EHS Today MachineDesign. NED NEW EQUIPMENT DIGEST PLANT SERVICES

EXECUTIVE SUMMARY

Applying ISO 13849 Functional Safety to Machines in the USA

Devin Murray, tec.nicum Services Manager, Schmersal USA

OCTOBER 25, 2023

KEY TAKEAWAYS

- What is ISO 13849? A brief overview.
- There are specific U.S. standards for machine builders and end users that are related to ISO 13849.
- How to apply ISO 13849 to machines.

in partnership with

SCHMERSAL
THE DNA OF SAFETY

Applying ISO 13849 Functional Safety to Machines in the USA

OVERVIEW

Functional safety and performance levels are key elements behind the machine safety standard ISO 13849. Being a global harmonized standard, it is accepted worldwide in designing the safety-related parts of the control system of a machine. Understanding the theory behind ISO 13849 and implementing the standard can be challenging, but doing so is critical to achieving functional safety.

In this summary, Schmersal tec.nicum Services Manager and FS Eng (TÜV Rheinland ID-No. 4274/11 Machinery) Devin Murray provides an overview of ISO 13849, when and how to use it, and how it applies to machine safety in the United States.

KEY TAKEAWAYS

What is ISO 13849? A brief overview.

IEC 61085 defines Functional Safety as "Part of the overall safety relating to the EUC [equipment under control] and the EUC control system that depends on the correct functioning of the E/E/PE [electrical/electronic/programmable electronic] safety-related systems and other risk reduction measures." Meaning, the ability or the reliability of a machine to effectively deliver its safety functions.

Many other standards have been built off this concept, including for process engineering, nuclear applications, and machinery. ISO 13849 for machinery defines **Performance Level** as a "discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions." Meaning, the description of how reliable the safety function is, within the range of performance levels a, b, c, d, or e (**a** being the lowest and **e** the highest).

> "Safety devices are designed to fail-to-safe. However, there exists the possibility of failing in a dangerous state. Functional safety as defined by ISO13849 looks into minimizing this possibility."
>
> *Devin Murray, Schmersal USA*

A performance level is made up of four different elements:

1. Category

This element describes the physical wiring of the safety circuit. Category classifications are:

- **B.** Basic controls (e.g. on/off) wired as a single channel.
- **1.** Single-channel, using well-tried principles and components.
- **2.** The characteristics of Category 1, with the addition of a test function to monitor for faults within the single channel system.
- **3.** A dual-channel system for redundancy with a monitoring component, resistant against a single fault.
- **4.** A dual-channel system for redundancy with a monitoring component, which can withstand multiple faults.

2. Diagnostic Coverage

This element describes the ability of the safety system to detect a dangerous failure. For the safety function to perform as expected requires a calculation to prove its effectiveness. One of the parameters in that calculation is diagnostic coverage.

Range classifications of diagnostic coverage include:

- None. Dangerous failure detected in less than 60% of instances.
- Low. Dangerous failure detected in 60-89% of instances.
- Medium. Dangerous failure detected in 90-99% of instances.
- High. Dangerous failure detected in 99% of instances.

Figure 1: A safety PLC can be used for system failure detection

3. Mean Time to Dangerous Failure ($MTTF_D$)

Components might experience wear and tear that can push a system beyond its mechanical limits. Calculating $MTTF_D$ provides an estimation of when a device may have a high probability of experiencing a dangerous failure, based on its demand rate.

4. Common Cause Failures

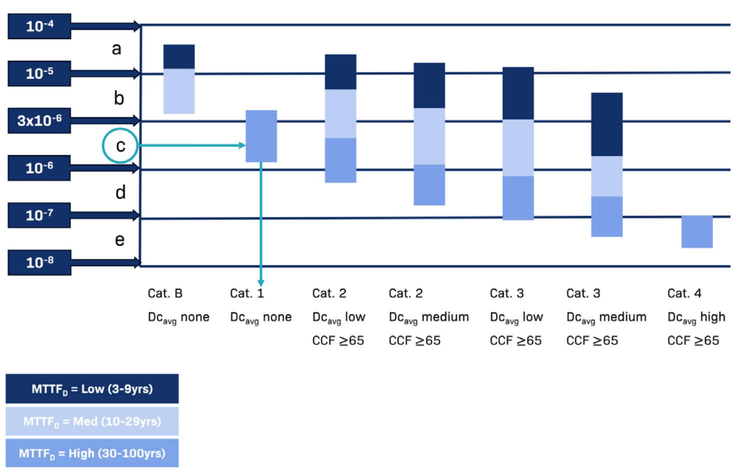
ISO 13849 outlines eight scored procedures to implement to help protect against a common failure that can affect the entire safety function. Executing enough of those procedures to obtain a score of 65 or higher ensures that the safety system is resistant against a common cause failure. Example procedures include separation between signal paths, component diversity, well-tried components, and competence/training.

Functional safety and performance levels are defined and measured for safety functions. According to ISO 13849, a Safety Function is defined as the "function of the machine whose failure can result in an immediate increase of the risk(s)." Examples of safety functions include presence-sensing devices used to initiate a safe stop, enabling devices, safe speed monitoring, and emergency stops. ISO 13849 provides guidance on how to wire these safety functions to achieve a specific performance level.

Tip: SISTEMA is a free, downloadable performance level calculator.

Figure 2: The table provided in ISO 13849 offers guidance on how to reach a desired performance level

Probability of Dangerous Failure per Hour (PFH_D)



Applying ISO 13849 Functional Safety to Machines in the USA

There are specific U.S. standards for machine builders and end users that are related to ISO 13849.

