EHSToday MachineDesign. NED NEW EQUIPMENT DIGEST

Machine Safety Functions — Design and Implementation

Presenter:
Devin Murray, tec.nicum Engineering Services Manager, Schmersal

APRIL 30, 2026

KEY TAKEAWAYS

- Risk assessment is foundational to machine safety functions.
- The design of safety functions must be guided by standards and clear documentation for effective risk reduction.
- Verification and validation are the final steps in the design and implementation of safety functions.

in partnership with

SCHMERSAL THE DNA OF SAFETY

OVERVIEW

Machine safety functions play a central role in reducing risk, protecting operators, and ensuring that equipment operates within safe parameters. Yet many safety functions are misunderstood, improperly designed, or incorrectly validated, leading to gaps in protection and a lack of compliance.

Safety functions are not standalone features—they are the result of a systematic approach to identifying hazards, evaluating risk, and implementing appropriate risk reduction measures designed to rigorous standards to ensure reliability.

Schmersal is a safety industry leader, with 80 years of experience in the design and manufacture of machine safety products, industrial switches, position sensors, and control accessories for a wide variety of applications, focusing on ways to protect machinery operators and maintenance personnel from recognized hazards without compromising productivity.

CONTEXT

Devin Murray explained the purpose and implementation of safety functions.

KEY TAKEAWAYS

Risk assessment is foundational to machine safety functions.

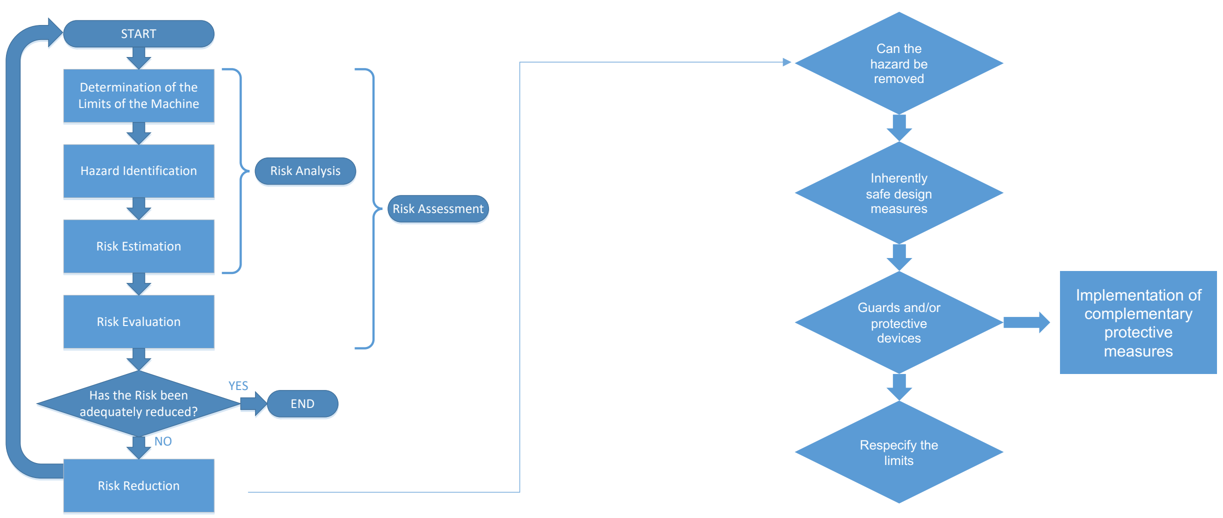
A machine **safety function** is an action specifically designed to reduce or eliminate hazards to personnel and equipment. Safety functions are crucial to ensure a machine maintains a safe state.

Risk assessment is foundational to safety functions. The risk assessment process starts with defining the limits of a machine—how it is used and by whom—followed by identifying the machine hazards. Risks associated with each hazard are then estimated and quantified (risk evaluation). While the exact numerical scale in use might vary between organizations, the goal of risk quantification is to determine whether a given risk is acceptable. If the risk's value is over the threshold of acceptability, a risk reduction measure must be applied.

