EHS Today | Machine Design | NED New Equipment Digest | Plant Services

EXECUTIVE SUMMARY

Commonly Overlooked and Misapplied Machine Safety Requirements

Devin Murray, tec.nicum Services Manager, Schmersal USA

APRIL 26, 2023

KEY TAKEAWAYS

- Risk assessments of a machine are required throughout its life cycle.
- Stop-time measurements are required to know where to install non-separating safety devices.
- Mechanical switches are frequently misapplied.
- Misapplication can occur when implementing safety categories in the physical design of a circuit.
- Using series connections for high-risk applications can result in fault masking.
- Collaborative robots must undergo a risk assessment.

in partnership with

SCHMERSAL
THE DNA OF SAFETY

Commonly Overlooked and Misapplied Machine Safety Requirements

OVERVIEW

Machine safety can be challenging and complex, for both machine builders and users. With so many safety aspects to consider, it is easy to overlook crucial elements to successfully implement a safety measure. Recognizing the most commonly overlooked and misapplied machine safety requirements and knowing how to correctly address them can reduce machine safety risks.

Schmersal is focused on machine safety devices and safety engineering services, to safeguard machines in compliance with current safety standards, without compromising productivity. The company's comprehensive range of more than 25,000 products includes safety switches, solenoid interlocks, emergency stop switches, security sensors, safety mats with safety function, photoelectric light barriers, and end switches, which include limit switches, position switches, and micro switches. Schmersal's tec.nicum group offers product- and manufacturer-neutral consultation on important matters relating to machine safety and work protection.

CONTEXT

Devin Murray discussed six commonly overlooked and misapplied machine safety requirements and explained how machine designers and operators can avoid making potentially deadly mistakes.

KEY TAKEAWAYS

Risk assessments of a machine are required throughout its life cycle.

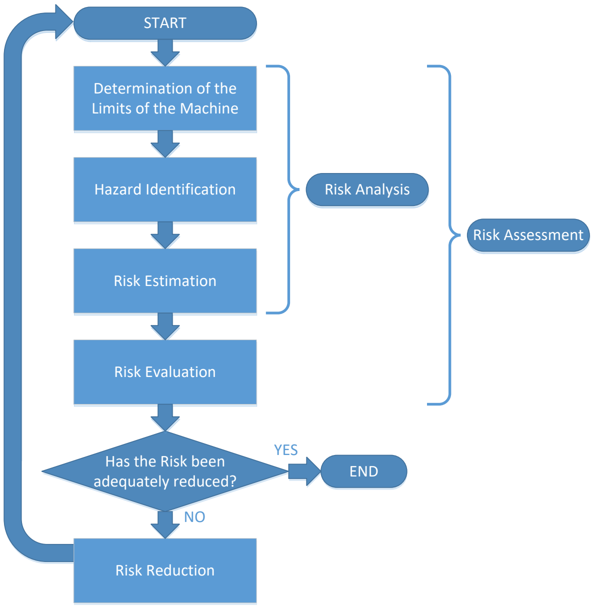
The rate of preventable deaths due to work-related injuries has remained over 3% for the past 20 years. While not all reported deaths are due to machine safety, machines do contribute to these preventable deaths.

Machine guarding has been among the top 10 most-cited OSHA violation for the past several years. Overlooked and misapplied machine safety requirements create hazardous conditions that are at odds with safety procedures that depend on a properly configured machine.

A machine safety risk assessment is a systematic approach of identifying reasonably foreseeable risks and hazards on a machine that can cause harm. Guarding against hazards is required by OSHA, which makes risk assessments highly useful systems for compliance with this requirement.

ISO 12100 provides a guideline for risk assessment, first walking through an evaluation of the whole machine before diving deeper into the individual tasks associated with the machine. This might include operative, maintenance, and technician tasks and corresponding hazards (e.g., electrical hazard) and risks (e.g., electrocution), as well as who is executing those tasks. An ideal risk assessment process will involve a risk assessment team that includes every person who uses the machine and management.

