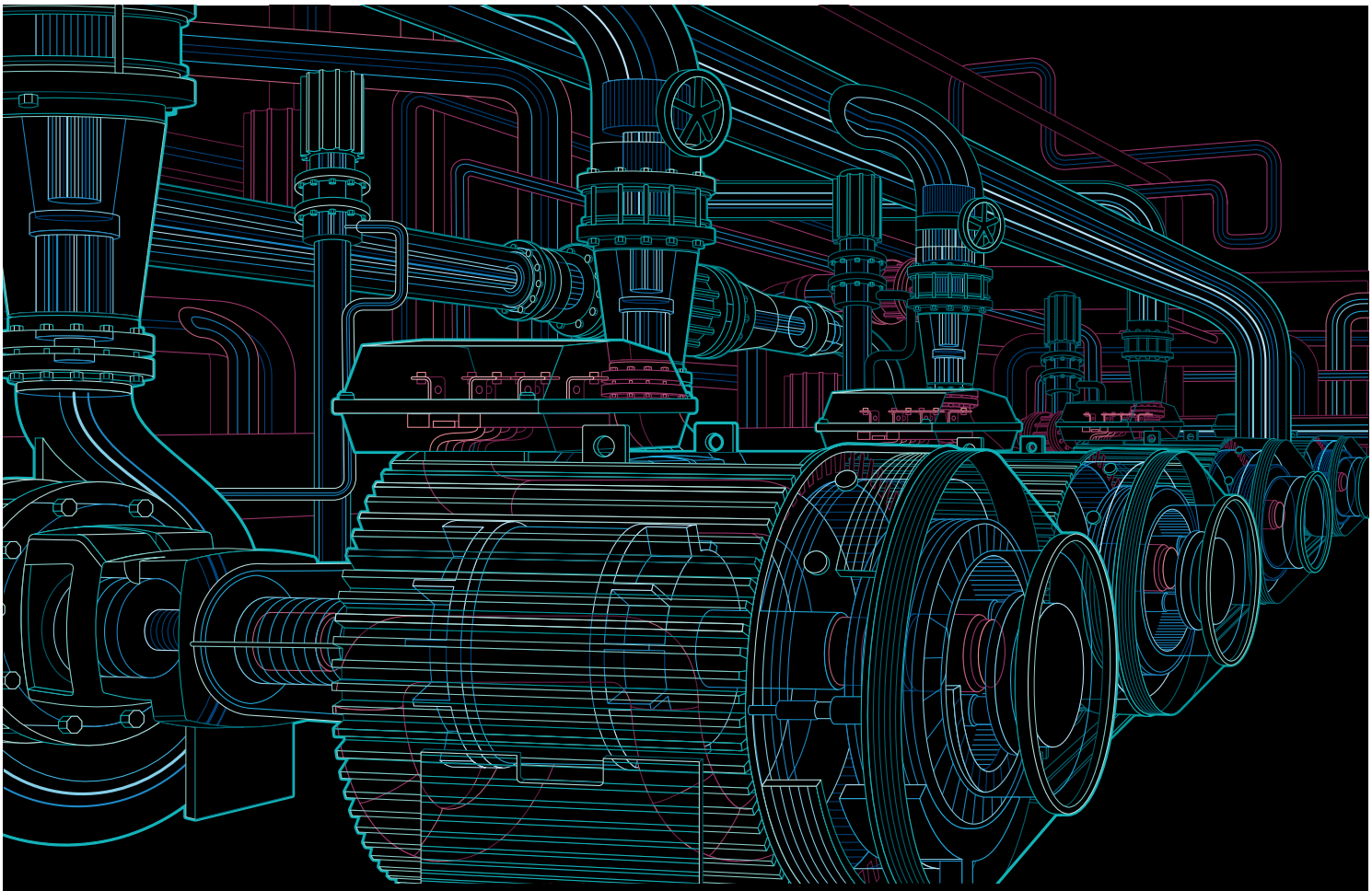


Safety and functional safety
A general guide

Power and productivity
for a better world™

This document is an informative aid only. The information and examples given are for general use only. They do not describe all the necessary details for implementing a safety system. The manufacturer of the machinery always remains ultimately responsible for the safety and compliance of the product. ABB does not accept any liability for direct or indirect injury or damage caused by the use of information contained in this document. The manufacturer of the machinery is always responsible for the safety of the product and its suitability under applicable laws. ABB hereby disclaims all liabilities that may result from this document.

