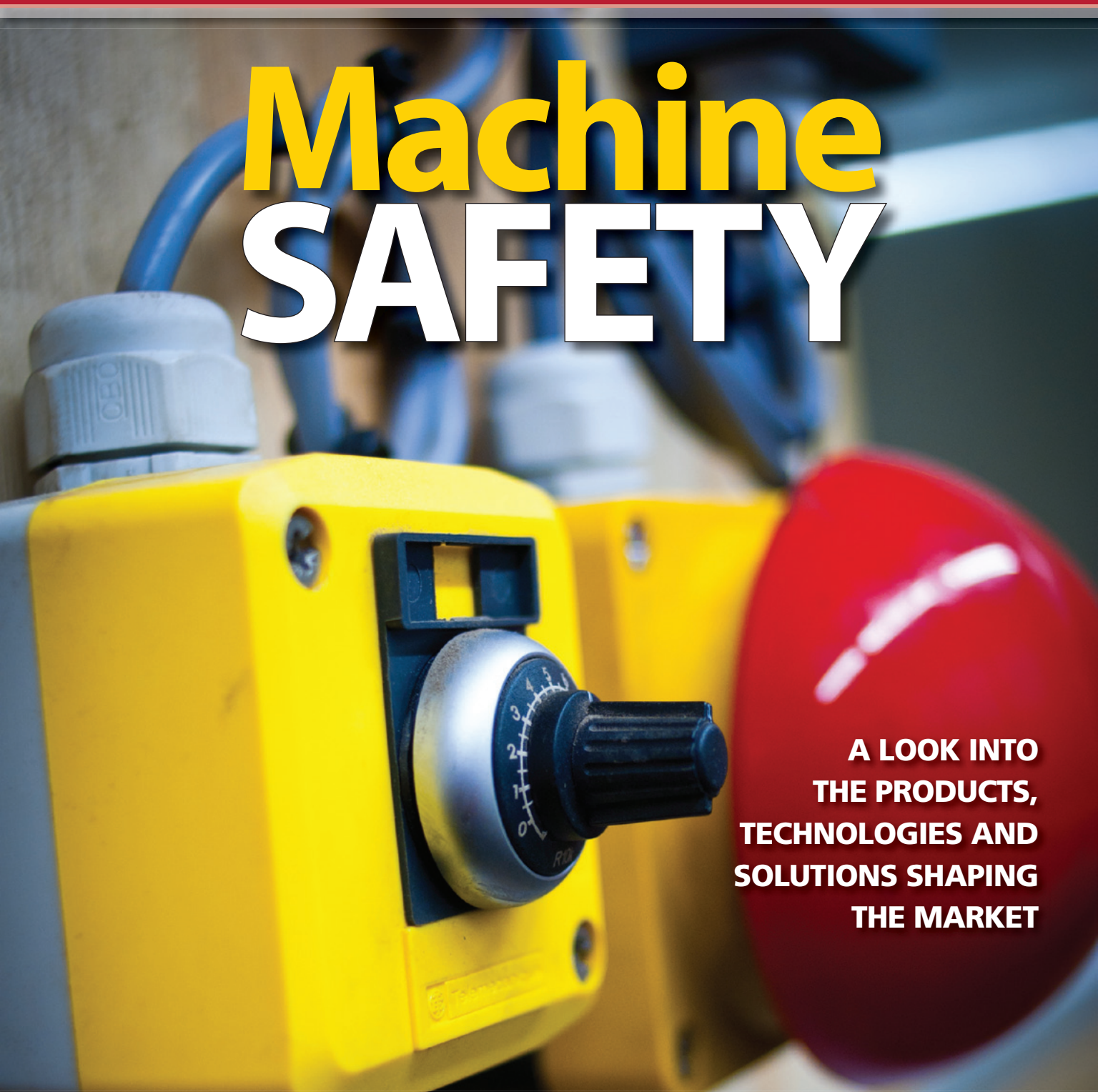
TECHNOLOGY HANDBOOK

Machine SAFETY



A LOOK INTO THE PRODUCTS, TECHNOLOGIES AND SOLUTIONS SHAPING THE MARKET

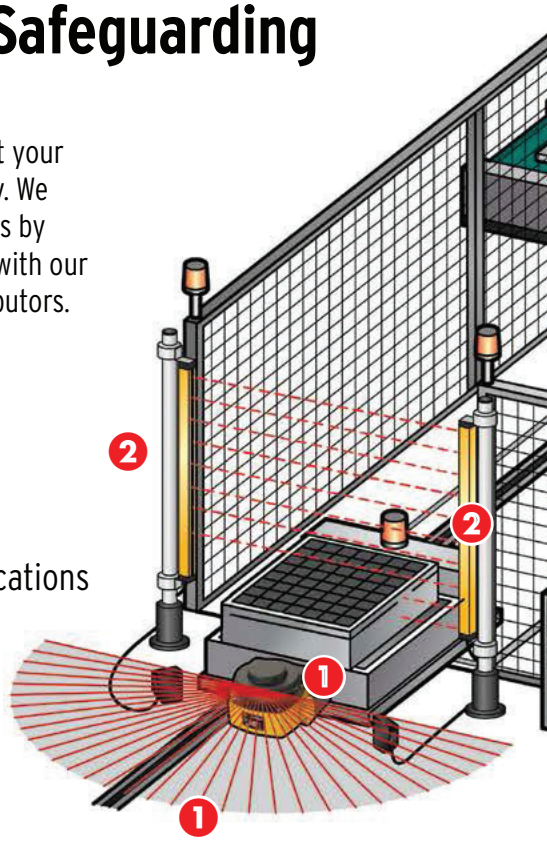
DIGITAL SUPPLEMENT TO
MANUFACTURING AUTOMATION
MACHINE DESIGN • SYSTEMS • TECHNOLOGY

We Make Safety Simple

From components to consulting, Omron is your single source for Machine & Process Safeguarding

Poised at the leading-edge of safety solutions worldwide, Omron's STI safety products focus on making safety work. We are aware of the many demands of automation safeguarding. Consequently, our automation safety products meet or exceed local and international safety standards.

Omron is committed to providing safeguarding solutions that meet your needs for safety and productivity. We design and engineer our products by listening to and working closely with our customers and authorized distributors.



We also provide:

- Experienced assistance
- Expert guidance in application, integration and maintenance
- World-class support through Omron's global network of 250 sales locations in 65 countries

Omron Automation & Safety

www.sti.com

Contact us at www.sti.com/info or 1.866.986.6766

1 Safety Laser Scanners

Our OS32C is a very compact safety laser scanner. It has 70 zone configurations for complex guarding parameters.

OS32C

New Industry First!
EtherNet/IP capable of status and measurement data reporting.

2 Safety Light Curtains

The MS4800 and F3SJ models are simple to install, and available in a wide selection of protected heights and resolutions.

MS4800

MSF4800

F3SJ

3 Safety Interlock Switches

Tamper resistant switches enhance mechanical guarding methods.

