a building support column, also causing a trapping point.

Both conditions are potentially fatal. The robot standard requires a minimum of 500 mm (20") between the restricted envelope of the robot and fixed objects in order to prevent trapping a person between the robot and the object. Robot 1 rarely needs maintenance work, but robot 2 frequently requires re-tipping and teaching to new points on the assembly.

A technician must enter the robot cell at least twice per shift to perform the tip maintenance work, exposing the technician to the trapping point. In the approach to robot 2, the technician must follow the only path between the entry gate of the cell and robot 2, taking the technician through the trapping point between the building column and robot 1.

The initial analysis shows that the company can move the barrier guarding away from robot 2 far enough to meet the 500-mm gap requirement. In addition, the company can mark the restricted envelope on the plant floor with paint to illustrate the danger zone. These modifications will cost about $7,500.

The alternative is to place safety mats on the floor around the base of the robot and extending out to the barrier guard. In addition, the mat must extend inside the cell about 132 centimetres beyond the edge of the restricted envelope. This ensures that motion can be controlled before a person reaches the restricted envelope based on the stop time calculation for the mat and the robot. This option will cost about $10,250 for each robot, but won't take up more floor space that is at a premium in the plant.

Another way to cope with the building column would be to move the entire line by enough to open the gap between the robot's envelope and building column. This would cause three weeks downtime, plus cost about $50,000 in labour to teardown and move the line.

The last alternative is to do nothing, hoping that no injury will occur. If an accident happens, the company faces fines and jail time. The current fine for a preventable fatality ranges from $250,000-$500,000 for the company, plus $25,000 in personal fines for the supervisors.

In this case, since floor space is valuable, the company decides to add the safety mats to both robots at a cost of $20,500, about 10 percent of the lowest fine. This action ensures that the plant personnel can safely operate the robots.

CASE 2: Power press and feeder

A stamping plant installs a 600-ton mechanical press. A coil feeder next to the press feeds sheet steel from a large coil into the press die. The press is fitted with interlocked barrier guards front and back, but the inter-

Hazards

How do you know what to classify as a hazard? In the kitchen, the edge on a carving knife and the point on that knife are both hazards, since they have a known capability to do harm by causing cuts or stab wounds. Similarly, a kettle fresh from a hot element is a hazard because its surface can burn skin and the steam and hot water can scald skin.

In the yard, a gas-powered string trimmer poses a whole host of hazards: noise, exhaust poisoning, gasoline related hazards, burns from hot surfaces, cuts from the string, etc.

If you are considering industrial machinery, the hazards' list is considerably longer. Happily, we have standards (see CSA Z432, *Safeguarding of Machinery*, for examples) that provide us with lists of hazard types found on many types of equipment and suitable ways to safeguard operators from those hazards.

Severity

Severity is another matter. We must classify (usually subjectively), how much damage a hazard could cause someone. In some cases, we know a lot about the effects of certain kinds of hazards. For example, experts have examined the effects of laser light over the last 40 years and can calculate how much laser light it is safe to expose people to. On the other hand, there is no data available about the amount of force necessary to amputate a finger, since this varies based on many factors.

In general, severity is assessed based on a scale that usually looks something like this:

- Multiple fatalities
- Fatality
- Severe injury (non-reversible, requires hospitalization)
- Moderate injury (reversible, requires hospitalization)
- Minor (reversible, requires first aid)
- Very minor (no first aid)

There are numerous systems published in different magazines that are variations on this type of scale. Refer to the publications mentioned in this article. Depending on your circumstances, you may need to modify this scale to suit your product or environment.

Don't toss the dice. Standards provide ways to safeguard operators from hazards.

locking circuits are a single channel design. The coil feeder has fixed guards over the drive chains used to feed the sheet into the straightening section and the final hitch-feed mechanism, but no guards are between the coil cradle and the in-feed rollers. The hitch-feed mechanism has no guarding since the plant personnel often make manual stroke adjustments on the fly.

The initial assessment shows that the guards on the press are acceptable, but the design of the interlocking circuit only meets ISO 13849-1 Category 2 reliability. Since severe injury or fatality is likely if the interlock fails, the company decides that the interlocks should meet at least ISO 13849-1 Category 3 reliability. So the company installs new interlock switches and new wiring to meet the higher degree of reliability. The press control is capable of two-channel interlocking, so all that is required is a minor modification to the control to enable this feature. The estimated cost is about $500.

The coil feeder needs 1.2-metre high handrails about one metre from the coil feed line to prevent accidental contact between the sharp edge of the moving sheet and anyone walking in the aisle beside the feeder. The handrail will require interlocked gates to allow tow-motor access for loading fresh coils into the cradle. Interlocked movable guards will need to be installed over the hitch-feed mechanism to protect operators from entanglement in the moving feeder. The risk assessment shows that ISO 13849 Category 3 reliable circuits are required on the feeder as well. The controls for the feeder are very simple, and a new safety circuit will be required. Total cost for the handrails, guards and safety circuit is $2,300.

