MachineDesign. NED New Equipment Digest. EHSToday.

EXECUTIVE SUMMARY

Why Machine Safety Is Not Complete Without Validation

Peter Rigakos, Professional Engineer, BSEE, Schmersal

APRIL 27, 2022

KEY TAKEAWAYS

- Risk assessment and validation are closely related and should always be done together.
- Validation is split into two phases. Phase 1 is analysis and review of schematics. Phase 2 is functional testing, where safety functions are tested after the system is built.

in partnership with

SCHMERSAL
THE DNA OF SAFETY

Why Machine Safety Is Not Complete Without Validation

OVERVIEW

Conducting a risk assessment is not enough to declare a system safe and ready to use in production. Validation is necessary to complete the machine safety evaluation process. Using the Schmersal machine safety mindset and fundamental building blocks, the design, installation, and testing of safety systems can be correctly executed, along with validation phases to establish machine safety.

CONTEXT

Following previous webinars on Building a Machine Safety Mindset and Risk Assessment Methods, Peter Rigakos discussed why validation is essential and summarized the phases and steps of validation required to complement risk assessment and ensure machine safety.

KEY TAKEAWAYS

Risk assessment and validation are closely related and should always be done together.

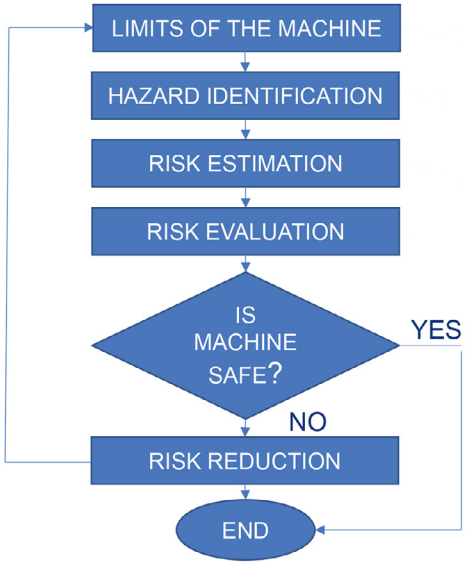
Risk assessment is fundamentally important to all safety. It's the beginning of the path—the discovery phase—to properly applying safety to facilities, equipment, and machines. At the other end of the path is validation; machine safety is not complete without validation.

Figure 1: Building blocks for machine safety

> Validation is our final step [in ensuring machine safety].
>
> *Peter Rigakos, Schmersal*

Many machine-related injuries in facilities could have been prevented. Sometimes, an injury is the result of a guard that was bypassed, or a legacy machine that did not have the safeguarding installed. At other times, the cause is clear negligence that is easy to spot. However, there are some cases in which determining why an injury happened it not so obvious. The answers are hiding in the wiring or how the machine was safety programmed. These cases point to fundamental errors that could have been caught if the machine was properly validated.

Figure 2: The steps of risk assessment



These steps (shown in Figure 2) are fundamental to ensure that risk assessments are properly conducted. The goal of risk assessment is not to determine whether the machine is worth upgrading. It is to determine if a machine is safe. If the risk assessment shows that a machine is not safe, it should be upgraded, regardless of how long it has left in service.

Why Machine Safety Is Not Complete Without Validation

The gap between risk assessment and upgrade is where validation needs to be done. On existing equipment, this should be addressed and prioritized, but not rushed. Rushing increases the risk of installing the wrong components, installing without review of the wiring, etc.

Part of the risk assessment process is identifying control measures that are chosen to mitigate risks. Control measures include Safety Integrity Level (SIL), which can only be used on electronic devices, while Performance Level can be used for electronic, pneumatic, or hydraulic devices. (When designing safety circuits for machines, typically electronic and either pneumatic or hydraulic are used.) Once the Performance Level or SIL has been chosen, this is where the validation process begins.

Performance Level is needed in a risk assessment if the solution to mitigate the risk is an electrical device. However, if the control measure to mitigate the risk uses a mechanical device, a Performance Level is not required.