- Guardlocking switches
- Hinge pin switches
- Non-contact switches
- Limit switches
- Tongue switches
- Explosion-proof versions

D4NS

D4B-□N

D4N

D4F

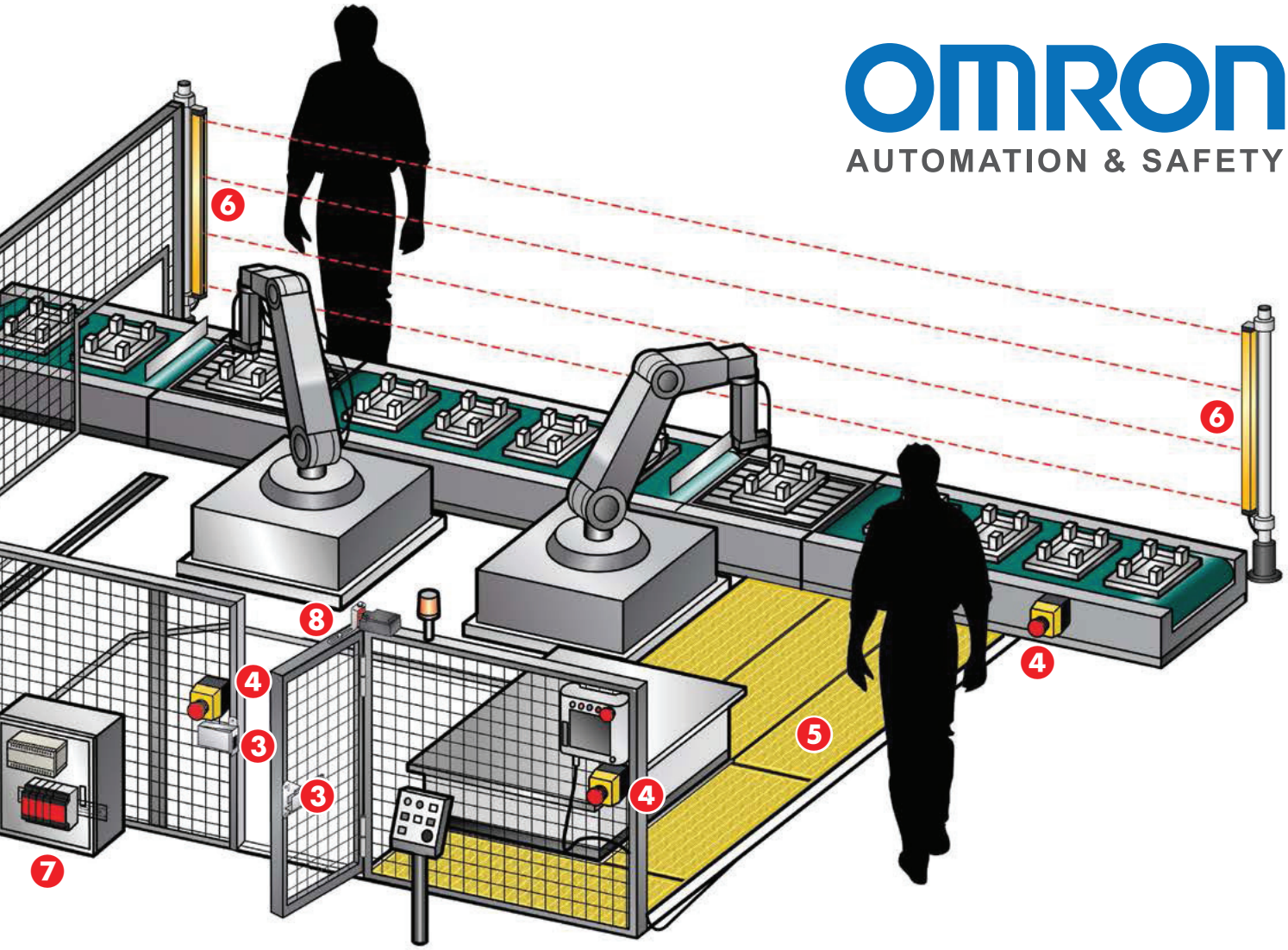
4 Emergency Stop Devices

- Enclosed and panel-mounted models available with key-operated reset
- Combination rope and push button actuated emergency stop switches
- Heavy duty housing offering rope spans to 200 meters

A165E

ER6022

OMRON
AUTOMATION & SAFETY



5 Safety Edges & Bumpers

5 Safety Mats & Area Guarding

Built tough for tough environments. Combine a mat with a controller to provide proven reliability.

6 Perimeter Guarding

PA4600 models are available with single and multiple-beam models with an operating range to 70 meters. They're perfect when installing fences is not practical.

PA4600

7 Safety Programmable Controllers

7 Safety Monitoring Relays

The G9SP stand-alone programmable safety controller for mid-sized applications supports direct connection to safety mats and non-contact switches. The NE1A DeviceNet safety network controller is well-suited for large complex applications, while safety monitoring relays are ideal for ensuring control reliability in smaller applications.

NE1A

G9SP

8 Enabling Switches

Provides the additional protection needed during set-up, programming and servicing of robotic and automatic equipment.

- Has distinct clicks for three easily discernible positions

A4EG

G9SX

PHOENIX CONTACT
INSPIRING INNOVATIONS

The New Age of Safety Integration

In machine automation, one of the primary objectives is the efficient and flexible integration of safety functions. Every automation system is different, but similar safety solutions are effective when comparing equally scaled applications. For small-scale applications, simple-to-configure safety relays are usually better suited, whereas large-scale applications usually employ highly integrated and networked fail-safe PLCs. A new approach encompassing both flexible and easy network communications would bridge these two solutions and support machine builders during the realization of an efficient, networked safety solution without the need for a full fail-safe PLC.

Phoenix Contact presents SafetyBridge Technology

Until now, de-centrally distributed signals always required a central safety controller or installations with parallel wiring to the classic relay solutions. The parallel wiring generates a significant increase in installation costs even in the case of a minimum expansion of the machine or system.

SafetyBridge technology from Phoenix Contact is a new approach to safe network communication in automation networks. The SafetyBridge Technology provides the user with an economical solution for the functional safety without the use of a safety controller or a safety bus system. The safe inputs and outputs are distributed in the network and do not require a higher-level safety controller or a separate safety bus system, making it very easy for users to integrate safety into the systems or technologies they have come to rely on.

The existing automation network and the standard controller only serve as a means to transport the safety-relevant data packets that are exchanged between the safe input and safe output modules. As a result, users do not have to choose a safe network and can continue using their own communication system. The complicated task of connecting the safety signals in parallel is no longer necessary. This provides users with an as yet unheard of degree of flexibility in the area of bus-based safety applications.

Phoenix Contact has incorporated SafetyBridge Technology into the tried and tested Inline installation system. No special safety-relevant guidelines need to be followed when installing the SafetyBridge modules. This means that downtimes can be reduced without additional programming or connection work.

The free and simple SAFECONF configuration tool is used to create, check, and simulate the safety system before being integrated into the standard PLC software. The SafetyBridge can be used for safety applications up to Category CAT. 4, SIL 3, PL e. and approved for Profibus, Profinet, Interbus, Ethernet and other networks.

