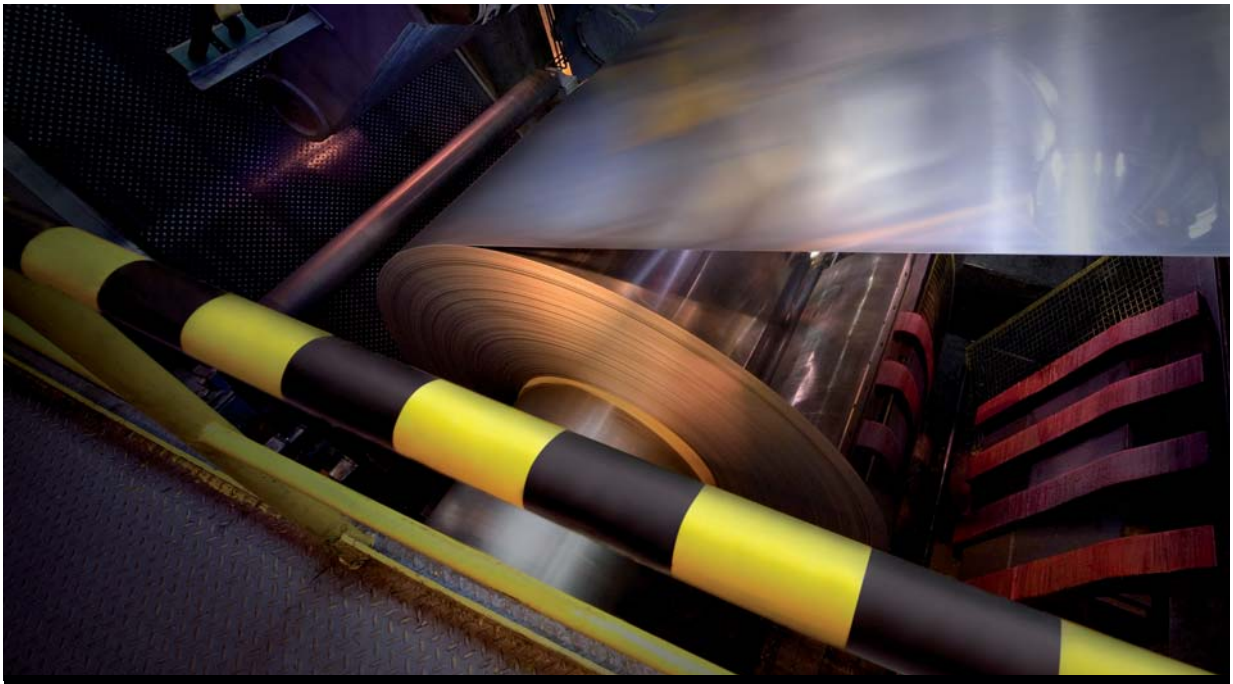


ABB drives

Technical guide No. 10
Functional safety

Power and productivity
for a better world™

Technical guide No. 10
Functional safety

3AUA0000048753 REV E EN 12.8.2014 #17212

Contents

Disclaimer

This document is an informative guide intended to assist the users, specifiers and manufacturers of machinery and the related people in achieving a better understanding of the requirements of the EU Machinery Directive, and the measures required to achieve conformity with the directive and the harmonized standards under it.

This document is not intended to be used verbatim, but rather as an informative aid.

The information and examples in this guide are for general use only and do not offer all of the necessary details for implementing a safety system.

ABB Oy Drives does not accept any liability for direct or indirect injury or damage caused by the use of information found in this document. The manufacturer of the machinery is always responsible for the safety of the product and its suitability under the applicable laws. ABB hereby disclaims all liabilities that may result from this document.

About this document

This document introduces the Machinery Directive and the standards that must be taken into account when designing a machine, in order to ensure operational safely.

The aim of the document is to explain, in general terms, how the process for meeting the requirements of the Machinery Directive is carried out and CE marking is obtained. CE marking indicates that the machinery conforms to the requirements of the Directive.

Note:
This document gives only an overview of the process for meeting the essential requirements of the Machinery Directive. The manufacturer of the machinery always remains ultimately responsible for the safety and compliance of the product.

The document is divided into three parts:

- Part 1 – Theory and Background – introduces the idea behind functional safety and how to comply with the Machinery Directive. It also presents the Machinery Directive and explains the hierarchy of the European harmonized standards system.
- Part 2 – Machinery standards – Introduces the two standard systems and lists a number of safety relevant standards and safety functions.
- Part 3 – Steps to Meet Machinery Directive Requirements – introduces nine steps that help in the process of fulfilling the essential requirements of the Machinery Directive.

Part 1 – Theory and background

The national laws of the European Union require that machines meet the Essential Health and Safety Requirements (EHSR) defined in the Machinery Directive and in the harmonized standards (EN versions of the IEC/ISO standards) under the Directive. This means that all new machinery must fulfill the same legal requirements when supplied throughout the EU. The same standards (IEC/ISO versions) are also recognized in many areas outside Europe, for example through equivalency charts, which facilitates machinery trade and machine shipments between countries within and outside the EU.

Why must machinery meet these requirements? Because conformity helps to prevent accidents and consequent injury. Furthermore, by complying with the Machinery Directive and the relevant harmonized standards or outside Europe complying with the relevant functional safety standards, machine manufacturers can rest assured they have met their obligations to design and deliver safe machines that comply with national laws.

For manufacturers, new and improved safety strategies are becoming a way of improving their productivity and competitiveness in the market. The aim of conventional safety systems has been to achieve comprehensive operational safety and meet legal obligations. This has been done by using add-on electrical and mechanical components, even at the cost of productivity. Operators can, in certain circumstances, override these systems when attempting to improve productivity, which can lead to accidents.

With modern safety systems, the safety of the processes and the operator can be taken into account while maintaining productivity. One example of this is keeping the machine running but at a lower speed to maintain safe operation. With modern safety solutions, safety can be an integrated part of machine functionality, and safety solutions are not just afterthoughts, added in order to meet regulations.

Safety systems can be implemented effectively through defined processes, to achieve specific risk reduction capability and use certified subsystems as building blocks for safety systems. The process concepts and the methods laid out in the functional safety standards are introduced in this guide. Meeting safety standards is expected in the industry, and certified subsystems such as drives with pre-designed safety functions are important in the industry. Machine safety is one of the most rapidly growing areas of importance in industrial automation.

Safety and functional safety

The purpose of safety is to protect people and the environment from accidents and risks caused by machines. Functional safety systems do this by lowering the probability of undesired events, so that mishaps are minimized when operating machinery. Safety standards define safety as freedom from unacceptable risk. Acceptable risk levels are defined by means of required risk reduction in the machinery safety standards. Machine builders should always use the same (the most stringent) acceptability criteria for all market areas, regardless of regional differences.

The most effective way to eliminate risks is to design machines to be inherently safe. But if risk reduction by design is not possible or practical, safeguarding through static guards or safety functions is often the best option. Machine safety functions can be used to reduce the risks caused by movement while maintaining machine productivity, uptime and usability. At the same time, the legal obligations are met and the safety of people and the environment is ensured.

Functional safety in machinery usually means systems that safely monitor and, when necessary, take control of the machine applications to ensure safe operation. Functional safety systems are designed to detect hazardous conditions or user's demand for safe state, and bring machine /process to a safe state, or to ensure that the desired action, such as safe stopping, takes place.

