**Session No. 565**

# The Best Use of Lockout/Tagout and Control Reliable Circuits

**L. Tyson Ross, P.E., C.S.P.**
**Principal**
**LJB Inc.**
**Dayton, Ohio**

## Introduction

Anyone involved in the design, installation, operation, or maintenance of industrial equipment is personally concerned with machine safety and safety procedures. There are two broad descriptions of machine safeguarding: prevention of contact with the hazard and control of the energy driving the hazardous operation. Machine barrier guarding is a way to avoid contact with a hazard, while lockout/tagout (LOTO) procedures and the use of control reliable circuits are ways to control the energy driving the operation. This paper provides information on the best uses of lockout/tagout and control reliable circuits.

LOTO 101

Lockout/tagout (LOTO) is the required safety procedure for maintenance tasks and those that are not part of a machine's normal production process. If any employee is required to remove or bypass a machine guard, or is required to place any part of his body into a machine where work is performed or where any other zone of danger exists, the LOTO procedures must be followed.

The essence of the safety requirement is that the danger of any and all hazardous energy sources must be relieved and removed before anyone enters a machine for repair, maintenance or service. The associated regulations require that the method to do that on a machine be formalized, documented and communicated to anyone who works around the equipment.

Tagout is a similar process required if lockout is not possible. A prominent tag is placed on or near the energy isolation device warning against hazardous conditions if the equipment is energized. Use of a tagout device illustrates a feature necessary to any energy control program—the need for employee training and communication. A tagout device does not physically prevent the equipment from being energized, but with training in the proper procedures to apply and remove lockout and tagout devices, employees can be effectively protected.

Energy control by lockout or tagout is required for all tasks that are not routine, repetitive, or integral to the use of the machine for production. For example, changing a grinding wheel is not part of the normal production operation, so to do this, the grinder must be locked out or tagged

out. Normal production operations and minor machine servicing are not regulated by the OSHA lockout/tagout regulation.

## Regulations and Standards

The increasing complexity of production processes and industrial equipment often precludes the use of LOTO to perform necessary work. The Occupational Safety and Health Administration (OSHA), the American National Standards Institute (ANSI) and other organizations have provided regulations and guidance to assess the level of risk present and apply alternative methods of personnel protection to decrease the risk to a tolerable level.

The federal regulation in the United States that governs the use of LOTO is OSHA regulation 1910.147. This standard establishes minimum performance requirements for the control of hazardous energy. NFPA 70 (National Electrical Code NEC) is listed as reference in Appendix A of OSHA 1910; therefore, the mandatory requirements of NEC are also mandatory OSHA requirements.

There are some exceptions where OSHA 1910.147 does not apply. Generally, if someone has to bypass or remove a machine guard, be near the point of operation, or perform an adjustment, the requirements of 1910.147 apply.

The American National Standards Institute (ANSI) has several standards that provide guidance and best practices for machine safeguarding:

- ANSI Standard B11.19-2003, Performance Criteria for Safeguarding
- Standard Z224.1-2003, Control of Hazardous Energy Lockout/Tagout and Alternative Methods
- ANSI/RIA R15.06-1999, Safety Requirements for Robots and Robotic Systems

Energy control procedures were first formulated prior to the publication of the OSHA regulation with the ANSI standard Z224.1. This ANSI standard was created to provide guidance and best practices for situations where the unexpected release of hazardous energy could occur. Later Z224.1 was revised and the name changed to reflect the need for greater flexibility through the use of alternative measures of energy control, risk assessments and the use of the hazard control hierarchy. One of methods contained in the hierarchy is the use of engineered safeguards, and the use of control reliable circuits.

Although the ANSI standards do not have the force of law, they are often cited by governing bodies as a requirement for compliance. Regardless they provide a foundation for good design and safe operation.

## Hazardous Energy Control Program

The first steps toward compliance should be the completion of a risk assessment and a written hazard energy control program. The purpose of the energy control program is to ensure that the risk of exposure to hazards will be eliminated or minimized before any authorized person performs work on the machine. The goal is to eliminate all hazards while realizing that the best that can be achieved is to make the overall hazard as slight as possible.

The elements of a hazardous energy control program are:

- Identification of the machine, equipment, or process. This includes every task to be performed on the equipment.
- Listing of all required energy-isolating devices and their locations
- Specific procedures for shutting down, isolating, blocking, securing, and relieving stored or residual energy
- Specific procedures for the placement and removal of lockout and tagout devices
- Specific requirements for verification that isolation and de-energization have been accomplished

The point often overlooked in examples is the requirement for specific procedures. Each piece of equipment or process must be evaluated, and the specific identifications and locations included in the procedures.

