Life Is On Schneider Electric

Machine Safety: Functional Safety and Implementation of the New Machinery Directive

Executive summary

This paper discusses the changes in standards for the design of safety-related control systems. EN 62061 and EN ISO 13849-1 both deal with the functional safety of machine control systems, but they use slightly different terms and techniques to determine performance. Many users are confused by conflicting guidance from suppliers, who may prefer one standard over another. This paper clarifies the differences between EN ISO13849-1 and EN 62061 and discusses the main points machine builders should keep in mind for each.

Contents

New European Machinery Directive

The European Machinery Directive 2006/42/EC, published in 2010, supersedes the former Machinery Directive 98/37/EC.

Users of EN 954-1 will be familiar with the old “risk graph” used to design safety-related parts of electrical control circuits in categories B, 1, 2, 3 or 4. Users had to subjectively assess the severity of injury, the frequency of exposure, and the possibility of avoidance in order to determine the required category for each safety-related part. This category then specified the required behaviour of the safety circuit when it is facing an error but did not address the likelihood of an error occurring.

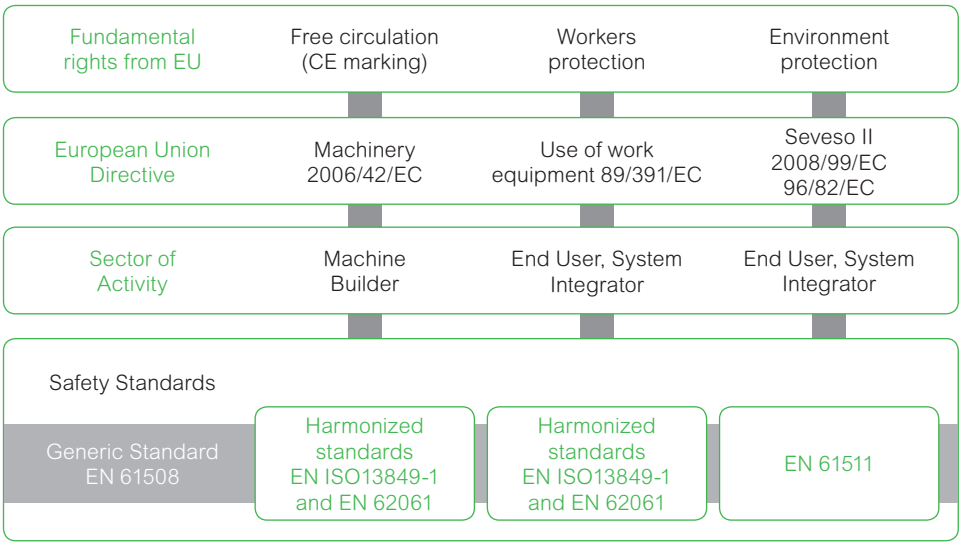
With the increasing use of programmable and non-programmable electronics in these systems, safety can no longer be measured purely in terms of categories. Furthermore, the previous standard provides no information on the probability of failure (EN ISO 13849-1).

In recent years, the concept of *functional safety* has emerged. It refers to the overall safety of the Equipment Under Control (EUC) and the EUC control system. Functional safety depends on the correct functioning or operation of the electrical/electronic/programmable electronic systems and other technology safety-related systems, as well as external risk reduction possibilities. It is not an attribute of any particular component or specific kind of device, but rather concerns the entire EUC and its control system. Functional safety applies to all the parts contributing to the performance of a safety function, e.g. input “devices”, such as safety switches or safety sensors, logic solvers such as safety modules, safety controllers and safety PLCs (including their software and firmware), as well as output devices such as contactors, variable-speed or servo drives.

The term *correct functioning* means that the operation is correct and not merely what is expected. Therefore, appropriate selection of the functions is essential. In the past, designers tended to choose components in the highest-level category of EN 954-1, instead of choosing components in a lower category which might actually offer more suitable functions. This was often due to the misconception that EN 954-1 categories are hierarchical, e.g. that category 3 is “better” than category 2.

