Automation Safety

Assessing the risks and understanding safeguards

By Yuvin Chinniah and Real Bourbonniere

AUTOMATED SYSTEMS are found in many industries, including food processing, pulp and paper, petroleum, textile and automobile manufacturing. In addition to advantages such as greater productivity, reduced production costs, improved product quality and greater manufacturing flexibility, these systems often eliminate the need for some repetitive, tedious and hazardous tasks.

Under normal operating conditions, workers do not access danger zones and are kept away from many hazards since the automated machines, often controlled by programmable logic controllers (PLCs), are designed to operate without human intervention. As such, these automated systems should inherently improve safety by eliminating the need for workers to reach into danger zones. Furthermore, since fewer workers are needed in automated factories, it could be argued that potentially fewer workers are at risk.

Despite this, automated systems have caused many serious injuries. For various reasons, workers still need to intervene in automated systems. These systems often use multiple technologies (hydraulic, electrical, pneumatic and mechanical) and, as such, they present numerous hazards that are not always easy to identify. Potentially dangerous tasks include maintenance, setting, commissioning, training, material loading/unloading, tool changes or adjusts, adjustments during production, removal of jammed materials, and repairs or interventions following malfunctions. Human error—such as miscommunication between workers who mistakenly energize or start a machine when a coworker is in the danger zone; incorrect use of safeguards; bypassing of protective devices; removal of guards; or changes in the program of electronic programmable safety devices—is also a potential contributing factor for incidents involving automated systems.

Yuvin Chinniah, Ph.D., *is a researcher in machine safety at the IRSST (Occupational Health and Safety Research Institute Robert-Sauve) in Montreal, Quebec. He holds a Ph.D.in Mechanical Engineering (with a specialization in mechatronics) from the University of Saskatchewan, and an undergraduate degree in electrical and electronic engineering from the University of Mauritius. Chinniah currently works in the area of safety-related control systems, predictive maintenance strategies for hydraulic systems, risk assessment and machine safeguarding. Before joining IRSST, he was a lecturer in the Mechanical Engineering Department at the University of Saskatchewan.*

Real Bourbonniere *has worked at IRSST since April 1991. He specializes in the area of safety-related control systems, lockout procedures, risk assessment and the use of safeguards. Bourbonniere was a member of the technical committees responsible for CSA Z432-04 on safeguarding of machinery and CSA Z460-05 on the control of hazardous energy. He holds an undergraduate degree in engineering automation from ETS Montreal, Quebec, and has helped to train inspectors of the Quebec Occupational Health and Safety Commission on machine safety and risk assessment.*

Recent Incidents in Quebec

Paving Block Factory

In June 2006, the Quebec Occupational Health and Safety Commission (CSST) reported on its investigation into the accidental death of a young worker in an automated factory that made paving blocks. The incident occurred when the worker accessed a danger zone located under an automated grabber arm used to stack (palletize) the paving blocks. While trying to rearrange a row of blocks that had become misaligned following a disruption in the normal production flow, the worker, who was younger than 25 years old and had limited experience with the automated machine, was hit and crushed by the grabber, which was located directly above him and moved downward suddenly and unexpectedly.

CCST identified several contributing factors:

- The worker accidentally activated a limit switch while rearranging the blocks. The switch sent an input signal to the PLC that started the palletizing cycle and initiated the grabber's downward movement.
- A light beam, wrongly used as a safeguarding device, had been bypassed. CSST reported that the guard had been circumvented because the "safety" beam frequently disrupted normal production; this was reportedly due to the dusty environment around the palletizing machine.
- The worker had received little or no training regarding the risks to which he was exposed or about safe techniques to use when intervening on the machine. The safe working methods that could have been used included 1) change from automatic

mode to manual mode so that the grabber is no longer controlled by the PLC when a worker intervenes under it; 2) use the existing belt conveyor that carries paving blocks to the grabber to carry the blocks away from the danger zone in order to align them; 3) use a proper lockout procedure to shut down electrical power supply to the grabber arm before any intervention.

CSST also found that no risk assessments had been conducted for the machine. According to CSST, a proper risk assessment would have identified such a hazardous situation (a worker intervening under the grabber) and that appropriate risk reduction methods—such as the use of a safety light curtain rather than a single light beam (the worker could access the danger zone simply by passing below the beam), the use of interlocked guards or the use of a nozzle to blow compressed air on the lens of the light beam to remove dust—could have helped to prevent this fatal incident.