The method of hazardous energy control selected depends on whether the task can be accomplished with the equipment energized or not. In all cases, the primary method of energy control should be lockout/tagout. If the task is routine, repetitive and integral to the production process, or traditional lockout/tagout procedures prevent completion of the task, alternative measures can be applied. It cannot be more strongly stressed that an alternate to lockout/tagout can only be used after an assessment of all risks and safety consequences.

## Alternative Measures

During normal production operation, it is often not feasible to stop and lock out a machine for minor adjustments. Some other techniques and equipment could be applied to safely work near potentially hazardous motions. Some examples given in the machine guarding standard are "barrier guards, two-hand tripping devices, or electronic safety devices."

The ANSI standard Z224.1-2003 provides guidance to using these alternative methods. The standard lists requirements and performance objectives for the procedures, techniques, designs and methods that protect personnel from the release of hazardous energy.

When choosing a protective method, be aware of the preferred ways that are listed in the ANSI standard. While always mindful of the risk reduction benefit and feasibility of the method, the final selection should be made in this order of preference:

- Eliminate the hazard by design
- Apply engineered safeguards
- Implement administrative controls

## Risk Assessment

Whenever an alternative method is considered, a risk assessment is required. Risk assessments include the determination of the severity and probability of harm that processes present to workers. The probability is determined by a number of factors including history, environment, level of training, human factors and many more.

ANSI has published a report that gives directions to complete a machine tool risk assessment, ANSI B11.TR3-2000, *Risk Assessment and Risk Reduction – A Guide to Estimate, Evaluate and*

*Reduce Risks Associated with Machine Tools.* In it is described the procedures and methods for completing a risk assessment and ways of reducing the risks associated with these hazards.

Broadly, risk reduction involves identifying hazards, rating them based on the severity of harm or injury they present and the probability of injury occurring. To determine the probability of injury, several factors are considered: the frequency of exposure, the personnel exposed and their training, the safety history of the machine, the workplace environment (housekeeping, lighting, noise, human factors) ergonomics, awareness of hazards, motivation to deviate from safe work practices, the reliability of the safety measures, and the ability to maintain or defeat the protective measures. A matrix of severity versus the probability of injury yields a level of risk. The matrix, including the ANSI naming of the risk levels, is shown below.

| **Probability of Occurrence of Harm** | **Severity of Harm** | | | |
|---|---|---|---|---|
| | **Catastrophic** | **Serious** | **Moderate** | **Minor** |
| Very Likely | HIGH | HIGH | HIGH | MEDIUM |
| Likely | HIGH | HIGH | MEDIUM | LOW |
| Unlikely | MEDIUM | MEDIUM | LOW | NEGLIGIBLE |
| Remote | LOW | LOW | NEGLIGIBLE | NEGLIGIBLE |

The level of risk tolerated is a decision of the machine users and those performing the risk assessment. It is an iterative process: assess the risk before protective measures are taken, and do it again with the measures in place to see if the new risks levels are tolerable.

Part of the evolution of the ANSI safety standards includes harmonizing them with other international standards. This recognizes the fact that many businesses operate and sell products in many countries around the world and streamlining requirements among nations will lower costs and simplify regulatory compliance. The International Electrotechnical Commission (IEC) Machinery Directive reviews important international safety standards. The IEC standards describe five categories of performance for the safety-related parts of control systems. They do not correlate directly to the risk levels of the ANSI matrix, but their individual performance requirements help build a control reliable circuit.

Category B: Forms the basis for the other safety categories, no special safety measures, by using parts in accordance with relevant standards faults can be prevented.

Category 1: Includes Category B requirements with higher safety reliability.

Category 2: Includes Category B requirements. The safety function shall be checked at machine start-up and periodically by the system. A loss of the safety function is detected by the check. If a fault is detected a safe state shall be initiated or a warning given.

Category 3: Includes the Category B requirements. The system is designed so that a single fault in any of its parts does not lead to the loss of the safety function. Some but

not all faults will be detected. An accumulation of undetected faults can lead to the loss of the safety function.

Category 4: Includes the Category B requirements. The system is designed so that a single fault in any of its parts does not lead to the loss of the safety function. When the faults occur the safety function is always performed.