Monitoring typically include speed, stopping, direction of rotation, and standstill. When the safety system is executing an active safety function, for example monitoring a crawl speed, and the system behavior deviates from what is expected (for example, the system runs too fast), the safety system detects the deviation and actively brings machine operation to a safe state. This can be done, for example, by stopping the machine safely and removing the torque from the motor shaft.

A safety system is not part of standard machine operation, and any failure in the safety system will immediately increase the risks related to machine operation (the machine might work normally, but the safety function is not available should a hazardous event occur).

Machinery Directive

The Machinery Directive, with the harmonized standards listed thereunder, defines the Essential Health and Safety Requirements (EHSR) for machinery at European Union level. The EHSRs are listed in Annex I of the Machinery Directive.

The idea behind the Machinery Directive is to ensure that a machine is safe and that it is designed and constructed so that it can be used, configured and maintained throughout all phases of its life, causing minimal risk to people and the environment.

The EHSR state that when seeking solutions for designing and building safe machines, machine manufacturers must apply the following principles in the given order (also known as the 3-step method, EN ISO 12100):

1. Eliminate or minimize the hazards as much as possible by considering safety aspects in the machine design and construction phases (design machine to be inherently safe).
2. Apply the necessary protection measures against hazards that cannot be eliminated.
3. Inform users of the risks that remain despite all feasible protection measures being taken, while specifying any requirements for training or personal protective equipment.

Complying with the EHSR of the Machinery Directive allows the machine manufacturer to affix the CE marking on the machine. With CE marking the manufacturer guarantees that the product meets all regulations on the free movement of goods, as well as the essential requirements of the relevant European Directives, in this case the Machinery Directive.

Note:
There might also be other directives that apply, e.g. Low voltage directive and EMC directive. Only Machinery Directive requirements are covered in this guide.

Note:
CE marking according to the Machinery Directive is affixed only on a complete machine, not to the components of which it consists. Thus, the manufacturer of the product, or the representative of the manufacturer, is responsible for CE marking, not the manufacturer of the component that is included in the final product.

As an exception, the safety components to be used in the safety functions of the machine, are CE marked according to Machinery Directive by the component manufacturer/representative in Europe.

The machine manufacturer is responsible for carrying out the related risk analysis, following through the steps presented in Part 3, and ensuring compliance with the requirements. The component manufacturer is responsible for realizing the risk reduction capability (indicated with SIL CL/PL level) of the said component's safety function, when the component is appropriately used. A component in this case could be a safety relay, or an AC drive with integrated safety functionality.

Hierarchy of the European harmonized standards system

The European Committee for Standardization, CEN, and the European Committee for Electrotechnical Standardization, CENELEC draw up the European "EN" versions of the standards, which can be then used as harmonized standards in all EU member countries. All harmonized standards carry the prefix "EN" (NOTE: not all EN standards are harmonized standards).

A list of the harmonized standards for machinery can be found on the European Commission Internet pages, http://ec.europa.eu.

The majority of harmonized standards are referenced by one or more Directives. To ensure that the essential requirements of the Machinery Directive are followed, it is advisable to apply the appropriate harmonized European standards. By designing machines according to these standards, manufacturers can demonstrate that they comply with the Machinery Directive and, generally, do not require certification by a third party.

Note:
Exceptions for the machines listed in Annex IV of the Machinery Directive must be noted.

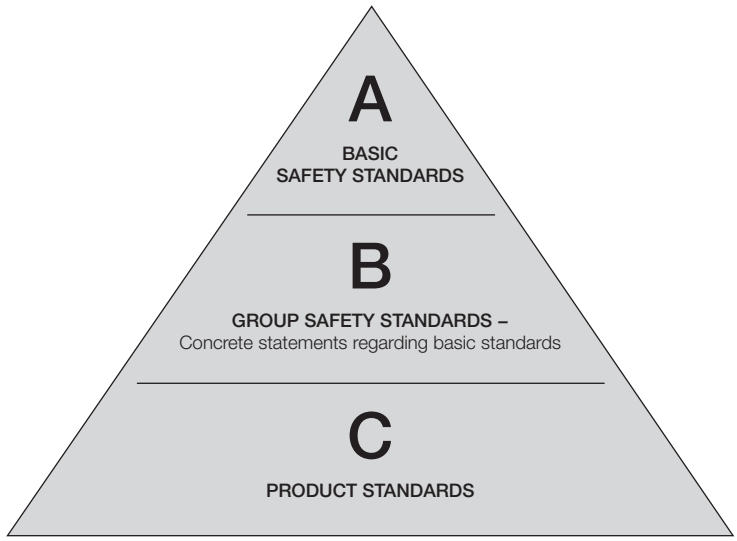


Figure 1-1 Hierarchy of European harmonized standards

– Type-C standards are specific to a machine or class of machine. If there is a type-C standard for a machine, the associated type-B and possibly also type-A standards become secondary. When designing safety functions, type-C standards define additional, mandatory requirements for the machines they are intended for. However, if no type-C standard exists for the machine, type-B and type-A standards offer help in

designing and constructing machines that meet the requirements of the Machinery Directive.

– Type-B standards deal with safety requirements that are common to the design of most machines. These standards give information on possible risks and how to handle them, with the help of a risk reduction process. Type-B standards can be divided into two groups, B1 and B2. Type-B1 standards deal with specific safety aspects and type-B2 standards handle safety-related equipment in general. Type-B1 standards are, for example, EN 62061:2005 and EN ISO 13849-1:2008. Type-B2 standards include standards for defining emergency stops, such as EN ISO 13850:2008.
– Type-A standards handle basic concepts, terminology and design principles. These standards alone are not sufficient to ensure conformity with the Machinery Directive. The only A-type standard harmonized under Machinery Directive is the basic safety standard for risk assessment and reduction, EN ISO 12100.

Note:
It is not mandatory to apply the harmonized standards, but they offer recommendations and guidance for meeting the requirements of the Machinery Directive, which must be conformed to.

Part 2 – Machinery standards

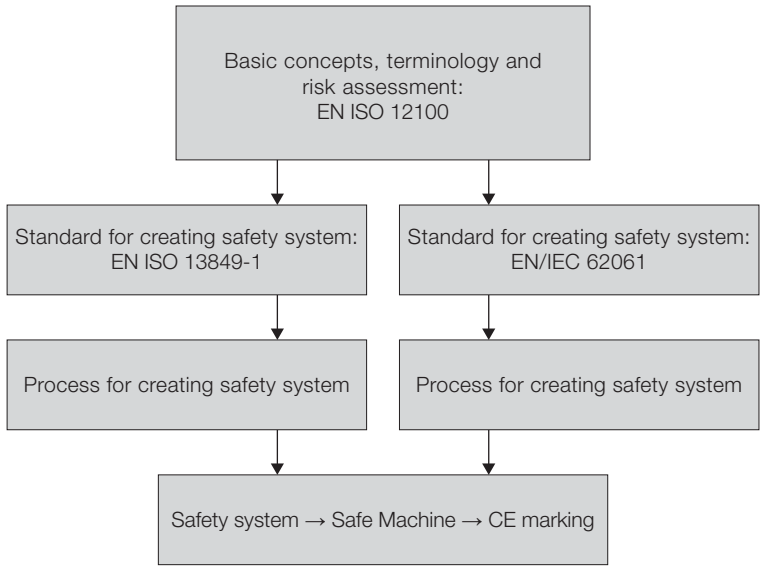


Figure 2-1 Introducing standards

Two standards – IEC and ISO

There are two alternative standards that can be followed when implementing functional safety systems in compliance with the Machinery Directive: The International Organization for Standardization (ISO) standard and the International Electrotechnical Commission (IEC) standard.