The report also revealed that a safety relay was not used and that the existing safety-related control circuit was not appropriate for the risk level to which the worker was exposed. Moreover, occupational safety and health regulations in Quebec mandate that proper lockout procedures be implemented in plants whenever tasks such as maintenance, setup and removal of jammed materials are performed. CSST strongly suggested the need to implement such procedures (explained in greater detail in CSA Z460-05 and ANSI/ASSE Z244.1-2003).

Farm Equipment

A fatal accident in 2004 involved an automated system on a farm. A farmer was strangled by his sweater, which had become entangled in the rotating shaft of a screw conveyor while he was programming an automated feeding machine. The PLC was found close to the unguarded rotating shaft. CSST found that a danger zone (mechanical hazard) was readily accessible in the automated system and that no safeguards were present.

Batten Packing Facility

In another incident from 2004, a worker was killed in a factory that made battens for wooden floors. An employee was packing battens near a conveyor that had its vertical displacements controlled by a PLC. When the worker tried to pick up a batten that had fallen off the conveyor, the latter suddenly moved downward and jammed the worker's head, killing him. Again, CSST found that no risk assessment had been conducted on this automated system and that several danger zones were readily accessible. CSST concluded that use of an interlocked mobile guard or a safety light curtain could have helped to prevent this fatality.

Paper Mill

Another fatality involving an automated stopper occurred in 2004 at a paper mill. A mechanic finished repairing the stopper controlled by a PLC. When he turned on the pneumatic system by opening a valve located behind the stopper, the latter retracted and the mechanic was seriously injured. CSST found that the mechanic had been performing the intervention while the machine was still being controlled by the PLC. Furthermore, a danger zone was readily accessible. CSST concluded that guards were needed and that a lockout procedure must be followed during maintenance or when removing material blocking or jamming the machine.

Abstract: *Safety in automated systems is an important issue. Several studies have been conducted to examine reports of automation-related accidents. This article summarizes some of these findings and identifies contributing factors to such accidents. In addition, safeguards and their limitations in preventing accidents are discussed, as is the need for proper risk assessment.*

Sawmill

In 2003, a sawmill worker was jammed between the fork elevator of a stacker and the stand for a conveyor of an automated wood piling system. The worker was standing near the fork elevator, waiting for it to stop before cleaning the floor. However, he was in the trajectory of the fast-descending fork and was killed.

Again, CSST found that a danger zone was readily accessible and that worker safety had been ignored when the automated stacking line was designed. Clearly, a risk assessment involving all tasks that required access to the machine had not been performed.

Automation-Related Accidents: An Overview

Incidents involving automated systems have been studied in order to understand their causes. Some studies referred to in this article were conducted several years ago, but as the few examples of recent accidents involving automated systems indi-

cate, their findings can be used to identify potential hazards associated with such systems.

The National Research Institute on Safety (INRS) in France has conducted two studies on the safety of automation systems. The first study analyzed 54 automation-related incidents in France between 1983 and 1987 (Vautrin & Dei-Svaldi, 1989). It showed that interventions following a malfunction of the automated system during production were hazardous and that operators, as well as maintenance personnel were the most frequent victims of those incidents.

INRS conducted another study based on 457 automation-related accidents occurring during a 20-year period in France (Dei-Svaldi & Charpentier, 2001). This study investigated the impact of automated systems on worker safety. The results showed that the accidents occurred mainly during use of the automated system (36%) and during ancillary phases (42%), such as adjustment, supervision, repair, cleaning, inspection or testing. Nearly 25% of the victims had fewer than 3 months' experience. The study confirmed results from the previous study in concluding that many incidents occur during interventions needed after the automated system malfunctions or during maintenance activities.

In another study, the U.K. Health and Safety Executive (HSE) analyzed 143 accidents involving automated systems that occurred between 1996 and 2000 (Edwards, 2001). The analysis revealed that activities such as maintenance tasks, setting, fault finding and rectification put workers at risk, and that 69% of victims were operators and 13% were maintenance staff. In addition, the injured worker was performing one of the following activities when the incident occurred:

- normal production operations, such as feeding and unloading of the machine; quality control, including dealing with minor disturbances to normal operation such as adjusting the position of the product being worked on; and clearing waste product from the work area (45% of the incidents);
- tasks to prepare the machine, including setting, adjusting, recalibrating, tool changing and cleaning (23% of the incidents);
- serious disturbances in normal machine operation, including fault-finding and rectification (15% of the incidents);
- maintenance activities (10% of the incidents).