Conclusion

Functional safety should no longer be viewed as a separate issue. Users can gain major competitive advantages by thoroughly integrating it into the automation solution of a machine or plant. Extensive diagnostic options reduce installation costs and downtimes and hence increase availability and productivity. The intelligent use of safety technology provides machine and plant manufacturers with a real competitive advantage that can prove decisive in a market where the speed with which a company can act is more important than its size.

Kian Sanjari, P.Eng.
Product marketing manager
I/O & Networking for Phoenix contact ksanjari@phoenixcontact.ca

PHOENIX CONTACT
INSPIRING INNOVATIONS

Phoenix Contact Ltd.
8240 Parkhill Drive, Milton, ON L9T 5V7
Phone: 1-800-890-2820
www.phoenixcontact.ca

Get connected.
Stay protected.

Safeguard critical oil and gas systems by protecting control and information networks from malicious attacks and accidental interruptions.

As a powerful cyber security appliance, FL mGuard RS2000 and RS4000 from Phoenix Contact provides firewall, NAT routing and VPN functionality. Configuration pages are accessed with our easy-to-use web-based management.

The FL mGuard RS4000 features:

- **SD card reader**
- **Rugged hardware to withstand harsh installation environments**
- **The RS4000 is Class 1, Division 2 certified.**

To learn more, call
1-800-890-2820 or visit
www.phoenixcontact.ca

PHOENIX CONTACT
INSPIRING INNOVATIONS

Accidents are Preventable with Machine Safety and Guarding

It's easy to understand why machine safety and guarding is such an important issue. Machine operation and maintenance causes approximately 1800 injuries and over 80 deaths in Canada each year, according to the Workers Health & Safety Centre of Ontario. Yet, most of these occurrences are preventable.

Machine safety is a vastly important workplace consideration. Many organizations don't have the internal resources or the expertise to ensure that their equipment and environments comply with safety standards; therefore, they must seek help from a trusted, external organization.

The critical first step to having a safe, hazard-free workplace is a comprehensive machine risk assessment. It will determine if machinery meets the latest North American standards, identify potential hazards, and provide detailed recommendations to diminish vulnerabilities.

For 20 years, Vickers-Warnick has been a leading expert in machine safety, machine guarding, and risk assessments. The company is a long-standing, actively engaged member of many machine safety standards bodies. Working collaboratively with clients, the Vickers-Warnick team develops machine safety solutions that reduce risks while keeping budgetary concerns in the forefront.

The Vickers-Warnick guarding and assessment process (GAAP) follows well-established procedures and guidelines to bring machinery environments up to standard and to ensure that personnel are protected:

- **Complimentary Safety Consultation –** An initial review will highlight risk areas, applicable safety standards, and potential solutions.
- **Machinery Risk Assessment –** A detailed safety assessment will evaluate all areas of risks and determine any compliancy issues.
- **Stop-Time Measurement Analysis –** Readings are taken on individual machines and analyzed to determine the minimum safety-distance from the risk-zone to make it impossible for personnel to be exposed to a hazard before the machine has completely stopped.
- **Recommendations –** Detailed recommendations are made for specific equipment and the machine environment.
- **The Vickers – Warnick** team presents this assessment to the client, providing consultation and guidance. Upon client's agreement, Vickers-Warnick will move ahead with scheduling and implementing the necessary safety solutions.
- **Vickers – Warnick** safety technology solutions include electronic light curtains, emergency stop switches, safety sensors, ergonomic safety mats, and more. Their fully owned subsidiary, Darlex, specializes in custom-designed physical guards.

To offer an example of how Vickers-Warnick has helped organizations in the past, we can examine the steel manufacturing industry. A major producer in the industry was concerned about the safety of its facilities due to a history of injuries.

Vickers-Warnick was tasked with assessing primary pinch-point hazards and wiring/electrical code deficiencies; however, the steel manufacturer needed to enhance the safety of the machinery while ensuring that the safety design would not interrupt production.

Vickers-Warnick applied a solution to hard guard using a complete enclosure with safety interlocked doors. A safety controller and new variable frequency drive with jog capabilities were integrated, and wiring schematics were provided. Darlex aluminum extrusion and steel guarding was installed where guards were exposed to heavy lift-truck traffic.

Furthermore, the recoiler area was updated to fulfill the requirements of the CSA Z432-04 safety standard.

Vickers-Warnick is able to customize safety solutions for a wide variety of organizations and industries. Keeping equipment and environments safe is the first priority, for the sake of the health and protection of operators and personnel.

Workplace accidents don't have to happen.

Vickers-Warnick Ltd.
870 Arvin Avenue, Unit 2, Stoney Creek, ON L8E 5P2
Phone: 1-800-263-6835
www.vickers-warnick.com

VICKERS WARNICK
Machine Safety Solutions

machinesafety.com
VICKERS WARNICK
Machine Safety Solutions

INJURIES DON'T HAVE TO HAPPEN

REDUCE THE RISK WITH VICKERS-WARNICK

At Vickers-Warnick, we are experts in machine safety.
We take care of everything: **Detailed machine risk assessments, Recommendations, Customized guarding solutions, Installation, Training, And on-going reviews.**
Accidents can be prevented.

See how we offer best-in-class machine safety
assessments and solutions at machinesafety.com

PLEASE CONTACT US AT

1-800-263-6835
stoney@vickers-warnick.com

Interlocking devices

The good, the bad and the ugly

BY DOUGLAS NIX, A.SC.T.

When designing safeguarding systems for machines, one of the basic building blocks is the movable guard — doors, panels, gates or other physical barriers that can be opened without using tools. Every one of these guards needs to be interlocked with the machine so that the hazards covered by the guards are effectively controlled when the guard is opened.

There are a number of important aspects to the design of movable guards. This article will focus on the selection of interlocking devices that are used with movable guards.

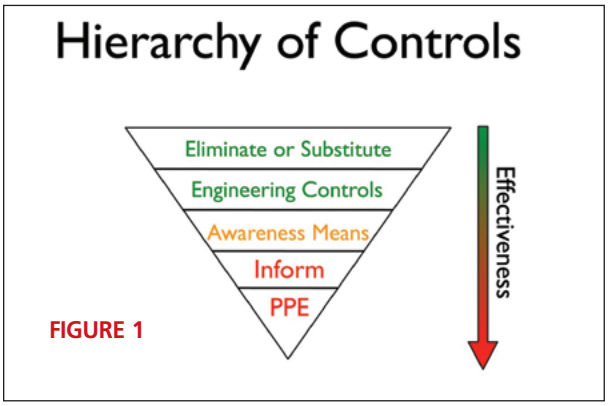


FIGURE 1

THE HIERARCHY OF CONTROLS

This article assumes that a risk assessment has been done as part of the design process. If you haven't done a risk assessment, start there, and then come back to this point in the process.

The hierarchy of controls describes levels of controls that a machine designer can use to control the assessed risks [1]. Designers are required to apply every level of the hierarchy in order, starting at the top. Where a level cannot be applied, the designer moves to the next lower level.

