EHS Today MachineDesign NED New Equipment Digest.

EXECUTIVE SUMMARY

Basic OSHA Requirements for a Control Reliable Safety Circuit

Devin Murray, tec.nicum Services Manager, Schmersal

OCTOBER 30, 2024

KEY TAKEAWAYS

- OSHA and ANSI both have requirements for machine safety.
- Industry standards exist for designing a control reliable safety circuit.
- ISO 13849-1 categories describe the physical wiring of safety circuits.

in partnership with

SCHMERSAL
THE DNA OF SAFETY

Basic OSHA Requirements for a Control Reliable Safety Circuit

OVERVIEW

Control reliability is a benchmark for the design of safety control circuits. Properly designed control circuits ensure the safety of the system overall. There are several categories of circuits for safety systems. OSHA refers to control reliable circuits for safety functions, while current ANSI and ISO standards refer to these safety circuit classifications as performance levels (PL) and safety integrity levels (SIL). Understanding the basic wiring designs of safety circuits is necessary for fulfilling OSHA requirements and meeting the conditions of a specific PL or SIL rating.

The Schmersal Group develops and produces systems and solutions for its customers worldwide to help boost machine safety and occupational health and safety. The specialists in tec.nicum, the department for services relating to machine and industrial safety, offer machine manufacturers and operators competent, product- and manufacturer-neutral advice on all current legal regulations, support companies in the safe design of their machines and workplaces, and design and implement safety solutions across all lifecycle phases of machines and plants.

CONTEXT

Devin Murray explained the regulations and designs applicable to control reliable safety circuits and highlighted important circuit behavior to consider when designing for control reliability.

KEY TAKEAWAYS

OSHA and ANSI both have requirements for machine safety.

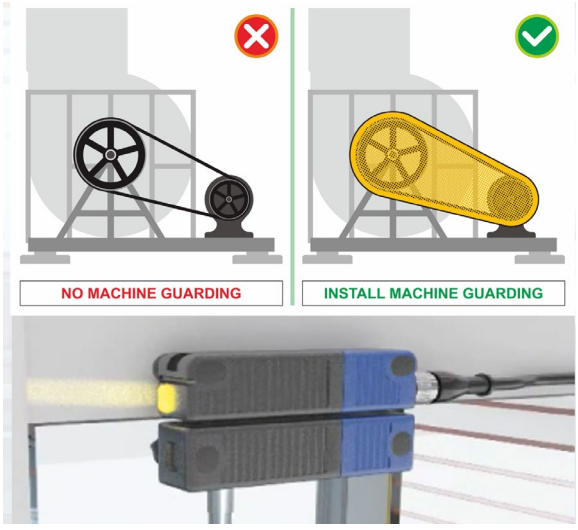
OSHA regulation requires employers to ensure a safe working environment for employees. At a high level, the process of ensuring a safe working environment has two parts: 1) risk assessment; and 2) guarding against hazards, including hazards on machines.

Did you know?

Machine guarding consistently appears on the Top 10 most frequently cited workplace safety standards list. In 2024, machine guarding ranked 10th, with 1,541 citations.

When it comes to machine safety, at a high level, OSHA **1910.212 - General Requirements for All Machines** mandates that hazards on machines must be guarded against. More specifically, the standard states that in machines with barrels, containers, or drums, enclosures must be interlocked to the drive mechanism, which prevents the container from revolving unless the guard enclosure is in place.

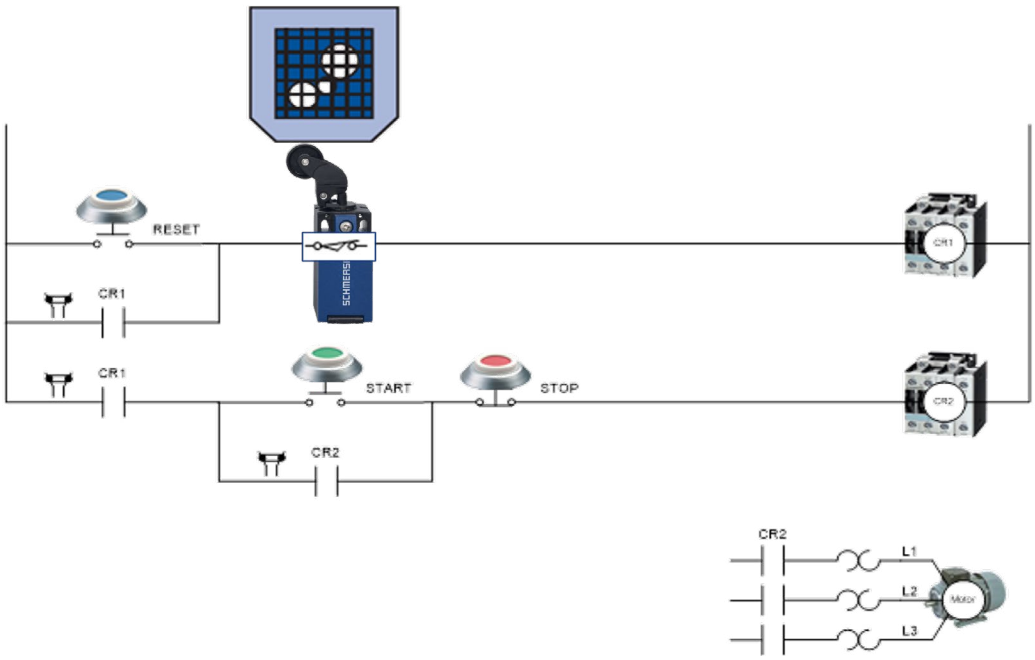
Figure 1: Machine guarding protects the operator and other employees