Contents

Background....4
Introduction....5

Two new standards
ISO 13849-1 – for making machines safe....6-7
EN 62061 - for designing electrical safety systems....6-7

Meeting Machinery Directive requirements....8-9

Steps to meet the Machinery Directive requirements
Step 1: Assessment and risk reduction....10-11
Step 2: Establish safety requirements....12-13
Step 3: Implement functional safety....14
Step 4: Verify functional safety....15-17
Step 5: Validate functional safety....18
Step 6: Document functional safety....18
Step 7: Prove compliance....18

Glossary....19

Background

Area of growing importance

This document helps specifiers, designers, manufacturers and users of machinery, plus related personnel, gain a better understanding of the requirements of the EU Machinery Directive 2006/42/EC, and of the measures required to conform with the directive and its harmonized standards.

National laws of the European Union require that machines meet the Essential Health and Safety Requirements (EHSR) defined in the Machinery Directive 2006/42/EC. Harmonized standards listed under the Directive are one preferred way of showing compliance. This means that all new machinery must fulfill the same legal requirements when supplied throughout the EU. The same standards are also recognized in many areas outside Europe, for example, through equivalency charts, which facilitates machinery trade and machine shipments between countries within and even outside the EU.

Machine safety is one of the most rapidly growing areas of importance in industrial automation. New and improved safety strategies offer manufacturers a way of improving their productivity and competitiveness in the market. Safety becomes an integrated part of machine functionality, rather than after-thoughts added to meet regulations.

Introdution
Safety and functional safety

Functional safety systems implemented through defined processes and using certified sub-systems to achieve specific safety performance are thus becoming a must in the marketplace.

This general guide describes the standards that must be taken into account when designing a machine in order to achieve functional safety. It explains, in general terms, the process for meeting the requirements of the Machinery Directive 2006/42/EC and how CE marking, which indicates that the machinery conforms to these requirements, is attained.

In the context of this guide, the purpose of safety is to protect people from harm. Functional safety achieves this via systems that lower the probability of undesired events, thereby minimizing mishaps.

Safety standards define safety as freedom from unacceptable risk. The most effective way to eliminate risks is to design them away. But as risk reduction by design is not always possible or practical, safeguarding with static guards are often the next best option, and for several reasons. Stopping a machine quickly and safely, not only reduces risk but also increases machine uptime and productivity compared with abrupt safety stops. 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, override the machine applications to ensure safe operation. A safety-related system thus implements the required safety functions by detecting hazardous conditions and bringing operation to a safe state, by ensuring that a desired action, e.g. safe stopping, takes place.

Safety system monitoring can include machine speed, direction of rotation, stopping and standstill. When executing a safety function, e.g. monitoring a crawl speed that deviates from the expected value (i.e. is too fast), the safety system detects this deviation and actively returns machine operation to a safe state by, for example, stopping the machine safely and removing the torque from the motor shaft.

Any failure in the safety system will immediately increase risks related to machine operation.

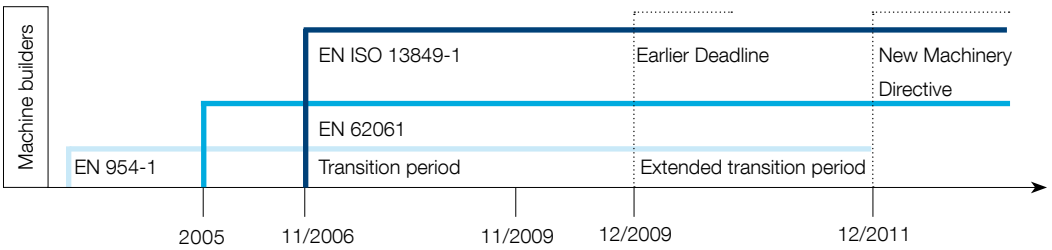
Role of the Machinery Directive 2006/42/EC

The Machinery Directive, with the harmonized standards listed under it, defines the Essential Health and Safety Requirements (EHSR) for machinery at European Union level. The idea behind the Machinery Directive is to ensure that a machine is designed and constructed to be safe 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 machine manufacturers must apply the following principles in the given order:

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

Two standards
ISO and IEC



Note: According to the convention used in the harmonized standards list, EN ISO standards are presented using the 'ISO' mark as well. EN IEC standards are presented without 'IEC', i.e. with EN only. This document now follows this convention.

Two new standards

Machine manufacturers implementing functional safety systems in compliance with the Machinery Directive can follow one of two alternative European standards developed by the International Organization for Standardization (ISO) the International Electrotechnical Commission (IEC). These are designated EN ISO 13849-1 and EN 62061 respectively. EN 62061 is applicable only to electrical control systems. Both replace the old standard EN 954-1, which will become obsolete on December 31, 2011, after a 3+2-year allowable transition period. Furthermore, both fall under the basic safety of machinery standards for risk-minimization (EN ISO 12100-1:2003) and risk-assessment in risk-reduction (EN ISO 14121-1:2007). Figure 1 illustrates this hierarchy.