Figure 1: ISO 12100 defines the process of a risk assessment



Commonly Overlooked and Misapplied Machine Safety Requirements

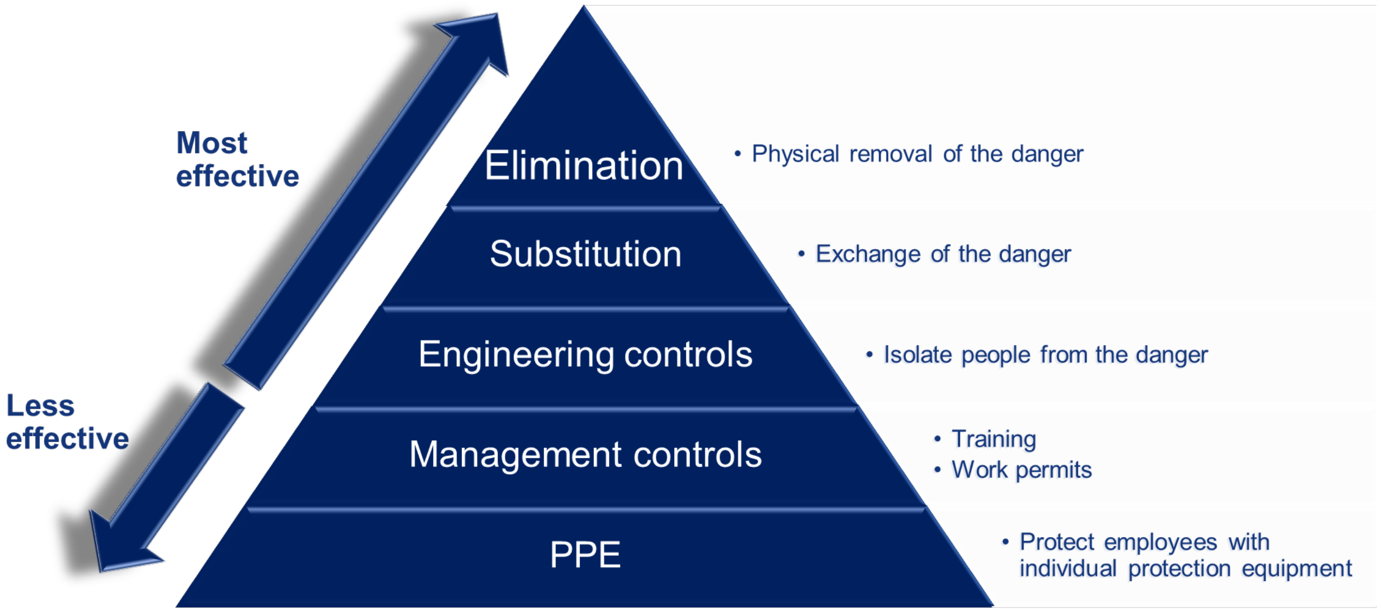
Part of the risk assessment process is quantifying the risk. While the ISO standard offers suggested parameters, companies can create more relevant organization-specific metrics. The primary goal of quantification is to demonstrate due diligence—that the degree, likelihood, and impact of possible harm has been identified and captured as a numerical value, such as a hazard rating number (HRN).

Numerical ratings can help create a system for prioritizing safeguards. For example, companies might use HRNs to determine whether resource priority is placed on guarding the highest-value hazards, guarding multiple low-value hazards, or implementing other control measures. Using number values also helps set checkpoints to confirm that risk is being reduced and whether there is further action that can be taken.

The hierarchy of control visually captures some actions that can be taken to reduce the chances of being exposed to a hazard, with the top items on the pyramid the most effective measures (e.g., removing the risk entirely) and the bottom items the least effective (e.g., PPE, signage). Ideally, an initial risk assessment would be conducted during the design phase to offer the optimal change to implement the most effective measures. However, risk assessments should be conducted anytime anything changes regarding the machine, whether due to an addition, removal, or simply a move.

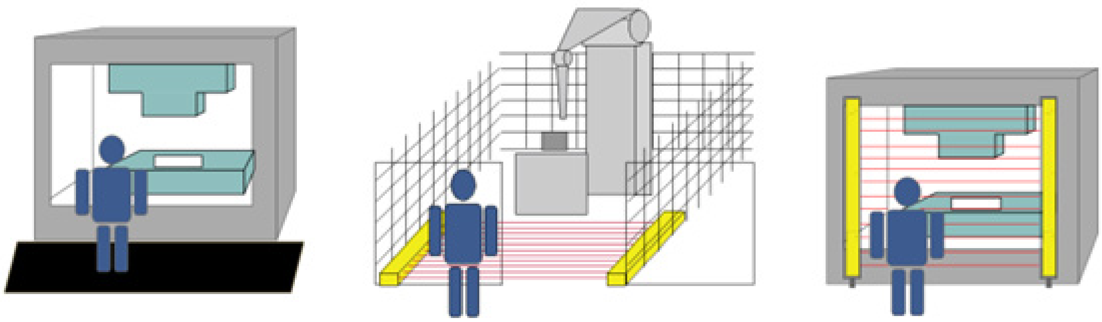
> "A risk assessment is not just a one-and-done deal. You have to do a risk assessment throughout the entire life cycle of the machine."
>
> *Devin Murray, Schmersal USA*

Figure 2: The hierarchy of control



Commonly Overlooked and Misapplied Machine Safety Requirements

Figure 3: Stop-time measurement provides an accurate minimum safety distance



Stop-time measurements are required to know where to install non-separating safety devices.