## Control Reliable Circuits

One method of ensuring that a piece of automation can be brought to a safe energy level is through the use of control reliable circuits. These circuits are part of the machine control system that, along with other machine safeguards, provide safety in the event of a failure. To paraphrase the OSHA/ANSI definitions, a control reliable circuit is one in which the failure of a single component will not prevent normal machine stopping action from taking place and will not allow a successive machine cycle from starting until the failure is corrected.

Control reliable circuits can take many forms, and control reliable machine operation often requires the combination of different types. Control reliable circuits can be applied to any type of circuit including electrical, pneumatic and hydraulic circuits, although this paper focuses on electrical and pneumatic circuits.

Control reliability is a design strategy that separates a system's safety related functions into modules that can be checked and monitored by other components. It includes redundancy, but redundancy alone is not control reliability. The monitoring process ensures that the safety features are present even after a component failure. The machine is stopped, or cannot be re-started, until the failed component is repaired. Two things should be noted. First, it is not possible to completely protect against multiple, catastrophic faults. Second, since some failures cannot be detected until the completion of a cycle, or a portion of a cycle, there may be a loss of the safety-related functions for a part of the machine cycle.

Not every machine will require a control reliable safety circuit. Some will require protective measures beyond just control reliability. That decision is made after the risk assessment. A traditional Master Control Relay (MCR) circuit of days past may not be adequate. Let's start with that MCR circuit to build a control reliable circuit.

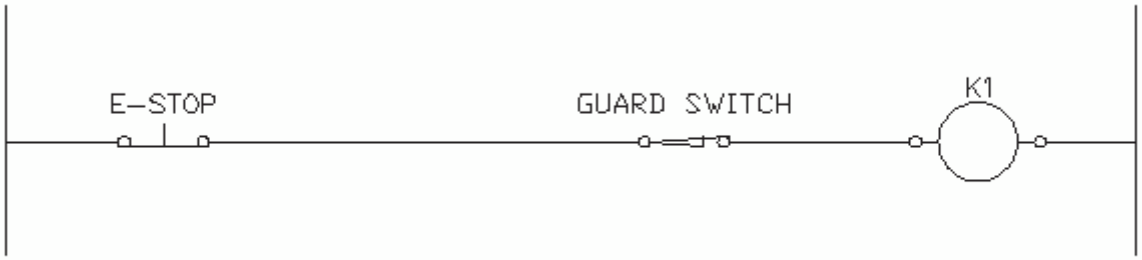


**Exhibit 1. This Master Control Relay circuit may be adequate if hazards are very small.**

This circuit may be adequate if the hazards are very small. The parts are chosen with suitable electrical ratings and approvals. This may be described as meeting Category B requirements.

There is no particular measure of safety performance in this circuit or its components. It is an arrangement of good equipment used within the limits of the components. This type of circuit will prevent a fault because of its construction, but the failure of any component will not be detected. Either the E-Stop or the guard switch contacts might weld in the closed position, and activating the switch will not open the relay.

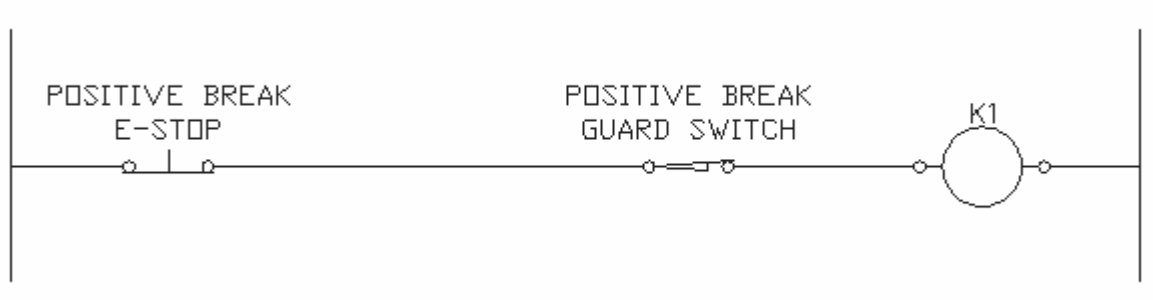


**Exhibit 2. This circuit is what the European Standard would consider a Category 1 E-Stop circuit.**

Exhibit 2 shows what the European Standard would consider a Category 1 E-Stop circuit. Positive break contacts are designed so that the mechanical action of the device will separate closed contacts that might be welded. The use of components with positive break contacts would satisfy the need for the use of "well tried safety components and safety principles." This still is not a control reliable circuit as there are no provisions for redundancy, fault detection, or self-checking.