Though much emphasis is placed on the correct selection of these interlocking devices, they represent a very small portion of the hierarchy. It is their widespread use that makes them so important when it comes to safety system design.

ELECTRICAL VERSUS MECHANICAL INTERLOCKS

Most modern machines use electrical interlocks because the machine is fitted with an electrical control system, but it is entirely possible to interlock the power to the prime movers using mechanical means. This doesn't affect the portion of the hierarchy involved, but it may affect the control reliability analysis that you need to do.

CATEGORIES

In Canada, CSA Z432 [2] and CSA Z434 [3] provide four categories of control reliability: simple, single channel, single channel monitored and control reliable. In the U.S., the categories are very similar, with some differences in the definition for control reliable. In the EU, there are five levels of control reliability, defined as Performance Levels (PL) in ISO 13849-1: PL a, b, c, d and e [4]. Underpinning these levels are five architectural categories: B, 1, 2, 3 and 4. Figure 2 shows how these architectures line up.

To add to the confusion, IEC 62061 [5] is another international control reliability standard that could be used. This standard defines reliability in terms of Safety Integrity Levels (SILs). These SILs do not line up exactly with the ISO 13849-1 PLs, but they are similar. IEC 62061 is based on IEC 61508 [6], a control reliability standard used in the process industries. IEC 62061 is not well suited to applications involving hydraulic or pneumatic elements.

The North American architectures deal primarily with electrical or fluid-power controls, while the EU system can accommodate electrical, fluid-power and mechanical systems.

From the single channel monitored or Category 2 level up, the systems are required to have testing built-in, enabling the detection of failures in the system. The level of fault tolerance increases as the category increases.

INTERLOCKING DEVICES

Interlocking devices are the components that are used to create the interlock between the safeguarding device and the machine's power and control systems. Interlocks can be purely mechanical, purely electrical or a combination of these.

Most machinery has an electrical/electronic control system, and these systems are the most common way that machine hazards are controlled. Switches and sensors connected to these systems are the most common types of interlocking devices.

Interlocking devices can be something as simple as a microswitch or a reed switch, or as complex as a non-contact sensor with an electromagnetic locking device.

Requirements for these devices are published in a number of standards, but the key ones for industrial machinery are ISO 14119 [7, 2], and ANSI B11.0 [8]. These standards define the electrical and mechanical requirements, and in some cases the testing requirements, that devices intended for safety applications must meet before they can be classified as safety components.

These devices are also integral to the reliability of the control systems into which they are integrated. Interlock devices, on their own, cannot meet a reliability rating above ISO 13849-1 Category 1, or CSA Z432-04 Single Channel. To understand this, consider that the definitions for Category 2, 3 and 4 all require the ability for the system to monitor and detect failures, and in Categories 3 and 4, to prevent the loss of the safety function. Similar requirements exist in CSA and ANSI's "single-channel-monitored," and "control-reliable" categories. Unless the interlock device has a monitoring system integrated into the device, these categories cannot be achieved.

ENVIRONMENT, FAILURE MODES AND FAULT EXCLUSION

Every device has failure modes. The correct selection of the device starts with understanding the physical environment to which the device will be exposed. This means understanding the temperature, humidity, dust/abrasives exposure, chemical exposures, and mechanical shock and vibration. Selecting a delicate reed switch for use in a high-vibration, high-shock environment is a recipe for failure, just as selecting a mechanical switch in a dusty, corrosive environment will also lead to premature failure.

The device standards do provide some guidance in making these selections, but it's pretty general.

Fault exclusion is another key concept that needs to be understood. Fault exclusion holds that failure modes that have an exceedingly low probability of occurring during the lifetime of the product can be excluded from consideration. This can apply to electrical or mechanical failures. Here's the catch: Fault exclusion is not permitted under any North American standards at the moment. Designs based on the North American control reliability standards cannot take advantage of fault exclusions. Designs based on the international and EU standards can use fault exclusions, but significant documentation supporting the exclusion of each fault is needed.

DEFEAT RESISTANCE

The North American standards require that the devices chosen for safety-related interlocks be defeat-resistant, meaning they cannot be easily fooled with a cable-tie, a scrap of metal or a piece of tape.

The International and EU standards do not require the devices to be inherently defeat-resistant, which means that you can use "safety-rated" limit switches with roller-cam actuators, for example. However, as a designer, you are required to consider all reasonably foreseeable failure modes, and that includes intentional defeat. If the interlocking devices are easily accessible, then you must select defeat-resistant devices and install them with tamper-resistant hardware to cover these failure modes.

Almost any interlocking device can be bypassed by a knowledgeable person using wire and the right tools. This type of defeat is not generally considered, as the degree of knowledge required is greater than that possessed by "normal" users.

DEVICE SELECTION

When selecting an interlocking device, start by looking at the environment in which the device will be located. Is it dry, wet or abrasive? Is it indoors or outdoors and subject to temperature variations?

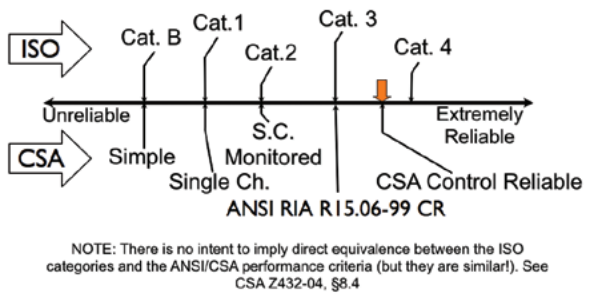
Is there a product standard that defines the type of interlock you are designing? An example of this is the interlock types in ANSI B151.1 [4] for plastic injection moulding machines. There may be restrictions on the type of devices that are suitable based on the requirements in the standard.

Consider integration requirements with the controls. Is the interlock purely mechanical? Is it integrated with the electrical system? Do you require guard locking capability? Do you require defeat resistance?

Once you can answer these questions, you will have narrowed down your selections considerably. The final question is: What brand is preferred? Go to your preferred supplier's catalogues and make a selection that fits with the answers to the previous questions.

The next stage is to integrate the device(s) into the controls, using whichever control reliability standard you need to meet. That is the subject of another article!

FIGURE 2



NOTE: There is no intent to imply direct equivalence between the ISO categories and the ANSI/CSA performance criteria (but they are similar!). See CSA Z432-04, §8.4

REFERENCES

[1] Safety of machinery - General principles for design - Risk assessment and risk reduction, ISO Standard 12100, Edition 1, 2010

[2] Safeguarding of Machinery, CSA Standard Z432, 2004 (R2009)

[3] Industrial Robots and Robot Systems - General Safety Requirements, CSA Standard Z434, 2003 (R2008)

[4] Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design, ISO Standard 13849-1, 2006

[5] Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems, IEC Standard 62061, Edition 1, 2005

[6] Functional safety of electrical/electronic/programmable electronic safety-related systems (Seven Parts), IEC Standard 61508-X

[7] Safety of machinery – Interlocking devices associated with guards – Principles for design and selection, ISO Standard 14119, 1998

[8] American National Standard for Machines, General Safety Requirements Common to ANSI B11 Machines, ANSI Standard B11.0, 2008

Douglas Nix, A.Sc.T., is managing director at Compliance InSight Consulting, Inc. (www.complianceinsight.ca) in Kitchener, Ont. He produces a blog and podcast called Machinery Safety 101, exploring a wide variety of machine safety topics. Check out his blog at www.machinerysafety101.com.