Stop-time measurement (or stop-time analysis) is a scientific measurement of the time between the triggering of a safety device and a standstill condition of the machine. Placement of guard devices such as light curtains, therefore, cannot be based on a stopwatch timer, an "eyeball" test, or other non-scientific method of measurement.

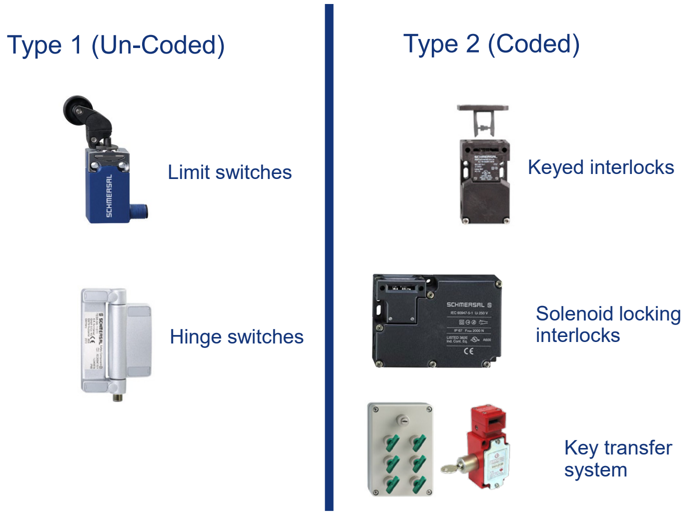
ISO 13855 outlines how to determine what is a safe distance based off a stop-time analysis, which can be conducted via a third-party stop-time analyzer or software in conjunction with a high-speed camera. The standards require that 10 measurements are taken. The highest measured value or the mean plus three standard deviations—whichever is the greater—is considered the stopping time of the machine. This measurement is then used to calculate the safe minimum distance.

Mechanical switches are frequently misapplied.

Positive-break, positive-mode mounting limit switches are activated when a guard door is opened. This requires normally closed contacts within the switch to send the signal to the "safe" function while the guard door is closed. When the door is opened, the limit switch and safety circuit are no longer engaged, stopping the machine. However, limit switches are commonly misconfigured to be manually manipulable, meaning the circuit is engaged when an operator physically presses the switch plunger even though the guard door is open.

A proper configuration that meets the safety standard IEC 60947-5-1—positive mode mounting with a normally closed, positive-break contact—will not engage the circuit when the plunger is manually pressed. These electromechanical devices are often labeled with an arrow in a circle, the international symbol for positive-break contacts. ➔

Figure 4: Electromechanical devices with a normally closed, positive-rate contact



Commonly Overlooked and Misapplied Machine Safety Requirements

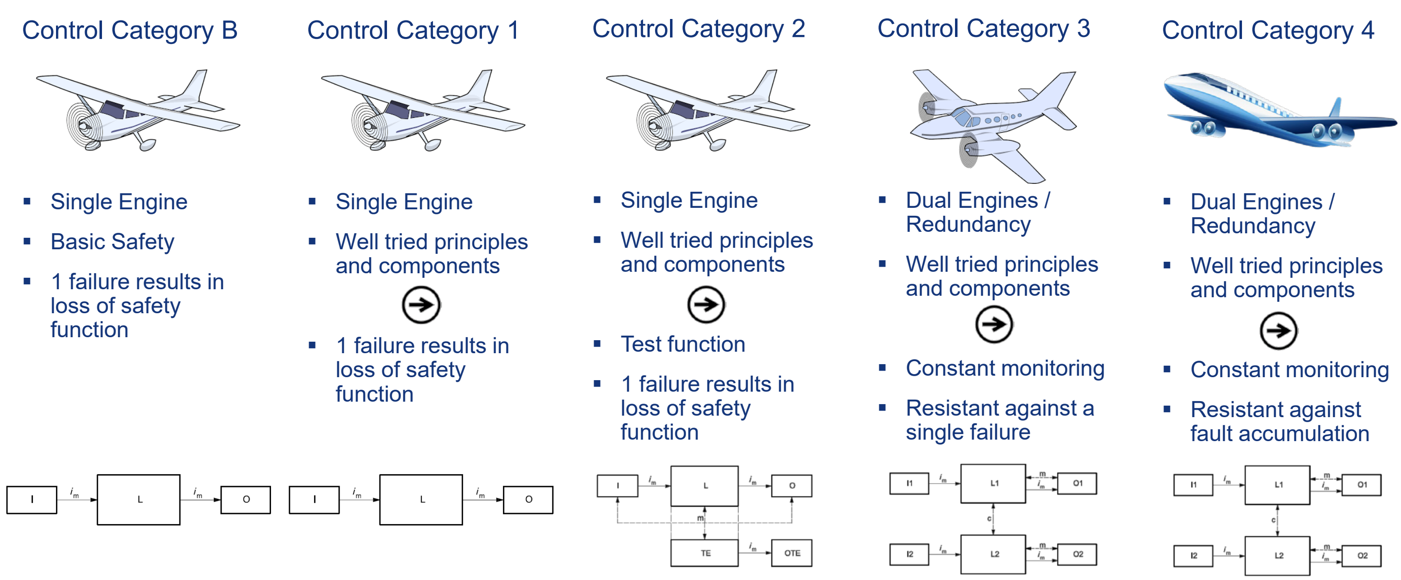
Misapplication can occur when implementing safety categories in the physical design of a circuit.