A safety standard can be categorized as three different types:

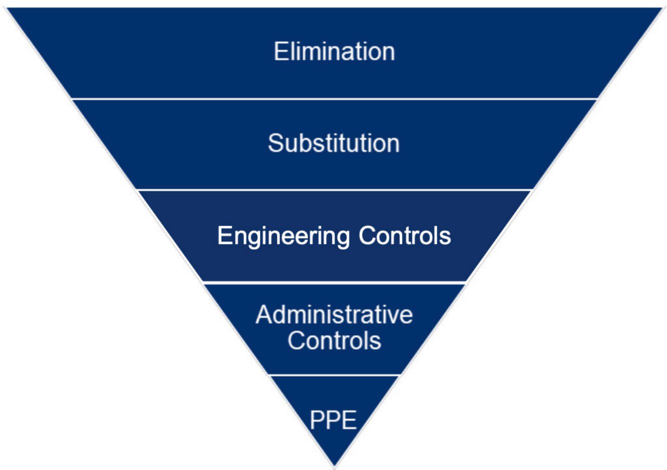
- Type-A standards (basic standards) give basic concepts, principles of design, and general aspects that can be applied to machinery. ANSI B11.0 (Safety of Machinery) is an example of a Type-A standard in the U.S.
- Type-B standards (generic safety standards) deal with one or more safety aspects or one or more types of engineering controls that can be used across a wide range of machinery. ANSI B11.19 (Performance Requirements for Risk Reduction Measures) and ANSI B11.26 (Functional Safety for Equipment) are examples of Type-B standards in the United States.
- Type-C standards (machine safety standards) deal with detailed safety requirements for a particular machine or group of machines. ANSI PMMI B155.1 (Packaging and Processing Machinery Safety Requirements) and ANSI RIA 15.06 (Robot and Robot Systems Safety Requirements) are examples of Type-C standards in the United States.

All examples listed reference "Control systems performing safety functions," categories, and/or ISO 13849.

How to apply ISO 13849 to machines.

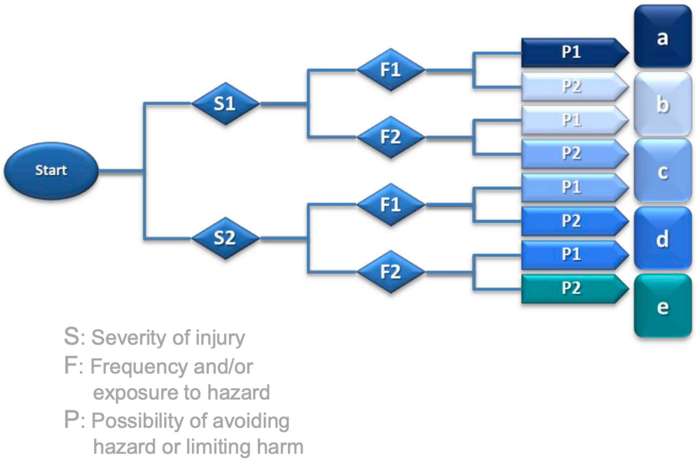
To apply ISO 13849, the first step is to conduct a hazard analysis, identifying potential sources of harm. For each hazard, a risk analysis is conducted next to determine the probability and severity of injury if exposed to the hazard. Regardless of the methodology used, quantifying the risk guides the actions taken to safeguard the hazard according to the Hierarchy of Control Over Hazards.

Figure 3: Hierarchy of control over hazards



Engineering controls are frequently applied to safeguard hazards. With the introduction of a safety function through engineering controls, the performance level of the control must be determined. ISO 13849 provides a decision tree for assessing functional safety based off severity of injury, frequency of exposure, and possibility of avoiding the hazard.

Figure 4: A decision tree for assessing functional safety of engineering controls



Applying ISO 13849 Functional Safety to Machines in the USA

Once the performance level requirement is determined, the circuit can be designed using guidance from the table provided in ISO 13849 to identify the optimal combination of category, diagnostic coverage, $MTTF_D$, and common cause failures.

After designing and implementing the safety function, the next step required by ISO 13849 is validation, or testing whether the safety function will work as expected.

When applying ISO 13849, beware of misconceptions surrounding the standard. Correctly understanding the standard requirements will yield a more efficient and effective application.

Table 1: Misconceptions surrounding the ISO 13849 standard

Misconception	Reality
Performance levels are for an entire machine	**Performance levels are for safety functions.** Certain safety functions may require a higher performance level than others. On a machine, there are usually multiple hazards requiring different control measures at varying performance levels.
Electrical mechanical devices cannot be used for a performance level.	**These devices can be used in the highest PL achievable.** Electrical mechanical components which meet their applicable Type B safety standard requirements are considered well-tried components. Therefore, they are relevant to machine safety and are capable of achieving PLe Category 4, if implemented correctly.
PL should be applied to existing safety functions.	**PL applies to new safety functions.** Because PL assesses probability of a dangerous failure with the considerations of demand rates, only upon replacement (new safety functions on new machines) or upgrade (new safety functions on old machines) of a machine should ISO 13849 be applied.
ISO 13849 is fulfilled once the PL is confirmed.	**ISO 13849 is a two-part standard.** ISO 13849-1 includes PL requirements and designs. However, ISO 13849-2 requires validation: proof that the system performs the way it is support to, even under foreseeable conditions.

ADDITIONAL INFORMATION

To learn more about Schmersal, visit schmersalusa.com

Applying ISO 13849 Functional Safety to Machines in the USA

BIOGRAPHY

Devin Murray, tec.nicum Services Manager, Schmersal USA

Devin Murray 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.