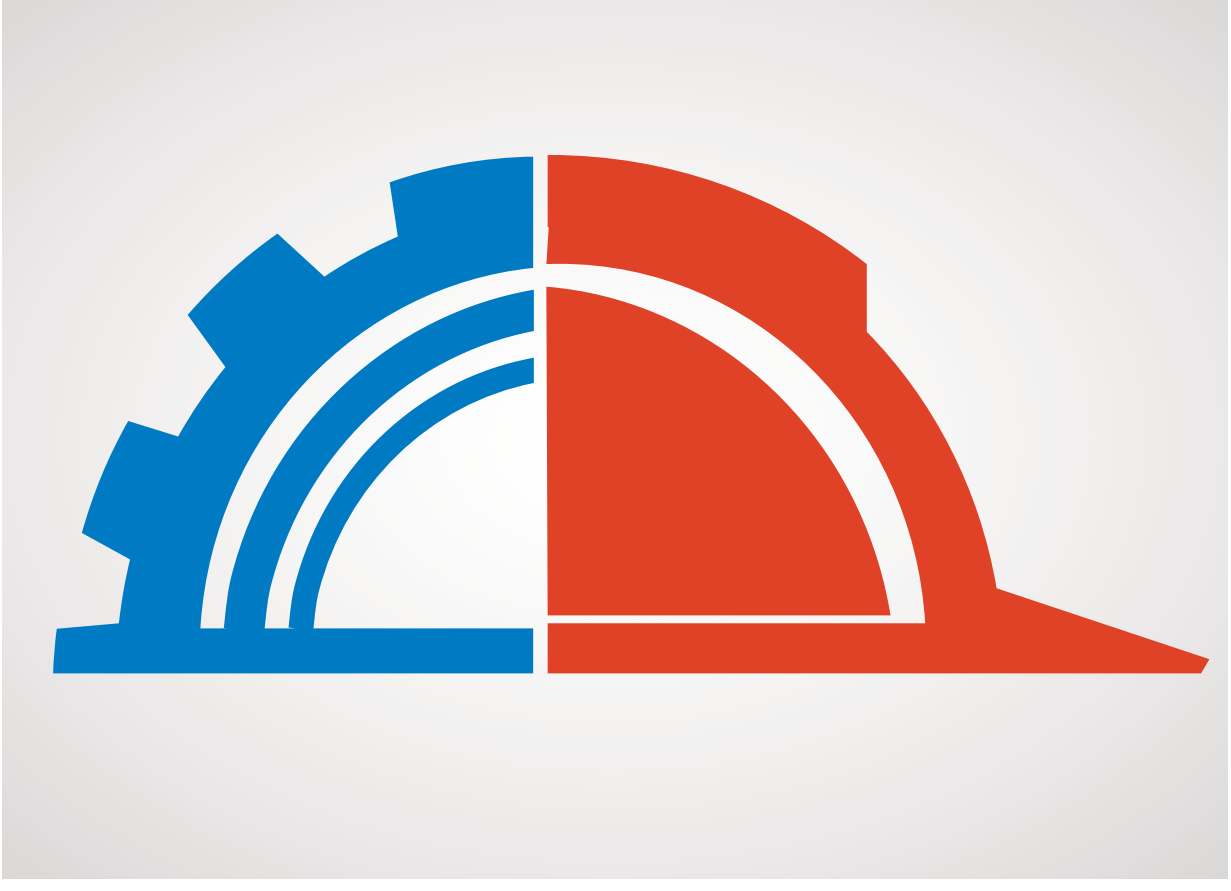
control design

TECHNOLOGY REPORT

Factory Safety in Automation



Sponsored by

rexroth
A Bosch Company

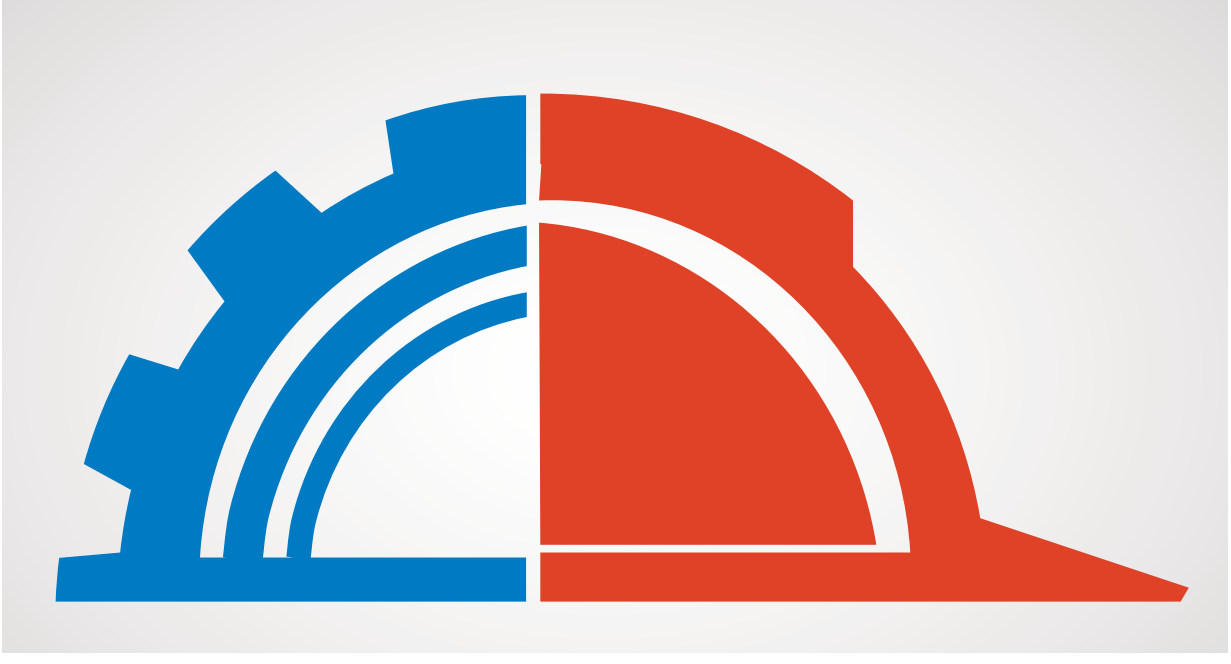
control design

TECHNOLOGY REPORT

CONTENTS

TECHNOLOGY IN ACTION

SPONSOR-SUPPLIED CONTENT



Basic automation safety requires not-so-basic safety

There are very few machines where installing a safety system will not reduce the risk

By Dave Perkon, technical editor

Your machine is going to need a safety system to protect the operator and equipment. How safe does it need to be; what safety sensors are needed; and what do the safety sensors connect to? In the distant past, it was just a start-stop circuit with a master control relay, which isn't very safe. Fortunately, both safety standards and safety hardware have advanced over the years.

Automation safety basics are not so basic today. Emergency stops, guard switches and light curtains are common safety sensors that connect to safety relays, safety controllers or safety PLCs. Many control designers are familiar with safety-sensor use but are not aware of, or do not understand, global safety standards.

A common disclaimer of any safety discussion is that you, the designer, are responsible for safety. You must comply with performance and safety requirements. There are many standards, codes and laws to follow, so, to be safe, get trained first. You will better understand a risk assessment and the design, hardware, software and testing requirements for a safety system.

Safety standards are learned and followed. Get with your automation manufacturers and vendors and get trained on safety standards. For example, according to ISO 13850, IEC 60204-1, IEC 60947-5-5 and probably NFPA 79, buttons used as actuators of an emergency-stop device shall be colored red. No big deal, but, a typical emergency-stop circuit must comply with many standards. The emergency-stop button must comply with these previous standards, the emergency stop control may need to conform to Stop Category 0 of IEC 60204-1, the safety relay may need to provide Cat. 3 PLd per IS013849-1, SIL CL2 per IEC 62061, or SIL 2 per IEC 61508 (they are all basically the same), and it must use force guided relays that conform to EN50205 and IEC 60947-5-1. It's a lot to sort out.

In addition to a need for training, the emergency-stop circuit example should make it clear that every safety sensor must be carefully designed into an overall safety system. Each sensor and circuit has its own safety requirements and safety rating. So, get trained, read some of the standards noted above and look up how to perform a risk assessment (ANSI B11.0, ANSI B11.19 and others) to determine the safety level required before continuing here. Manufacturers, vendors and standards organizations have it well-documented online.