The new EN ISO 13849-1 and EN 62061 standards help address the weaknesses of EN 954-1. Although they still require consideration of circuit architecture as in EN 954-1, they also take into account the reliability of the safety circuit components and the circuit's ability to detect/diagnose errors as well as the probability of common cause failure (EN ISO 13849-1). The performance of each safety function is specified as either a SIL (Safety Integrity Level 1, 2 or 3) under EN 62061, or a PL (Performance Level a, b, c, d or e) under EN ISO 13849-1.

European Directives and Safety Standards Overview according to sector of activity

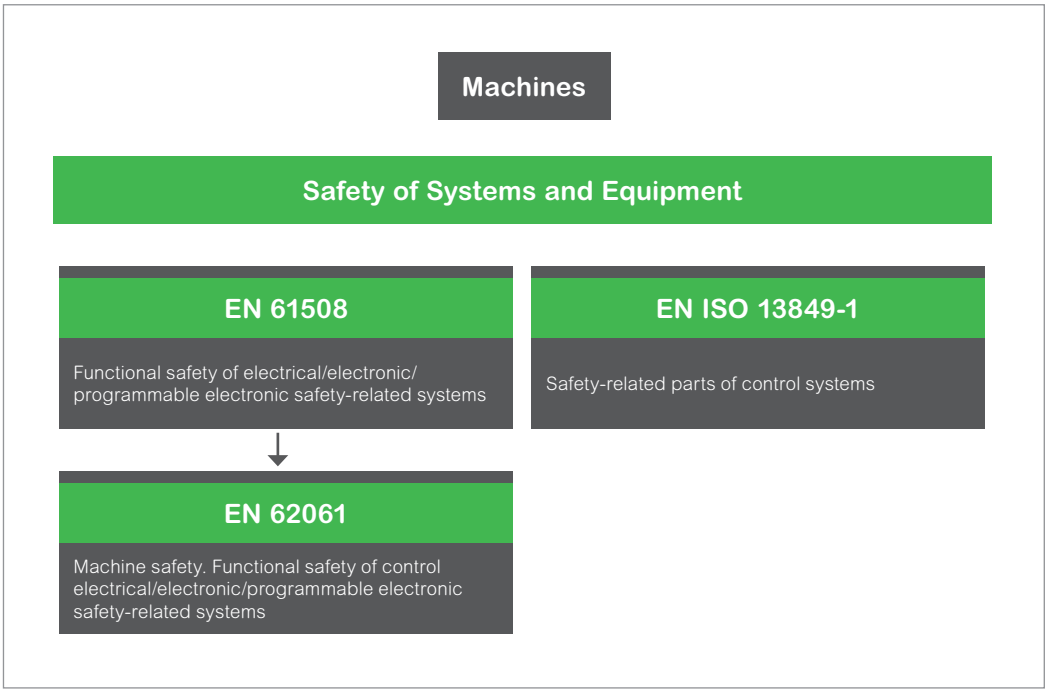


Functional Safety Approach

The new functional safety standards are intended to encourage designers to focus more on the functions that are necessary to reduce each individual risk as well as the performance required for each function, rather than simply relying on particular components. These standards make it possible to achieve greater levels of safety throughout the machine's life.

Under the old standard, EN 954-1, categories (B, 1, 2, 3 and 4) dictated how a safety-related electrical control circuit must behave when facing an error. Designers can follow either EN ISO 13849-1 or EN 62061 to demonstrate conformity with the Machinery Directive. These two standards consider not only whether an error could occur, but also how likely it is to occur.

This means there is a quantifiable, probabilistic element in compliance: machine builders must be able to determine whether their safety circuit meets the required Safety Integrity Level (SIL) or Performance Level (PL). Panel builders and designers should be aware that manufacturers of the components used in safety circuits (such as safety detection components, safety logic solvers and output devices like contactors) must provide detailed data on their products.



This data can be a minefield and the new standards have different requirements, it can be difficult to understand the meaning of all the figures and acronyms.