Ideally, hazards would be removed from the system or even eliminated in the design. However, especially for legacy machines, this is often not possible. In these cases, this is where machine safety functions are introduced, along with complementary protective measures.

Whether or not safety functions are applied, a post risk assessment must be conducted after hazard mitigation, to assess whether the limits of the machine can or should be respecified.

Figure 1: From hazard identification to safety function: the ISO 12100 risk assessment framework



The design of safety functions must be guided by standards and clear documentation for effective risk reduction.

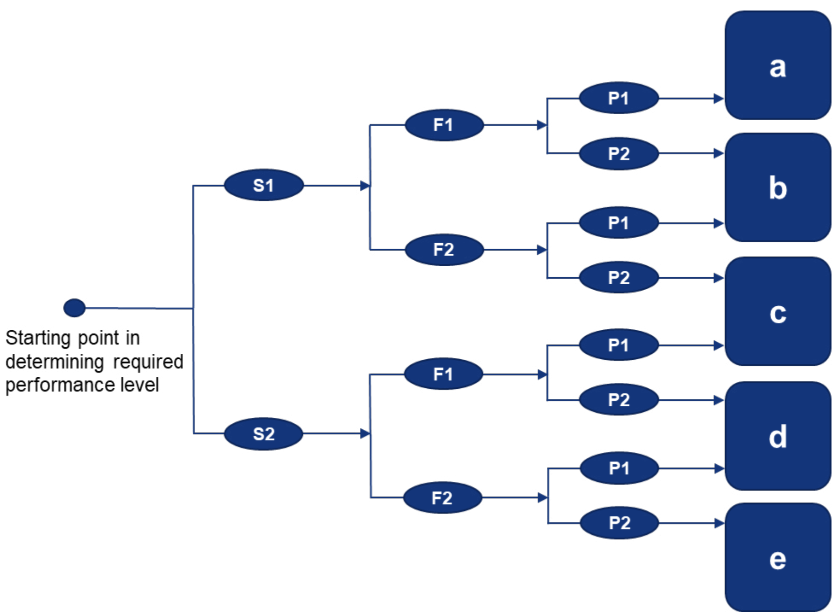
A **safety function** is a function of the machine whose failure would immediately increase risk, for example a guard door interlock that should stop a machine when opened is a safety function.

Safety functions play an important role in functional safety. **Functional safety** (IEC 61508) is the part of overall safety that relates to the control system, ensuring that safety functions work as designed, even under foreseeable faults.

When designing safety functions, safety standards such as ISO 13849 and IEC 62061 provide valuable guidance for how robust the system should be, to ensure that safety functions behave predictably under real-world conditions. ISO 13849 defines five **Performance Levels** (PLs), while IEC 62061 uses three **Safety Integrity Levels** (SILs). Both standards calculate levels using factors such as severity of injury, frequency of exposure, and the probability of avoiding hazards.

> "Whether looking at performance levels . . . or SIL ratings, at the end of the day, it's: 'How reliable is this particular safety function?'"
>
> – *Devin Murray, Schmersal*

Figure 2: Performance Levels (L) and Safety Integrity Levels (R) guide safety function design