Evaluating the incentive to defeat protective devices

BY FRANCO TOMEI

Many enterprises seem to accept the high risk generated by defeated protective devices placed on machinery. By "defeated," I mean safety devices that have been altered so as to render their intended function ineffective. There are also safety integrators that install protective devices that render the machine unusable. While this may sound far fetched, I have, on at least two occasions, been called upon to review machinery that became unusable because of the protective devices.

Use of protective devices on machinery is necessary to protect the worker. If the moral obligation isn't enough to ensure their effectiveness, there are regulatory requirements that must be fulfilled. Yet, many workplaces end up with machinery whereby defeating the protective device is part of a company's everyday life.

Time and again, defeated protective equipment causes severe injuries and, in some cases, fatalities. From a realistic viewpoint, it must be stated that defeating protective devices could not happen if there was not some willingness on the part of the employer/supervisor to permit the defeating to happen. Rather than criticize these actions, we must refrain from placing blame and learn why such actions take place. If we can learn the why, we may be able to prevent the defeating of safeguards.

Given that a worker is a rational, thinking person, defeating a protective device for no reason simply would not occur. Similarly, given that the employer is a rational, thinking person, he or she would also not permit the defeating of protective devices. To get to the root of the problem, it must be concluded that the defeating takes place because there is something to gain — whatever that gain may be perceived to be by either party.

In a study conducted in Germany, it was found that 37 percent of protective elements were defeated. In presenting this study a few years ago in Mississauga, Dr. Friedrich Adams of Schmersal GmbH did not call for greater enforcement, nor did he place blame on the employer or worker. Rightfully, in my opinion, Dr. Adams stated that we as machine builders or safety integrators have failed in our mission to the worker and the employer. We have failed because we have created the conditions such that the performance of a task is so inconvenient or cumbersome that we are providing an incentive to the worker and/or employer to defeat the protective device.

If defeating the protective device is foreseeable, the manufacturer and/or safety integrator has to take this into account at the design stage or during the retrofit. Essentially, as designers/users, we know the tasks that are to be performed on the machine. Once the tasks are identified, we need to ensure the worker is protected in the course of performing each of those tasks, but we must do so without any significant "inconvenience" to the worker or process. If the protective device creates an "inconvenience," then the first thing that will be done by the individual worker or in collusion with others and with the blessing of supervisors/employers, is the protective device will be defeated — and sooner or later this will result in an injury.

In the machinery industry, the manufacturer of the machinery and the user of the machinery should have a collaborative program whereby information is exchanged to ensure there is no task whereby there is a significant incentive to defeat the protective device. This would assist the manufacturer in seeking solutions to prevent such events.

How can one assess whether or not their own machinery's protective devices are defeated? Several tools can be used, such as supervisory inspections of the protective devices, reports from the manufacturers (although not common), and asking the worker for input on the adequacy of the machine in performing their work. However, the better approach is to, at the design stage, assess whether or not there is a foreseeable significant enough incentive for a protective device to be defeated in performing a specific task.

Assessing whether or not a safeguard will be defeated is not insurmountable. The steps necessary to do so are as follows:

- Identify each activity required for the machine;
- Break the activity down into the various tasks; and
- For each task, assess whether or not the task needs to be performed with a protective device to protect the worker.

Assess whether there is a significant enough incentive to defeat the safeguard by considering the following 11 common incentives:

1) Will defeating the safeguard make the job easier or more convenient?
2) Will defeating the safeguard result in faster and/or greater productivity?
3) Will defeating the safeguard result in increasing the capacity of the machine?
4) Will defeating the safeguard result in greater precision?
5) Will defeating the safeguard result in better visibility?
6) Will defeating the safeguard result in better audibility?
7) Will defeating the safeguard result in less physical effort?
8) Will defeating the safeguard result in reduced travel?
9) Will defeating the safeguard result in greater freedom of movement of the worker?
10) Will defeating the safeguard result in material flow improvement?
11) Will defeating the safeguard result in avoidance of interruptions?

The above questions could be answered with a straight yes or no, but life is never that simple as there are degrees of incentives. It is therefore recommended that a score be given to each of the questions, whereby an acceptable number is defined. In addition, one should also look at the greater picture since, while all of the answers may be low enough to be a no, the total may result in a yes.

Where the answer is yes, action must be taken on the possible various fronts that will permit the worker to perform the task without having significant incentive to defeat the protective device.

Franco Tomei, B.A.Sc. P.Eng, is a professional engineer with more than 40 years of industrial experience — 12 years of that directly in the safety field. He can be reached at ftomei@yahoo.com.

Stand on guard: Preventing access is key to machine guarding

BY FRANCO TOMEI

Sections 24 and 25 of the Regulations for Industrial Establishments should be considered the primary but not the only requirements for machine guarding. They read as follows:

24. Where a machine or prime mover or transmission equipment has an exposed moving part that may endanger the safety of any worker, the machine or prime mover or transmission equipment shall be equipped with and guarded by a guard or other device that prevents access to the moving part.

25. An in-running nip hazard or any part of a machine, device or thing that may endanger the safety of any worker shall be equipped with and guarded by a guard or other device that prevents access to the pinch point.

If we look at these closely, they are general but encompassing. The first thing to note is that there must be exposed moving parts. Secondly, that moving part must be such that it endangers the safety of any worker (and not just the operator). Implicitly, there is the statement that not all moving parts may endanger a worker. Thirdly, the worker is to be prevented from having access to the exposed moving part.

A hazard identification and hazard analysis would be the first step in identifying hazardous circumstances whereby a worker has access to exposed moving parts or nip points that may endanger the safety of any worker.

In any case, what is to be noted is that the provisions place the onus on the employer to prevent access and not on the worker not to gain the access. This is often very hard for many of us to accept simply because, on the surface of it, it would not rational for anyone to do so. But things are not always as they appear and, with a closer look, we must acknowledge that there are various reasons why a worker may reach into these hazardous zones. Some of these are as follows:

- Some people will reach where they should not because in a moment, split-second decisions are made often on emotion (as part of the body's reaction) and not using rational thinking.
- The worker is not able to perform a specific function without reaching "in there"—the result of poor design.
- The worker believes that the gods (or fate or luck) are on his or her side and somehow feels exempt from a hazardous event or the person simply "knows" what he or she is doing, unlike a person who was injured. The reality is that nobody has a monopoly on errors in judgment—we all make our fair share of mistakes.
- We must also consider the reality of life in that while a worker may be expected to concentrate 100 per cent of the time on the task at hand, a person working eight to 10 hours a day cannot concentrate 100 per cent of the time. Everyday life ensures that we have other issues to deal with (like our finances, marriages, children, aging parents, personal health issues and so much more). How can we reasonably expect 100 per cent concentration 100 per cent of the time?