The standards for electronic safety systems are formally designated as follows: EN ISO 13849-1:2008 (Safety of machinery – Safety-related parts of control system – General Principles for design), EN 62061:2005 (Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems). References to these standards in this document always apply to the above-mentioned versions.

Note: A table explaining the suitability of the two new standards for designing systems with particular technologies can be found in the standards.

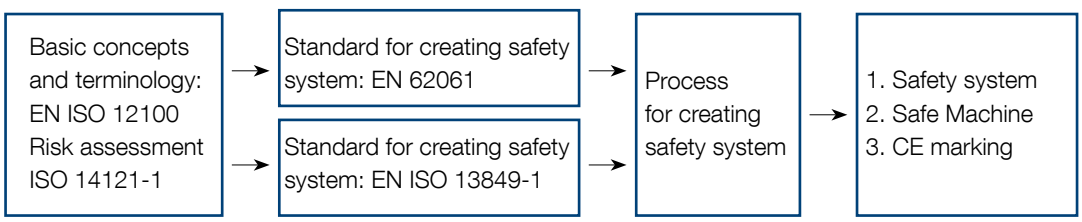
Manufacturers can choose which – if any – of the two safety system standards to use (i.e. ISO 13849-1 or EN 62061). However, to ensure congruity, it is recommended to follow the same, chosen standard all the way from beginning to end.

Following either standard leads to a very similar outcome and their resulting safety integrity levels (SIL) and performance levels (PL) are comparable (see Table 7). This document includes safety performance/integrity examples for both standards.

ISO 13849-1 – for making machines safe

ISO 13849-1 provides instructions to designers to make machines safe. These instructions include recommendations for system design, integration and validation. The standard can be used for the safety-related parts of control systems and various kinds of machinery, regardless of the technology or energy source used. It also includes special requirements for safety-related parts that have programmable electronic systems. This standard thus covers the entire safety function for all included devices (i.e. a complete safety chain such as sensor-logic-actuator).

Fig. 1.



Performance Level (PL)

ISO 13849-1 defines how to determine the required Performance Level (PL) and how to verify the achieved PL within a system. PL describes how well a safety system is able to perform a safety function under foreseeable conditions. Five possible PLs are available: a, b, c, d and e. PL ‘e’ has the highest safety reliability, PL ‘a’ the lowest. See the example on page 13.

EN 62061 – for designing electrical safety systems

EN 62061, a machine-sector-specific standard within the IEC 61508 framework, is the standard for designing electrical safety systems. It includes recommendations for the design, integration and validation of safety-related electrical, electronic and programmable electronic control systems for machinery.

EN 62061 also covers the entire safety chain, e.g. sensor-logic-actuator. As long as the entire safety function fulfills the defined requirements, individual sub-systems need not be certified.

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

Safety Integrity Level (SIL)

EN 62061 defines how to determine the Safety Integrity Level (SIL). SIL represents the reliability of safety functions. Four SIL levels are possible: 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. See the example on page 12.

Meeting Machinery Directive requirements

The Machinery Directive 2006/42/EC requires machinery to be safe. However, as zero risk can never be achieved in practice, the key objective is to minimize risk. Compliance with this goal 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.

Achieving and managing functional safety

Achieving functional safety that fulfills the EHSR of the Machinery Directive, i.e. the first of the above alternatives, involves several steps, all of which must consider the system as a whole as well as the environment with which it interacts. These steps include risk assessment, identification of required safety functions risk reduction through implementing the safety function, and ensuring that the safety function performs as intended.

All functional safety activities must be managed during the lifecycle of the machine. A project management and quality management system specified in the form of a safety plan will help meet these goals.

Note: Unlike EN 62061, ISO 13849-1 does not specify the safety plan activities listed above. However, similar activities are needed to fully meet the requirements of the Machinery Directive.

Safety plan

A safety plan for meeting the requirements of the Machinery Directive is specified in EN 62061. It 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 a strategy for configuration management, and includes plans for verification and validation. This plan needs to be designed and documented for each safety system, and updated when necessary.

When a safety plan according to EN 62061 has been created, the more practical aspects can begin. These follow the step-by-step procedure summarized in Table 1, starting with risk assessment and reduction.

Table 1. Steps to meet Machinery Directive requirements for functional safety. Each of these seven steps is explained in more detail below.