An interlock switch is a mechanical, electrical, fluid power or other type of device or means to prevent a hazardous situation(s) under specified conditions. While OSHA specifically defines the interlock switch

Basic OSHA Requirements for a Control Reliable Safety Circuit

Figure 2: A commonly used safety circuit design for a limit switch monitoring a guard door



requirement to machines with barrels, containers, and drums, the concept can be applied to all machines.

Industry standards exist for designing a control reliable safety circuit.

The type of safety circuit used will depend on the machine hazard. The concept of **control reliability** can be used to guide the design of safety circuits for many machines, to guarantee safe operation even in the event of failure.

OSHA standard **1910.217 – Mechanical power presses** describes control reliability as construction of the control system in such a way that a failure within the system will not prevent the normal action used to stop a machine from being applied. Control reliability ensures that a single failure will not cause loss of the safety function, but also will prevent the next operation cycle from being initiated.

ANSI B11.19 – Performance Requirements for Risk Reduction Measures: Safeguarding and Other Means of Reducing Risk outlines required safety functions that must occur in the event of a failure:

- Preventing operators from starting the machine
- Performing an immediate stop of the machine
- Allowing a cycle to complete before the machine is stopped, then preventing operators from restarting the machine

ANSI names control reliability as one of the design strategies that may be used to achieve these safety functions, but cautions that if multiple failures or an accumulation of failures occurs, control reliability may not be able to maintain safety. According to ANSI, a control reliable circuit requires more than simple redundancy and must also incorporate monitoring to verify that redundancy is maintained.

Basic OSHA Requirements for a Control Reliable Safety Circuit

Control reliability and ISO 13849-1

ANSI B11.19 defines control reliability as "The capability of the [machine] control system, the engineering controls—devices, other control components, and related interfacing to achieve a safe state in the event of a failure."

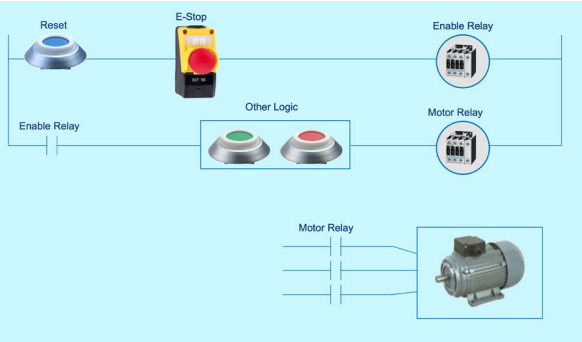
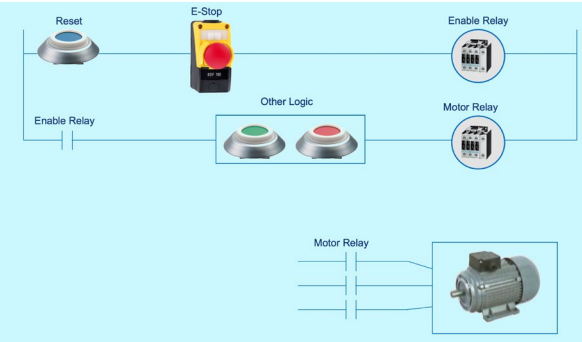
Although the ANSI B11.19 standard is not directly comparable to ISO 13849-1, ANSI names two ISO 13849-1 requirements that would achieve compliance with control reliability requirements:

- Category 3 or Category 4 circuit; or
- Performance Level of "d" or "e"