In analyzing the subject provisions, it becomes clear that the core requirement of sections 24 and 25 is to prevent access. On a personal basis, I often demonstrate to an employer that I have access to exposed transmission elements. The response is like a deer looking into a headlight: "why would you put your hands in there?"

You cannot use whether or not there is an injury as the basis for judging if you meet the standard. Instead, you need to look at whether or not the person has access to an area that has potential for injury.

The purpose of the regulations is to prevent any injury from occurring by preventing the access. Saying "I have been here 37 years and nobody has ever been hurt" is not a defense. The reality is that the absence of an accident does not constitute a safe situation. Sooner or later the hazardous event will occur with the possibility of very serious consequences.

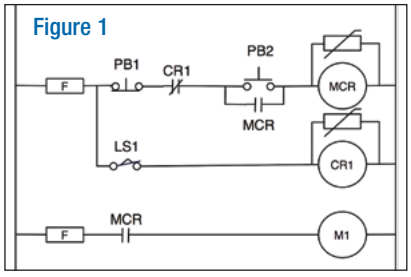
Let's look at preventing access in more detail. We often see signs posted and the question becomes: "will a sign prevent access?" Of course not. A sign may provide information, but only if it is read. Anecdotally, we have all seen a sign that says "WET PAINT DO NOT TOUCH." Of course, now we need to ensure the sign is not giving false information and we touch the paint. Since signs do not prevent access, we must resort to engineering solutions that either prevent access to the hazard by virtue of a physical barrier or eliminate the hazard before any worker can gain access (as in the case of providing an interlocking device that signals the apparatus to stop).

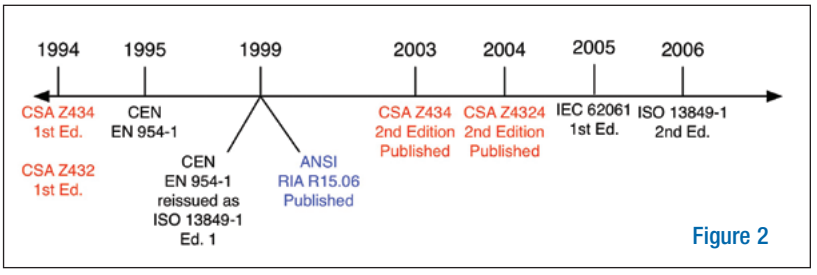
Whether or not some of the readers agree with these requirements of these provisions, is not the issue—this is a matter for government policy and the regulators to deal with.

Franco Tomei, B.A.Sc. P.Eng, is a professional engineer with more than 40 years of industrial experience—12 years of that directly in the safety field. He can be reached at ftomei@yahoo.com.

Get up to speed on functional safety standards and machinery design

BY DOUG NIX





Functional safety is a growing field in engineering, and one that is having increasing influence in most products that include active control systems. If you haven't heard this term before, you can find one definition in an IEC Standard: "Functional safety is part of the overall safety that depends on a system or equipment operating correctly in response to its inputs."

Since the mid-1990s, functional safety has been slowly creeping into the industrial machinery design field. Prior to that, most machines had a simple emergency stop circuit, one that often did double-duty as the main power control for the machine. In many cases, a simple interlock was added to that circuit, and voila! You had the safety-related parts of the control system. Figure 1 shows a simple master control relay circuit with interlock.

In this figure, the 'MCR,' or Master Control Relay, would typically be a fairly beefy contactor, usually with a DC contact rating so that both AC and DC control circuits could be directly switched.

'PB2' is the 'Power On' button, 'PB1' is the 'Power Off' button, and if it was fitted with a red mushroom-head operator, could also operate as the Emergency Stop button. 'LS1' is the guard interlock limit switch, and 'CR1' is the interlock relay. 'M1' represents the machine prime mover, like a conveyor motor or a hydraulic pump, for example.

To really understand the problems we are facing, a little history is needed. The timeline shown in Figure 2 illustrates the development of the standards.

Functional safety was described in the first editions of both CSA Z432 and Z434, but little direction was given to designers about the appropriate use of these approaches. In 1995, EN 954-1 was introduced in Europe and was harmonized under the Machinery Directive of the day, introducing the reliability categories that have become familiar: Categories B, 1-4. EN 954-1 marked the first time that prescribed control circuit architectures were described, and also gave designers more specific guidance on when to use the different categories to achieve effective risk reduction. ISO would later take over responsibility for EN 954-1, renumbering it as ISO 13849-1 and publishing the first edition in 1999; this edition was virtually unchanged from EN 954-1.

In 1999, ANSI published the second edition of RIA R15.06 and detailed the prescribed control circuit architectures in a North American standard. The categories were not identical to those in EN 954-1 or ISO 13849-1, and were called SIMPLE, SINGLE CHANNEL, SINGLE CHANNEL MONITORED and CONTROL RELIABLE. These categories were quickly adopted with some changes by CSA and included in CSA's Z432 and Z434 standards in 2003 and 2004 respectively.

In 2006, everything changed with the publication of ISO 13849-1, Edition 2. This edition expanded on the prescribed architectures from the first edition, introducing the ideas of Performance Level or PL, Mean Time to Failure (dangerous) or MTTFd, Diagnostic Coverage or DC, and Common Cause Failures or CCF.

A big problem had been created: North America had the SIMPLE to CONTROL RELIABLE categories, but the U.S. and Canadian definitions were different. Internationally, ISO had PLa-e, and IEC had SILs (Safety Integrity Levels) SIL1-SIL4. All of these standards were applicable to machinery, but there was no clear guidance on how to choose the most appropriate standard.

Since the second Edition of ISO 13849-1 was published in 2006, ANSI has adopted ISO 10218-1 for Industrial Robots, and this standard brings ISO 13849-1 in with it. This may spell the end of the SIMPLE-CONTROL RELIABLE definitions, since the coming adoption of ISO 10218-2 for Industrial Robot Systems will incorporate ISO 13849-1 into the requirements for the safeguarding systems on robot systems in the U.S. It is reasonable to expect that CSA will not be far behind in adopting these same standards.