Here are the main points machine builders should keep in mind for EN ISO 13849-1:

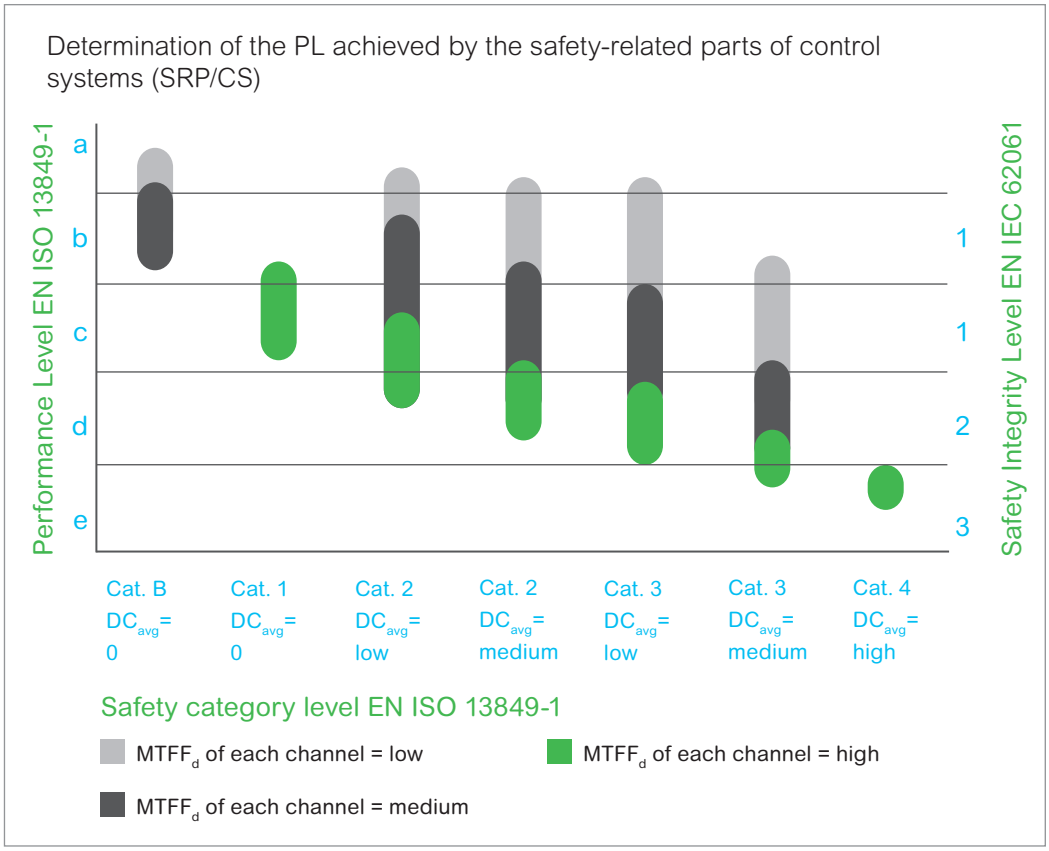
- **Performance Level (PL)** is determined by the circuit architecture (similar to categories B, 1, 2, 3, and 4 in EN 954-1) as well as by the MTTFd and DC. The ISO standard defines five Performance Levels ranging from PL a (the highest error probability) to PL e (the lowest). If a manufacturer states a specific PL for a component (such as a safety module), it means this is the highest PL that a circuit incorporating the component can achieve.
- **Mean Time To Dangerous Failure (MTTFd) (EN ISO 13849-1)** is the average period before the failure of a component will cause a failure of a safety function. MTTFd is rated as high (30-100 years), medium (10-30 years) or low (3-10 years). Note: if the component's MTTFd is 100 years, this does not guarantee it will not have an error before.
- **Diagnostic Coverage (DC)** is the ability of a component or circuit to detect/ diagnose an error concerning it (a short circuit, for example). The higher the DC, the lower the probability of unidentified, potentially hazardous hardware errors.
- **Common Cause Failures (CCF) (EN ISO 13849-1)** are issues in dual channel architecture due to a similar error in both channels (such as a short circuit). Steps can be taken to prevent common cause failures; for instance, the designer can use different components operated in different modes in dual-channel systems.