Many accidents involving automated systems occur when addressing production disruptions. During these malfunctions or disturbances, the automated machine often operates in an abnormal mode. For example, machine movement may have been initiated but was interrupted and is ready to resume once the hindrance is removed. Another example is when an already received start signal stored in the PLC's memory prompts a machine movement as soon as a wedged work piece is freed (Backstrom & Doos, 2000).

Based on the studies and accident reports reviewed, several factors that contribute to automation-related incidents can be identified.

- **Unexpected start-up or machine movement.** This can arise from inappropriate design of the machine's control system; presence of a worker in the danger zone who accidentally activates a sensor; human error at the control panel; software errors in the PLC; or restoration of the energy supply after an interruption.
- **Insufficient or incorrect safeguarding.**
- **Inadequate worker training.**
- **Underestimation of risk.** Workers may either be unaware of or downplay the risks, often because of limited training. Insufficient risk analysis during the design of a system also impacts the perception of risk.
- **Workers tampering with existing safety devices.** Often, this is done to reduce downtime caused by frequent disturbances to normal production.
- **Evolution of automated systems.** This can be caused by modifications in the PLC software; addition or removal of sensors; or changes in safeguarding methods.

Consequences of Automation Accidents

As revealed by Vautrin and Dei-Svaldi (1989), automation-related accidents occur less frequently than other types of machine-related accidents, but they often cause serious injuries, resulting in amputations and death. Of the incidents they reviewed, 26% of the injuries resulted in death; 23% resulted in amputation; 23% required hospitalization; and 28% required no hospitalization.

Of the tasks being performed during those incidents, the person involved was intervening after a malfunction (54%); performing a normal operation (16%); changing settings and making adjustments (20%); and conducting preventive maintenance and supervision (10%).

The injuries reported involved the upper limbs (12%), head (22%), chest (40%) and lower limbs (12%). Those involved were operators (46%); maintenance personnel (22%); adjustment and setup personnel (24%); and supervisors (6%).

Similarly, Dei-Svaldi and Charpentier (2001) found that 27% of workers suffered amputations while 28% experienced fractures; in addition, 16% of the incidents studied were fatal. Edwards (2001) found that 42% of automation-related incidents resulted in major injuries, including amputation and fractures other than fingers and toes.

Risk Management Process: Risk Assessment

As the review of incident reports reveals, risk assessment is an essential part of the overall process to ensure the safety of automated systems. Risk assessment is a series of steps to examine the hazards associated with machines. It can be divided into two phases: risk analysis and risk evaluation (ISO, 1999a).

Risk analysis consists of three stages: determining machine limits; identifying hazards; and estimating risk. The risk evaluation process allows decisions to be made regarding a machine's safety.