Following either of the standards leads to a very similar outcome, and their resulting safety integrity levels (SIL) and performance levels (PL) are, in fact, comparable. For more information, see the comparison table in Part 3, step 6.

Note:
It is up to the machine manufacturer to decide which – if any – safety system creation standard is to be used (EN ISO 13849-1 or EN/IEC 62061), and then they shall follow the same, chosen standard all the way from beginning to end to ensure congruity with the said standard.

CEN standards are based on ISO standards and are basically for mechanical equipment – new standards have numbers in the 1xxxx series, while CENELEC standards are based on IEC standards – new standards have numbers in the 6xxxx series.

Note:
ISO standards are presented in this document as EN ISO, using notation found in the harmonized standards list. IEC based standards are presented as EN/IEC, showing both prefixes, although the IEC standards are shown with just the EN prefix in the harmonized standards list (eg EN 62061).

Standard for risk minimization

Basic safety standards for risk minimization include:

– **EN ISO 12100:2010**
(Safety of machinery – Basic concepts, general principles for design)

EN ISO 12100 gives designers the basic terminology, a general framework and guidance, providing instructions and requirements for risk assessment and and risk reduction (the three-step method).

Note:
All other references to this standard in this document always apply to the above mentioned versions of the standard.

Standards for electronic safety systems

The standards for electronic safety systems are as follows:

– **EN ISO 13849-1:2008/AC:2009** (Safety of machinery – Safety-related parts of control system – Part 1: General Principles for design),
– **EN ISO 13849-2:2012** (Safety of machinery – Safety-related parts of control system - Part 2: Validation)
– **EN/IEC 62061:2005+AC:2010** (Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems),
– **IEC 61508:2010** (Functional safety of electrical/electronic/programmable electronic safety-related systems), and
– **EN/IEC 60204-1:2006+AC:2010** (Safety of machinery – Electrical equipment of machines – General requirements).

Note:
All other references to these standards in this document always apply to the above mentioned versions of the standards.

EN ISO 13849-1 is a standard that provides instructions to designers to make machines safe. These instructions include recommendations for the design, integration and validation of the systems. It can be used for the safety-related parts of control systems and various kinds of machinery, regardless of

the technology and energy it uses. The standard also includes special requirements for safety-related parts that have programmable electronic systems. This standard covers the entire safety function for all devices included (a complete safety chain, for example sensor–logic–actuator).

The standard defines how the required Performance Level (PL) is determined and the achieved PL verified within a system. PL describes how well a safety system is able to perform a safety function, under foreseeable conditions. There are five possible Performance Levels: a, b, c, d and e. Performance Level "e" provides the highest risk reduction capability, while PL "a" provides the lowest.

EN ISO 13849-2 specifies the validation process and required design measures/techniques for safety functions designed according to EN ISO 13849-1.

EN/IEC 62061 is a standard for designing electrical safety systems. It is a machine sector specific standard within the framework of IEC 61508. EN/IEC 62061 includes recommendations for the design, integration and validation of safety-related electrical, electronic and programmable electronic control systems for machinery. The entire safety chain – for example sensor–logic–actuator – is covered by this standard. Individual subsystems need not be certified, as long as the entire safety function fulfills the defined requirements. However, using certified subsystems as building blocks is still strongly recommended, as this will potentially save considerable effort in the design and verification process.

Note:
Unlike EN ISO 13849-1, EN/IEC 62061 does not cover requirements for non-electrical safety-related control equipment for machinery.

This standard uses a Safety Integrity Level (SIL) for complete safety functions and SIL Claim limit (SIL CL) for safety subsystems (individual devices like relays). SIL/SIL CL are is a representation of the risk reduction capability of the safety functions/ subsystems. There are four possible safety integrity levels:
1, 2, 3, and 4. "SIL 4" is the highest level of safety integrity and "SIL 1" the lowest. Only levels 1-3 are used in machinery."

IEC 61508 is a basic functional safety standard. It covers the life cycle of systems comprised of electrical and/or electronic and/or programmable electronic components that are used to perform safety functions. IEC 61508 is not a harmonized standard, but it is the main standard that outlines the requirements and methods for designing safety related control systems with complex hardware and software. IEC 61508 is generally

used when designing certifiable safety subsystems. Standards EN ISO 13849-1 and EN/IEC 62061 are based on the principles set in IEC 61508.

EN/IEC 60204-1 gives recommendations and requirements for the electrical equipment of machines in order to enhance safety and usability.

Product-specific safety standards (type-C standards)

Product-specific safety standards, known as type-C standards, handle a specific machine or class of machines and are based on a presumption of conformity with respect to the EHSRs covered by the standard.

It should be noted that:

- The requirements specified in the type-C standards generally overrule the requirements set by the general safety standards (EN/IEC 62061, EN ISO 13849-1, etc.).
- Type-C standards may have set SIL/PL requirements for specific safety functions. At least these requirements must be met, regardless of the results of the risk assessment (however a risk assessment must always be conducted as well).

Note:
Even if the lists of hazards possibly affecting the machine, composed during the risk assessment, and the type-C standard are identical, the standard may not take account of all of the relevant EHSRs. The standard must always be inspected thoroughly to determine what hazards might have been excluded from the list.

Specific standard for safety-related drive systems

A specific standard for safety-related drive system is:

- **EN/IEC 61800-5-2:2007** (Adjustable speed electrical power drive systems - functional safety requirements).

Note:
All other references to this standard in this document solely apply to the above mentioned version of the standard.

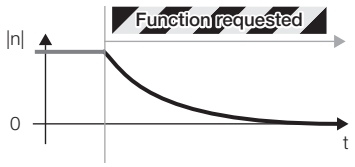
EN/IEC 61800-5-2 gives specifications and recommendations for power drive systems used in safety-related applications. It is a product standard that presents safety-related aspects in terms of the framework of IEC 61508, and introduces requirements for power drive systems when used as subsystems in safety systems.

Standardized safety functions

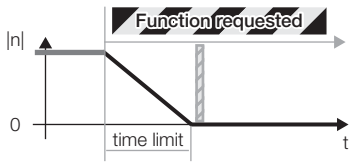
Standard EN/IEC 61800-5-2 defines safety functions for drive systems. A drive may offer one or more of these functions. Here are some examples:

Safe torque off (STO)
When activated, this function brings the machine safely into a non-torque state and/or prevents it from starting accidentally.

Note: Safe torque off does not protect against electrical hazards.



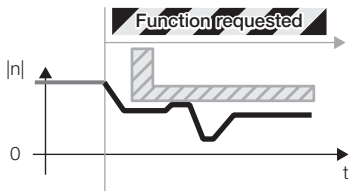
Safe stop 1 (SS1)
When activated, this function stops the motor safely, initiating the STO function below a specified speed (close to standstill) or after a defined time limit.



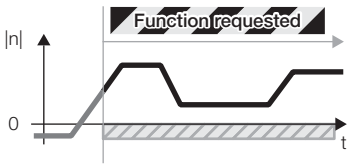
Safe stop 2 (SS2)
When activated, this function stops the motor safely, initiating the SOS function below a specified speed or after a defined time limit.

Safe operating stop (SOS)
When active, this function keeps the motor in a safe standstill while holding the motor torque.

Safely-limited speed (SLS)
When active, this function prevents the motor from exceeding the defined speed limit.