Hardware at the heart of a safety circuit includes safety relays, safety controllers and safety PLCs. Which device used depends on an application because it is not one size fits all. On small, simple machines, safety relays are often a more cost-effective solution. A machine with a few emergency stops, a few guard door switches and a light curtain may work with a couple single-function safety relays. One safety relay would handle a power-off function, for the whole machine, based on the state of the emergency stops and the guard switches. The other safety relay would handle the light curtain zone stop function for when an operator reaches into a machine to load and unload a part, for example.

Again, the safety relay should be used for a single function, and, with the new safety standards, connecting multiple sensors in

series, daisy-chaining them, can reduce the safety level. With multiple sensors, consider using modular safety relays or configurable safety relays. They can increase the safety level and will work in this example and where multiple safety circuits and zones are required.

On larger machines with many safety sensors and where complex logic using distributed safety I/O, interlocks to other controllers and multiple zones are needed, a safety controller should be used. These software-programmable safety controllers are a cost-effective choice to add safety logic, making them flexible and scalable. A suitable application would be for a packaging line with many guard-door sensors and multiple zones including manual load, material change, heat seal, slitter and final pack out areas. The safety controller may also work well retrofitted onto an existing piece of equipment where additional functions and safety are needed.

A safety PLC works on many applications. However, it works best on large complex systems. Advanced multi-station assembly, process and conversion lines are a good fit due to their flexibility and connectivity. Regardless of what safety platform is chosen, it has little effect on the safety field devices. Whether safety relay, controller or PLC, the risk assessment, safety functions, testing and evaluation remains the same.

On the other side of a safety platform chosen, opposite safety sensors are power contactors. These contactors are needed when the contacts in the safety device cannot handle the load being controlled. Use of force-guided contactors, per EN50205, is common if the load is inductive or in excess of 6 A, but be sure to check the safety device's rating. Also, be aware that, in some cases, energizing the contactor may exceed the inrush current limits of the safety device. For example, a contactor capable of operating three-phase, 230 Vac, 15-hp motor or larger may weld the safety contacts closed.

Considering the Industrial Internet of Things and improving status and diagnostics capabilities, it is good practice to monitor the safety device's status. This can be done with discrete inputs to a controller, but the use of an Ethernet fieldbus is becoming common. Depending on hardware used, standard devices and safety devices can be mixed on the same network cable. Safety protocols can provide fail-safe network communication up to Safety Integrity Level (SIL) 3 based on IEC 61508 standards. Safety PLCs, light curtains, safety interlock switches and I/O blocks can safely shut down a machine through an Ethernet cable. ◻

Dave Perkon is technical editor for Control Design. He has engineered and managed automation projects for Fortune 500 companies in the medical, automotive, semiconductor, defense and solar industries.

On the other side of a safety platform chosen, opposite safety sensors are power contactors.

Intrinsic safety comes with requirements

How to design a control circuit for use while keeping barriers in mind

By Dave Perkon, technical editor

Once an areas is classified as hazardous with a potentially explosive atmosphere, many steps must be taken to eliminate ignition sources. When looking at a fire triangle with oxygen, fuel and source of ignition, two of the three are often present in these areas. It's the designer's responsibility to eliminate all sources of ignition, and that includes limiting both electrical and thermal energy to a level below what could ignite the hazards present. Depending on the area classification, even the tools used for installation must not cause sparks and are therefore made with aluminum or similar material.

Intrinsic safety (IS) barriers are devices designed to limit the current and voltage that can cause sparks in a device's power and signal conductors.

When IS barriers are used in hazardous locations, some of the basics that must be considered beyond area classification are methods to eliminate hazards; certification of device or apparatus; and design and wiring methods.

It is important to point out that installing a control system in a hazardous area is not a one-man show. The facility is required by law to properly classify any area that may contain an explosive atmosphere. The control-system designer must check with plant engineering, operations or safety personnel and determine the area classification. A facility that appears to be nonhazardous may have several hazardous areas, including explosive fumes or powders, so always check.

When specifying IS barriers or any hazardous area control system components, work closely with the vendors and manufacturers. They are great sources of information and should be leveraged, along with training, if you are new to designing control systems for use in hazardous areas. Even if you are an expert, the standards and requirements change. Take a close look at your standard intrinsic safety system design, and, with a critical eye, check the components to ensure they are suitable for use in the hazardous area.

There are many applications where a spark, heat or small explosion ignites an explosive, such as a gas grill spark igniter, a hot bridge wire setting off an exothermic chemical reaction (gas generation) in an airbag initiator and a primer in a cartridge initiating propellant combustion.

On the other hand, IS devices do just the opposite. An IS barrier limits the sparks and heat in electrical devices that can cause explosions, under normal or abnormal conditions, to a level incapable of causing ignition of a hazardous atmosphere. They work well protecting low-power devices such as instruments, sensors, LEDs and solenoids.

Other protection from explosion methods includes explosion-proof equipment or enclosures and purging or pressurization of the device or enclosure. These methods are often used in combination with IS barriers as the barriers are not suitable for all applications. For example, an IS barrier typically limits voltage and current, but safe energy levels vary depending on the area classification. In some areas, such as with hydrogen gas, a circuit

with about 24 V and 150 mA may provide enough energy to create a spark large enough to ignite the mixture of gas and oxygen.

The National Electric Code Article 504 discusses intrinsic safety. Not only must the IS barrier be certified for use per the hazardous location class and division, it must be certified by a local, third-party agency such as UL and the Canadian Standards Association (CSA Group). The IS barrier must meet requirements and standards based on the geographical location of the plant. Equipment installed in Europe often must have certifications for the specific country.

Zener diode barriers are one way to implement intrinsic safety. This barrier type is connected to a safety earth ground which can cause electrical noise that may cause problems, especially with analog circuits. Isolated IS barriers are also available and provide galvanic isolation, which eliminates the dedicated safety ground. These galvanic barriers typically require a separate power supply, but only one is needed to power all barriers.

Zener barriers are a simple cost-effective method to connect discrete sensors and solenoids. The isolation provided by galvanic barriers work well with transmitters, thermocouples and other analog circuits.

The field devices connected to intrinsic safety barriers must be FM approved for that use along with the class, division or zone, group and temperature ratings of the area or must be a simple device or apparatus that does not store or generate more than 1.5 V, 0.1 A or 25 mW such as simple switches, sensors, LEDs or thermocouples.

The installation and wiring of IS barriers must carefully match the design drawings. A standard industrial enclosure can be used with intrinsic safety devices and apparatuses, and it does not need to be sealed. However, a conduit seal must be used between hazardous and nonhazardous enclosures to isolate the hazardous atmosphere from the safe area.

The same wiring methods can be used for intrinsically safe and non-intrinsically safe conductors, but they must be kept physically separate using 2-inch air space, conduit or partition. The IS wiring must also be clearly labeled to not confuse it with safe area wiring, and light-blue wire is often used for IS circuits to highlight its purpose.

There are many requirements for application of intrinsic safety barriers. Be sure to understand the hazards and how to eliminate along with certifications, design and wiring requirements. There are many beyond the few basics noted here. ◻

Dave Perkon is technical editor for Control Design. He has engineered and managed automation projects for Fortune 500 companies in the medical, automotive, semiconductor, defense and solar industries.

Take a close look at your standard intrinsic safety system design, and, with a critical eye, check the components to ensure they are suitable for use in the hazardous area.

How to plan a safety upgrade

Consider design, integration, testing and operation

By Mike Bacidore, editor in chief

A Control Design reader writes: I work at a packaging plant where safety upgrades to palletizing equipment excessively stopped the machine and confused multiple technicians, ultimately leading to some of the safety measures being bypassed, which resulted in an operator injury. This is unacceptable and a review of the plant found many safety concerns that must be fixed.

The plan is to upgrade several bottling lines, fillers, palletizers and wrappers to a standardized safety platform, likely safety controllers, and then carefully train all personnel on the safety system and procedures. The systems involved are various and have a wide range of safety devices to integrate. Can you suggest how to plan this out, design, integrate, test and operate the system? Quick installation, integration, configuration and testing are required. Can you help with this safety upgrade?

ANSWERS

ASSESS THE RISK FIRST

This is a tough one. There is so much we can do with a clean sheet of paper that you can't do with existing hardwired safety, and you can't do without a controls retrofit, which is typically not cost-effective. This user would be well-advised to attend a PMMI risk assessment workshop and work with their current machinery and controls supplier to achieve the safety levels prescribed by the risk assessment.