A Category 1 safety circuit may even include a safety relay. Whether to include one is determined by the complexity of the safety circuit. The circuit shown in Exhibit 2 is quite simple. Exhibit 3 shows another Category 1 safety circuit that includes a safety relay.

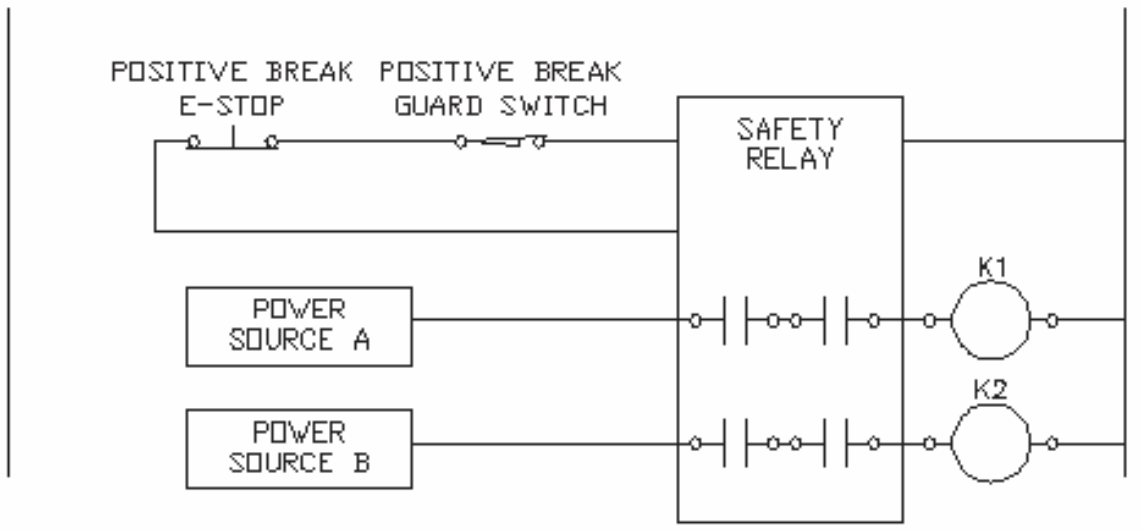


**Exhibit 3. This Category 1 safety circuit includes a safety relay.**

This circuit is more complex, controlling multiple relays, each fed from a different source. An ordinary relay could have been used to send the signal to K1 and K2, but it could still fault in the closed position and therefore would not be acceptable. Still, this circuit is Category 1 rated, as there is only a single safety input channel, and there is no checking of the safety circuit.