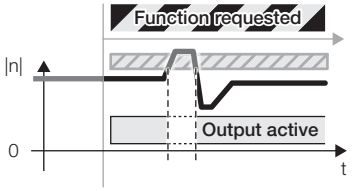


Safe direction (SDI)
When active, this function prevents the motor shaft from moving in an unwanted direction.



Safe brake control (SBC)
When active, this function provides a safe output for controlling external (mechanical) brakes.

Safe speed monitor (SSM)
When active, this function provides a safe output indicating that the speed is under the specified speed limit.



See standard EN/IEC 61800-5-2 for more examples of safety functions.

Note:
Functions SOS, SLS and SDI of the above functions are monitoring functions, ie safety they monitor that movement or standstill are within defined limits. If these functions detect that movement is not within a defined limit, they activate a fault reaction function, which typically is Safe torque off (STO).

Emergency operations
Standard EN/IEC 60204-1 defines two emergency operations, emergency switching-off and emergency stop.

Emergency switching-off
The emergency switching-off function disconnects power to a system or part of it should the risk of an electric shock arise.

This function requires external switching components, and can not be accomplished with **safe torque off (STO).**

Emergency stop
An emergency stop must operate in such a way that, when it is activated, the hazardous movement of the machinery is stopped and the machine is unable to start under any circumstances, even after the emergency stop is released. Releasing the emergency stop only allows the machine to be restarted.

The emergency stop can stop hazardous movement by applying the following actions:
– optimal deceleration rate until the machine stops
– by using one of the two emergency stop categories, 0 or 1, or
– by employing a predefined shutdown sequence.

Emergency stop, stop category 0 (according to EN 60204-1) means that the power to the motor is cut off immediately. Stop category 0 is equivalent to the **safe torque off (STO)** function, as defined by standard EN/IEC 61800-5-2.

Emergency stop, stop category 1 (according to EN 60204-1) means that the machine speed is brought to a standstill through controlled deceleration and then the power to the motor is cut off. Stop category 1 is equivalent to the **safe stop 1 (SS1)** function, as defined by standard EN/IEC 61800-5-2.

When actuated, the emergency stop function must not create any additional hazards or require any further involvement by the machine operator.

Note:
The principles for the design of an emergency stop function are introduced in standard EN ISO 13850:2008.

Prevention of unexpected startup
Ensuring that a machine remains stopped when persons are present in danger area is one of the most important conditions in safe machines.

The **safe torque off (STO)** function can be used to effectively implement the prevention of unexpected startup functionality, thus making stops safe by preventing the power only to the motor, while still maintaining power to the main drive control circuits. Prevention of unexpected startup requires for example a lockable switch in addition to the STO function.

The principles and requirements of the prevention of unexpected startup are described in the standard EN 1037:1995+A1 2008. Another standard covering the prevention of unexpected startup is ISO 14118:2000.

Part 3 – Steps to meet Machinery Directive requirements

The Machinery Directive requires machinery to be safe. However, there is no such thing as zero risk. The objective is to minimize the risk.

Compliance with the Machinery Directive can be achieved:

- by meeting the requirements set by the harmonized standards or
- by having a machine acceptance investigation carried out by an authorized third party.

The process for fulfilling the EHSRs of the Machinery Directive using harmonized standards can be divided into nine steps:

- **Step 1: Management of functional safety** – managing functional safety during the life cycle of the machine.
- **Step 2: Risk assessment** – analyzing and evaluating risks.
- **Step 3: Risk reduction** – eliminating or minimizing risks through design and documentation.
- **Step 4: Establishing safety requirements** – defining what is needed (functionality, safety performance) to eliminate the risk or reduce it to an acceptable level.
- **Step 5: Implementing a functional safety system** – designing and creating safety functions.
- **Step 6: Verifying a functional safety system** – ensuring that the safety system meets the defined requirements.
- **Step 7: Validating a functional safety system** – reviewing implemented safety system against the risk assessment and making certain that the safety system actually succeeded in reducing risks as specified.
- **Step 8: Documenting a functional safety system** – documenting the design, producing user documentation.
- **Step 9: Providing compliance** – proving the machine's compliance with EHSR of the Machinery Directive through compliance assessment and a technical file.

Each of these steps is explained in more detail in the following chapters.

Updating existing machinery
The following issues must be considered when updating safety requirements for existing machines:

- For machines that already have a CE marking – new components that are added to the machine must also have a CE marking according to relevant directives such as Low Voltage Directive and EMC directive(safety components also

according to Machinery directive). It must be case-specifically defined how the new components are applied to the old system according to the Machine Directive.
– For machines that do not have a CE marking – the safety level of the machine can be maintained by replacing components with new ones that have a CE marking.

Ultimately, it is the relevant authority's decision as to whether the change was extensive enough to require an update of the safety level.

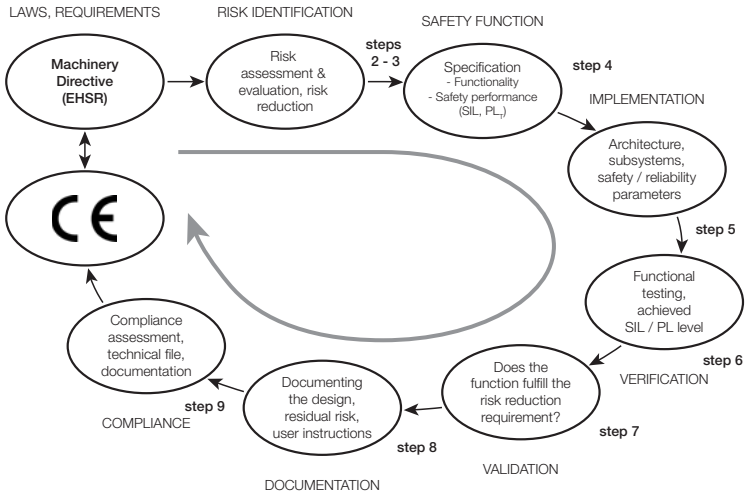


Figure 3-1 Process flow for meeting Machinery Directive requirements

STEP 1: Management of functional safety

To achieve the required functional safety, it is necessary to implement a project management and quality management system that is compliant to, for example, IEC 61508 or ISO 9001 standards. This management system can be specified in the form of a safety plan.

Safety plan

Standard EN/IEC 62061 specifies a safety plan for the process for meeting the requirements of the Machinery Directive. This plan needs to be created and documented for each safety system and updated, when necessary.

Safety plan:

– identifies all relevant activities,
– describes the policy and strategy for fulfilling functional safety requirements,
– identifies responsibilities,
– identifies or establishes procedures and resources for documentation,
– describes strategy for configuration management, and
– includes plans for verification and validation.

Note:
Even though the activities listed above are not particularly specified in EN ISO 13849-1, similar activities are needed to fully meet the requirements of the Machinery Directive.

When the safety plan (according to EN/IEC 62061) has been created, risk assessment starts.

STEP 2: Risk assessment

The risk assessment is a process whereby risks are analyzed and evaluated. A risk is a combination of the consequence of harm (ie how severe is the injury or damage should the hazard lead to an accident) and the probability of the harm occurring when exposed to a hazard.

Note:
According to the Machinery Directive 2006/42/EC, it is mandatory to perform and document a risk assessment for a machine.