John Kowal
director, business development / B&R Industrial Automation / www.br-automation.com

7 STEPS TO SAFETY

A plan for safety is a good thing. The first step of the plan is to have a risk assessment done by a trained and certified safety engineer or risk assessor. This safety engineer or assessor many times can come from the company's general liability insurance carrier. If the insurance company does not offer this service, then there are many companies that offer this service. There are "independent" organizations such as TUV and UL, or there are the manufacturers of the safety devices. They will assess each operating system—be it a simple machine to a complex system such as a palletizing line—and determine the level of protection that is required to meet the local and national requirements.

Once the assessment is complete, the level of protection will dictate the type of safety system that will be used—safety relays/controllers/PLCs in conjunction with e-stops/interlocks/area scanners. In fact, the large manufacturers and their distributors will provide a recommended list of components to be used and, in most cases, assist with integrating and training. However, you and your company are the only ones that know how you use the equipment, and you are the ones responsible for successfully implementing a safety program within your facility. The safety device providers, their distributors and their integrators can only provide so much.

In a numbered list form here are my suggested steps:

1. Perform a risk assessment of each individual machine and complex system (multiple machines). Use existing records of injuries to determine the cause.
2. Using the results of the risk assessment, determine the level of safety required for each machine and complex system. The level of safety is determined by assessed risk (severity) and probability of injury. The solution will be based on local and national requirements.

3. Work with a qualified, reputable distributor that has a wide product breadth to meet the needs of the safety level.
4. Obtain all of the electrical schematics of each machine, whether on its own or within a complex system. This will allow you to determine if and how you will integrate the necessary safety devices. Contact the manufacturer of the machines. They may have made upgrades to their offerings that you may retrofit into the existing equipment.
5. For complex systems, develop a safety schematic to show how all of the safety devices interact with the system. This should include the "brains," as well as all of the interlocking devices.
6. If you don't have a safety-trained electrician in-house, hire an integration company. This will be an additional cost, but they will guarantee their work and could assist with the above steps.
7. Even though this is listed last, it should by no means happen last. Develop the training module. It should include all of the information gathered and developed along the way. It will be specific to your needs, and you can add it to your training matrix, if you keep training records.

Pat Klingberg
general manager / Global Controls / www.global-controls.us

INDEPENDENT SYSTEMS

We have worked in this industry for three decades and have seen how safety has evolved.

Current practice for most OEMs is to provide relatively simple e-stop safety systems incorporating safety relays and switches that are safety-rated double-contact type, as well as safety-rated output devices. In contrast to traditional e-stop safety systems, these types of e-stop systems are inherently safe and prevent an operator from easily bypassing.

This type of hardware is standard issue and readily available off-the-shelf from Allen-Bradley and others. It will not break the bank and can typically be installed in a few weeks, provided complete prints of the existing systems are available to be used for designing the new e-stop systems.

While it is possible to use PLCs with integrated safety, such as Allen-Bradley GuardLogix, we have not seen this approach used in this industry. This is largely because each of the systems you mentioned—bottling, filling, palletizing—is independent and each has its own safety system. You have to have one system with quite a few safety I/O to make the safety-controller route look economically attractive.

Stan Prutz, P. E.
systems engineering manager / QDS Systems / www.qdssystems.com / Control System Integrators Association (www.controlsys.org) member

PHASED PROJECT MANAGEMENT

Polytron's approach for any machine-safety remediation effort follows the same phased project management approach we use for capital projects. First, we utilize our TUV-certified machine-safety experts to develop a machine-safety risk assessment to identify all of the machine hazards associated with the operation and maintenance of the machine. If the owner has already obtained a machine-safety hazard assessment from the OEM or another entity, we'd review it and address any missing details. Then, we'd work with the owner's operations, maintenance and EHS resources to define the necessary safety category and performance level for each piece of equipment assessed. We'd identify the gaps between the current machine design and the target safety category/performance level and work with the owner to define acceptable mitigation designs. In this phase, it's really important to evaluate the proposed mitigation design against the machine's current OEE to determine the impact. In many cases, an alternative machine safety design approach can limit or eliminate any negative effect on the equipment's overall equipment effectiveness (OEE) . And, in all cases, personnel training and standard-operating-procedure (SOP) development should be

considered, based upon the level of change required by the safety mitigation design.

Once the proposed safety mitigation design has been reviewed and the machine hazards reduced to an acceptable risk level, the next step in our process is to develop a safety functional design specification (SFDS) that would detail the scope of the mechanical and electrical modifications required for each machine. This document would detail the bill of material, preliminary fabrication and/or installation drawings and a functional description of the safety mitigation changes. The SFDS is then utilized to generate equipment fabrication and installation costs and timelines. Most importantly, the SFDS is the basis for developing the safety validation plan that is the documentation utilized to validate the safety mitigation changes have been installed and verified upon the completion of the effort.

Once all of the equipment has been assessed and the execution cost and timelines have been identified, the execution phase of the safety mitigation project is managed like any other project. Equipment downtime is requested and coordinated for the installation, startup and validation of the mitigation changes on each piece of equipment. Strong project management acumen is required to coordinate the schedule of the safety mitigation execution efforts and the available operational downtime.

Damian Stahl
vice president / Polytron / www.polytron.com / Control System Integrators Association (www.controlsys.org) member

CLOSE THE SAFETY GAPS

The situations you describe are not unique to Optimation Technology and have been addressed during design-build and upgrades for our clients. When equipment and facilities are barriers to safe work, the flow of business can be impeded. Optimation uses a multifaceted approach to these types of concerns. Approaches include but are not limited to assessing hazard recognition, equipment functionality, operator interface, maintainability and desired production throughput. Assessing the following and closing any gaps discovered will be critical.

Hazard recognition: Determining the inherent risk factors for the entire process. Ensure machine and worker safe guards are adequate, compliant and not overkilling production and throughput.

Equipment functionality: Evaluate if the machine will operate as desired. Over- or under-engineered equipment can inhibit functionality.

Operator interface: Discover all the tasks and activities the operators will be involved in while operating the equipment. Knowledge of the what, where and how operators interface allows for effective and efficient design the first time.

Maintainability: Ensure maintenance personnel have ready access to all necessary pieces of equipment appropriate for the work. Knowledge of the what, where and how maintenance mechanics interface allows for effective and efficient design the first time.

Desired production throughput: Determine and deliver the appropriate quantity of product on time and at the highest level of quality. Without addressing the items listed above, desired production throughput will be extremely difficult if not impossible to attain.

Optimation's multifaceted approach to these situations can improve not only the safety functionality of an equipment process. But the cost, schedule, quality and worker satisfaction also will be byproducts of the enhancements.

Al Manzer
corporate safety engineering manager / Optimation / www.optimation.us / Control System Integrators Association (www.controlsys.org) member

STANDARDS-BASED APPROACH

This unfortunate scenario seems to play out repeatedly. In most cases, the root cause is failure to consider how people interact with the machine when selecting safeguarding. This is why we see some organiza-

tions dragged kicking and screaming into safeguarding projects. The belief is that safety upgrades will result in lower productivity, which often happens when using the wrong safeguarding approach.

The goal is to proactively engineer a safety system that complements the tasks operators and maintenance technicians need to perform on machinery and allows them to perform those tasks quickly and safely. To start, follow the functional safety lifecycle and consider modularization and reuse. If you have more than one copy of each machine, begin with the most complex example and then use the assessment, specification and design as a template for the others. You still need to look at each machine individually, but make it easy on yourself by reusing what you have already done.

The first step in the lifecycle is a good risk assessment. Hazard identification should be completed by looking at the tasks people are performing on the machine and the hazards they are exposed to while performing those tasks. This must be a team exercise. The input and buy-in of the people who are bypassing the current safeguards are very important. Anywhere you discover an unacceptable risk, consider the full range of safeguards. This includes many options: designing the hazard out; using fixed guarding, interlocking guards and/or presence sensing devices; building awareness; implementing training and procedures;, and using personal protective equipment (PPE). When you examine all of the possibilities, you will likely end up with several options that will help to keep people safe. You are then free to choose the best options based on their effect on productivity. If you are unfamiliar with this process, get help.

Now, you'll have a design concept that should either minimally affect productivity or improve it. Additionally, you should have buy-in from the people who will be working on the machine. At this point, you can focus on the things that we traditionally associate with a safety-system implementation, such as specification, safety-circuit design and safety-software development. Each one of these pieces of the project should be used as a template for other machines of the same type. This applies to the end of the process, as well. Perform a good validation, and use the validation plan as a template. The time and cost requirements for other machines should go down with each iteration.

Overall, it is important to remember that this process is not focused on safety components or technology. Rather, it is a standards-based approach to designing a safety system that makes all human-machine interactions more efficient, safer and in compliance with requirements.