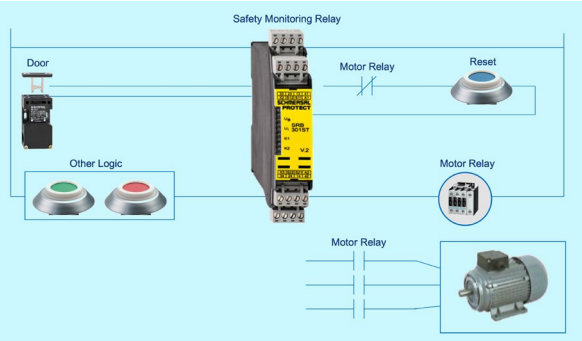
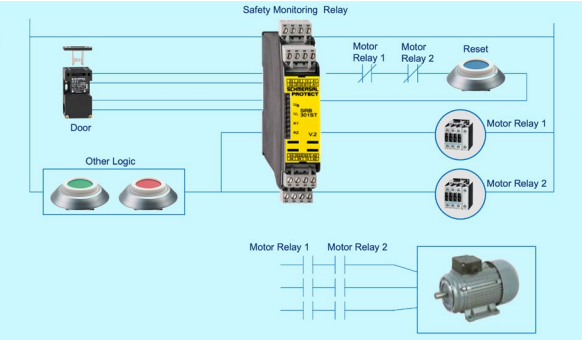
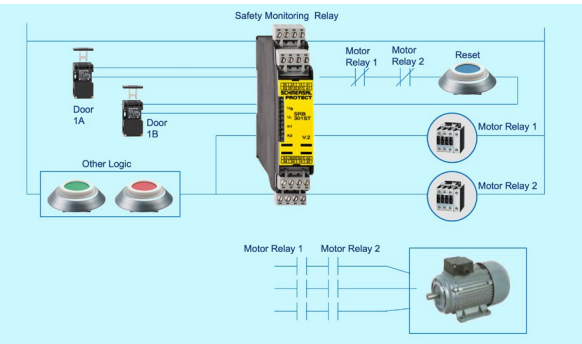
ISO 13849-1 categories describe the physical wiring of safety circuits.

An ISO 13849-1 category is a "classification of the safety-related parts of a control system in respect of their resistance to faults and their subsequent behavior in the fault condition." Only Category 3 and Category 4 circuits are considered control reliable.

Table 1: ISO 13849-1 categories

Control Category	Description	Pictorial Representation
B	A single-channel system with no monitoring using components such as a simple on/off switch. The occurrence of a fault can lead to the loss of the safety function.	
1	A single-channel system with no monitoring (similar to Category B, but using well-tried principles and components). The occurrence of a fault can lead to the loss of the safety function, but the probability of occurrence is lower than for category B.	

Basic OSHA Requirements for a Control Reliable Safety Circuit

2	A single-channel system that includes a test function using components such as a safety-rated interlock switch with a monitoring device. The occurrence of a fault can lead to the loss of the safety function between the checks. The loss of safety function is detected by the check.	
3	A two-channel safety system with redundancy on both the input and outputs sides, with monitoring. When a single fault occurs, the safety function is always performed. Some, but not all, faults will be detected. Accumulation of undetected faults can lead to the loss of the safety function.	
4	A two-channel safety system with redundancy on both the input and outputs sides, with monitoring. When a single fault occurs the safety function is always performed. Detection of accumulated faults reduces the probability of the loss of the safety function (high DC). The faults will be detected in time to prevent the loss of the safety function.	

Category design considerations

When designing circuits for a given ISO 13849-1 category, it is important to also evaluate the impact of fault masking and fault exclusion.

Consider a Category 3 safety circuit being used to monitor multiple doors on a machine, including a two-channel safety switch on each door, with each switch connected in series to a safety monitoring device and output-side redundancy. This ensures that if any of the guard doors on the machine are opened during operation, a safe stop is triggered.

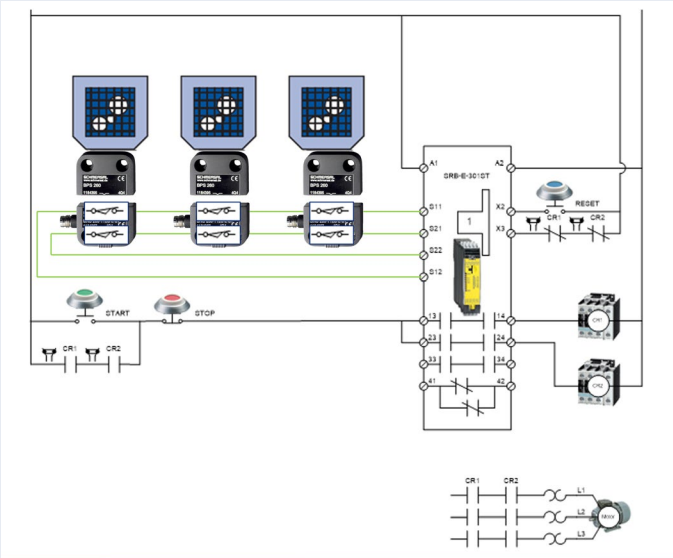
In this configuration, a failure in the middle door, such as a welded contact in the door sensor, will cause the safety monitoring device to register the failure, stop the machine, and place it into fault mode, which will prevent a machine reset until the failure is corrected.