Key points for EN 62061:

- **Safety Integrity Level (SIL)** is the discrete level for determining the safety integrity requirements of the safety-related control system. The standard defines three levels, from one (low) to three (high). Should a manufacturer claim a specific SIL for a component (such as a safety PLC), then that is the maximum SIL that can be claimed for any system using this component as a subsystem.
- **SIL Claim Limit (SILCL)** applies to subsystems within a safety system. A subsystem is defined as a part of a safety system/circuit, of which an error would bring about a breakdown of the safety function. SILCL is the highest SIL that can be claimed regarding architectural constraints and systematic safety integrity.
- **Probability of Dangerous Failure per Hour (PFH) (EN 62061)** is a measure of the dependability of a component, a subsystem, or an entire safety system/ circuit – it corresponds to MTTFd in EN ISO 13849-1.
- **Safe Failure Fraction (SFF) (EN 62061)** of a subsystem is the ratio of the average rate of safe errors plus dangerous detected errors of the subsystem to the total average error rate of the subsystem.

B10 and B10d, used for compliance with both standards, are reliability parameters for electromechanical components. B10 is the number of operations at which 10% of the population will experience errors and B10d is the number of cycles after which 10% of the population has faced an error to a dangerous state.

Normally there are no published MTTFd or PFHd figures for electromechanical components, since error rates depend upon the hourly actuation rate, which is application-specific. However, designers can use B10 or B10d with known machine data (e.g. guard switches might activate a known number of times per hour when loading a machine), in order to calculate the MTTFd or PFHd of subsystems containing these components.



Which Standard?

EN 62061 and EN ISO 13849-1 both deal with the functional safety of machine control systems, but they use slightly different terms and techniques to determine performance. Many users are confused by conflicting guidance from suppliers, who may prefer one standard over another.

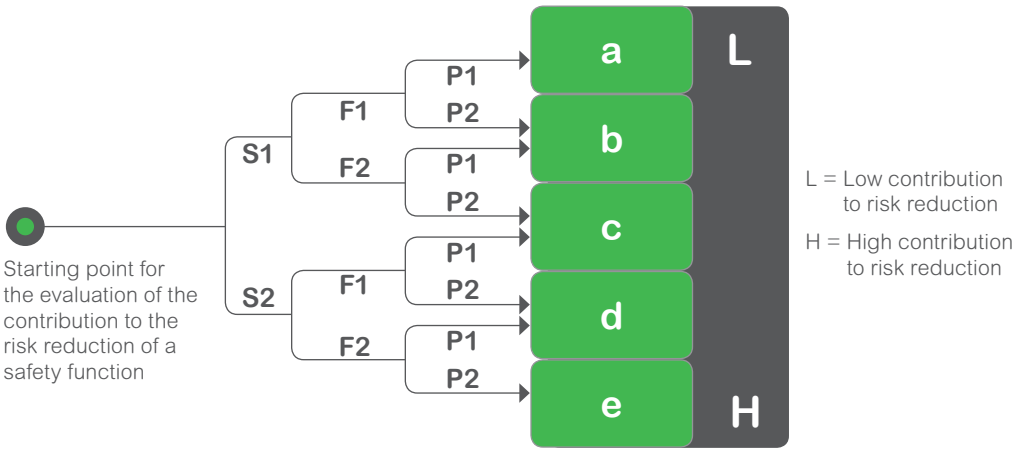
It is not ideal to have two standards for designers to choose from. This can lead to integration issues between components and can affect relationships between manufacturers, machine builders and end users. However, the European Committee for Electrotechnical Standardization (CENELEC) and the European Committee for Standardization (CEN) both have clear ideas of how to regulate functional safety when building machines. As such, both have set out standards that can provide a presumption of conformity to the relevant Machinery Directive requirements.

Both EN 62061 (published by the CENELEC) and EN ISO 13849-1 (published by the CEN) have the same objective: to de-emphasize the behavior of individual components and to focus instead on the functional safety of the overall machine. Both standards are intended to reduce the possibility of injury. Used correctly, therefore, they often reduce the likelihood of machine error. While these standards can provide similar risk reduction levels, they achieve that goal in very different ways.