Pat Barry
safety regional manager /
Rockwell Automation /
www.rockwellautomation.com

SAFE AND PRODUCTIVE

We are sorry to hear that there was an operator injury, and we hope everyone is well.

For this opportunity at the packaging plant we would like to offer a solution to make the operations at the packaging plant safe and increase work ergonomics and productivity. The following plan will expedite the implementation of the required safety functions.

Risk assessment: To implement safety on a machine, first a risk assessment must be done to identify the risks of the machine and the process.

Identification of required safety functions: After the risk assessment is complete, the required safety functions have to be identified. What are the conditions that put a machine in safety state? For example, if Door A is opened, what happens to the machine? All of these scenarios must be documented.

Identification of safety equipment: Next, the proper equipment must be selected to accomplish the safety functions. The following questions have to be answered. Will it be drive-based safety or will a safety PLC be used? Will it be a

combination of drive-based safety with a safety PLC? Is the safety PLC going to have remote safety I/O of local safety I/O? Will safety equipment be installed, or will older equipment be replaced with new safety equipment?

Testing: Once the equipment has been selected, it must be tested and validated to ensure it performs as expected.

Training: Training can be done after this last step. The machines perform as expected, and this information must be shared with the operators. Operators must understand the conditions that put the machine in safety state and how to use it for their safety and to reduce downtime.

The above plan will ensure a fast and efficient implementation of machine safety to increase protection of the operators and machines.

Joaquin Ocampo
product manager / Bosch Rexroth / www.boschrexroth-us.com

SAFE OPERATION IS NOT A GIVEN

What your company needs is an overall safety plan. Adding guarding to a machine is not enough, and in some cases guarding alone may never be able to stop a determined operator. On the other hand, an operator should never feel compelled to bypass safety controls to continue production. Regarding safety, the roles of operators, maintenance/engineering and management should be clearly defined by the safety plan. What that means in reference to your situation is that both the production manager and the operator should be trained to stop production and contact maintenance if there is an issue with the guarding causing excessive stopping on the equipment.

To implement a safety plan, it is best practice to follow accepted and up-to-date industry standards. We will restrict the discussion to safety of machinery and functional safety since your interest is to integrate a PLC-based safety system. In the United States, please refer to the ANSI B.11 standards; however, there are also many EN/ISO (European standards) that apply.

To design the system properly, you will want to perform a risk assessment, for which EN ISO 12100:2010 is generally used. The risk assessment will help you to get a baseline idea of where, how severe and how frequent your hazards are present. Because you are integrating a system with existing machines, the machine manufacturers may already have some of this information available to you in their user manuals.

Once you understand these hazards, you will want to perform risk reduction analysis. This involves examining each hazard to come up with a mix of physical guarding, safety controls and personnel training to eliminate or reduce this risk to an acceptable, residual level. Remember, this is an iterative process, so it may take a few passes.

Finally, make sure you are paying attention to standards specific to your machines. The high-level standards will help to lay out the architecture and performance level of your safety functions, but the lower-level standards contain specific requirements that vary from machine to machine.

At this point, you should have a system designed that includes physical guarding, electronic safety functions and other measures of risk reduction, including signage and training for all employees. Each safety function has been assigned a performance level, as well as a reaction time, a known safe state and a restart acknowledgement procedure; your test cases are now done. These test cases should be carried out when commissioning the system, as well as periodically, according to your calculated proof test interval for each safety function.

Integration of the safety functions with safety PLCs allows you to build diagnostics into your functional safety system, and these diagnostics can then be used to troubleshoot issues that come up with the safety system, as well as perform continuous improvement efforts within the system.

If a door guard switch is false tripping periodically, it may be

appropriate to add some debounce time and still fulfill the requirements of the safety function; otherwise, it may be necessary to move to a different guarding technology that is more immune to the disturbance. Remember that you always have the performance level and proof test requirements from your design phase to guide you on what is safe and what is not.

Remote safety I/O should also be able to provide diagnostics.

Operating the system in a safe manner is not a given unless everyone in the organization buys into the safety plan and plays their roles. Safety training and continuous improvement is always the most important step to operating a safe work environment.

Kyle Hall
product engineer—fieldbus technology / Turck / www.turck.com

EFFICIENCY IMPROVEMENT

Challenges like outdated safety components are hidden opportunities to improve overall plant efficiency. AS-Interface Safety at Work is the obvious choice to overhaul your safety systems. This PLC-independent technology allows safety devices such as door switches, e-stops and light curtains to coexist on standard AS-Interface networks. So your safety systems—and, in turn, your entire plant—can benefit from the advantages of AS-Interface: easier installation with piercing technology, drastically reduced cabling, flexible network topologies, and extensive diagnostics. Furthermore, AS-Interface Safety at Work systems satisfy the most stringent safety requirements of PL e/SIL 3. And don't overlook integrating Safe Link, which gives you the ability to link multiple AS-Interface gateways and safety monitors via standard Ethernet—Profinet, EtherNet/IP and Modbus/TCP. AS-Interface Safety at Work provides flexibility and increased uptime and, most importantly, ensures staff and equipment are operating in a safe environment.

Danius Silgalis
product manager / Pepperl+Fuchs / www.pepperl-fuchs.us

FUNCTIONAL SAFETY

The first step in implementing any safety plan is to confirm the appropriate standard. In the case of machine automation, the predominant standard would be ISO 13849-1 / ISO 13849-2. The first part is the general principles for design; the second part is validation. Before the design process of the safety system can take place, another process— the risk assessment—must be carried out. This is represented by another standard, ISO 14121, and is very important to determine the hazards that are present in the existing machinery—bottling lines, fillers, palletizers. This necessary function is typically carried out by the machine builder or the people most intimate with the machine and its functions or by a third party certified in the safety of machinery. Quite often the end user or the purchaser of the machinery will get involved, since they are the ones who will operate the machine day to day.

Once the risks have been identified, the design process can begin. Another standard, ISO 12100, can be used. This standard identifies the basic concepts and general principles for design, identifying the necessary steps for risk reduction. The design of the safety-related parts of the control system (SRP/CS) may require iterative steps to determine the appropriate safety function and the necessary SRP/CS to satisfy the safety function. For instance, it may be determined that simple gating can be used in particular areas of a machine to comply with appropriate safety standards, such as EN ISO 13857, to effectively mitigate the hazard inside the gating. If, however, it is required for a person to enter and exit a work area during the operation of the machine, other SRP/CS must be used to mitigate the hazard. This may require reiterative steps in the control design process.

Before any build or integration of the SRP/CS can take place,

the decided-upon solutions must be validated to determine if they will achieve the required level of safety determined in the risk assessment/evaluation. This requires the designers of the safety system to calculate the performance level (PL) using such information as the component reliability data (MTTFd, B10d), common cause failures (CCFs) and diagnostic coverage (DC). The performance level is the "discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions." Once calculated, the PL, along with the category, determines if the designed system can achieve the level of safety identified in the previously mentioned risk assessment/evaluation.

After the build and integration have been completed, the operating and testing (validation) of the safety system (SRP/CS) need to take place. ISO 13849-2 identifies the steps necessary to validate the safety process, including validation by analysis and validation by testing. The validation and testing also includes the determined safety function: the function of the machine whose failure can result in an immediate increase of the risks. To clarify, the safety function is the "safety state" that is initiated when a person breaches a safety input device, such as a safety light curtain or safety area scanner. The complete evaluation of all hardware and software SRP/CS need to be validated.

The efficiency of integration, installation, configuration and testing depends on:

- utilization of existing components
- delivery times of new SRP/CS
- validation and testing requirements
- category and PL required
- knowledge base of staff.

If this type of upgrade to a safety system has never been done prior, it is recommended that a third party who is certified, such as a functional safety expert (FSE) or certified functional safety expert (CFSE), handle the project. They will be able to identify the hazards, what should be done and who can be used for SRP/CS. It is also possible to check in with your current controls supplier; most of them have an existing functional safety program and can provide complete service from beginning to end.

As a supplier of SRP/CS, we would be able to work with the third party and supply necessary pneumatic components/systems that would satisfy the required safety level.

If a specific safety standard will not be followed, the process outlined is still relevant and suggested.

Jeff Welker
project manager / Emerson Automation Solutions / www.emerson.com/en-us/automation-solutions

UNITED STATES AND ABROAD

Your objective is to reduce risks to a value lower than acceptable risk. This is typically achieved by:

- good machine design
- safety-related systems and procedures
- external risk reduction devices.