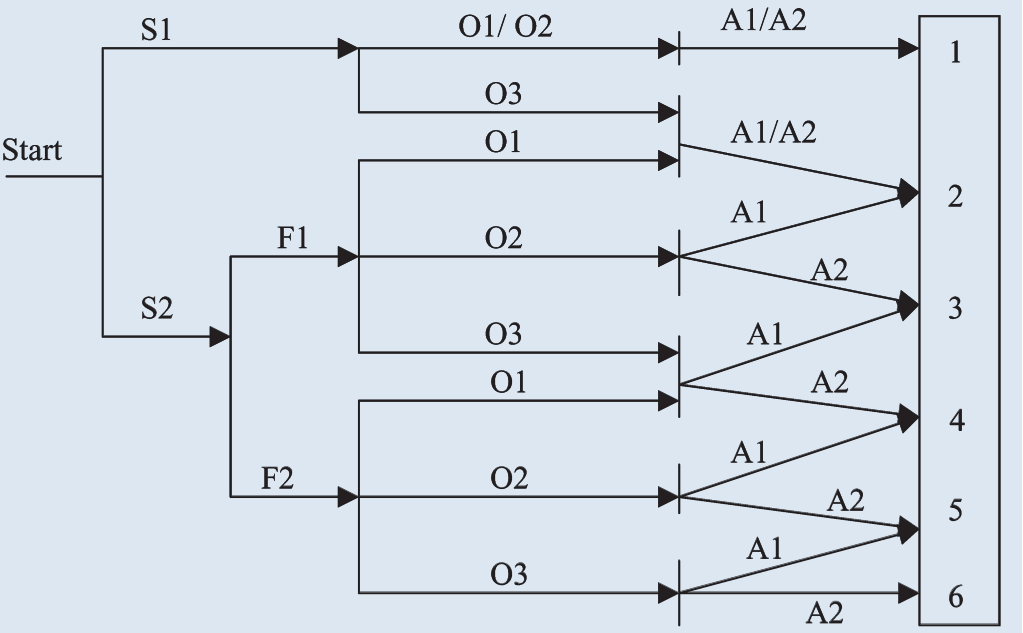
Machinery Limits

Knowing the limits of the automated system includes considering all phases of the machine life—design, construction, transport, installation, commis-

sioning, operation, start-up/shutdown, setting or process changeover, cleaning and adjustment. One must look beyond the intended use and operation of the machine to consider the consequences of reasonably foreseeable misuse or malfunction, as well as the anticipated level of worker training and experience.

Figure 1

Risk Graph: 6 Indices



(S) = severity of the harm
(F) = frequency and/or duration of exposure
(O) = probability of occurrence of the hazardous event
(A) = possibility of avoiding the harm

Hazard Identification

For each task that requires access to a danger zone of the automated systems, associated hazardous conditions must be identified (i.e., hazard, hazardous situation, hazardous event and possible harm, as detailed in ISO 14121). According to Annex A of ISO 14121, hazards in automated systems and for machinery in general fall into two main categories—mechanical and electrical hazards (ISO, 1999a).

Forms of mechanical hazards include crushing, shearing, cutting, entanglement, entrapment, impact and abrasion. These hazards can be produced by various machine parts depending on their shapes, relative motions, masses, stabilities, velocities and strength. Workers can be injured by mechanical hazards in an automated system as a result of being:

- trapped between a machine and a fixed structure;
- struck by material ejected from the machine;
- struck by ejected part of the machine;
- struck by jet of fluid under pressure;
- in contact/entangled with material in motion;
- in contact or entangled with the machine.

Workers can also be injured by electrical hazards, which include situations such as contact with live parts, contact with parts becoming live under fault conditions, approach to live parts carrying high voltage and thermal radiation. Electrical hazards can lead to electrification (injuries), electrocution (death), heart attacks and burns. Thermal hazards, as well as hazards generated by noise, vibration, radiation and dangerous substances are examples of other dangers that should be considered at this stage.

Risk Estimation & Evaluation

Once hazards are identified, the risk of each identified hazard and hazardous situation must be estimated. Risk is a combination of the severity of the harm and the probability of occurrence of that harm. The probability of occurrence of harm can be estimated by considering exposure frequency and duration, the probability of occurrence of a hazardous event and the possibility of avoiding the harm. The combination of these four factors, including the severity of the harm, is used to estimate risk values that can then be used for comparison purposes.

The risk estimation process is usually completed using a risk matrix or graph (Figure 1), where parameter values are combined to produce a resulting risk level. For example, the severity of the harm (S) could be defined as 1) S1, minor injury that is usually reversible (scratches, lacerations, bruises); or 2) S2, serious injury that is usually irreversible (broken or crushed body parts, fractures, death).

The frequency and/or duration of exposure (F) could be defined as 1) F1, twice or less by work shift, or less than 15 minutes cumulative exposure by shift; or 2) F2, more than twice by work shift or more than 15 minutes cumulative exposure by shift.

The probability of occurrence of the hazardous event (O) could be defined as 1) O1, when a mature, tested, robust technology, proven and recognized in safety application, is being used; 2) O2, where technical failure has been observed in the last 2 years or inappropriate human action has been taken by a well-trained employee, aware of the risks, with more than 6 months' experience at the workstation; and 3) O3, when technical failures occur regularly; when an inappropriate human action has been taken by an untrained person with less than 6 months' experi-

ence at the workstation; or a similar accident has been observed within the last 10 years.