Validation is more than testing the machine physically once it is built. It also requires checking the drawings to ensure the safety function is wired as per the Performance Level called out in the risk assessment. Then, when the system is built, validation continues with physical checks of the safety function by applying test faults.

When risk assessment is provided as a service, if the assessment suggests the use of an electronic, pneumatic, or hydraulic device, it is important to ensure that the Performance Level required is also noted as part of the service.

Validation is split into two phases. Phase 1 is analysis and review of schematics. Phase 2 is functional testing, where safety functions are tested after the system is built.

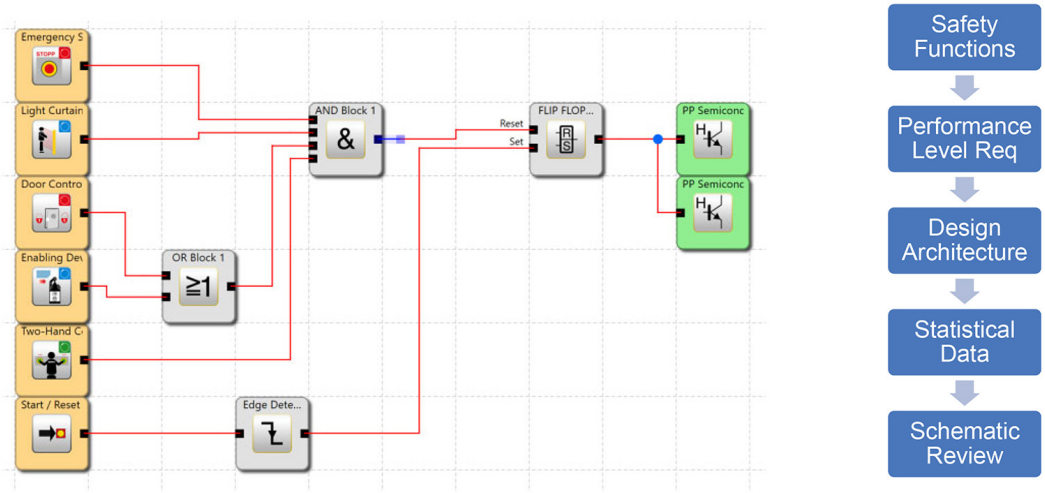
Details of each phase of validation are summarized below.

Phase 1, Design Validation — This includes:

- **Safety functions.** Each safety function (input, logic, output) needs to be determined and listed accordingly.
- **Performance Level required.** This is needed for each safety function and comes from the risk assessment.
- **Design architecture.** Determine which category applies to the design. Category B, 1, 2, 3, or 4, and Performance Levels work together to make a circuit safe. The controls safety standard ISO 13849 offers guidance on the Performance Level required.
- **Statistical data.** This is data about architecture, common cause failure (CCF), diagnostic coverage rate (DCavg), and average component quality (MTTF). The majority of this information is provided by the manufacturer of the device and can be put it into a formula to calculate Performance Level. If statistical data for a device is unavailable, the Annex of ISO 13849 provides approximate data to input. Remember: A chain is only as strong as its weakest link.
- **Review schematics.** Schematic review should be done by a professional other than the original designer and should confirm all items in the previous three steps. Safety PLC (SPLC) programs, or any kind of safety device programming, should be a part of the schematic review process to catch any potential errors.

Why Machine Safety Is Not Complete Without Validation

Figure 3: An example of block programming



Phase 2, Functional Testing — This is the process of testing each safety function after Phase 1 is complete. Functional testing can be conducted on a new machine if the machine is built first, in the location where it will be in production, and on an existing machine, provided it will not be moved to a new location. If the machine is moved, validation should be repeated.

For each safety function, short circuits and faults should be deliberately applied to confirm that the system will fail to a safe state.