Table 1.

Step	Task
Step 1: Assessment and risk reduction	Analyze risks and evaluate how to eliminate or minimize them (3 steps strategy see EN ISO 12100-1)
Step 2: Establish safety function requirements	Define what functionality and safety performance is needed to eliminate the risk or reduce it to an acceptable level.
Step 3: Implement functional safety	Design and create the safety system functions
Step 4: Verify functional safety	Ensure that the safety system meets the defined requirements
Step 5: Validate functional safety	Return to risk assessment and ensure that the safety system actually succeeds in reducing risks as specified
Step 6: Document functional safety	Document the design and produce user-documentation
Step 7: Prove compliance	Prove the machine‘s compliance with EHSR of the Machinery Directive through compliance assessments and technical file

Step 1: Assessment and risk reduction

Risk assessment

Risk assessment is a process that analyzes and evaluates risks, which are regarded as a combination of the consequence of harm and the probability of the harm occurring when exposed to a hazard. According to the new Machinery Directive 2006/42/EC, it is mandatory to perform a risk assessment for a machine, and the results must be taken into account when designing a machine.

Any risk considered 'high' must be reduced to an acceptable level via design changes or by applying appropriate safety measures. The assessment process helps machinery designers design inherently safe machinery. Assessing risks at the design phase is very important as it is generally more effective than providing user instructions on how to operate the equipment safely. Risk assessment according to ISO 12100-1 (the safety of machinery standards for risk-minimization, see Fig. 1) consists of two parts: risk analysis and risk evaluation. Risk analysis means identifying and estimating the risks, risk evaluation means deciding whether the risk is acceptable, or if risk reduction is necessary.

Risk evaluation thus depends on the results of the risk analysis. Similarly, decisions regarding the necessity of risk reduction are made according to the risk evaluation procedure. Note that risk evaluation must be carried out separately for each identified hazard.

Fig. 2 outlines the risk analysis and evaluation steps according to ISO 14121-1, the safety of machinery standards for risk-assessment in risk-reduction (see Fig. 1).

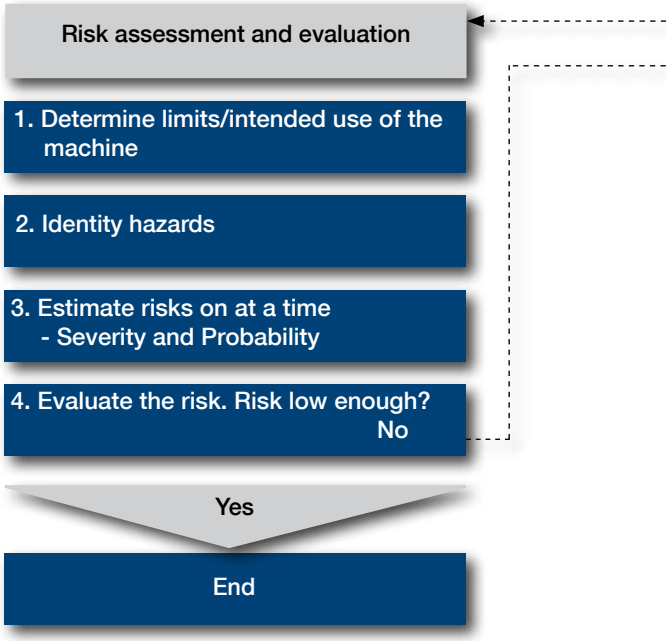
The limits of the machine referred to in Fig. 2 include limits of use, spatial limits, ambient or environmental limits, and lifetime limits. Estimating risk severity covers its potential consequences, while risk probability covers frequency, probability and avoidance.

Fig 2. Risk assessment and evaluation according to ISO 14121-1. Always document this process and its results for each individual hazard.

If the outcome of the risk analysis and evaluation outlined in Fig. 2 is YES, the risk reduction target is considered met and the risk process ends. In the latter case, the machine has reached the adequate level of safety required by the Machinery Directive.

If the outcome is NO, i.e. the risk remains unacceptable, apply risk reduction measures and then return to step 2 in the risk analysis.

Fig. 2.



Risk reduction

The most effective way to minimize risks is to eliminate them in the design phase, for example, by changing the machine design or work process.

However, if this is not possible, reduce risks and ensure conformance in accordance with the Machinery Directive requirements by applying the harmonized standards under it. ISO 12100-1 divides the method for risk reduction into three main steps:

- Inherently safe design measures (creating a safer design, changing the process).
- Safeguarding and complementary protective measures (safety functions, static guarding).
- Information for use (warning signs, signals and devices on the machine and in the operating instructions, protective measures taken by the user for example training).