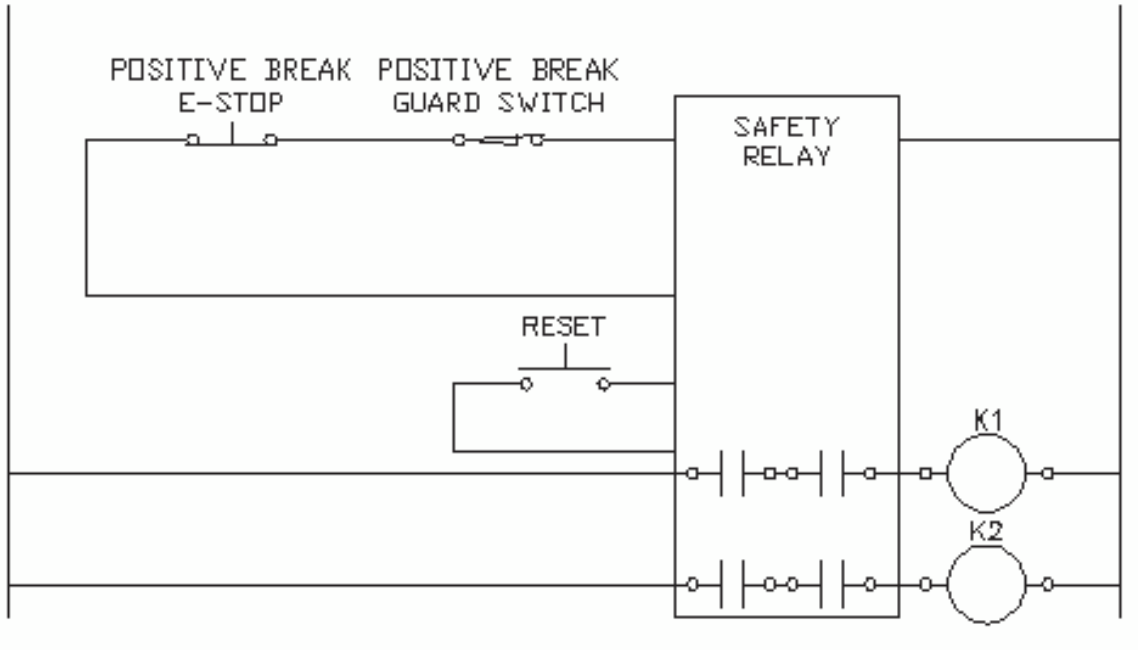


**Exhibit 4. This circuit qualifies as Category 2 protection.**

Exhibit 4 adds a safety relay with a manual reset input, requiring an operator to push the reset button following the re-closure of the input circuit. This circuit qualifies as Category 2 protection. Every time the safety relay input opens, either the E-Stop or the guard switch, or power drops off, the safety relay must be reset for K1 and K2 to energize. This fulfills the Category 2 requirement for a periodic check of the safety function. To ensure a good design, consider whether the E-Stop and guard switch are operated frequently enough to check that the safety function is still performed. It may be necessary to exercise the devices periodically to ensure no undetected faults have occurred. This still is not a control reliable circuit.

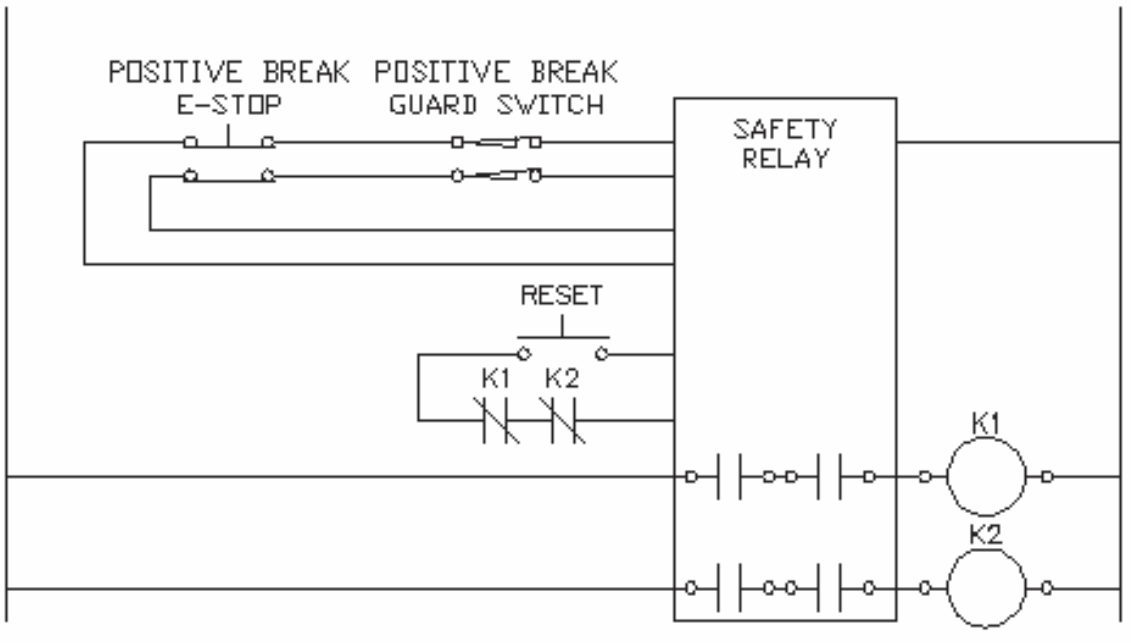


**Exhibit 5. This circuit can be described as control reliable.**

The circuit shown in Exhibit 5 can be described as control reliable:

- A second input channel was added to maintain safety monitoring should one of the contacts on the E-Stop or guard switch fail to open.
- N.C. contacts of the output relays K1 and K2 were added to the reset channel. Both relays must be off for the safety relay to reset and re-energize the outputs again.

In this particular example, the safety relay will reset after the E-Stop or guard switch is opened and re-closed and the reset button is pushed. This circuit includes features necessary for control reliability: redundancy of the input circuits, monitoring of the output relays, and periodic testing through the manual reset circuit. This circuit qualifies as Category 3 protection.