A well-designed system reduces the risk to an acceptable level. It does not make a machine completely safe.

These are the most common reference materials and standards used. Have these standards on-site and use them as references.

OSHA—Occupational Safety and Health Act of 1970: Mandatory and legally binding in the United States. It assures "safe and healthful working conditions," and the focus is on work-related safety.

OSHA 1910 focuses on machine safety. Lock-out-tag-out is biggest impact. It recommends robots comply with ANSI/RIA R15.06.

ANSI—American National Standards Institute (founding member of ISO): B11 technical reports provide guidelines and tools for risk assessment, risk reduction and safeguarding. ANSI does not develop standards. It acts as a facilitator in establishing voluntary consensus standards with various groups.

NFPA—National Fire Protection Agency: Covers all industrial machinery. NFPA 79 is the electrical standard for industrial machinery. E-stops and stop categories are the biggest impact.

RIA—Robotic Industries Association, recommended by OSHA: Several sections focus on safeguarding. A key thing to remember is that OSHA has incorporated ANSI and NFPA standards into its own, and OSHA1910.6 states: "Organizations which are not agencies of the U.S. government which are incorporated by reference in this part, have the same force and effect as other standards in this part."

Key U.S. machine safety rules include due diligence. Due diligence in assessing and removing hazards is required to be performed by machine builders and machine users. At a minimum, this means compliance with OSHA standards.

Proving in a court of law that you did your due diligence requires documented evidence that a risk assessment has been performed and corrective actions taken when needed.

The document must demonstrate that all hazards have been addressed and removed using "state of the art" equipment, which is interpreted as compliance with globally accepted machine safety standards.

Your core proof is the "requirement" to perform and document the "risk assessment and hazard abatement means," per IEC-62046 safety of machines.

To help you, Sistema Performance level (PL) software packets are available to document the risk assessment phase.

Before we start designing our safety circuit, let's review some key U.S. rules.

Who is responsible? OSHA states, the user (employer) is responsible for ensuring the safeguarding equipment is installed and maintained correctly and that the various personnel are trained in the operation and maintenance of the safeguarding. U.S. rules focus on the safety of employees.

In Europe, the European Machinery Directive requires machine builders, not the employer, to make safe machines. It requires TUV certification for all components used in machine safety circuits.

Another key difference is that OSHA is legally binding in the United States, while the European Machinery Directive is a harmonized standard that has no legal ability to enforce the rules. Any legal action to enforce is the sole responsibility of each member state.

Who is responsible is a main difference between U.S. and European rules. If you only use machine safety hardware that has TUV certification, the devices have documented proof that they conform to internationally accepted machine safety standards. While they are like U.S. standards, the TUV rules tend to be better defined and have implementation plans that are easier to understand and execute.

TUV-certified machine safety hardware is the highest, well-defined, globally accepted standard you can use. Hardware that has this certification enables faster implementation and shows a great "due diligence" approach to selecting your machine safety hardware. This can help to protect your organization from frivolous lawsuits and excessive penalties.

Another advantage, the risk assessment on TUV-certified components is already done and well documented when it arrives at your plant. This can be a big-time saver.

ANSI B11.19 defines a user as:

- an entity that utilizes machines, systems and related equipment
- an individual, corporation, partnership or other legal entity or form of business that employs individuals to operate and maintain manufacturing systems/cells.

ANSI B11.19 states the user's responsibilities:

- The user shall be responsible for ensuring that safeguarding is provided, integrated, installed, maintained and used in accordance with the requirements of this standard.

The user shall be responsible for ensuring that supervisors, operators, maintenance and service personnel are trained in the proper installation, adjustment, operation and maintenance of the safeguarding, within the scope of their work activity.

Have a solid, well-documented trail for all training. OSHA and ANSI have also defined an "authorized (qualified) person" to perform tasks and that the authority is given by the employer to this person. This person has also received training on the hazards involved in the tasks they are to perform.

In another area, OSHA 1910.211 Definitions—Safety System (d)(60) (d)(62) "Safety system" means the integrated total system, including the pertinent elements of the press, the controls, the safeguarding and any required supplemental safeguarding, and their interfaces with the operator, and the environment, designed, constructed and arranged to operate together as a unit, such that a single failure or single operating error will not cause injury to personnel due to point of operation hazards.

This implies redundant electric circuits for high-risk machine-safety hazardous areas. OSHA 1910.211 Definitions—Authorized Person (d)(63) "Authorized person" means one to whom the authority and responsibility to perform a specific assignment has been given by the employer.

The NFPA 79 definition of a qualified person is one who has skills and knowledge related to the construction and operation of the electrical equipment and installations and has received safety training on the hazards involved. Do you have documented proof to back this up?

Many standards require conformance to NFPA 79 for electrical equipment. Two such standards are ANSI B11.19 and ANSI B11.20. NFPA 79 defines emergency-stop devices and stop categories.

Control reliability is very similar to the intent of Category 3 and 4 as defined in European Harmonized Standard EN/ISO 13849-1. In all cases, if a single component fails, it shall not prevent the normal stopping action of the machine, and it does prevent the machine from restarting.

It stands to reason that, if a single component fails, there must be a similar component available to complete the stopping action, and that there must be some type of checking circuit to acknowledge that single component failure and prevent a restart of the machine. This would suggest some type of redundancy of the various components and some type of additional self-checking circuitry would be required in order for a circuit is to be reliably controlled.

I really don't like using suggestions and guidance as advice to build a system. There are too many gray areas that can come back to bite you. TUV certification has a major advantage in this area. TUV tends to use performance specifications with well-defined limits that make it easier to build a solid, reliable system. TUV certification also requires the hardware manufacturer to make a safe system and that it be well-documented. This can save a bunch of time during the documentation phase of the project.

The control system shall be constructed so that a failure within the system does not prevent the normal stopping action from being applied to the press when required, but does prevent initiation of a successive stroke until the failure is corrected. The failure shall be detectable by a simple test or indicated by the control system. This requirement does not apply to those elements of the control system that have no effect on the protection against point-of-operation injuries.

ANSI B11.19 and ANSI/RIA 15.06 both provide a definition of control reliability as:

The control system shall be designed, constructed and installed such that a single control component failure within the system does not prevent stopping action from taking place but will prevent successive system cycles until the failure has been corrected.

The first step is putting together a team of experienced people to identify the hazards. This team should be made up of line people, production, safety, quality engineering and other people that have extensive knowledge of the machine and how it is used and operated throughout the day.

Hazards must be identified before the machine safety hardware architecture can be designed.

The team's job will be to identify hazards.

The first corrective action used is good machine design. Ask yourself what can you change in the existing design to make it safer? Are all safety gates, panels and guards in place? Can more be added?

Next, try to improve safety-related systems and procedures used in the facility. Some common questions to ask: Have operators been trained on the hazards, and do they know how to operate the machine in a safe way? What procedures are in place to keep unskilled people from operating a dangerous machine?

If the above steps do not drive the risk down to an acceptable level, then machine safety monitoring equipment will need to be added to the equipment. The first step is risk assessment.

After a dangerous area is defined, you need to build a solution. A machine safety monitoring system requires the following three basic building blocks:

- acquiring information
- monitoring and processing
- stopping the machine.

Sensors are needed to acquire information on the machines state. Is the door open or closed? This information on the state of the machine is fed back to the machine safety monitoring device.

Machine safety-rated monitoring hardware and processing software then process the sensor data. It has two primary functions.

1. The first is to detect when the machine is in an unsafe condition. When this condition is detected, it sends a shutoff signal to the power circuit that is creating the dangerous energy in the system.
2. Another critical function of the safety relay, PLC or controller is to do automatic, continuous self-checks. This is required by most standards.

Also, use machine-safety relays that are designed with universal inputs. These devices are very flexible and can handle a wide range of machine safety sensors such as mechanical door interlocks, e-stops, e-stop cable pulls and light curtains. Universal-input machine safety relays will simplify your system design.

In the United States, stop categories define the way we stop the machine. It explains approved ways to remove dangerous power from machines. Power can be generated by electricity, high-pressure air, hydraulic fluid, chemistry or high-temperature components that need to cool before allowing entry.

In the United States, stop categories are identified in EN 60204-1 and NFPA 79 2007 (9.2.2). There are three types of stop categories:

Stop Cat. 0 removes all power. It is typically used on simple machines such as a hand-operated drill press.

Stop Cat. 1 adds an interlock device to the circuit. This is used when operator access time is faster than the time it takes to remove the danger. The machine safety sensor will have a remote-controlled locking/unlocking solenoid. It is controlled by the machine safety analysis device. Its job is to "only allow operator entry after the danger has been removed and power disconnected."