Machine users/organizations are a valuable source of safety feedback and designers should seek their input when defining protective measures.

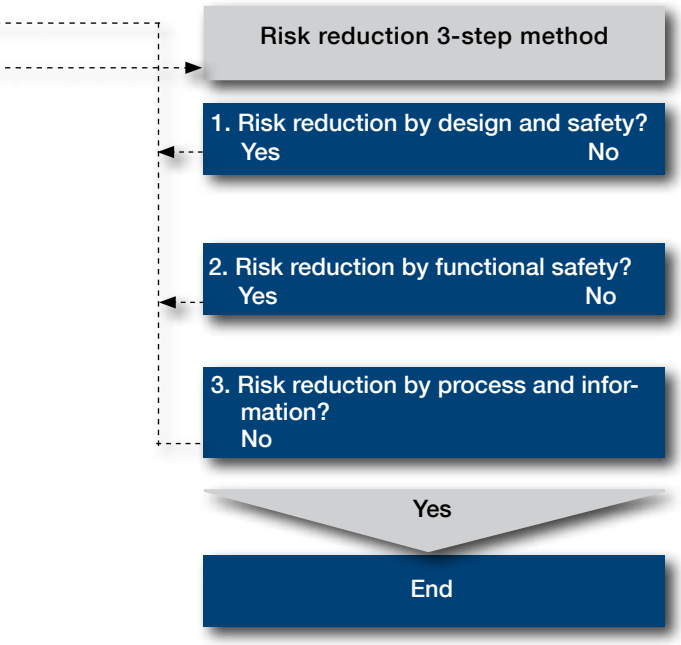
Fig. 2 illustrates this three-step risk-reduction workflow.
Fig. 2 Risk reduction according to ISO 12100-1. Always document residual (remaining) risks in the operating instructions.

The latter aspect (information on use) is called residual risk management. Residual risk is the risk that remains when all protective measures have been considered and implemented. Technology measures alone are never able to achieve a state of zero risk, hence some residual risk always remains. These risks must be documented in the operating instructions.

Machine-users and organizations have an important role to play in risk reduction and are generally provided with relevant information by the machine designer (manufacturer). Reduction measures commonly undertaken by an organization include:

- Introducing safe working procedures, work supervision and permit-to-work systems.
- Provision and use of additional safeguards.
- Use of personal protective equipment.
- User training.
- Ensuring that operating and safety instructions are read and acted on.

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. Repeat the risk assessment process to achieve this.



Step 2: Establish safety requirements

Additional safeguarding needs to be specified once the risk reduction that can be achieved via design changes has been obtained. This additional risk reduction measure uses functional safety solutions.

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

Table 2. SIL assignment table showing the procedure to follow when determining safety integrity. The overall result of the above example is SIL 2.

Safety functions

A safety function is a function of a machine whose failure can result in an immediate increase in risk. Simply put, it is a measure taken to reduce the likelihood of an unwanted event occurring and exposing a hazard. A safety function is not part of machine operation: if such a function fails, the machine can still operate normally, but the risk of injury from its operation increases.

Defining a safety function is a key issue. This always includes two components:
- Action (what must be done to reduce the risk).
- Safety performance (SIL or PL – Safety Integrity Level and Performance Level respectively).

Example of a safety function:

Hazard: An exposed rotating shaft may cause injury if a person gets too close.
Action: To prevent personal injury, the motor must stop within one (1) second from opening the safety gate. After the safety function that executes the action has been identified, its required safety level is determined as described below. This completes defining the safety function.

Safety performance/integrity

Safety integrity measures the performance of a safety function. It helps quantify the likelihood of the safety function being achieved when requested. The required safety integrity for a function is determined during risk assessment and is represented by the achieved SIL or PL, depending on the standard used. SIL and PL use different evaluation techniques for a safety function, but their results are comparable and the terms and definitions are similar for both.

How to determine the required SIL (EN 62061)

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

Table 2.

Probability of occurence of harm

Fr **Frequency, duration**		**Pr** **Probability of hazardous event**		**Av** **Avoidance**	
<= hour	5	Very high	5		
> 1h <= day	**5**	Likely	4		
> day <= 2 wks	4	Possible	**3**	Impossible	5
> 2 wks <= 1 yr	3	Rarely	2	Possible	**3**
> 1 yr	2	Negligible	1	Likely	1
					Total: 5 + 3 + 3 = 11

Severity of harm

SIL Class

Se **Consequences (severity)**		**Class Cl** **3-4**	**5-7**	**8-10**	**11-13**	**14-15**
Death, losing an eye or arm	4	SIL2	SIL2	SIL2	SIL3	SIL3
Permanent, losing fingers	**3**			SIL1 →	**SIL2**	SIL3
Reversible, medical attention	2				SIL1	SIL2
Reversible, first aid	1	Other measures				SIL1
						SIL2 safety function is required.