The possibility of avoiding the harm (A) could be defined as 1) A1, possible under certain conditions if mechanical parts are moving at a low speed and the exposed worker is familiar with the risks and with indications of its apparition; and 2) A2, impossible.

At the last stage of the assessment process, a decision is made about the safety of each situation. If the risk is deemed intolerable, the process continues with the search for the proper risk reduction method. Risk estimation results are often used as a tool in the evaluation process with the determination of a risk hierarchy.

Without prior risk assessment, relying solely on safeguarding to reduce risks associated with automated systems is troublesome.

Risk Reduction

If the risk evaluation shows that risk reduction is needed, the method used to reduce the risk to a tolerable level should follow a hierarchical approach:

- Eliminate the hazard.
- Substitute less-hazardous materials.
- Use safeguarding.
- Ensure that safe working procedures are used, provide training and protective equipment.

However, it is not always possible to eliminate hazards, and certain tasks require access to danger zones. In such situations, the use of safeguards should be considered. The proposed safeguarding methods then must be assessed. In most cases, existing safeguards should not be considered when conducting a risk assessment. This helps to ensure that all possible hazards associated with a task are identified. It can also enable inherent prevention to be considered—that is, finding means to eliminate the hazard itself. In all cases, the risk reduction method selected must be assessed after its implementation.

Problems with Safeguarding

The machine safeguarding industry is expanding, with an expected compounded annual growth rate of 8.4% over the next 5 years. The market represents $1 billion in 2004 and is forecasted to surpass $1.5 billion by 2009 (Machine safeguarding, 2005). According to ISO 12100, safeguarding is "a protective measure using physical barriers or protective devices to protect persons from the hazards which cannot reasonably be eliminated or risks which cannot be sufficiently reduced by inherent design measures" (ISO, 2003).

Without prior risk assessment, relying solely on safeguarding to reduce risks associated with automated systems is troublesome. The presence of safeguards alone does not guarantee safety since incidents occur despite these protective measures. In fact, the need for workers to intervene into a danger zone imposes additional demands on safeguards.

Vautrin and Dei-Svaldi (1989) highlight the importance of safeguards in automated systems. In their study, the automated systems under investigation had:

- no safeguards;
- wrongly designed or deteriorated safeguards;
- safeguards that had been bypassed or removed during maintenance or repair.

It was concluded that a proper risk assessment, coupled with the use of fixed guards, interlocked mobile guards, safety mats, light curtains and safety procedures could have reduced the risks of accidents (Vautrin & Dei-Svaldi, 1989)

Dei-Svaldi and Charpentier (2001) suggest that during the design stage, engineers should use an appropriate risk assessment method to analyze every operating mode of the system—automatic, semiautomatic, adjustment, manual and degraded. These researchers found that 90% of all incidents reviewed could have been prevented had appropriate safeguards been used.

Edwards (2001) notes that 44% of incidents which occurred during normal production involved machines in automatic mode and reported that this factor, along with the need for workers to gain access to danger zones when the machine was in automatic mode, implied fundamental design problems which should have been identified by proper risk assessments. This study also revealed that existing safeguards did not allow workers to intervene safely in the production process when necessary. Maintenance staff gained access to the machine by suspending the operation of some safety devices and designers need to take that into consideration as well (Edwards, 2001).

Backstrom & Doos (2000) also report that problems with safeguarding in automated systems could cause accidents. This study examined problems related to safety devices in 76 accidents involving automated production. Four common safeguarding problems were reported:

1) not using safeguards, including removing, circumventing, defeating decoupling and failure (54%);

2) failure to stop all machine movement, arising from a) residual pressure in pneumatic and hydraulic systems; b) stalled pneumatic system as a result of a jam and sudden movement when the equipment is freed; c) movement starting when a person is correcting a malfunction in the danger zone; d) time taken for all machine movement to cease not considered (20%);

3) limited range of safeguards, arising when material barriers and presence-sensing devices do not protect workers during work in the danger zone and during work which requires that a machine be energized (18%);

4) safeguard failures, including barrier failure, faulty interlock and a faulty component (5%).