The standards use different terms for circuit functional safety levels: EN 62061 defines three Safety Integrity Levels (SILs), whereas EN ISO 13849-1 specifies five Performance Levels (PLs). Despite these differences in terminology, some requirements (such as the probability of dangerous failure per hour (EN 62061)) are simple to compare. The standards take different approaches however.

Both EN 62061 and EN ISO 13849-1 have strengths and weaknesses, and there is an argument for and against using either one, depending on the application and manufacturer's individual preferences. Unless a machine-specific type-C standard specifies a SIL or PL, designers are free to choose which standard to use. Whatever the standard, however, it must be used in its entirety and the two cannot be mixed in a single safety function.

Risk graph to obtain the Performance Level required (PLr) according to EN ISO 13849-1



Designers familiar with the old categories of EN 954-1 may find EN ISO 13849-1 easier to use. Like its predecessor, the standard applies a simple looking “risk graph” to determine the required Performance Level (PL) of individual safety functions after a risk assessment has been performed in accordance with EN ISO 12100. This means safety functions can be assigned to the appropriate performance in order to deal with each individual risk. However, use of the risk graph alone is often insufficient; the system designer must also make further choices.

The PL is not determined by the system architecture alone. It is also based on the Mean Time to Dangerous Failure (MTTFd) (EN ISO 13849-1) and the Diagnostic Coverage (DC). A major benefit of this approach is that designers can use simpler circuitry as long as they choose high-reliability components, or components with higher MTTFd figures. This is because the five Performance Levels (PLs) defined in EN ISO 13849-1 are bands of values rather than discrete categories.

The advantage of EN ISO 13849-1 over the old standard is that it can make safety more cost-effective for designers, allowing them to design safety circuits using fewer, more reliable components. For example, with the new standard a PL d can be achieved using either a category 2 single-channel design with higher reliability components, or category 3 dual-channel architecture with lower reliability components. Thus the designer has a broader choice.

Tools are available (such as SISTEMA from the German Institute of Occupational Safety and Health Insurance) to help developers and testers evaluate machine safety according to EN ISO 13849-1.

For applications with more robust requirements for managing functional safety, EN 62061 may be more suitable. It provides more guidance on the organizational requirements to ensure functional safety is achieved and maintained. In addition, this standard is better at considering the effect of modifications that might be made either when commissioning new equipment or during the machine’s operating lifetime. For example, commissioning engineers need to consider the likely effects of any proposed modification, and how much the control system can be modified before revalidation was required.

A joint IEC-ISO working group has developed a comparison of the two standards. This document has been published by both organizations as a Technical Report — not the same status as a standard report but quicker to publish.

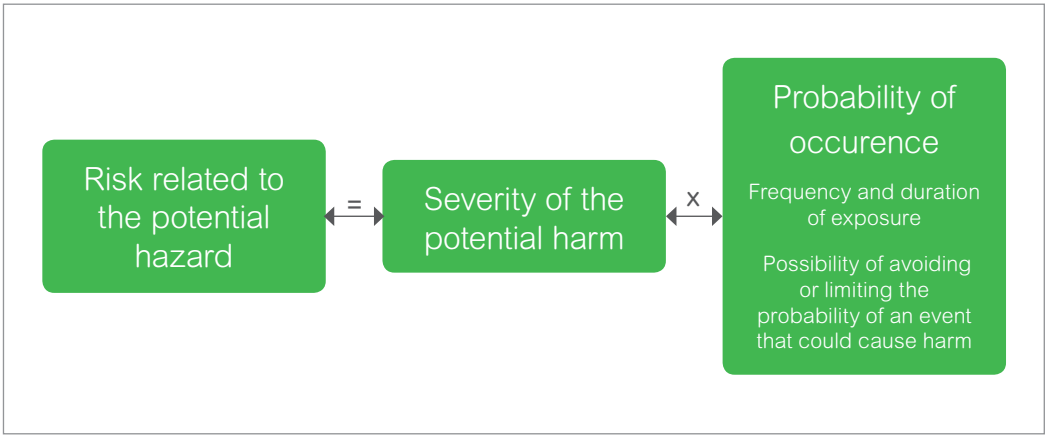
Putting Functional Safety in Context

Functional safety is an integral part of the design of safe control systems. Other factors need to be considered when designing control systems, however.