Example:

Table 2 shows a SIL assignment table containing parameters used in determining the point values in the example of a hazard analysis carried out for an exposed rotating shaft.

- A person is exposed to the hazard several times a day. Frequency (Fe) is thus high = 5.
- It is possible that the hazard will take place. Therefore probability (Pr) = 3.
- The hazard can be avoided, so avoidance (Av) = 3.
- The sum of Fe, Pr and Av (5 + 3 + 3) = 11.
- The determined consequence of the hazard is permanent injury, possibly loss of fingers. Hence severity (Se) = 3.

The overall result as read from Table 2 is SIL 2.
The tables used for determining these points are presented in the standard. After the required SIL has been defined, implementation of the safety system can begin (see Step 3: Implement functional safety).

How to determine the required PL (ISO 13849-1)

PL is an alternative parameter to SIL. To determine the required PL, select one of the alternatives from the following categories and create a 'path' to the required PL in the risk graph (Fig. 3), which lists the resulting performance level as a, b, c, d or e.

Determine the severity of injury/damage:
- S1 Slight, usually reversible injury
- S2 Severe, usually irreversible injury, including death

Determine the frequency and duration of exposure to the hazard:
- F1 Rare to often and/or short exposure
- F2 Frequently to continuous and/or long exposure

Determine the possibility of preventing the hazard or limiting the damage caused by the hazard:
- P1 Possible under certain conditions
- P2 Hardly possible

Fig. 3 PL risk graph showing the procedure to follow when determining safety performance level. The overall result of the above example is PL d.

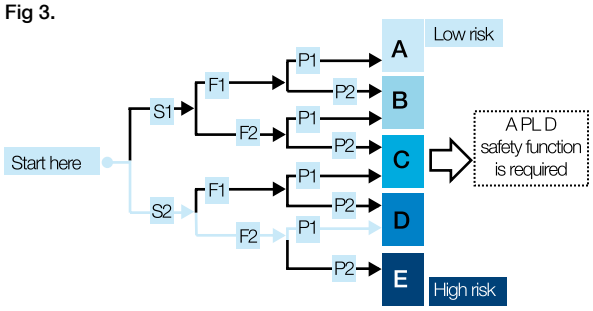
Example:

Hazard analysis for an exposed rotating shaft.
- The consequence is severe, irreversible injury. Severity = S2.
- A person is exposed several times a day. Frequency = F2.
- It is possible to avoid or limit the harm caused. Possibility =P1.

The path leads to the Required PL (PLr) value d.

As with SIL, the tables used to determine the points are presented in the standard. Similarly, once the PLr has been defined, implementation of the safety system can begin.

Fig 3.



Step 3: Implement functional safety

To construct a safety function, design it to meet the required SIL/PL specified in step 2: Establish safety requirements. Using certified sub-systems when constructing functional safety systems could save safety system designers a lot of work. For example, implementing safety functions is more convenient when certain safety and reliability calculations are already made and the sub-systems are certified.

Implementation and verification processes are iterative and run parallel with each other. Use verification as a tool during implementation to ensure that the defined safety level is reached with the implemented system. For more information on verification, see Step 4: Verify functional safety. Several calculation software programs for verifying functional safety systems are available. These programs make creating and verifying the system more convenient.

Note: If certified sub-systems are not used, it may be necessary to carry out safety calculations for each sub-system. Standards EN 62061 and ISO 13849-1 include information on the process and calculation parameters needed.

Note: To fulfill the EHSR set by the Machinery Directive, all sub-systems of a functional safety system must meet at least the required SIL/PL value of the system.

The general steps for implementing a functional safety system include:

1. Defining the safety requirements as SIL or PL according to standard EN 62061 or EN ISO 13849-1.

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

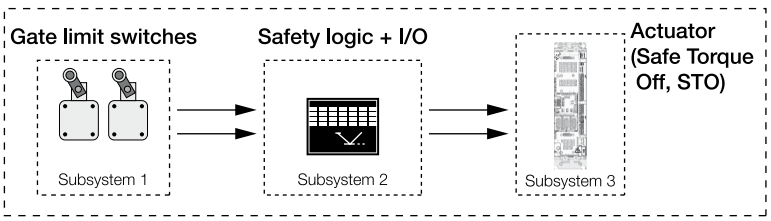
   Determine category B, 1, 2, 3 or 4 as presented in ISO 13849-1, or designated architecture A, B, C or D as presented in EN 62061. Do this for the sub-systems and the whole system. For more information on designated architectures, see the respective standards.