Stop Cat. 2 also removes high inertia/slow stop energy and is typically used when VFD or motion-control devices are in the system. The main difference is low-level power is left on to power the control system so it can retain control of the system.

Per EN/ISO 13849-1 there is a specific way that the power-disconnect device code must be implemented. In addition to Stop Category, OSHA 1910.147 Subpart J, General Environmental controls control of hazardous energy must be followed.

This is known as the lockout/tagout (LOTO) procedure. It was adopted to help to safeguard personnel from hazardous energy while maintaining or servicing equipment.

Energy source can be electrical, mechanical, hydraulic, pneumatic, chemical, thermal or other forms of energy. Multiple energy sources may need to be locked out or tagged. Section (b) of this

standard states, "Push buttons, selector switches and other control circuit type devices are not energy isolating devices." This would include limit switches, safety interlock switches, cable pull switches and other types of control equipment. These devices can have power after a safety shutdown event. 1910.147 may be the most far-reaching standard OSHA has adopted and is similar in principle to the European Machinery Directive 98/37/EC, Annex 1, Isolation of Energy Sources.

Check to be sure you have the certifications and markings you need for your area. TUV, even though it is not required in the United States, is a very useful standard to incorporate. It has strict guidelines on the performance, system reliability, hardware performance and layout of the safety systems that are better defined and easier to implement and understand than the OSHA rules.

Allan D. Hottovy
TUV-FSCEM functional safety certified automation & machine safety sensor expert / Telemecanique Sensors / www.tesensors.us

THE ULTIMATE GOAL

Ironically the only way to do a quick installation is to spend the time up front and perform a thorough risk assessment. It is critical that you analyze the current operations, identifying areas of risk to determine how critical they are based on frequency and consequence of failure. The ultimate goal is to ensure that each operation can carry out its intended function safely and reliably even if a failure were to occur. After this assessment, you will have selected the appropriate safety standard and performance level to comply with. We can then move on to reviewing the hardware and software requirements. For instance, you may want an integrated safety controller which can control both safe and non-safe devices over an Ethernet-based network. It is also important to make sure that this integrated safety system is designed with operator feedback to complement practical machine operation. The safest machine design may be pointless if your operators resort to bypassing safety functions in the name of efficiency. Once the specification and design has been validated, we will move on to create an installation and test plan. Some things to test for:

- confirm that each safety input and output is in working condition and responsive to the controller logic
- validate that safety devices are responding to every mode of operation
- check that resets, e-stops and any zone controls are responsive
- finally execute fault testing to ensure that we are in compliance with the selected safety standards.

Throughout this entire process it is imperative to create user instructions; document all revisions of prints, diagrams and bill of materials; and keep track of every component's lifecycle. Finally, safety upgrades are part of an ongoing process, and it is best practice to regularly validate and review the safety mechanisms and implement improvements.

Deana Fu
senior product manager / Mitsubishi Electric Automation / us.mitsubishielectric.com/fa/en/

IEC 61511

It's difficult to give a complete answer without knowing the specifics of the application and the safety knowledge/capability of the organization. I'll try, however, to give some broad guidance based on industry common practices, standards and guidelines.

Without going too deeply into standards, many in the industry take a machine functional safety lifecycle approach. This considers various phases in the design, startup and operation of a machine, in general there are several steps to the process:

1. analysis: this includes a risk assessment, which must always be conducted
2. implementation
3. operation

4. ongoing functions.

These are the steps in the process defined by the IEC 61511 standard; it has multiple sub-steps. You can find similar processes from other organization and suppliers by searching the Internet. Since you are likely located in the United States, you'll be focused on meeting OSHA's requirements and any standards which are referenced by OSHA. In general, if you follow a well-organized process, such as the one referenced by IEC 61511, you'll create the basis for better compliance with OSHA regulations and other standards.

Once you have decided on a machine functional safety lifecycle approach, you can start working on the different elements of the process. In this case, there are a variety of machines to safeguard, and each may require a different strategy and solution. It also seems that machine-to-machine coordination and complete process integration is desired. A functional safety approach will allow use of safety PLCs and safety fieldbus communications tied into the standard control and networking platform. It may be beneficial to use a single supplier for the standard and safety controls and to choose a single Ethernet-based control network which can handle both standard and safety communications, such as Ethernet IP/CIP, ProfiNet/ProfiSafe or EtherCAT/FSoE. This will simplify programming, setup, integration and maintenance. It may also be possible to use a modular control, network, I/O and software design, allowing reuse of basic design elements and documentation across multiple machines.

These controllers and networks will also enable the use of local, remote and remote IP67 I/O, which simplifies wiring, startup and troubleshooting of the individual machines and complete process. If the I/O count is high enough and the process is spread out, such as a filling line, it can be advantageous to add a device-level network, such as IO-Link and Safety over IO-Link, below the Ethernet network. Using a networked remote I/O approach also allows integration of various safety and non-safety devices from multiple suppliers, including safety light curtains, door switches, e-stops and safety laser scanners. Users will often need to mix and match components for a variety of reasons.

If this seems daunting, there are several companies that can be hired to do everything from a just a risk assessment to the complete machine safety lifecycle, including integration and installation.

Tom Knauer
safety champion / Balluff /
www.balluff.com

Compliance verification provides better protection against liability claims and accusations of negligence, which may result in claims for damages.

5 STEPS TO SAFETY

There are five steps to consider for your safety upgrade.

The first step is to conduct a risk assessment. Most North American and European machine safety standards call for mandatory risk assessment for the construction or modification of a machine or machine part. The risk assessment should be implemented and documented by qualified personnel.

Next, reduce the risks. The purpose of risk reduction is the attainment of an acceptable residual risk. For this purpose, suitable safety measures are defined on the basis of a three-step method by a team from the respective specialist departments. The architecture of the safety functions is defined and the overall safety concept is implemented and commissioned in future steps.

Third, implement technical protective measures. Components should be selected in accordance with the applied standard requirements.

Fourth, the manufacturer prepares the technical documents as proof of conformity.

And finally, validate and verify. Prepare a validation plan, theoretically examine and test all safety functions and finalize documentation as applicable. In case of damage, the manufacturer can verify that the machine's design is compliant with the directive. Compliance verification provides better protection against liability claims and accusations of negligence, which may result in claims for damages.

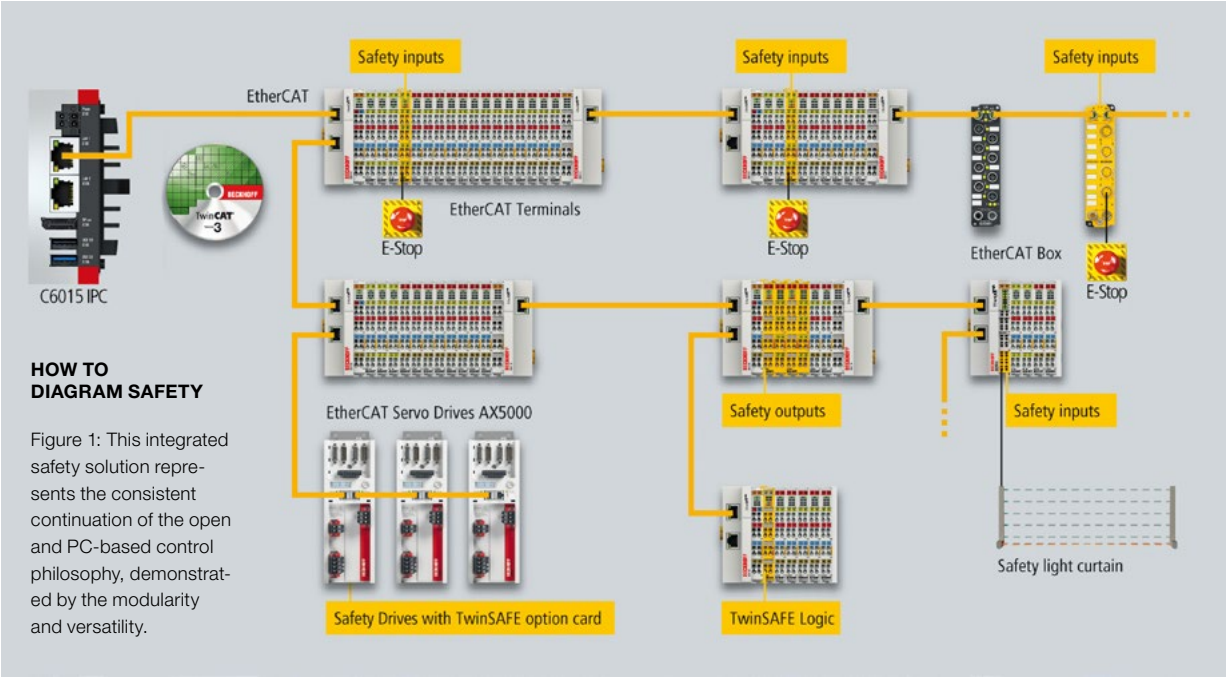
John D'Silva
safety technology manager / Siemens Industry / www.siemens.com

AVOID THE BYPASS

Where exactly does the confusion lie? Bypassing safety measures should never occur in a production environment, as this could lead to potential hazards, which seems to have happened in this case. Before any technological answer, plant safety standards must be understood by all team members and adhered to.