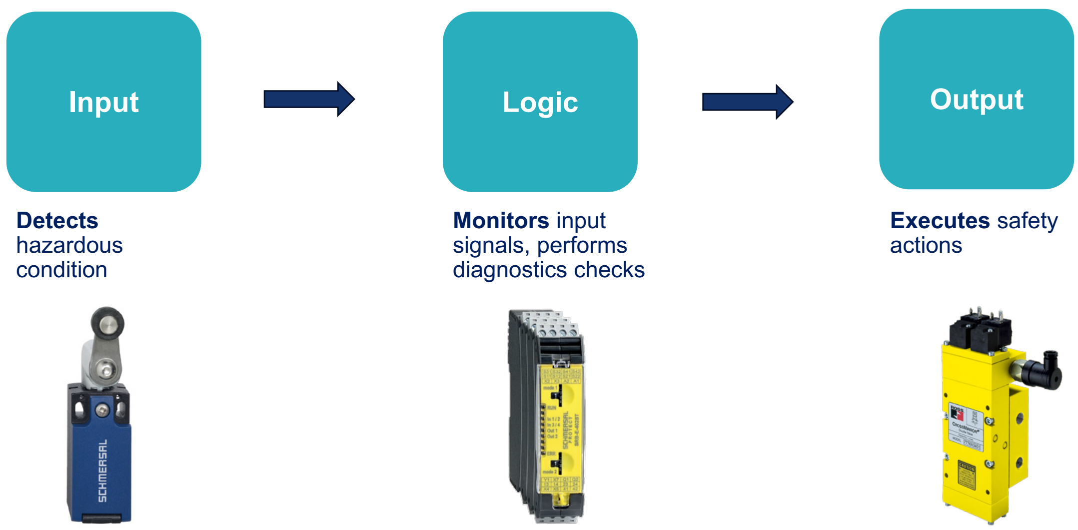


Severity (Se)	Class (Cl)				
	3 to 4	5 to 7	8 to 10	11 to 13	14 to 15
4	SIL 1	SIL 2	SIL 2	SIL 3	SIL 3
3		(OM)	SIL 1	SIL 2	SIL 3
2			(OM)	SIL 1	SIL 2
1				(OM)	SIL 1

Categories are the classification of the subsystem with respect to its resistance to faults and define how a safety circuit should be wired. Every safety function comprises three subsystems:

1. **Input** detects a hazardous condition (e.g., light curtain senses intrusion, limit switch detects position).
2. **Logic** monitors the input signals, performs a diagnostic check to ensure safety function components operate correctly, and determines whether to trigger a response.
3. **Output** executes the safety action.

Figure 3: All safety functions have input, logic, and output subsystems



According to ISO 13849, a **Safety Requirements Specification (SRS)** should contain the requirements for the safety functions that have to be met by the safety-related control system—it is a blueprint that details key information such as the description of the safety function, under which conditions it is triggered, what the safety function should do, and what performance level it must meet.

A well-defined SRS will provide detailed guidance for safety function design and component selection, to ensure safety objectives are met. All safety functions must be implemented so they are not easily bypassed.

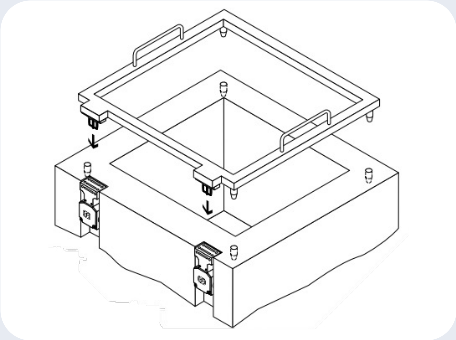
Common Types of Safety Functions

There are several different types of commonly used safety functions:

Safety stop initiated by a safeguard

Guard monitoring uses a key, limit, or hinge switch to trigger an immediate stop when a guard door is opened. These safety devices must not be used as an end stop, as this can damage switches, resulting in a single point of failure.

Figure 4: Lifting a guard door disengages redundant monitoring switches, signaling to stop a motor



Guard locking

Guard locking builds on guard monitoring and is typically used when there is residual motion. It ensures the guard door remains locked after a stop command has been issued until the machine reaches a safe state, and prevents restarting until the guard door is again closed and locked.

Figure 5: Using a solenoid for guard locking

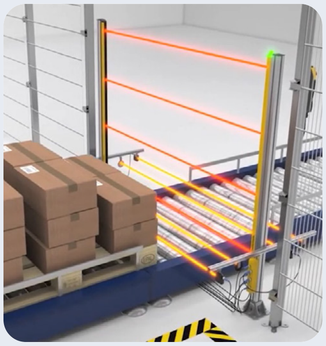
Presence-sensing

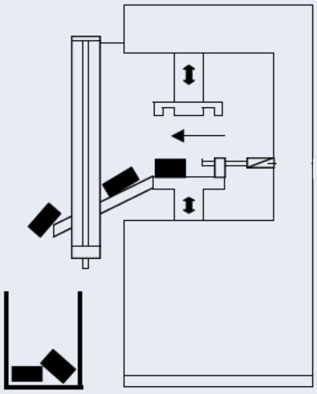
Presence-sensing safety functions signal a safe stop upon detection of an operator's body or hand tool using input devices such as light curtains, scanners, and safety mats. Standards such as ISO 13855 use machine stop time measurement to calculate the safe minimum distance for the safety device installation.