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

   Use either certified sub-systems (strongly recommended) or perform safety calculations for each sub-system. Add together the sub-system safety levels to establish the safety level of the complete system. Fig. 4 shows the structure of a safety function.

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 does not perform correctly due to careless installation is of little use. It may even pose a risk in itself.

Fig. 4



Step 4: Verify functional safety

Step 4: Verify functional safety

Verifying safety system SIL (EN 62061)
Verify safety integrity levels by showing that the safety performance of the created safety function, i.e. its reliability, is equal to or greater than the required performance target set during risk evaluation. Certified sub-systems are again recommended because their manufacturer has already defined values for determining systematic safety integrity (SILCL) and random hardware safety integrity (PFHd) for them.

To verify the safety system SIL where certified sub-systems are used:

1. Determine the systematic safety integrity for the system using SIL Claim Limit (SILCL) values defined for the sub-systems.

   SILCL represents the maximum SIL value for which the sub-system is structurally suitable. SILCL is an indicator for determining the achieved SIL: the SILCL of the whole system can not be higher than the SILCL for the lowest sub-system.

2. Calculate the random hardware safety integrity for the system using Probability of a dangerous Failure per Hour (PFHd) values defined for the sub-systems. PFHd is the random hardware failure value that is used for determining the SIL. Manufacturers of certified sub-systems usually provide PFHd values for their systems.

3. Use the Common Cause Failure (CCF) checklist to make sure that all necessary aspects of creating the safety systems have been considered. CCF checklist tables can be found in EN 62061 standard, Annex F.

4. Calculate the points according to the list and compare the overall score to the values listed in the standard EN 62061 Annex F, Fig. 6 and Table 4 results in the CCF factor (β). This value is used to estimate the probability value of PFHd.

5. Determine the achieved SIL from Table 3.

Fig. 5

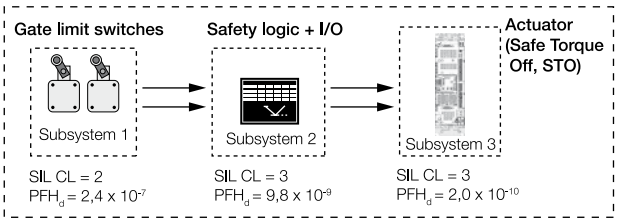
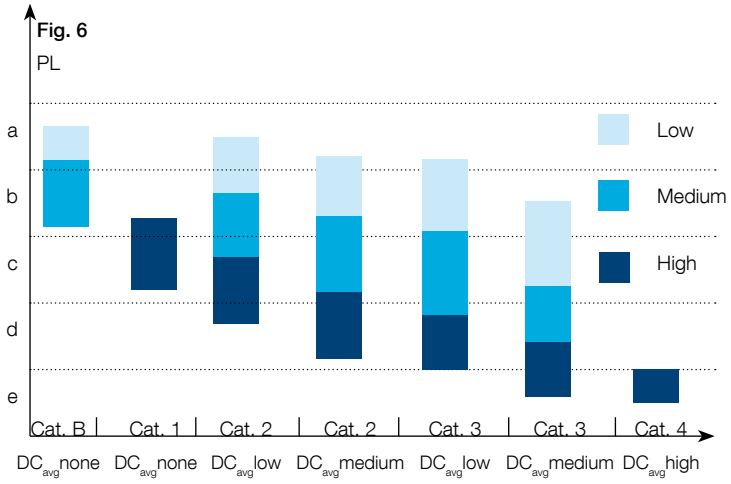


Table 3. High demand mode values shown here.

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

Fig. 6



MTTFd: Low 3 years ≤ MTTFd < 10 years
Medium 10 years ≤ MTTFd < 30 years
High 30 years ≤ MTTFd ≤ 100 years

Note: Channel MTTFd can only be up to 100 years. Single component (subsystem) MTTFd can be higher

Example:

Verifying SIL for the rotating shaft functional safety system (Fig. 5).

Systematic safety integrity:
SILCLsys ≤ (SIL CLsub-system)lowest -> SIL Claim Limit 2

Random hardware safety integrity:
PFHd = PFHd1+PFHd2+PFHd3 = 2.5 x 10-7 < 10-6

The system meets SIL 2 according to Table 3.
Table 3. Determine SIL according to the PFHd value obtained from the whole safety system. In the above example, the system meets SIL 2.