Safety (or control) categories describe how a safety circuit is physically wired (architecture). The term "control category" originated from a European standard (EN954). Although EN954 has been rendered obsolete, the term is still used today in current relevant safety standards. Current relevant safety categories include B, 1, 2, 3, and 4.

- **B, 1, and 2:** To visualize how safety categories should apply, consider a comparison to airplanes. In a single-engine plane, an engine failure means the plane can no longer fly. The same applies to categories B, 1, and 2. In all categories, a single failure results in loss of safety function and a machine is no longer safely functional.
- **Category 3** introduces redundancy, similar to a dual-engine plane, where a single failure will not render the machine non-functional (control reliability).
- **Category 4** is resistant against fault accumulation.

> "We want to make sure we're using theright category for our safety system. We see this quite often when we look at the schematics on a machine—whether it's a new machine or an old machine that had some upgrades to it—that the control category or the physical wiring of those safety circuits aren't what they need to be to help protect against that hazard."
>
> *Devin Murray, Schmersal USA*

Figure 5: Comparing safety categories to airplanes



Commonly Overlooked and Misapplied Machine Safety Requirements

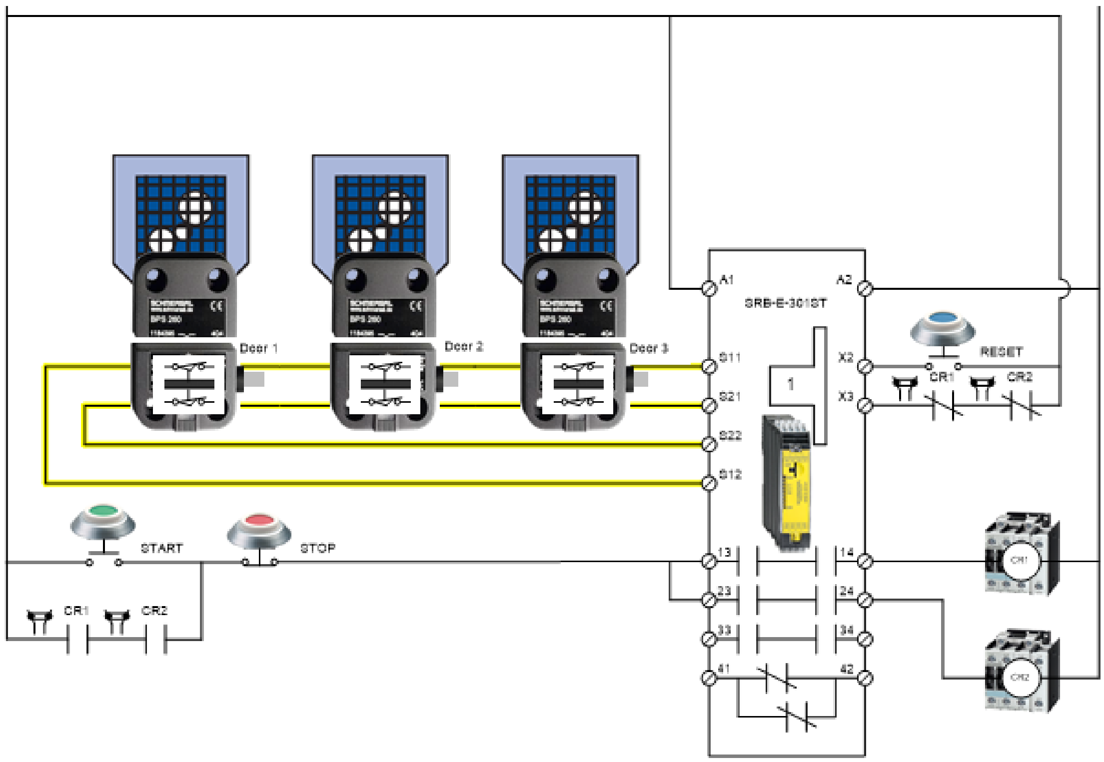
Using series connections for high-risk applications can result in fault masking.