The Machinery Directive 2006/42/EC requires that manufacturers perform risk assessments and take the results into account when designing a machine. Any risk considered as “high” must be reduced to an acceptable level using design changes or by applying appropriate safeguarding techniques. Standards EN/IEC 62061 and EN ISO 13849-1 provide numerical methods for risk evaluation and reduction levels.

The risk assessment process provides the machinery designer with requirements on how to design inherently safe machinery. It is very important to assess and reduce risks at the design phase, because it is always more effective than providing user instructions on how to operate the equipment safely.

The risk assessment process according to EN ISO 12100 consists of two parts: risk analysis and risk evaluation. Risk analysis means identifying and estimating the risks and risk evaluation means deciding whether the risk is acceptable or risk reduction necessary.

Risk evaluation is carried out based on the results of the risk analysis. Decisions on the necessity of risk reduction are made according to the risk evaluation procedure.

TIP: ABB’s Functional safety design tool is a PC tool that provides a convenient way to conduct the risk evaluation numerically according to machinery standards EN/IEC 62061 or EN ISO 13849-1.

Note:
Risk evaluation must be carried out separately for each hazard.

Four steps of risk analysis:

1. Determine the limits and intended use of the machine.
   These limits include:
   - limits of use
   - spatial limits
   - ambient or environmental limits
   - lifetime limits

2. Identify the hazards that might be generated by the machine.

3. Estimate identified risks one at a time.
   - Severity of the risk (potential consequences)
   - Probability of the risk (Frequency, Probability, Avoidance)

4. Evaluate the risk: Is risk reduction necessary?
   - **YES:** Apply risk reduction measures and return to step 2 in the risk analysis.

Note: The 3-step method for risk reduction according to EN ISO 12100 is presented in the next chapter.

   - **NO:** Risk reduction target is met and risk assessment process ends.

Document the risk assessment process and its results for each individual hazard.

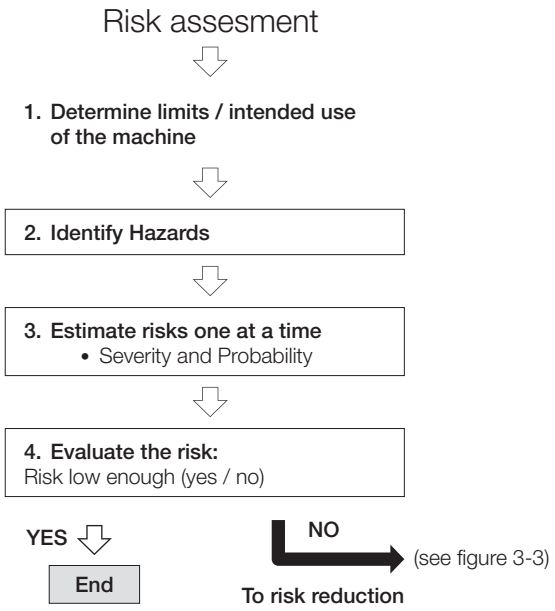


Figure 3-2 Risk assessment and evaluation according to EN ISO 12100

After the risk assessment has been carried out, there are two options, depending on the outcome of the assessment:

Option 1
If the assessment reached the conclusion that risk reduction was not needed, the machine has reached the adequate level of safety required by the Machinery Directive.

Note:
The remaining risks must be documented in the appropriate operation and maintenance manuals. There is always some residual risk.

Option 2
If the assessment revealed that the risk remains unacceptable, the process for risk reduction is started.

STEP 3: Risk reduction

The most effective way to minimize the risks is to eliminate them in the design phase, for example by changing the design or the work process of the machine. If this is not possible, one way to carry out the risk reduction process and ensure conformance with the requirements is to apply suitable harmonized standards under the Machinery Directive.

If the risk assessment process concludes that risk reduction is needed, a strategy for risk minimization is created. According to standard EN ISO 12100, risk reduction can be divided into three steps (the three-step method):

3-step method

1. Inherently safe design measures – creating a safer design, changing the process, eliminating the risk by design.

2. Safeguarding and complementary protective measures – safety functions, static guarding.

3. Information on use (residual risk management):
   - on the machine – warning signs, signals and warning devices – and
   - in the operating instructions.

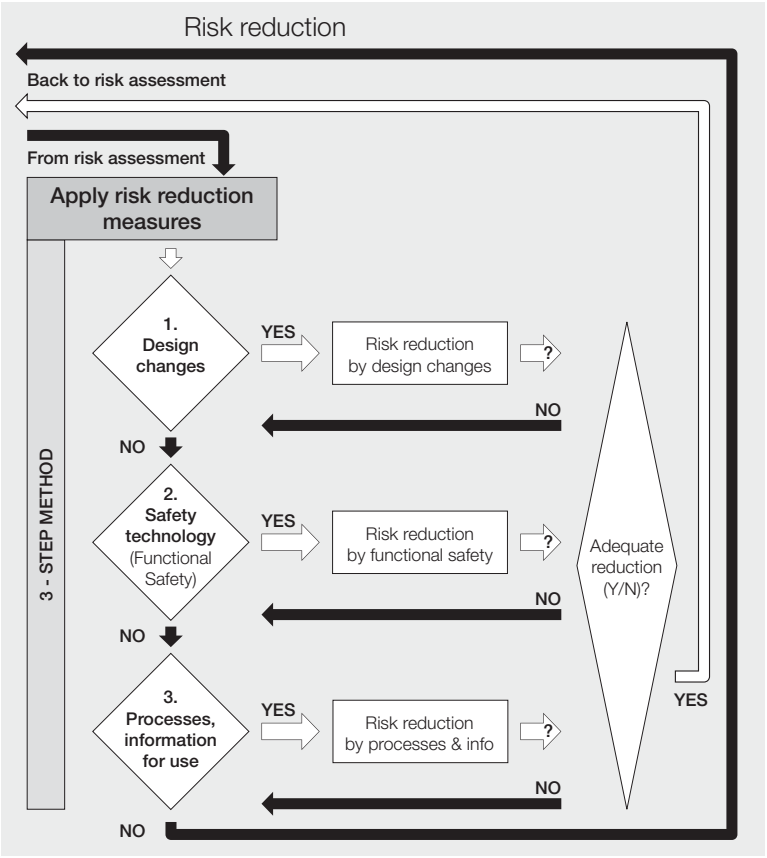


Figure 3-3 The 3-step method for risk reduction according to EN ISO 12100

Residual risk is the risk that remains when all protective measures have been considered and implemented. Using technology, it is not possible to achieve a state of zero risk, since some residual risk always remains.

All residual risks must be documented in the operating instructions.

The user's part of risk reduction includes information given by the designer (manufacturer). Risk reduction measures for the machine user/organization are as follows:

- Risk reduction measures typically taken by the organization:
  - introducing safe working procedures
  - work supervision
  - permit-to-work systems
- Provision and use of additional safeguards
- Use of personal protective equipment
- Training users
- Reading operating and safety instructions and acting accordingly.

Designers should also seek valuable user input when defining protective measures.

When the risk reduction has been executed, it must be examined to ensure that the measures taken were adequate for reducing the risk to an appropriate level. This can be done by repeating the risk assessment process.

The following, remaining steps describe option 2 of the 3-step method: safeguarding through a functional safety solution.

STEP 4: Establishing safety requirements

After all the risk reduction that can be undertaken through design changes has been performed, additional safeguarding needs to be specified. Functional safety solutions can be used against the remaining hazards as an additional risk reduction measure.