Although functional safety is important, it is only relevant when other factors have been considered in order to put the functional safety calculation into context. This means looking at aspects such as the basic design of the machine and its electrical equipment, as well as its pneumatic and hydraulic equipment.

Furthermore, functional safety standards are only useful in the context of more fundamental standards such as EN ISO 12100 (Safety of Machinery – General Principles for Design – Risk Assessment and Risk Reduction), and EN 60204-1 (Safety of Machinery – Electrical Equipment of Machines).

Although EN ISO 13849-1 and EN 62061 are the preferred functional safety standards for control systems, they do not replace the need for a risk assessment and a risk reduction plan prior to designing safety-related control systems. In addition, they do not replace good engineering practice. Performance Levels (PLs) and Safety Integrity Levels (SILs) are not a precise science but rather figures of merit, and should be used for guidance only.



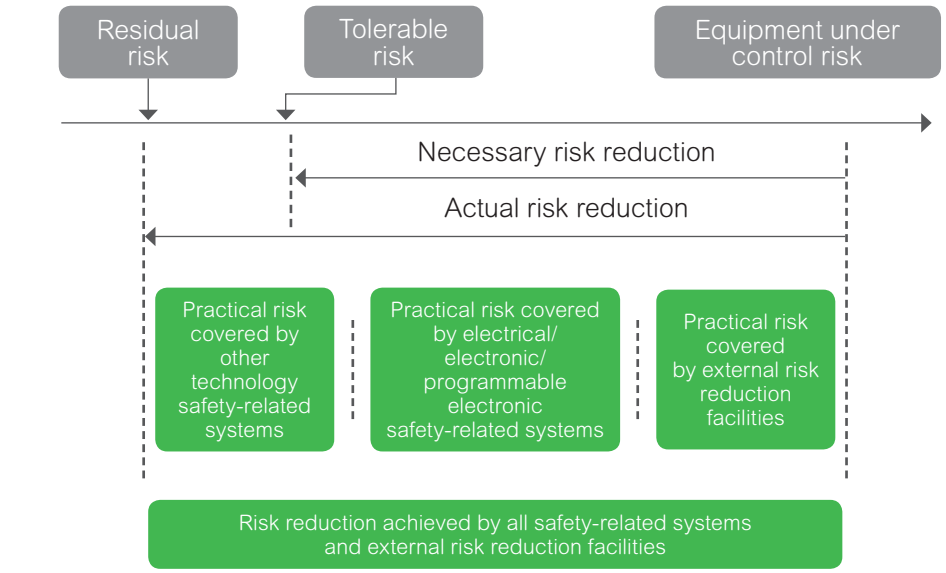
Risk assessment and reduction should be carried out in accordance with EN ISO 12100. The main focus is on reducing risk as far as is reasonably practicable. The risk reduction hierarchy can be described in three stages.

- **Stage 1:** eliminate the potential hazard if possible (inherently safe design) following EN ISO 12100. Example: place a protective barrier around the dangerous moving part to protect the user.
- **Stage 2:** safeguard against potential hazards where inherently safe design is not practical. Example: implement protective measures via safety-related control systems such as guards with interlock switches or open access areas protected by a light curtain.
- **Stage 3:** apply complementary protective measures. Example: provide staff training, warning signs, usage guidance, and personal protective equipment.

Users should repeat this cycle of risk assessment followed by risk reduction in order to reduce the risks to a tolerable level, and to ensure no additional risks have been introduced.