But is this circuit safe enough? Some faults are possible that would not be detected. Even though the requirement for control reliability is that the safety function still be performed with a single fault, if it is not detected, another fault could cause a devastating accident. Exhibit 6 below shows the same circuit if there was a short circuit around a channel of the guard switch. A wire strand not completely under the terminal, or a cut in cable insulation could cause this.

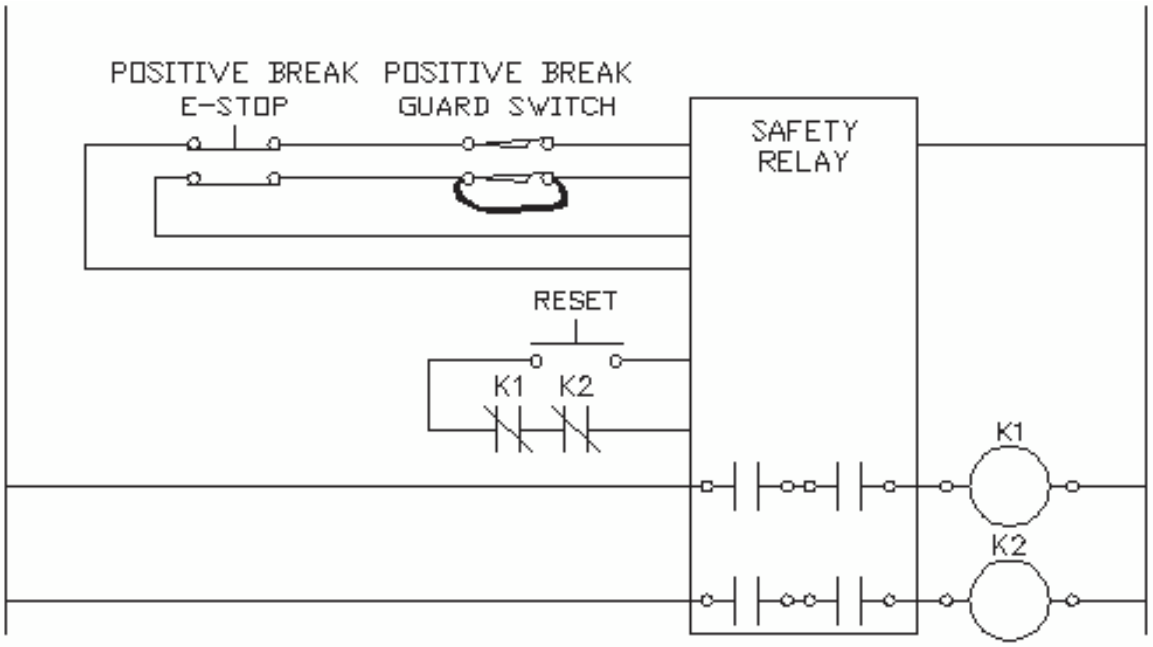


**Exhibit 6. This illustration shows the same circuit as Exhibit 5, but with a short circuit around a channel of the guard switch.**

In this case, opening the guard would still stop the motion, as the safety relay will still see the other channel go low. Re-closing the guard and cycling power will allow the safety relay to be reset. The short circuit condition would not be detected. Should the second guard switch channel experience a short, opening the guard would not stop machine motion. For this reason, in extremely hazardous applications, some argue that daisy chaining of safety inputs should not be done. This is one demonstration of the need for a thorough assessment of risks and hazards

Category 4 protection is usually reserved for very hazardous situations that include the use of protection devices more complex than limit switches and E-Stop buttons, such as light curtains. Relays and electro-mechanical devices cannot usually accommodate the Category 4 requirement that if a component fault occurs, the safety function is immediately performed. Solid-state equipment can incorporate high frequency monitoring that can better achieve this requirement.

## Closing

Despite the prevalent use of control reliable circuits, they are often used incorrectly or do not adhere to the appropriate industry regulations. As the average costs—both direct and indirect—of industrial accidents continue to rise, it is critical that safety supervisors understand the appropriate use of control reliable circuits and the requirements posed by regulations and standards.

In this paper, the basic steps to create a safe, control reliable electronic circuit have been outlined, using broad guidelines that all circuit designers must take into consideration. It is imperative that all the hazards and risks are found and reduced to minimize negative consequences.