The plant-engineering department suggests an alternative solution using a three-beam light fence around the area. This still requires the guards over the hitch feeder, but makes access to the feeder simpler. When the analyst investigated this suggestion he determined that the company needed safety mats inside the fence due to the safety distance calculated. This brings the cost of this option to $8300.

A third option is to simply cover the hitch-feeder with interlocked guards and leave the coil feed line exposed. The worst-case injury from this would be a significant cut. This reduces the cost to $1,100.

Failure of the press guarding can cause a fatality, so the potential fines are similar to Case 1. A similar degree of injury is possible from involvement with the hitch feeder. The feed line injury would be less severe and may be tolerable.

The joint health and safety committee and management met to decide on the final course of action. They decided to modify the guard interlocking on the press and install the physical handrails and interlocked guards on the feeder, replacing the interlocked gate in the handrail adjacent to the coil cradle with a three-beam light fence to allow tow-motor access for loading fresh coils.

The cost of these modification is $500 for the press changes, $2,100 for the handrails plus an additional $1,500 for the three-beam fence for a total of $4,100. The company made changes during a planned plant shutdown, so no downtime costs were incurred.

Probability

We can assess probability mathematically, but we often assess it subjectively like severity. Probability scales might look like this:

- Constant exposure
- Hourly
- Daily
- Weekly
- Monthly
- Yearly
- Never

The specific scales that you choose for subjective assessments are not critical. They only need help you decide whether the risk is significant enough to require action.

Risk is relative to the situation and the culture. In some cultures, the prevailing attitude is that well-trained employees are the best defence. These cultures tend not to use sophisticated safeguarding systems. If the employee is not paying attention and is injured, conventional wisdom judges the accident as the employee's fault, not the employer's or the equipment manufacturer's fault.

In North America and Europe, the prevailing philosophy is that people are fallible, no matter how well-trained they may be, and that it's worthwhile to prevent all accidents. In our culture, we make a substantial effort to ensure that the machinery is as safe as possible to use.

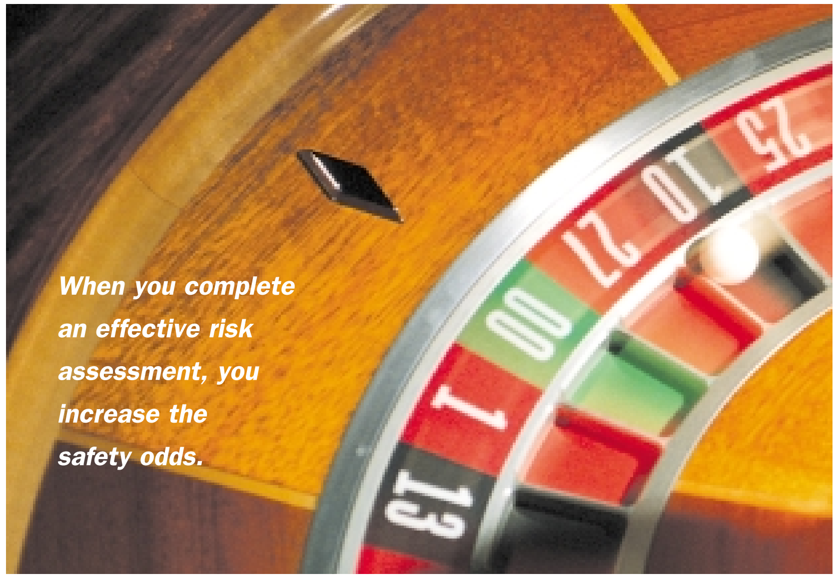
The medical device industry provides another interesting example. Medical devices include products as diverse as implantable heart pacemakers and vinyl surgical gloves. Medical devices must be effective, efficient and must not do harm to the patient. The wrinkle here is the condition of the patients who will use the device. If someone may get cancer from using the device, but they will certainly die if they do not use it, then the risk of getting cancer may be acceptable.

Assessment methods

It's important to remember that formal risk assessment is a team activity — the team approach works best with a group of three to five people knowledgeable in the equipment or the process. Larger groups can slow the process and smaller groups may not have a wide enough perspective to do a good job. Leaving the entire job to one person is rarely acceptable.

You can use several risk assessment methods, including the following:

- **What-if analysis**. What-if analysis is usually the first approach and is a method that most people intuitively understand. The process starts by identifying hazards and then asking the question (for example): What if a person's hand contacts the spinning saw blade? The answer to the question guides you to other questions until you find a safe state. This method is suitable for simple situations only.
- **Preliminary hazard assessment (PHA)**. PHA allows you to delve more deeply. In this method, you begin by defining the various life stages of the product — transportation, installation, commissioning, set-up, manual operation, automatic operation, maintenance, failure, de-commissioning, dismantling and disposal. Then you identify the hazards that exist and relate them to the different life stages.



Finally, you assess the risk presented by each hazard in each life stage. If you conclude that a significant risk exists, then you figure out a remedial action. After completing the remediation, you reassess the risk to ensure that the risk has been reduced and that the stage has introduced no new hazards.