Given your plan to upgrade existing production lines using a standardized safety system, it would be beneficial to seamlessly integrate it into the existing machine design and control platform. Separate/standalone development tools for standard and safety signals should not be used because they are not necessary considering the system-integrated safety platforms available today. The most comprehensive solutions can be found with PC-based control architectures that integrate a programmable safety solution within the same programming environment used for PLC, motion control and all other control functions.

This makes it easier for controls engineers to support the system, and it's easier to train operators because all control aspects reside on one software platform. Connections to the field safety devices are handled via standard I/O hardware. Distributed safety solutions offer great flexibility, without having to rely on separate safety controllers. Modern programmable safety technology promotes simpler handling of the safety functions and eliminates confusion. It also offers more effective diagnosis of the safety system for faster troubleshooting. As important as it is to safely shut down the machine, it is also important to pinpoint via diagnostics exactly where any problem is for the fastest possible resolution. EtherCAT and Safety over EtherCAT (FSoE) provide a wealth of diagnostic features that can identify errors and faults down to an individual field device or I/O terminal. Alternate industrial Ethernet solutions can only identify an entire I/O segment with an error or perhaps a cable break without much precision. Also, since EtherCAT can be directly integrated within the PC-based control software, all diagnostic information can be brought into the PLC or conveniently viewed on an HMI display.



HOW TO DIAGRAM SAFETY

Figure 1: This integrated safety solution represents the consistent continuation of the open and PC-based control philosophy, demonstrated by the modularity and versatility.

(Source: Beckhoff)

More flexible expansion options mean vastly improved scalability; compliance with SIL and IEC 61508 standards; and independence from legacy protocols that may still be used on machines. Without having to change your existing fieldbus, an EtherCAT gateway can be added that will allow the addition of a safety logic controller right alongside the standard I/O hardware in the same rack. Once the safety platform is networked via EtherCAT, all the benefits of the protocol—real-time Ethernet technology; operation without requiring switches; virtually unlimited network expansion; flexible network topology; and no IP addressing in EtherCAT devices—are accessible to the user. An added benefit already described is the ability to mix safety and standard, non-safety I/O on one piece of DIN rail.

Vendors offer digital I/O safety terminals and single-channel I/O terminals for analog signals, and, in cases where safety hardware needs to be machine-mounted, the scalability of EtherCAT permits simple connection of IP67-rated I/O boxes that are ideal for use outside of electrical cabinets (Figure 1). Using these inputs and outputs, you can connect standard safety devices such as e-stops, light curtains, interlocks and safety scanners. The programming environment is achieved via multipurpose PC-based control software and the resulting safe parameters are set and password-monitored by the safe logic controller. This prevents unwanted changes to the safety program and limits the possible areas where safety measures can be improperly bypassed. ◻

Andy Garrido
I/O product marketing / Beckhoff Automation / www.beckhoff.com
Sree Potluri
I/O application specialist / Beckhoff Automation / www.beckhoff.com

The competitive value of machine safety

How machine builders unlock automation efficiencies by designing safety into machines

By Joaquin Ocampo, Tim Loria and Allen Tubbs, Bosch Rexroth

Machine safety is not a new concept, but we at Bosch Rexroth and our customers are seeing how machine safety unlocks a host of previously untapped production benefits.

From long experience working with machine builders, we are sure about one thing: Machine safety goes far beyond safe machine operations. It's a catalyst for productivity and a source of valuable data that can help to streamline shop-floor operations.

We approach machine safety holistically. Safety can improve productivity and provide considerations for designing safety functions into machines. Machine safety is used as a competitive advantage by machine builders, and safety data can be used to foster shop-floor transparency.

SAFETY FUNCTIONS IMPROVE PRODUCTIVITY

In addition to providing workplace security to employees, implementing safety procedures and software increases overall productivity in multiple ways.

Improved machine uptime: Safety functions reduce downtime and increase productivity and speed up operations by negating the need to power off the machine when in a safe state. Since the machine does not need to be powered-up again to restart production, downtime normally lost in the restart process is reduced.

Easier troubleshooting: Safety functions aid in troubleshooting by using safety-Ethernet protocols, such as CIPSafety on Sercos. With safety-Ethernet protocols, all the safety data is transferred in the same wire along with the motion commands. Because the safety data and non-safety data are in one channel, the protocol aids with troubleshooting and allows the user improved awareness of the entire system's functions. Now, machine builders can accomplish the necessary safety requirements with fewer components and less wiring, making commissioning much faster. Integrating safety diagnostics will also help users to identify wiring errors by clearly indicating the location of the inputs/outputs that are causing the fault. Additionally, using the same software for commissioning, programming and troubleshooting makes it easier for the user to manage the project.

Scrap reduction: Safety functions improve scrap reduction by putting the machine in a safe state, which stops the machine's operation and

SLOW STOP

Figure 1: By stopping the process in a controlled manner instead of abruptly interrupting the process by just cutting power or e-stop, the machine can continue production without having to realign material and scrap the material that was restricted when safe state was activated.

holds the material in its place. By stopping the process in a controlled manner instead of abruptly interrupting the process by just cutting power or e-stop, the machine can continue production without having to realign material and scrap the material that was restricted when safe state was activated (Figure 1).

Reduced floor spacing: By using motor-integrated technology with safety functions, the footprint of a machine can be drastically reduced while simultaneously increasing machine efficiency. Cabinet-free technology, such as Bosch Rexroth's IndraDrive Mi, provides the necessary features to make the machine lean, safer and productive. Additionally, shorter reaction times allow the machine to reach safe state more quickly, reducing the necessary distance to reach a protected area.

Increased operator safety and efficiency: At the forefront of machine safety is the machine operator's safety. If safety is applied correctly, not only will it keep the operators safer, the efficiency of the machine will also be increased. For example, if an operator is injured during production, the machine cannot continue to run because it needs to be stopped for an injury investigation. Implementing safety functions reduces the chances of this scenario happening, resulting in a safer environment in which employees can feel confident and where production runs uninterrupted by injury investigations.

While operator safety should always be the main concern, safety for the machine shouldn't be overlooked. A machine with the capability to run in a safe state, even during normal operation, will help to protect the machine from mechanical or electrical damage. If an operator accidentally sets the wrong machine speed, the incorrect setting could result in damaged internal components, forcing the machine to stop. Safety functions aids in preventing this error and more from stopping production, damaging the machine and maintaining operator's safety. According to Joaquin Ocampo, Bosch Rexroth product manager, machine safety unlocks a host of previously untapped production benefits.