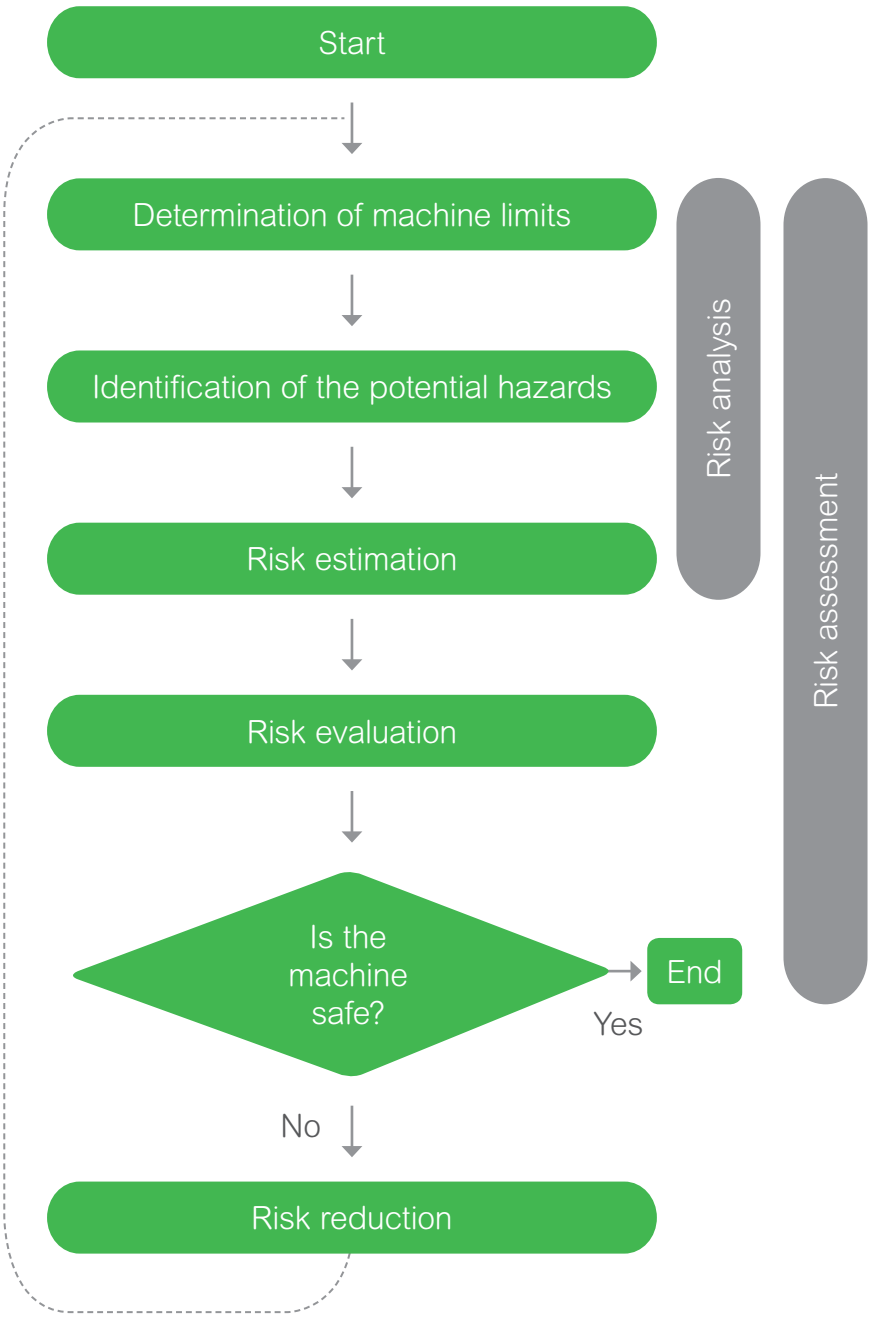
The risk reduction process may require the use of safety-related control systems designed with EN ISO 13849-1 and EN 62061. However, the overall safety of a machine will also depend on compliance with other standards such as EN 60204-1 for the complete electrical equipment.

Risk reduction according to EN 62061 and EN ISO 13849-1



A clear and concise guide detailing the requirements of these two functional safety standards and offering concrete examples is available for download from the Machine Safety page of the Schneider Electric website.

Iterative process of risk assessment and reduction in accordance with EN ISO 12100 Standard



For further information, please visit:
http://www.se.com/sites/corporate/en/solutions/oem/machine-safety/machine-safety.page

Schneider Electric Automation GmbH
Schneiderplatz 1, 97828 Marktheidenfeld, Germany Tel.: +49 (0)9391 6060
www.se.com

998-20499581

Life Is On Schneider Electric