Safety functions
A safety function is a function of a machine whose failure can result in an immediate increase in risk. Simply put, it comprises the measures that must be taken to reduce the likelihood of an unwanted event occurring during exposure to a hazard. A safety function is not part of machine operation itself. This means that if the safety function fails, the machine can operate normally, but the risk of injury from machine operation increases.

Defining a safety function always includes two components:
– **required action** (what must be done to reduce the risk) and
– **safety performance** (Safety Integrity Level - SIL or Performance Level - PL).

Note:
It is also important to specify the timing requirements for the safety function, ie the maximum allowed time to bring the system into a safe state.

Also the environment for the safety system has to be specified, so that suitable safety components can be selected.

Note:
A safety function must be specified, verified (functionality and safety performance) and validated separately for each identified hazard.

Example of a safety function:
Requirement: An exposed rotating shaft may cause an injury if one gets too close to the shaft.

Action: In order to prevent personal injury from the shaft, the motor must stop in one (1) second, when the safety gate is opened.

After the safety function that executes the action has been defined, the required safety level is determined for it.

Safety performance/integrity
Safety integrity measures the performance of a safety function. It presents the likelihood of the safety function being achieved, upon request. The required safety integrity for a function is determined during the risk assessment and is represented by the achieved Safety Integrity Level (SIL) or Performance Level (PL), depending on the standard used.

The two standards use different evaluation techniques for a safety function, but their results are comparable. The terms and definitions are similar for both standards.

Determining the required SIL (EN/IEC 62061)
The process for determining the required safety integrity level (SIL) is as follows:

1. Determine the severity of the consequence of a hazardous event.
2. Determine the point value for the frequency and duration a person is exposed to the harm.

Tip:
Determining the required SIL can be conveniently done with ABB Functional safety design tool (FSDT) PC-tool.

3. Determine the point value for the probability of the hazardous event occurring when exposed to it.
4. Determine the point value for the possibility of preventing or limiting the scope of the harm.

Example:
The parameters used in determining the point values are presented in the following example of an SIL assignment table.

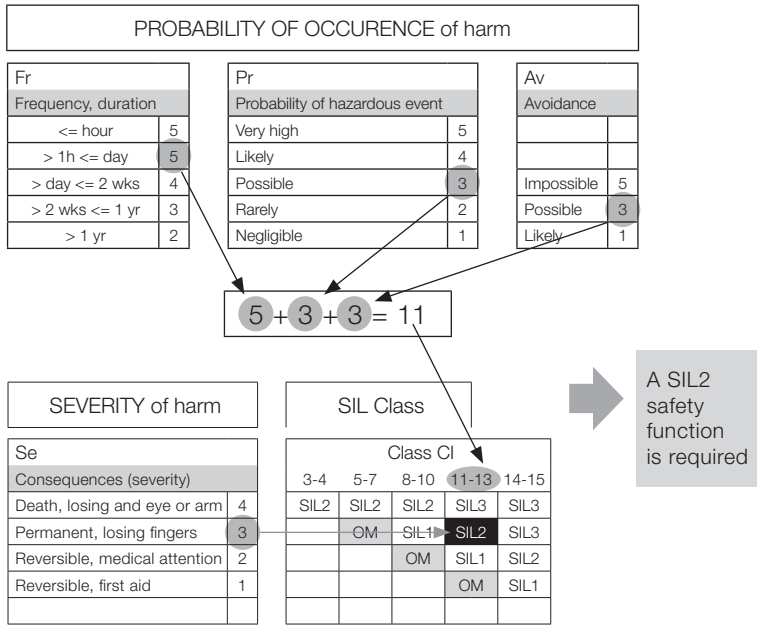


Figure 3-4 Example of SIL assignment table (based on EN/IEC 62061 figure A.3)

In this example, the hazard analysis is carried out for an exposed rotating shaft.

1. Severity (Se) = 3. The consequence of the hazard is permanent injury, possibly losing fingers.
2. Frequency (Fr) = 5. A person is exposed to the hazard several times a day.
3. Probability (Pr) = 3. It is possible that the hazard will take place.
4. Avoidance (Av) = 3. The hazard can be avoided.
   - 5 + 3 + 3 = 11, with the determined consequence, this equals SIL 2.

The tables used for determining the points are presented in the standard.

After the required SIL has been defined, the implementation of the safety system can begin.

Determining the required PL (EN ISO 13849-1)
To determine the required PL, select one of the alternatives from the following categories and create a “path” to the required PL in the chart.

1. Determine the severity of the damage.
The severity parameters are
S1 Slight, usually reversible injury
S2 Severe, usually irreversible injury, including death

2. **Determine the frequency and duration of exposure to the hazard.**
   The frequency and duration parameters are
   F1 Rare to often and/or short exposure
   F2 Frequently to continuous and/or long exposure

3. **Determine the possibility of preventing the hazard or limiting the damage caused by the hazard.**
   The hazard prevention and damage limiting parameters are
   P1 Possible under certain conditions
   P2 Hardly possible

Tip:
Determining the required PL can be conveniently done with ABB Functional safety design tool (FSDT) PC-tool.

Example:
The resulting performance level is represented by a, b, c, d and e in the following example of the PL risk graph.

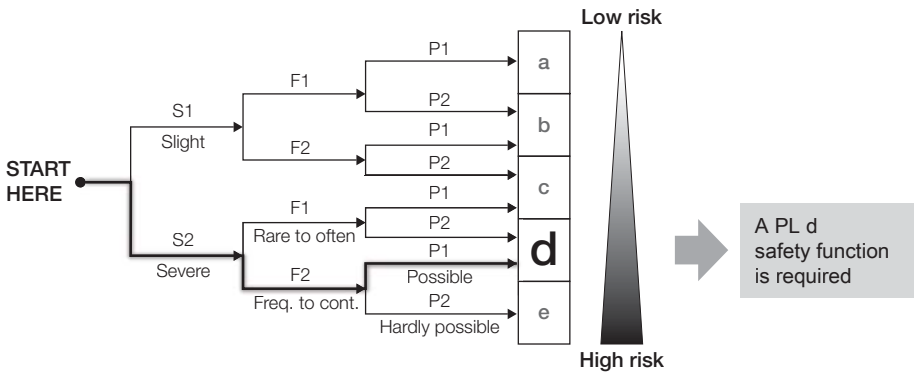


Figure 3-5 Example of PL risk graph (based on EN ISO 13849-1, figure A.1)

In this example, the hazard analysis is carried out for an exposed rotating shaft.
– The consequence of the hazard is a severe, irreversible injury. Severity = S2.
– A person is exposed to the hazard several times a day. Frequency = F2.
– It is possible to avoid or limit the harm caused by the hazard. Possibility = P2.

The path leads to PL value d. The tables used for determining the points are presented in the standard. After the PL has been defined, the implementation of the safety system can begin.

STEP 5: Implementing a functional safety system

When designing and constructing a safety function, the idea is to plan and construct the safety function in order to at least

meet the required SIL/PL specified for the function (as shown in the previous chapter). Using certified subsystems in functional safety systems can save the safety system designer a lot of work. Implementing safety functions becomes more convenient when some of the safety and reliability calculations are already made and subsystems are certified.

Note:
If certified subsystems are not used, it may be necessary to carry out safety calculations for each of the subsystems. Standards EN/IEC 62061 and EN ISO 13849-1 include information on the process and calculation data needed.

Tip:
Selecting a suitable safety function architecture, performing the required safety calculations and SIL/PL verification can be conveniently done with the Functional safety design tool -PC tool.