For more information, see Risk Estimation Techniques, by Chris Steel in *The Safety & Health Practitioner*, June 1980; ISO 14121 Safety of machinery, principles of risk assessment and Mathematical Evaluation for Controlling Hazards, by William T. Fine, in the *Journal of Safety Research*, December, 1971.

- **Failure modes and effects analysis (FMEA)**. FMEA provides a much finer tool than PHA, but it is also considerably more time consuming. In this method, analysts determine the failure modes of the component, equipment or process and then rate the severity, probability and criticality of the failure. This is a bottom-up method because it requires the analyst to review each component, decide if it has a critical function, and then determine its failure modes. Once the analyst knows the failure modes, he or she can assess each one for severity.

For more information, see the IEC 60812 standard called *Analysis techniques for system reliability — Procedure for failure modes and effects analysis*.

- **Fault tree analysis (FTA)**. See the IEC 61025 standard called Fault Tree Analysis. FTA is an even finer tool than FMEA, but is a top-down approach. In FTA, analysis determines all the faults that could occur in the equipment operation. Analysts then break down each fault using a graphical method similar to a Boolean logic diagram. If the information is available, analysts assign mathematical probabilities to each branch of the tree. Analysis continues until the analyst can make no further progress, or until they determine the end event.
- **Hazard and operability studies (HazOP)**. Analysts use HazOp studies most frequently in process industries such as petroleum refining or chemical production, however, other

industries are starting to use it to analyze operator interface characteristics and process-related hazards.

See IEC 61882 standard called *Hazard and operability studies — Application guide*.

- **Hazard analysis critical control point (HACCP)**. The food and medical device industries typically use the HACCP system to analyze production processes and implement control methods at the appropriate points in the analyzed process.

As a way to compare the methods, consider what-if to be a general walk-around the product, PHA to be a close look, FMEA to be a magnifying glass examination and FTA to be a microscopic examination. Make the choice between these methods carefully because FMEA and FTA take a lot of time. In many cases, analysts use FTA to carefully examine very critical failure modes found during FMEA, thereby limiting the very detailed analysis to those areas where it is absolutely necessary.

Risk versus cost

Another important consideration in the process is the relative cost of the safety improvements. Depending on the particular case, there may be several different ways to control a given hazard. Some may be simple and relatively inexpensive, while others may be extremely expensive.

Some of the resources cited in the article give detailed examples of ways to relate the cost of the modifications to the risk.

The cost of failure here is increasingly large. A recent story published in *OHS Canada* magazine reports that the provincial government fined the Ontario Power Generation $350,000 for a guarding violation on a coal conveyor at the Nanticoke Generating Station. The violation resulted in a worker being injured when he was drawn into a nip point at the tail pulley of the conveyor while he was cleaning the conveyor with a scraper.

Another cost is the possibility of a criminal conviction. The federal government recently amended the Criminal Code of Canada to include new charges for occupational health and safety violations. These charges can come on top of the fines and possible jail sentences that are already available under the Occupational Health and Safety Act in Ontario.

More information on relating risk and cost can be found in A Practical Safety Analysis System for Hazards Control, an article written by Graham and Kinney, published in the Spring 1980 edition of the *Journal of Safety Research*.

State-of-the-art

So what is reasonable? How can you determine how far to go without overdoing things?

The courts use the reasonable person test to determine what is reasonable in any given situation. In this case, we ask the question: "What would the reasonable technologist do in this situation?" The theoretical reasonable technologist would be aware of the current safeguarding techniques, including the use of safeguarding devices such as interlocking switches, safety relays, light curtains, safety mats, etc.

The current consensus standards offer another measure of adequacy. In Canada, these standards exist as generic documents, such as CSA Z432, *Safeguarding of Machinery*, and as product family standards such as CSA Z142, *Code for Punch Press and Brake Press Operation: Health, Safety and Guarding Requirements*.

The requirements in the standards set the minimum measures. If the company can show that it took all of the measures required by the standard, it lends credence to any defence of adequacy. Because they are considered to be the minimum requirement, meeting the standards on their own is not enough if the state-of-the-art approach exceeds the requirements in the standards.

The short answer to this question is to do the following:

- Understand the state-of-the-art approach by researching current safeguarding methods;
- Study the current standards that apply to the situation and implement them;
- Complete a risk assessment with a team of three to five knowledgeable people who understand the use and maintenance of the equipment;
- Implement the changes that are mandated by the risk assessment; and
- If you are unsure about how to proceed, hire a knowledgeable consultant to assist you.

Are you reasonable?

The power of risk assessment in making reasonable decisions about safeguarding is undeniable. The many available methods provide tools to fit almost any situation, from the simplest situation to the most complicated.

You can consider your approach to safeguarding reasonable if you apply all of the available information following the steps above. If you aren't using risk assessment techniques today, it's time to start.

Doug Nix, C.E.T., is program manager, CE Marking and Machinery Safety at QPS Evaluation Services, Inc. in Kitchener, Ontario. Readers can contact him at 519-729-5704; e-mail: dnix1@rogers.com; Web site: www.qps.ca