HOW SAFETY SYSTEMS WORK: FINDING A SAFETY SOLUTION THAT WORKS FOR YOU

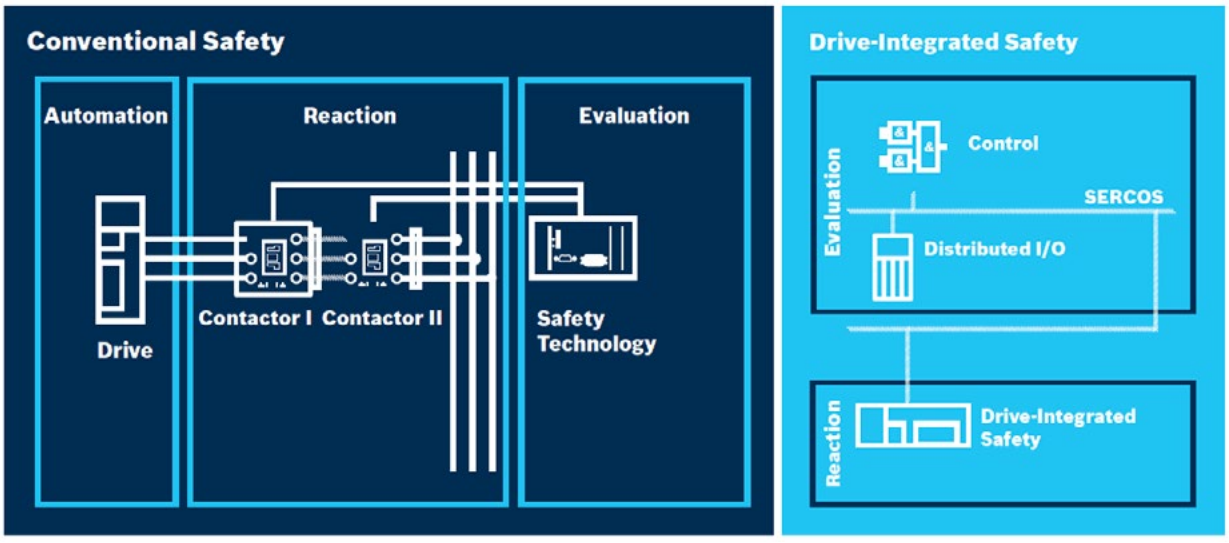
As safety technology advances and more options become available, deciding on the right safety solution for your company's application can be a daunting task. Here's a breakdown of how functional safety systems work and which implementation adds the most value to your application.

In the past, safety functions were realized with additional hardware components such as contactors or redundant electromechanical safety devices. The result—machines and production lines had to be shut down in hazardous situations leading to long and costly downtime.

Drive-integrated safety brings more flexibility to the shop floor by reducing the electromechanical footprint and components of machines (Figure 2). Furthermore, it simplifies troubleshooting and wiring as safety-relevant signals can be transferred via the automation bus Sercos. Drives perform continuous safety monitoring with control-reliable safety action inside the drive through dual-channel safety inputs. Safe stop of the drive can be done without disconnecting the main power, which means faster restarts and less downtime.

The decision for the right drive-based safety solutions mainly depends on the required machine functions and interactions with operators. For machines with minimal functionality or operator interaction, we recommend a safety solution that puts the machine in a safe state, which means the axis will not move because the power to the motor is safely interrupted and the necessary safety signals are directly connected to the drive. For this scenario, Bosch Rexroth offers the drive-integrated safety technology IndraDrive with Safe Torque Off (STO) solution.

For machines that require more functionality or operator interactions such as safe limited



DRIVE-INTEGRATED SAFETY

Figure 2: Drives perform continuous safety monitoring with control-reliable safety action inside the drive through dual-channel safety inputs.

speed (jogging), IndraDrive with SafeMotion would be the recommended solution. One benefit of IndraDrive with SafeMotion is that the necessary safety signals are directly connected to a zone module, which brings very rapid response times of just 2 ms upon triggering of the internal monitors. Furthermore, it eliminates the need for additional external safety components. Multiple modules can be used to separate safety zones. Alternatively, safety signals to the IndraDrive with SafeMotion can be realized via an Ethernet communication protocol. The advantage of using IndraDrive with SafeMotion is evident when the drive is in safe state. The drive can monitor itself and ensure that the motion from the control is within the safety parameters. With this technology, there is no need to go through a safety control since it is all done at the drive level where the motion is created.

CENTRALIZED OR DECENTRALIZED SAFETY?

Drive-based safety can be realized with central or decentralized/distributed safety controls.

Benefits of centralized safety: Centralized-safety PLCs are a solution that can be centralized with a motion/logic PLC. When the entire motion/logic program is combined with the safety program, the whole application is contained in a single project, making the commissioning and troubleshooting process easier.

With centralized safety PLCs, for example, Bosch Rexroth's SafeLogic controls can be networked together to share safe and non-safe data between controls if required for the application (Figure 3). SafeLogic uses remote safety input/output (I/O) technology, which gives the user freedom to locate safety I/O around the machine.

An advantage of having remote I/O is that the I/O can be either safe I/O or standard I/O on the remote module, making it easier to start up and reducing labor costs.

Benefits of decentralized safety: Decentralized safety solutions include remote safety PLCs with easy-to-use function block programming to set conditions of safety I/O to achieve a safe state. A remote safety PLC, such as Bosch Rexroth's SafeLogic compact, is the ideal solution for distributed control machines, such as transfer lines, because it allows individual

CENTRALIZED SAFETY
Figure 3: Controls can be networked together to share safe and non-safe data if required for the application.

control of the complete line. This means the safety control is independent of the motion control, allowing users to program and see separate PLCs for motion and safety. Remote safety PLCs can also be networked, providing a path for safety information to be shared among stations within a machine or separate machines.

KEY CONSIDERATIONS FOR DESIGNING SAFETY INTO MACHINES

The need for integrated safety is an important aspect of automation machines. Safety for the user or operator is the main concern, but there are other points to be considered. Many times, a machine builder or manufacturer will acknowledge the need for a safety function but doesn't know how to get started. Questions such as "What safety functions and how can they be implemented while staying within industry safety standards and protecting production?" hinder and slow down the implementation process. Implementing safety functions on a machine is a unique process for every company. A good start for implementing safety functions would be to conduct a risk assessment.

1. Do a risk assessment: This service identifies the necessary protective measures for risk reduction; the limits of the machine are determined; the hazards on the machine are reviewed; the risk estimate and risk evaluation are defined; and the measures taken for risk reduction are understood for implementation.
2. Define trigger events: The next recommended step would be to define trigger events and what happens in those events. Manufacturers may notice that opening a guard door makes an axis stop or breaking a light curtain will make the machine run at a slow speed.
3. Define safety functions: Now that the trigger events are identified, manufacturers will know what will happen if safe zones are interrupted. They need to figure out how these functions are going to be accomplished. There isn't a one-size-fits-all implementation process, but a few good starter questions include:

- Will a safety PLC be used?
- Will the safety be in the drive?
- Will it be a combination of PLC safety and drive safety?
- Will it have a centralized or decentralized safety PLC?

These answers will depend on the safety functions required and the number of safety I/O of the machinery. Depending on the number of safety I/O required safety functions and logic decisions/combinations, the customer can determine which scalable solution fits with the application.

SMART SAFETY FOR SHOP FLOOR TRANSPARENCY: MAKING USE OF SAFETY DATA

The Industrial Internet of Things (IIoT) is most often thought of as a way to collect data to increase machine or process efficiency. With IIoT and Industry 4.0 technology, safety data can be analyzed and turned around to provide a safer environment for the worker.

One way to use data to improve safety is when the data about the operator is available. By using operator data, such as biometrics, training levels and even language skills, the machine can be programmed to react to the unique characteristics of its user in order to provide the safest environment for individual operators. Repetitive-motion injuries and ergonomic issues can be resolved by having the machine react to the operator's height or reach. Certain procedures or operations can be limited according to the operator's training level, and digital instructions can be adjusted to accommodate the operator's native language or preferences.

Additionally, data can also be used to validate the risk assessment. One variable in calculating risk is judging the likelihood that a hazardous event will occur. This probability is then combined with the severity of the event to calculate an overall risk. In new designs, an educated estimate is often made by a qualified designer to set the protection level around specific circumstances or mechanics around the machine. By tracking events on a machine, once the machine is in operation, the risk assessment can be verified over time to prove the efficiency and effectiveness of the safety system, or the data can reveal that the initial risk assessment was wrong and needs to be re-evaluated.

Machine learning can also play a role in predicting unsafe conditions or events. By collecting large sets of operational data, the data can be correlated together to detect events and machine conditions that can lead to unsafe conditions.

SUMMARY

The benefits of safety technology extend beyond keeping workers safe. Ultimately, integrating safety is not a daunting financial investment when the productivity benefits of applying safety functions is considered alongside employee satisfaction. The return on investment may depend on the industry application and products manufactured.

As machinery and employees must work together, operators can only work efficiently and achieve maximum productivity if the safety technology does not slow them down. □

Joaquin Ocampo is product manager at Bosch Rexroth. Tim Loria is principle engineer and a certified functional safety professional at Bosch Rexroth. Allen Tubbs is product manager, Internet of Things, at Bosch Rexroth.

KEY INSIGHTS & CONSIDERATIONS

- Machine safety protocols bring competitive value by improving plant productivity.
- Safety protocols offer invaluable data that can be analyzed to further improve productivity.
- Operator safety is at the forefront of machine safety and integrating safety protocols help to keep employees safer in industrial environments.
- Find a complete safety solution that works for your company's specific application.
- Start the process of implementing safety protocols by conducting a risk assessment.