Using a series or daisy chain connection on multiple guard doors can lead to a fault or error being hidden due to the way that the connection is wired. In this case, the system begins in a default input state.
If the interlock sensor on the first guard door in series has a fault on a single channel, the machine will stop running because the monitoring devices will detect a discrepancy in the state change when the door is opened. With this failure detected, the machine will not reset.

However, if an operator then opens a second door downstream, the monitoring device will see all the inputs cleared since the channels (including the faulted channel) are in series. The input state conditions will once again be satisfied, thus masking the fault on door one and negating the safety failure functionality. If the faulted sensor on door one is not corrected, over time a failure can result on channel 2, allowing the machine to run even if the guard door is opened.

Putting policies and procedures in place to immediately troubleshoot and repair in the event of a switch failure will help avoid this issue.

Figure 6: Series connections can lead to fault masking



Commonly Overlooked and Misapplied Machine Safety Requirements

Collaborative robots must undergo a risk assessment.

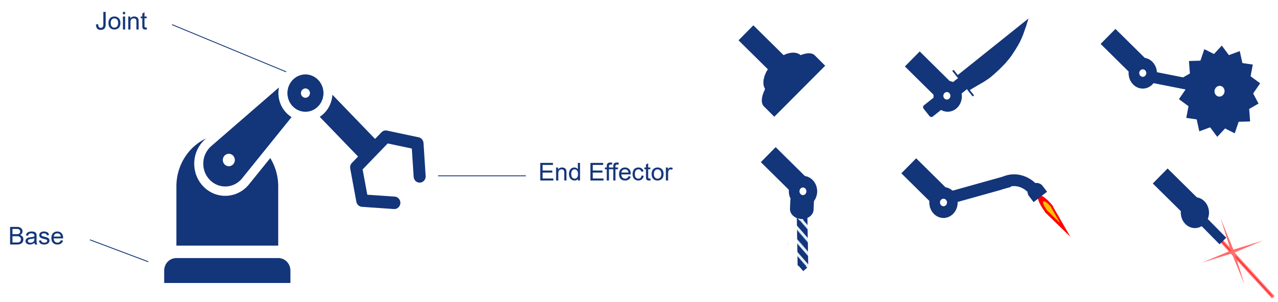
Collaborative robots are machines or equipment designed to be inherently safe. They move at slow speeds, can pick up only low or small payloads, and there are no pinch points. While documentation often references the safety standards met by the collaborative robot, the design and documentation do not automatically qualify the application of the robot as safe. Other factors, such as the environment in which the robot will be used, accompanying equipment in the application, end or arm tooling, and the payload being manipulated, must be considered. A risk assessment that takes these factors into account is still required.

> "You can't say, 'This application is safe because we have a collaborative robot.' What you can say is, 'We can safely use this collaborative robot because we have a safe application.'"
>
> *Devin Murray, Schmersal USA*

Methods to safeguard collaborative robots include:

- **Safety-rated monitored stop** brings the collaborative robot to a safe condition. However, unexpected movement or condition while the monitored stop is enabled will trigger an emergency stop function.
- **Speed and separation monitoring** allows a person to be in the collaborative space while the robot motion is running but within a defined protective distance that prevents the person from coming in contact with the robot.
- **Hand guiding** allows an operator to utilize a hand-operated controller, or even hand-moving the robot directly, to initiate motion commands.
- **Power and force limiting** restricts the power and force to a safe level as determined by predefined thresholds.

Figure 7: The safety of collaborative robots depends on the safety of the application



ADDITIONAL INFORMATION

- **Schmersal.** To learn more, visit schmersalusa.com/home.

BIOGRAPHY

Devin Murray

tec.nicum Services Manager, Schmersal USA

Devin is the tec.nicum services manager for Schmersal's engineering services group in North America. He has written many white papers related to safety standards and general machine guarding, conducted risk assessments and validations, and developed and reviewed the implementation of corporate safety standards. 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.