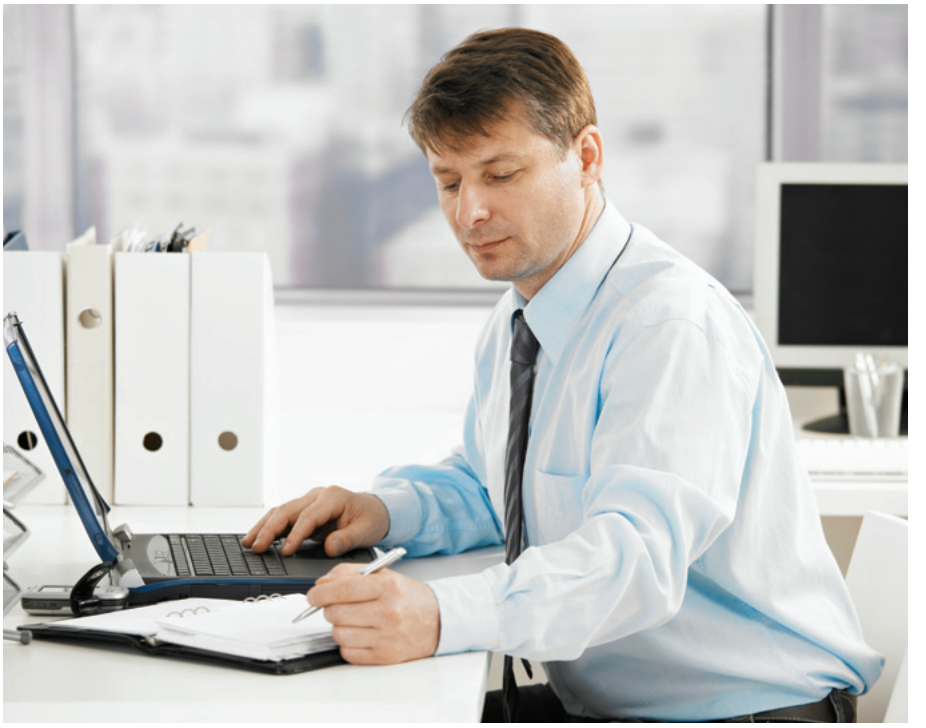
ISO and IEC recognize that a problem exists for users. While ISO 13849-1 has been harmonized for machinery and has replaced EN 954-1, IEC has a competing standard. IEC 62061, which uses SILs, is also harmonized under the machinery directive, but doesn't explicitly include pneumatics and hydraulics while ISO 13849-1 does. You can use the IEC standard to assess the reliability of fluid power systems; it just takes a bit more work. A Joint Working Group was formed under ISO TC199 - Safety of Machinery, called 'JWG1.' The sole task of this group is the merger of ISO 13849-1 and IEC 62061. Although the work started in 2011, publication of the merged document is unlikely to come soon. We may have to wait until 2018 to see the finished product.

Designers need to ensure that they have reduced the risks on their machinery following the hierarchy of controls, and that the safeguarding systems selected are appropriate for the application.

Doug Nix, A.Sc.T., is Managing Director & Principal Consultant, Compliance InSight Consulting Inc.

Making sense of international standards development

BY DOUG NIX



Standards development is one of those activities that seems mysterious to many. The Technical Committees (TC) are made up of people from industry, academia, government, user associations and the general public for standards developed within a country, like the CSA standards we use in Canada. In the international arena, things are a bit different. ISO and IEC TCs are made up of delegations from member countries. The delegates come from the same sources within each country as the national standards TCs, and the work is generally organized by national standards bodies. In Canada's case, this is the Standards Council of Canada. If you are qualified and there is space available, all you need to do is volunteer to participate, and then be ready to contribute by attending meetings, preparing submissions and traveling to meetings.

In September, a meeting of ISO TC199 - Safety of Machinery, Joint Working Group 1 (JWG1) was held in Paris, France. This group is working on merging two important machinery standards: ISO 13849-1 and IEC 62061. If you design machinery that uses electrical or electronic controls as part of the safety system, then one of these standards may apply to your designs. How do you know if you should be using one of these standards? Ask yourself a few questions:

1. Do we use interlocked guards or other safeguarding devices like light curtains, two-hand controls or presence-sensing mats to reduce risks from our designs?
2. Do we use complementary protective measures including emergency stop systems in our designs?
3. Where do we sell our machinery?
4. Do we foresee a time in the next few years where we may want to expand our market internationally?

If you answered 'YES' to either or both of the first two questions, these standards may be used to analyze the reliability of these systems. If you answered, 'just Canada' or 'just North America,' then these standards could be used to replace sections of the CSA or ANSI standards covering control reliability that apply to your machinery, but this is not required.

If you sell outside of North America and the European Union, using ISO and IEC standards for your designs means that your products are much more likely to be ready for foreign markets, with few changes needed to meet local requirements.

If you sell in the European Union, both of these standards are harmonized under the Machinery Directive, so using these standards helps to open the door to a market of 27 countries. If you are selling only in Canada or North America, and you can foresee a time in the near future when you will want to branch out into international markets, supplementing the Canadian and U.S. National Standards with ISO and IEC standards will help get your product ready for these markets.

There is a problem, however, and JWG1 was assembled to deal with it. The two standards, while not in conflict, use different terminology and different methodology to assess control reliability. The results of the analysis are described as 'Performance Levels' or 'PL' by the ISO standard, or as 'Safety Integrity Levels' or 'SIL' by the IEC standard, and this is just the tip of the iceberg. Why are there two standards, and what are the advantages and disadvantages for each? These problems have to be resolved, and JWG1 is making plans to do just that.

Doug Nix, A.Sc.T., is Managing Director & Principal Consultant, Compliance InSight Consulting Inc. Reach him at dnix@complianceinsight.ca.

When can you use interlocks to protect the worker?

BY FRANCO TOMEI

In my experience one of the questions that arises the most is "when is interlocking permissible to protect the worker?"

Ideally, using interlocking to protect the worker would never be acceptable since, as stated in CSA Z460-05, lockout is always the preferred method of protecting a worker, as long as it is practicable. Practicable may mean, for example, that providing a guard completely over a grinder is not practicable, since no grinding would be possible. However it is practicable to allow the wheel to be exposed sufficiently so as to permit the grinding to take place.

Another example would be that it may not be practicable economically to perform a full lockout, as would be the case on a CNC machine. In this case, requiring a worker to perform a full lockout each time a workpiece needs to be unloaded may make the operation so economically unviable that the work would be lost. In such a case, we would need to provide adequate protection to the worker so that the risk is as low as reasonably practical (ALARP). In essence, ALARP involves weighing a risk against the trouble, time and money needed to control the risk. This long-standing issue has been tackled by a technical committee that developed CSA Z460-05 (R2010) Controlling Hazardous Energy – Lockout and Other Methods.

In this standard, the distinction is made between tasks that are integral to the production process and, by implication, tasks that are not integral to the production process. In short, the standard distinguishes that lockout is not always doable in an economic sense and there is a need to use "other methods" to control the hazardous energy.

This "other method" of controlling hazardous energy is, for the purpose of this article, the use of interlocks. However, interlocks can only be used if – and only if – the task to be performed is integral to the production process.

At this juncture it is worth reviewing the regulatory requirements of section 24 and 25, which can be surmised to state that where there is an exposed moving part or nip point that endangers the safety of a worker, the worker must be prevented from gaining access to the exposed moving part and/or nip point. It is to be noted that the emphasis is on the employer to prevent access and not on the worker not to gain access. We can hope and pray all we want that nobody will access the exposed dangerous parts, but at the end of the day, the regulations only require that a person have access to be non-compliant with the regulatory requirement. That is the point of interlocking – that with the interlocking, there are no exposed moving parts, thereby removing the source of the hazard that has the potential to cause harm to the worker.