Implementation and verification processes are iterative and run parallel with each other. The idea is to use verify during implementation to ensure that the safety functionality and SIL/PL level reached with the implemented system. For more information on the verification processes, see the next step.

ABB's Functional safety design tool is a PC-tool available for establishing a SIL/PL target for a safety function, as well as to design, verify the achieved SIL/PL and document the safety function.

The general steps for implementing a functional safety system include:

1. **Defining the safety requirements in a form of SIL and PL, according to standard EN/IEC 62061 or EN ISO 13849-1.**

2. **Selecting the system architecture to be used for the safety system.**
   EN/IEC 62061 and EN ISO 13849-1 standards offer basic architectures with calculation formulas.

– category B, 1, 2, 3 or 4, as presented in standard EN ISO 13849-1, or
– designated architecture A, B, C or D, as presented in standard EN/IEC 62061 for the subsystems and the whole system.

For more information on designated architectures, see the respective standards.

3. **Constructing the system from safety-related subsystems – sensor/switch, input, logic, output, and actuator.**

Either:
– by using certified subsystems (recommended) or
– by performing safety calculations for each subsystem.

The safety level of the complete system is established by adding together the subsystem safety levels.

4. Installing the safety system.

The system needs to be installed properly to avoid common failure possibilities due to improper wiring, environmental, or other such factors. A safety system that is not performing correctly due to careless installation is of little or no use, or even poses a risk in itself.

5. Verifying the functionality of the system.

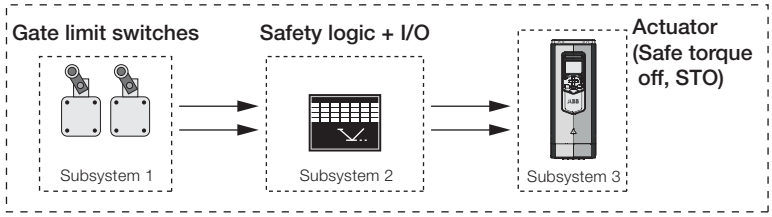


Figure 3-6 Structure of a safety function

STEP 6: Verifying a functional safety system

Verification of the functional safety system demonstrates and ensures that the implemented safety system meets the requirements specified for the system in the safety requirements phase.

Verification should not be carried out after the implementation process, but together with it as an iterative process, so that the implementation can indeed produce a system that will meet the specified requirements.

In addition to verifying the achieved SIL or PL of the system, the correct operation of the safety system must also be verified by carrying out functionality testing.

Verifying SIL of safety system (EN/IEC 62061)
To verify safety integrity levels, it must be shown that the safety performance, in other words the risk reduction capability, of the created safety function is equal to or greater than the required performance target set during the risk evaluation. Using certified subsystems is advisable, because the manufacturer has already defined values for determining systematic safety integrity (SILCL) and probability of dangerous faliures per hour (PFH_d) for them.

Tip:
Verifying the achieved SIL can be conveniently done with ABB Functional safety design tool (FSDT) PC-tool.

To verify the SIL of a safety system where certified subsystems are used:

1. **Determine the systematic safety integrity for the system using SIL Claim Limit (SILCL) values defined for the subsystems.**

   SILCL represents the maximum SIL value the subsystem is structurally suitable for. SILCL is used as an indicator for determining the achieved SIL: the SILCL of the whole system should be no higher than the SILCL for the lowest subsystem.

2. **Calculate the random hardware safety integrity for the system by using the Probability of a dangerous Failure per Hour (PFH_d) values defined for the subsystems. Manufacturers of certified subsystems usually provide the PFH_d values for their systems.**

   PFH_d is the random hardware failure value that is used for determining the SIL.

3. **Use the Common Cause Failure (CCF) checklist to make sure that all the necessary aspects of creating the safety systems have been considered.**

   CCF checklist tables can be found in EN/IEC 62061 standard, Annex F.

   Calculating the points according to the list and comparing the overall score to the values listed in the standard EN/IEC 62061 Annex F, Table F.2 results to the CCF factor (β). This value is used for estimating the probability value of PFH_d.

4. **Determine the achieved SIL from the table for determining SIL.**

Example of verifying SIL (Calculation data is fictional):
Verifying the rotating shaft functional safety system:

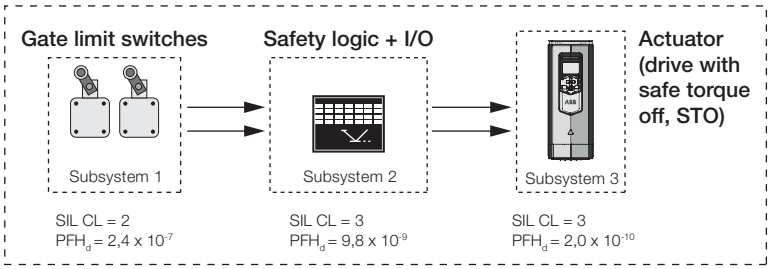


Figure 3-7 Example verification of SIL

– Systematic safety integrity:
  SIL $CL_{sys} \leq (SIL\ CL_{subsystem})_{lowest}$ -> SIL Claim Limit 2

– Random hardware safety integrity:
  $PFH_d = PFH_{d1}+PFH_{d2}+PFH_{d3} = 2{,}5 \times 10^{-7} < 10^{-6}$

  = the system meets SIL 2.

Table for determining SIL according to PFH_d value obtained from the whole safety system (in high demand/continuous mode):

SIL	Probability of dangerous failures per hour (1/h)
SIL 1	$\geq 10^{-6}$ up to $< 10^{-5}$
SIL 2	$\geq 10^{-7}$ up to $< 10^{-6}$
SIL 3	$\geq 10^{-8}$ up to $< 10^{-7}$

Table 3-1 Table for determining SIL (based on EN/IEC 62061, table 3)

Verifying PL of safety system (EN ISO 13849-1)
To verify the performance level, it must be established that the achieved PL of the corresponding safety function matches the required PL. If several subsystems form one safety function, their performance levels must be equal or greater than the performance level required for the said safety function. Using certified subsystems is advisable, because the safety performance values have already been defined for them.

Tip:
Verifying the achieved PL can be conveniently done with ABB Functional safety design tool (FSDT) PC-tool.

Note:
According to EN ISO 13849-1 MTTFd is used in defining PL and PFHd for subsystem. Only PFHd is used for defining PL for whole system!

To verify the PL of a safety system where certified subsystems are used:

1. **Determine the system's susceptibility to Common Cause Failure (CCF) using the CCF checklist.**

   CCF checklist tables can be found in EN ISO 13849-1 standard, Annex I. The required minimum score is 65 points.

2. **Determine the achieved PL with the bar graph utilizing the established:**

   – Category
   – Mean Time To dangerous Failure ($MTTF_d$)
   – Diagnostic Coverage (DC)

$MTTF_d$ is the average time it takes for a dangerous failure to occur. DC represents the portion (percentage) of all dangerous failures that can be detected by diagnostics.

More information on calculation details can be found in the EN ISO 13849-1 standard.