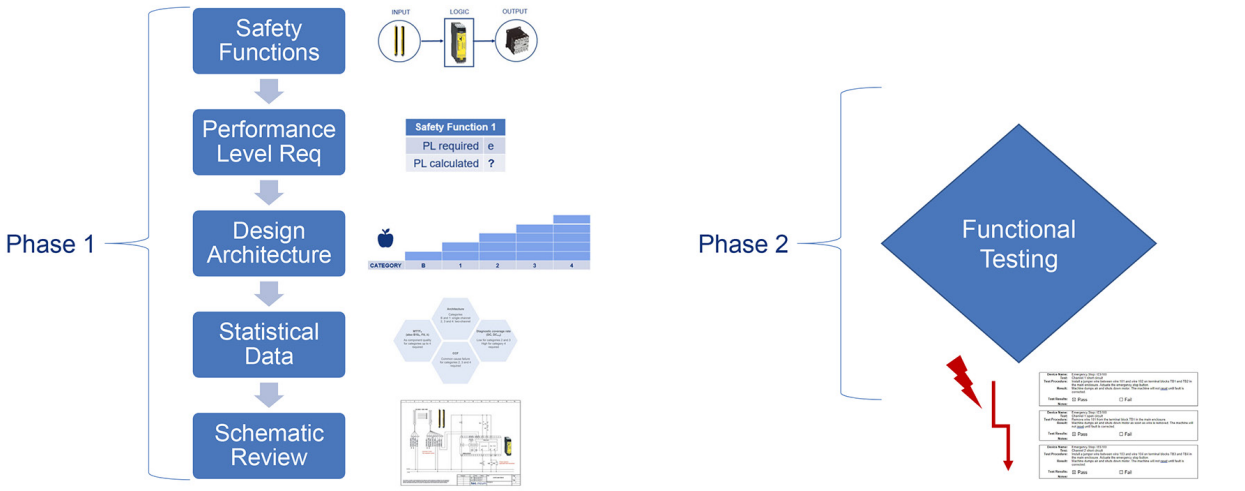
Although testing is done during Phase 2 of validation, test plans can be prepared by the designer in Phase 1 as the system is being designed. Some organizations create test plans after the design is complete and/or use a third-party company to create the test procedure using drawings and information from Phase 1. Review of SPLC programming should be happening during the schematic review of Phase 1; however, if this was not completed in Phase 1, it must be tested as part of Phase 2.

After the design process and initial testing, subsequent testing should occur any time components are affected by an update or installation, when adding other systems, or when growing a system or machine. In addition, when standards change or there is new research released internally, staff should be updated on the changes and the associated new requirements.

Third-party companies can help with some or all of the validation steps and provide the documentation.

Why Machine Safety Is Not Complete Without Validation

Figure 4: Phases 1 and 2 of validation



ADDITIONAL INFORMATION

- **SISTEMA.** The SISTEMA software utility provides developers and testers of safety-related machine controls with comprehensive support in the evaluation of safety in the context of ISO 13849-1.
- **PLx.** The PLx device can assist in testing M12 devices effectively. To learn more, visit https://www.plxdevices.com.
- **Schmersal.** Schmersal is focused on machine safety devices and safety engineering services to safeguard machines in compliance with current safety standards, without compromising productivity. To learn more, visit https://www.schmersalusa.com/home.

BIOGRAPHY

Peter Rigakos

Professional Engineer, BSEE, Schmersal

Peter is a licensed Professional Engineer; he holds a Bachelor of Science in Electrical Engineering from Saginaw Valley State University and an MBA from Purdue University West Lafayette. Peter started his career as an Electrical Engineer designing and reviewing automated safety systems primarily for automotive manufacturing facilities. Since that time, Peter has gained extensive knowledge in machine safety for various industries, allowing him to obtain his TUV Functional Engineering certification.

Before joining Schmersal in 2012, Peter worked for a diverse range of organizations, including consulting, integration, and engineering design, all within the industrial automation industry. Each of these roles prepared him to understand the industrial machine safety industry. Peter also supports technical colleges by offering a strategic plan for instructors to implement topics related to machine safety automation into their curriculum. The safety curriculum includes hands-on workshops and lectures on issues related to machine safety automation.