Recommendations for Improving Safety

Automated systems must be assessed, preferably during the design phase, in order to identify all hazards that workers may potentially face. ANSI B11.TR3-2000 (ANSI, 2000) and ISO 14121 (ISO, 1999a) both provide guidance on performing such assessments. Workers should participate in both the risk assessment and in the evaluation of safeguards implemented. The experience of operators, mechanics, setup personnel, electricians and other workers who intervene on the automated machines is crucial.

Ideally, a small team consisting of at least one

operator, maintenance personnel, safety engineer, technician and representative from plant management should conduct the risk assessment. A team approach is best since no one person will know enough about the various tasks performed on the automated systems and have the technical background to conduct a proper risk assessment.

In practice, the team will create a risk assessment table. Column headings may include tasks, hazards, hazardous situations, hazardous events, harm, severity of the harm, exposure duration and frequency, probability of occurrence of the hazardous event, probability of avoiding the hazard, resulting risk level, possible risk reduction methods, and risk reduction method selected.

The rows of the table are used to described different tasks involved with the automated system throughout its life cycle. These tasks could include, for example, feeding and unloading; dealing with minor disturbances to normal operation; clearing waste product from the work area; serious disturbances in normal operation, such as fault-finding and rectification; setting, adjusting, recalibrating, tool changing and cleaning; and maintenance. It helps to use a video camera and photographs to study interventions that require access to danger zones. This way, tasks can be analyzed carefully offline, in a less-stressful environment.

Furthermore, risk reduction methods should be applied in a hierarchical order, as explained in ISO 12100. The first step is to seek ways to eliminate the hazard or to reduce its consequences through design (e.g., eliminate the need for the worker to intervene; reduce speed and force involved in danger zones; avoid danger zones where workers can be trapped or struck by material; use ergonomic principles).

The next step is to install fixed guards that are permanent and that can only be removed with tools. When frequent access to the danger zones is required, an interlocked guard (installed with the proper safety-related control circuitry) should be used. Presence-sensing devices such as light curtains, safety mats, two-hand controls and laser scanners should then be considered. Use of warning signs and alerting techniques, safety procedures, worker training and protective equipment are the least-effective risk reduction methods.

In addition, existing safeguards should be evaluated. Safeguarding techniques such as interlocking of mobile guards, light barriers, pressure mats and two-hand controls often provide an effective level of protection when suitable to the specific tasks and when installed properly (Table 1).

However, their presence alone does not guarantee safety. To identify problems with existing safeguarding, workers should be asked several questions:

- Have you experienced an unexpected movement of the machine or been in a situation where a machine movement occurred when you believed that the machine had safely stopped?
- Do you have to perform tasks where it is impossible or impracticable to use existing safeguards?
- Have you ever bypassed or defeated safeguards? If so, how easily was this achieved?
- What type of safeguards do you think would be more appropriate?
- What kinds of interventions require entry into a danger zone, how often and for how long?
- Do you stop all machine movements before intervening in the danger zone? If not, why?
- Was the training you received sufficient to help

Programmable Logic Controllers & Safety

Industrial automation often involves the use of PLCs. These digital electronic devices have programmable memories to store instructions and to implement functions such as logic, sequencing, timing, counting and arithmetic in order to control machines and processes. PLCs can be programmed to control a wide range of machines and they come in different sizes, generally designated according to the number of inputs and outputs, and the memory capacity. PLCs are similar to microcomputers, with additional features related to their use in industrial environments.

However, the use of the standard PLC for safety functions—such as the interlocking of mobile guards and the connection of emergency stop push buttons—is generally not recommended for three main reasons (Paques, 1990).

First, PLCs are more susceptible to failure than electromechanical relays since environmental conditions can interfere with their operation. PLCs may become sensitive to electromagnetic interference, temperature variation, vibration and humidity if not properly enclosed.

Second, the failure mode for the electronic components is not fully predictable and software problems can cause the program to get hung up in a loop or stopped, making the output erroneous.

Third, the ease of program modification, which is a main attraction of a PLC when it is compared to bulky and expensive relay panels, can pose safety hazards if unauthorized personnel modify the program without proper documentation or verification. This is particularly hazardous if the safety function is what has been modified. Standard PLCs are not designed for safety applications and they exhibit limited fail-safe characteristics, limited redundancy in their architecture and limited software reliability. Therefore, it is typically better to use hardwired circuits involving safety relays to ensure critical safety functions in a way that the safety control circuits are kept independent of the process control circuits.