3. Enter the resulting values into the PL graph diagram, from which the resulting PL can be determined.

Example of verifying PL:
Verifying the rotating shaft functional safety system:

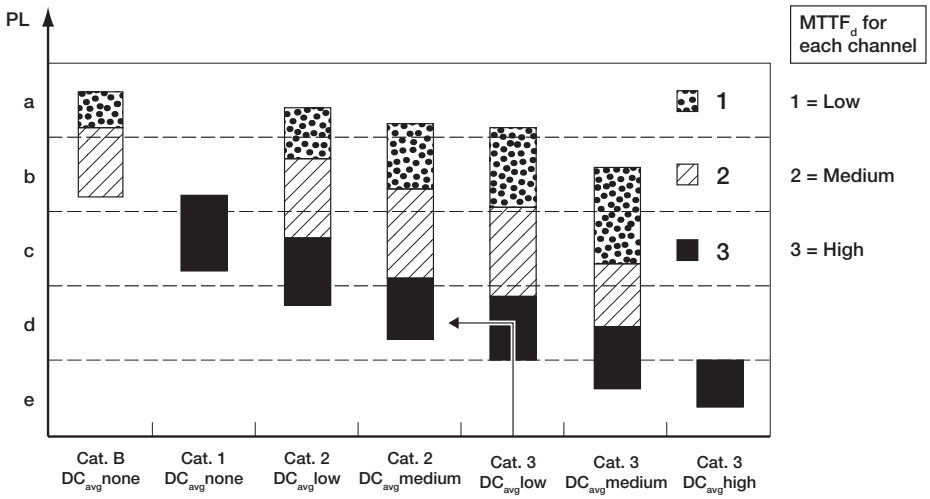


Figure 3-8 Example verification of PL (based on EN ISO 13849-1 figure 5)

To determine the achieved PL defined in the earlier example:

– designated architecture is in Category 3,
– $MTTF_d$ value is high, and
– DC average value is low.

= the system meets PL value d.

Table for determining PL according to PFH_d value obtained for the whole safety system:

PL	Probability of dangerous failures per hour (1/h)
a	$\geq 10^{-5}$ up to $< 10^{-4}$
b	$\geq 3 \times 10^{-6}$ up to $< 10^{-5}$
c	$\geq 10^{-6}$ up to $< 3 \times 10^{-6}$
d	$\geq 10^{-7}$ up to $< 10^{-6}$
e	$\geq 10^{-8}$ up to $< 10^{-7}$

Table 3-2 Table for determining the PL (based on EN ISO 13849-1 table 3)

Comparing SIL and PL values

Although methods of evaluation differ between the two standards, the evaluation results can be compared on the basis of random hardware failure.

Safety integrity level SIL	Performance level PL
no correspondence	a
1	b
1	c
2	d
3	e

Table 3-3 Table for comparing SIL and PL (based on EN ISO 13849-1 table 4)

STEP 7: Validating a functional safety system

Each safety function must be validated in order to ensure that it reduces risk as required in the risk assessment phase.

In order to determine the validity of the functional safety system, the system must be inspected against the risk assessment process carried out at the beginning of the procedure for meeting the EHSR of the Machinery Directive (see step 2 page 22). The system is valid, if it truly reduces the risks analyzed and evaluated in the risk assessment process.

STEP 8: Documenting a functional safety system

The design of the machine must be documented and relevant user documentation produced before the machine fulfills the requirements set in the Machinery Directive.

Documentation needs to be carefully produced to serve its purpose. It has to be accurate and concise, but at the same time informative and easy for the user to understand. All residual risk must be documented in the user documentation, with proper instructions on how to operate the machine safely. The documentation must be accessible and maintainable. The user documentation is delivered with the machine.

For more information on the documentation required and its nature, see the EHSR in Annex I of the Machinery Directive.

STEP 9: Proving compliance

Before a machine can be placed on the market, the manufacturer must ensure that the machine is implemented in conformance with harmonized standards. It must also be proved that the combination for each safety function of the safety-related parts meets the defined requirements.

To prove the conformance with the Machinery Directive, it must be shown that:

- Machinery fulfills the relevant Essential Health and Safety Requirements (EHSR) defined in the Machinery Directive.
- Machinery fulfills the requirements of other possible Directives related to it.
- Conformity with these requirements can be ensured by following the relevant harmonized standards.
- The technical file is up-to-date and available.
  The technical file demonstrates that the machine is in accordance with the regulations presented in the Machinery Directive.

  Note:
  Technical file has to be made available within a reasonable time should it be needed by eg authorities, and a missing technical file could provide reason to doubt the machine's compliance with the EHSR.

  The technical file should cover the design, manufacture and operation of the machinery in so far as necessary to demonstrate compliance. For more information on the contents of the technical file, see Annex VII of the Machinery Directive 2006/42/EC.

- Conformity assessment procedures have been applied.
  Special requirements for machines listed in the Machinery Directive's Annex IV are met, where appropriate.
- The EC declaration of conformity has been produced and is delivered with the machine.

Once conformity has been established, a CE marking is affixed.

Machinery that carries CE markings and is accompanied by an EC declaration of conformity is presumed to comply with the requirements of the Machinery Directive.

Glossary

CE marking
A mandatory conformity mark on machinery and many other kinds of products placed on the single market in the European Economic Area (EEA). By affixing CE marking to the product, the manufacturer ensures that the product meets all of the essential requirements of the relevant European Directive(s).

CCF, Common Cause Failure
A situation where several subsystems fail due to a single event. All failures are caused by the event itself and are not consequences of each other.

DC, Diagnostic Coverage
Diagnostic Coverage (DC) is the effectiveness of fault monitoring of a system or subsystem. It is the ratio between the failure rate of detected dangerous failures and the failure rate of total dangerous failures.

EHSR, Essential Health and Safety Requirements
Requirements that machinery must meet in order to comply with the European Union Machinery Directive and obtain CE marking. These requirements are listed in the Machinery Directive's Annex I.

EN
Stands for "EuroNorm". This prefix is used with European standards (or European versions of the IEC/ISO standards) from European organizations CEN and CELELEC. Harmonized standards also carry the prefix EN.

Harm
Physical injury or damage to health.

Harmonized standard
A European standard that has been prepared under the mandate of the European Commission or the EFTA Secretariat with the purpose of supporting the essential requirements of a directive and is effectively mandatory under the EU law.

Hazard
Potential source of harm.

IEC, International Electrotechnical Commission
A worldwide organization for standardization that consists of all national electrotechnical committees.
www.iec.ch

ISO, International Organization for Standardization
A worldwide federation of national standards member bodies. www.iso.org

$MTTF_d$, Mean Time To dangerous Failure
Expectation of the average time for a dangerous failure to occur.

PFH_d, Probability of dangerous Failure per Hour
Average probability of dangerous failure taking place during one (1) hour. PFH_d is the value that is used for determining the SIL or PL value of a safety function.

PL, Performance Level
Levels (a, b, c, d, e) for specifying the capability of a safety system to perform a safety function under foreseeable conditions.

Risk
A combination of how possible it is for the harm to happen and how severe the harm would be.

Safety function
A function designed for adding safety to a machine whose failure can result in an immediate increase in risk(s).

SIL, Safety Integrity Level
Levels (1, 2, 3, 4) for specifying the capability of an electrical safety system to perform a safety function under foreseeable conditions. Only levels 1-3 are used in machinery.

SILCL, SIL Claim Limit
Maximum safety integrity level (SIL) that can be claimed for an electrical safety system, taking account of architectural constraints and systematic safety integrity.

Subsystem
A component of a safety function that has its own safety level (SIL /PL) that affects the safety level of the whole safety function. If any of the subsystems fail, the whole safety function fails.

Index

Contact us

For more information please contact your local ABB representative or visit:

www.abb.com/drives
www.abb.com/drivespartners

3AUA0000048753 REV E EN 12.8.2014 #17212

Power and productivity
for a better world™