This reliability of the functioning of the interlock is not in itself absolute, as there is some risk of failure of the interlocking system. But the risk must be reduced to as low as reasonably practicable under the circumstances to protect the safety of the worker.

As referenced earlier, the interlocking should be applied for specific tasks under specific circumstances and, by implication, not all tasks under all circumstances. It is clear therefore that one must be able to assess whether or not a task can be considered as integral to the production process or is part of some other activity.

To be considered integral to the production process, the designed task will exhibit most of the following characteristics:

1. **Duration:** Of course, the question then becomes how short is short? This may depend on the nature of the activity, but one must recognize that if a machine needs to be fiddled with for a disproportionate period of time, that task is not part and parcel of the production process.
2. **Minor in nature:** This is, once again, relative, but one could define minor as meaning that no tools, or perhaps a specific tool only (to keep parts of the body out of hazardous areas) only, are to be used.
3. **Occurrence:** If the task needs to be performed infrequently or sporadically, then the task is required not because of production requirements but because of defects within the machine itself. Clearly the root cause of the required task needs to be addressed and not have a worker subject him or herself to a potentially hazardous event because of the machine deficiency.
4. **Operator skill level:** If the task requires a person with specific skill sets not normally attributable to the operator, then the task itself is distinct from the production task. Clearly, such a task would not be integral to the production process.
5. **Pre-determined cyclical activities:** As an example, we can look at a spot welder, whereby the operator is required to change the welding tip every 5,000 weld cycles. Changing the tip may be considered integral to the production process.
6. **Production interruption:** If the task to be performed requires a lengthy amount of time, then that task cannot be said to be integral to the production process.
7. **Exists all the time:** It sometimes happens that an operator needs to make some adjustment on the machine and that the adjustment is the result of a defect due to a defective or worn part. These things start slowly and the operator tolerates the deficiency. Over time, it is no longer deficiency but becomes part of the "normal" operation of the machine.
8. **Personnel training:** As was noted earlier, these tasks are designed tasks, not tasks merely performed at the whim of the operator. The task must be designed so as to minimize worker exposure in the course of performing a specific task.

The preceding is all fine and well, but please remember that if an incident with consequences occurs, labour officials in your province will need to look at any violation. If an injury has occurred, it becomes difficult to state that access to exposed moving parts or pinch points has been prevented.

Franco Tomei, B.A.Sc. P.Eng, is a professional engineer with more than 40 years of industrial experience — 12 years of that directly in the safety field. He can be reached at ftomei@yahoo.com.

The evolution of functional safety

BY KIAN SANJARI

Over the last few decades, the functional safety of machines and systems has been ensured solely through the use of safety relays. In large-scale systems, this meant long parallel runs of dedicated wires from safety input devices to safety relays and, in turn, to the safety output devices. These functional safety systems were cumbersome to troubleshoot and inflexible in case of expansions or retrofits.

With the growth and availability of safe controllers and networks, two established approaches for implementing safety technology are made possible.

The first involves the use of remote safety controllers that feature their own separately installed safe network. Compared to traditional safety relays, this approach dramatically increases the flexibility of the safety application at the expense of increased costs.

In the second approach, the safe controller is integrated into the standard controller and uses the "existing" network to communicate with the safe devices. In practice, this approach has proven to be the better option in terms of technical and economic efficiency. Since the existing networks and infrastructure can be used, the installation and connection work needed to integrate functional safety into the machine or system is significantly reduced. This approach is therefore ideally suited for distributed applications with a medium to high number of safe I/Os. A special safety controller or safe bus system is no longer necessary.

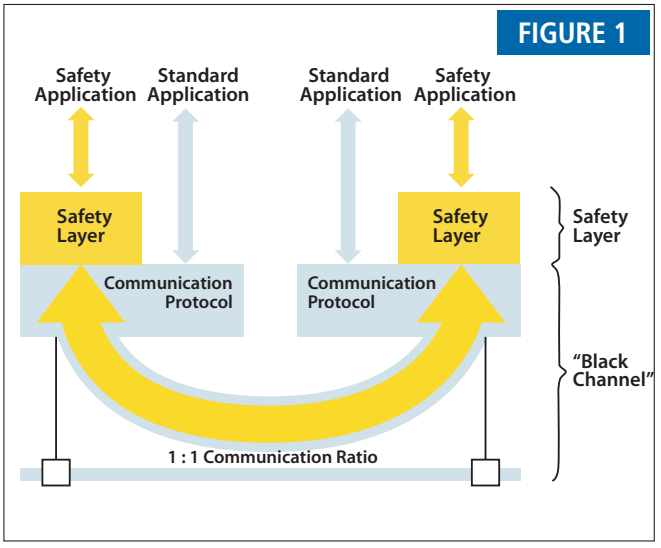
Recently market studies show that less than 50 safe I/Os are built into most of the applications for machine and plant engineering. Based on these findings, the use of a safe controller makes economic sense only in situations where a large number of safe I/O are used in an extensive area. Many users are therefore looking for a solution that combines the flexibility of a safe controller plus the associated safe I/Os distributed in the network and the intuitive operation of the safety relay.

Automation safety without the need for a safety controller

Today, however, a different approach to distributed safety in an automated industrial network is available. New technology makes it possible to eliminate the strong dependencies between the fail-safe PLC and the safety protocol by achieving two conditions:

1. The safe logic must not be an integrated part of central PLC, but rather decentralized and separated from the standard PLC as in the case of a configurable safety relay.
2. The safe logic must communicate via special protocol over an already installed standard network to read safety input signals from distributed sensors and write safety outputs to actuators.

To reach these conditions, a special logic module can act as a standard network device. This logic module is distributed in the network and handles all safety logic processing on-site. Processing this safety data is done via internally redundant processors, much like a configurable safety relay can process its own safety program. Unlike a configurable safety relay, however, the distributed logic module can communicate to its associated safe input and safe output signals via a special protocol on the standard network.



Safety failure detection is only implemented at the end points of communication, which can detect failures within the black channel with a residual failure probability.

This safety protocol does not contain any network or PLC-specific dependencies, but operates on the "black channel" principle, like that of a PROFIsafe system. The entire network, including the standard PLC and all infrastructure components located in the data path of the safety signals, is part of the black channel. Safety failure detection is only implemented at the end points of communication, which can detect failures within the black channel with a residual failure probability for the highest safety levels (i.e. PL e, Cat 4, SIL 3, as seen in the figure above).

Using this communication principle, the safe I/O can be distributed throughout the network, while still communicating back to the same logic module. This creates even more system flexibility. Input and output devices can be wired where they are needed, eliminating the need for long bundled sensor and actuator wire runs throughout the system.

Functional safety should no longer be viewed as a separate issue. Users can gain major competitive advantages by thoroughly integrating it into the automation solution of a machine or plant. Extensive diagnostic options reduce installation costs and downtime and hence increase availability and productivity.

Kian Sanjari, P.Eng., is product marketing manager for I/O & Networking for Phoenix Contact. Reach him at ksanjari@phoenixcontact.ca.