Table 1

Safeguard Methods, Advantages & Limitations

Safeguard	Advantages	Limitations	Problems in automation[a]
Fixed guard A casing, cover, screen, door or enclosure preventing access in the danger zone. The guard is kept in place by means of screws and nuts, preferably by permanent means such as riveting or welding. Tools are needed to remove the fixed guard.	•Can provide maximum protection. •Requires little maintenance. •Less costly.	•May interfere with visibility. •Gaps and safety distances may have wrong dimensions. •Limited to specific operations. •Machine adjustment and repair may require its removal. •Not suitable where frequent access to guarded zone is needed.	•Guard had to be removed for setup. •Guard was circumvented on the ground since it disturbed the work. •Guard not suitable.
Interlocking guard Prevent starting a machine when the mobile guard is opened. Mobile guards are usually connected by mechanical means (hinges or slides) and need to be interlocked with devices such as cam-activated switches, trapped-key systems, mechanical systems and electrical controls.	•Can provide maximum protection. •Allows access to the machine without removal of fixed guards.	•Requires careful adjustment and maintenance. •May be easy to disengage. •Time required for movement to stop before worker reaches the danger zone must be considered. •Safety interlocking switches may be damaged or misaligned.	•Interlock did not stop all machine movement in the danger zone. •Interlock was defeated. •The cam disk of the interlock switch had become detached. •Interlocked gate was open while workers intervened on the machine on manual mode.
Two-hand control Requires the use of both hands simultaneously to initiate and maintain operation.	•Operator's hands are at a predetermined location, away from the danger zone.	•Protects only the operator. •Blocking the control and enabling one-hand operation may be possible. •May be disconnected.	•The buttons on a two-hand control were activated by mistake by the operator's body as he stretched over the control.
Presence-sensing device Used for detecting danger-zone intrusion or for use inside the danger zone. Sensor types include optical beam, ultrasonic, capacitance, infrared, tactile, pressure-sensitive mats and vision.	•Can allow free movement of operator. •Leaves operator's hand free to work. •Self-testing and fail-safe characteristics possible.	•Does not protect against mechanical failure and object or machine parts being projected toward worker. •May require frequent alignment and calibration. •Excessive vibration may cause sensor damage (e.g., optical beams). •Environmental factors may affect the device and signals. Safety mats risk wear and tear, as well as damage from chemicals. •Light beams are sensitive to dust. •May be possible to work on the dangerous side of the intrusion detection device. •May cause production disturbances. •Time required for movement to stop before worker reaches the danger zone must be considered.	•Ultrasound sensors deactivated since they gave false alarms. •Failure to stop all machine movement. •One person started the machine after the light curtain stopped all movement, while the operator remained inside the danger zone.

[a]*From "Problems with Machine Safeguards in Automated Installations," by T. Backstrom and M. Doos, 2000,* International Journal of Industrial Ergonomics, 25*(6), pp. 573-585.*

you perform tasks correctly and safely? If not, what are some specific deficiencies?

•Are safeguards inspected? Are the inspections effective?

•Do maintenance activities require you to remove or bypass safeguards?

A routine check of safety devices could prove to be an important action before each shift, between operator changes and especially after maintenance activities. The cited studies revealed that maintenance personnel are particularly at risk when performing complex fault-finding and adjustment tasks which require access to danger zones when machine parts are able to move. Therefore, having a post-maintenance testing and inspection program can ensure that equipment is returned to service only after it is verified to be ready.

Maintenance workers might also be expected to perform work when safeguards are removed or when machines are faulty. A proper risk assessment will identify these high-risk situations and will evaluate existing safeguards during maintenance actions. In cases where the use of safeguard is not deemed sufficient, the use of a well-devised and executed lockout procedure (such as that detailed in ANSI/ASSE Z244.1-2003 or CSA Z460-05) will be necessary. Furthermore, if possible, it is best to have a maintenance or setting mode in which the speed of moving parts and the forces involved are lower than those found during normal operating conditions.

Properly designed safety-related control systems, independent of the process control, are also highly recommended for some safeguards to be fully effective (HVBG, 1997). ISO 13849-1:1999 provides guidelines on how to design and implement correct safety-related control systems (ISO, 1999b). More complex systems, such as programmable electronic systems, when used for safety applications, should comply with IEC 62061 (2005).