If the upstream door is opened, the system will work as expected: the fault will not be cleared and the

Basic OSHA Requirements for a Control Reliable Safety Circuit

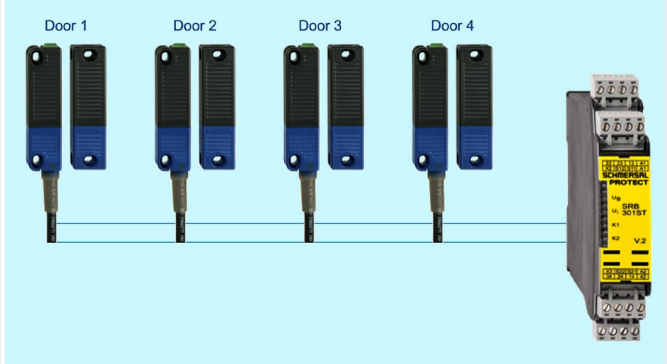
machine will not be able to be re-engaged. However, if the downstream door is opened, both channels will drop out, satisfying the safety controller and allowing the machine to be re-engaged without the failure being corrected—fault masking.

Figure 3: An example circuit with potential for fault masking



To prevent fault masking and achieve Category 4, electronic devices, such as RFID switches, can be used instead. In the same scenario described above, the failure will be stored in the microprocessor inside the switch, with the only way to clear the fault being to correct the issue.

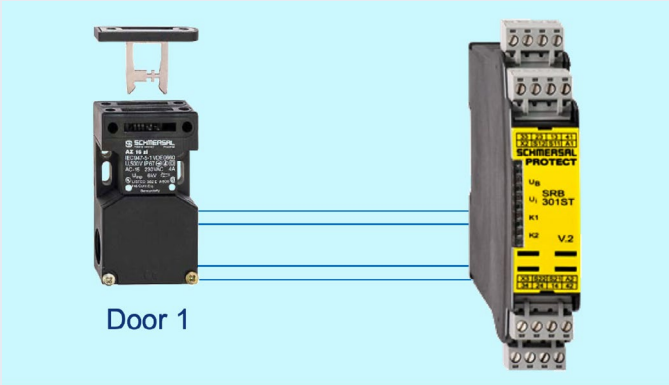
Figure 4: A Category 4 safety circuit wired in series



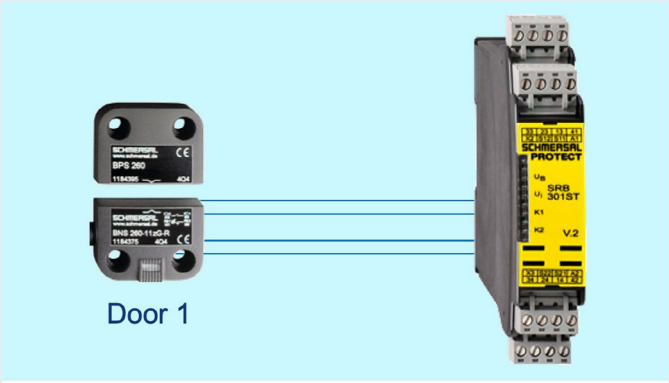
Fault exclusion accepts certain fail conditions in a safe device. For example, if a keyed interlock switch is not mounted correctly, the key can break off into the switch. Although key breakage can occur, as it is a single fault that allows the safety circuit to remain satisfied, key breakage is considered a fault exclusion.

In this keyed interlock scenario, Category 3 is the maximum control category possible, as the safety function is single-fault tolerant. However, Category 4 can be achieved by instead using a coded magnetic switch, which does not have the same single mechanical failure aspects as key actuated switches.

Figure: 5: Control category depends on the type of device and the installation.



Up to Control Category **3**



Up to Control Category **4**

Basic OSHA Requirements for a Control Reliable Safety Circuit

ADDITIONAL INFORMATION

To learn more visit Schmersal

BIOGRAPHY

Devin Murray
tec.nicum Services Manager
Schmersal

Devin is the tec.nicum Services Manager for Schmersal's engineering services group in North America. He has written many whitepapers related to safety standards and general machine guarding, conducted risk assessments and validations, and developed and reviewed the implementation of corporate safety standards. As a founding member of our tec.nicum team, Devin helped develop a curriculum of machine safety training courses and recently lead our successful efforts to be an IACET Approved Provider. He holds a Bachelor of Science in Electrical Engineering and an MBA from Alfred University and is a TÜV certified Functional Safety Engineer for Machinery.

©2024 Endeavor Business Media. All Rights Reserved.