Muting is the automatic temporary suspension of a safety function by the safety-related control system, typically to allow materials to pass through (e.g., a pallet moving through a light curtain) without stopping the machine but still preventing access by personnel.

Blanking is an optional function that permits an object of a size greater than the detection capability of the light curtain to be located in the detection zone without causing an OFF state. Blanking defines a specific beam (or two consecutive beams, depending on the application) along the light curtain to be non-triggering if interrupted, enabling objects to remain in the sensing area without triggering a safe stop.

Figure 6: Muting (L) and blanking (R) allow some passing without triggering a stop





Two-hand control

Two-hand control systems are designed to keep an operator's hands away from a hazardous condition by requiring both hands to actuate and maintain the machine cycle. Two-hand control systems require anti-tie-down monitoring logic to ensure both palm buttons are actuated at the same time. It should not be possible for operators to actuate both buttons using only one hand.

Other safety functions include:

- **Safe enable/Hold-to-run**, which requires continuous hold to maintain machine function and is often used along with additional safety functions (e.g., safe speed, safe direction).
- **Safe speed/motion**, which monitors machine speed, torque, force, position, etc. to ensure it stays within safe limits.
- **Mode selection**, which allows operators to switch between operational modes, engaging secondary safety functions if mode switching disables primary safety functions.
- **Reset** allows the safety circuit to be reengaged and is also considered a safety function. Resets must not create hazard situations and must be placed outside the hazard zone.
- Emergency stops (E-stops) are **secondary safety functions**. E-stops should only be added after primary safety functions have been applied, to further reduce risk in emergency situations only.

Figure 7: Two-hand control systems protect only the operator

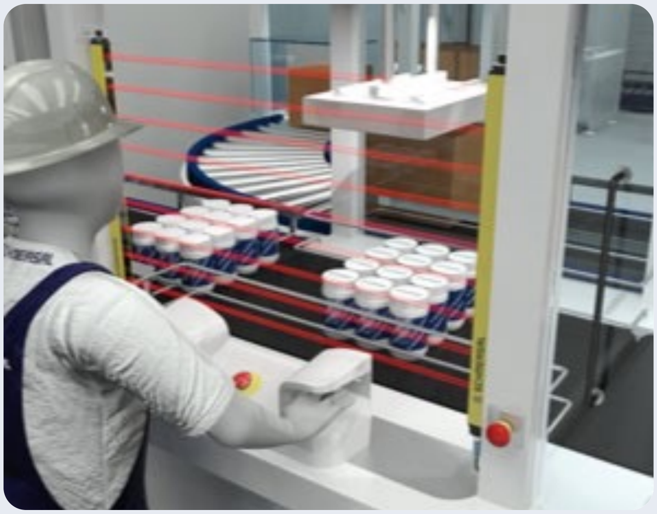


Figure 8: E-stops must be initiated by a single human action

> "Emergency Stop is not a primary safety function . . . that is not how the E-stop is intended to be used. . . Hopefully, we never have to use the E-stop, but it is for an emergency condition."
>
> – *Devin Murray, Schmersal*

Verification and validation are the final steps in the design and implementation of safety functions.

After adding safety functions, the machine must be reassessed to determine whether any unmitigated hazards remain. The verification process ensures that the safety function meets its required performance level, usually through specific calculations using software tools such as SISTEMA.

Validation confirms, by examination or other provisions of objective evidence, that the requirements for a specific intended use are fulfilled by introducing faults to the system and testing it to ensure it responds with the appropriate safety actions.

ADDITIONAL INFORMATION

To learn more, visit Schmersal

BIOGRAPHY

Devin Murray
tec.nicum Engineering 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. 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.