As noted, use of standard PLCs for safety applications is not recommended, nor is it advisable to connect interlocked guards or light barriers to standard PLCs. Instead, if deemed necessary, safety PLCs should be used. They are certified to meet rigid safety and reliability requirements of international standards and emphasize internal diagnostics that allow the device to detect internal faults.

Conclusion

Sound working principles, such as proper training, use of proper tools and equipment during interventions, use of PPE, and respect of ergonomic principles such as adequate location of control panels in terms of visibility of danger zones can reduce the risks of injury-producing incidents. Worker training should cover how to operate the automated system safely; how to identify and recognize (when possible) potential hazards; existing safeguards and the reasons to not circumvent them; risks associated with their tasks; and recommended safe working methods.

Automated systems offer many advantages—from greater productivity and reduced production costs to improved product quality and a reduced need for employees to perform repetitive tasks. However, they bring with them additional hazards that must be identified, assessed and controlled.

All stakeholders play a role in this process. Design engineers must work to eliminate hazards by considering worker interactions with the automated systems—particularly in danger zones—during the design phase. Management must evaluate the systems once installed to assess risks, develop and enforce safe work practices, and implement appropriate safeguards. Management must also communicate hazards to workers and provide them with the proper tools and training to avoid those hazards. Finally, workers must recognize the hazards associated with these machines, follow safe work practices and understand the need for safeguards. ■

References

ANSI. (2000). Risk assessment and risk reduction: A guide to estimate, evaluate and reduce risks associated with machine tools. ANSI B11.TR3- 2000. New York: Author.

ANSI/ASSE. (2003). Control of hazardous energy: Lockout/tagout and alternative methods. ANSI/ASSE Z244.1-2003. Des Plaines, IL: ASSE.

Backstrom T. & Doos, M. (2000). Problems with machine safeguards in automated installations. *International Journal of Industrial Ergonomics, 25*(6), 573-585.

Canadian Standards Association (CSA). (2005). Control of hazardous energy: Lockout and other methods. CSA Z460-05. Mississauga, Ontario: Author.

Dei-Svaldi, D. & Charpentier, P. (2001). *Study of automation accidents based on the reports of accidents in the EPICEA database.* Paris, France: National Research Institute for Safety (INRS).

Edwards, R. (2001). Learning from mistakes: Experience gained from accidents associated with complex technology. *Proceedings of Safety of Industrial Automated System, U.K.,* 39-44.

HVBG. (1997). *Categories for safety-related control systems in accordance with EN 954-1. BIA-Report 6/97e.* Bonn, West Germany: Author. Retrieved March 20, 2006, from http://www.hvbg.de/e/bia/pub/rep/rep02/bia0697.html.

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

ISO. (1999b). Safety of machinery: Safety-related control system parts. Part 1: General design principles. ISO 13849-1. Geneva, Switzerland: Author.

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

IEC. (2005). Safety of machinery: Functional safety of safety-related electrical, electronic and programmable electronic control systems. IEC 62061. Geneva, Switzerland: Author.

Machine safeguarding market to grow. (2005, Nov.) *Automation,* 1-48.

McConnell, S. (2004, Jan.). Machine safeguarding: Building a successful program. *Professional Safety, 49*(1), 18-27.

Manuele, F. (2005, Nov.). Global harmonization of safety standards: Examining the European influence on the practice of safety. *Professional Safety, 50*(11), 41-46.

Mitchell, C. & Williams, K. (1993). Failure experience of programmable logic controllers used in emergency shutdown systems. *Reliability Engineering and System Safety, 39*(3), 329-331.

Paques J.J. (1990, Feb.). Basic safety rules for using programmable controller. *ISA Transactions, 29.*

Pilz Automation Technology. (1999). *Guide to machinery safety.* Northants, U.K.: Author. Retrieved March 20, 2006, from http://www.pilzsupport.co.uk/downloads_gms.htm.

Roudebush, C. (2005, Oct.). Machine safeguarding: A process for determining tolerable risk. *Professional Safety, 50*(10), 20-24.

Vautrin J.P. & Dei-Svaldi, D. (1989). *Work accidents in automated plants: Evaluating a preventive method.* Paris, France: INRS.