Verifying safety system PL (ISO 13849-1)

To verify performance level, establish that the PL of the corresponding safety function matches the required PLr.
If several sub-systems make up one safety function, their performance levels must be equal to or greater than the performance level required for the safety function. Certified sub-systems are recommended as the safety performance values will have already been defined for them.

To verify the PL of a safety system where certified sub-systems are used:

Determine the system's susceptibility to Common Cause Failure (CCF) using the CCF checklist. The required minimum score is 65 points. (CCF checklist tables can be found in ISO 13849-1:2008 standard, Annex I).

Determine the achieved PL with the bar graph utilizing the established:
- Category
- Mean Time To dangerous Failure (MTTFd)
- Diagnostic Coverage (DC)

MTTFd is the average time it takes for a dangerous failure to occur. DC represents the number of dangerous failures that can be detected by diagnostics. More information on calculation details can be found in the ISO 13849-1 standard.

Enter the resulting values into the PL graph diagram (Fig. 6), from which the resulting PL can be determined.

Example of verifying PL:

Verifying the rotating shaft functional safety system (Fig. 6).

Fig. 6. Verifying PL for the rotating shaft example. In the above example, the system meets PL d.

To achieve the PLr defined in the earlier example:

- The designated architecture is in Category 3.
- MTTFd value is high.
- DC average value is low.

The system thus meets PL value d according to Fig. 6. Table 4 shows how to determine PL according to PFHd value obtained for the whole safety system. The result (d) is the same.

Comparing SIL and PL values

Although the methods of evaluation between the two standards differ, the results can be compared on the basis of random hardware failure, as Table 5 shows.

Table 4. Determine PL according to PFHd value

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 5. Comparing SIL and PL values

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

Steps 5, 6 and 7

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

Step 5: Validate functional safety

Each safety function must be validated to ensure that it reduces risk as required/defined in Step 1: Assess and reduce risks.

To determine the validity of the functional safety system, inspect it against the risk assessment process carried out at the beginning of the procedure for meeting the EHSR of the Machinery Directive. The system is valid if it truly reduces the risks analyzed and evaluated in this process.

Step 6: Document functional safety

Before the machine can fulfill the requirements of the Machinery Directive, its design must be documented and relevant user documentation produced.

Documentation needs to be carefully produced. It has to be accurate and concise, but at the same time informative and easy for the user to understand. User documentation must document all residual risk and contain proper instructions on how to operate the machine safely. It must be accessible and maintainable. User documentation is delivered with the machine.

Step 7: Prove compliance

Before a machine can be placed on the market, the manufacturer must ensure that the EHSR are fulfilled and presumption is given by conformance with harmonized standards. It must also be proved that the combination of the safety-related parts meets the defined requirements for each safety function.

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

- The machinery fulfills the relevant Essential Health and Safety Requirements (EHSR) defined in the Machinery Directive.
- The machinery fulfills the requirements of other Directives related to it. (Conformity with both above 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.
- 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.

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 VI of the Machinery Directive 98/37/EC, or Annex VII of the new Machinery Directive 2006/42/EC after the new directive is applicable.

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
CE marking shall mean a marking by which the manufacturer indicates that the product is in conformity with the applicable requirements set out in Community harmonisation legislation providing for its affixing; (NLF R1 16)

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

DC, Diagnostic Coverage
The effectiveness of fault monitoring of a system or sub-system. 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 thereby obtain CE marking. These requirements are listed in the Machinery Directive's Annex I.

EN
Stands for European Standard ('EuroNorm').

Functional safety
Functional safety is part of the overall safety that depends on a system or equipment operating correctly in response to its inputs.

Harm
Physical injury or damage to health.

Harmonized standard
'harmonised standard' shall mean a standard adopted by one of the European standardisation bodies listed in Annex I to Directive 98/34/EC on the basis of a request made by the Commission in accordance with Article 6 of that Directive; (NLF R1 9)

Hazard
Potential source of harm.

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

Other references:

Technical guide No.10	Doc.No: 3AVA000048753 rev.B
Safety Handbook	Doc.No: 1SAC103201H0201
Approach to Functional Safety and reliability - Electromechanical and electrical components	Doc.No: 2CMT002568
Functional Safety and reliability data	Doc.No: 2CMT00254

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

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

PFHd, Probability of dangerous Failure per Hour
Average probability of dangerous failure taking place during one (1) hour. PFHd 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.

PLr
Required Performance Level (based on risk evaluation).

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

Safety
This is freedom from unacceptable risk of physical injury or of damage to the health of people, either directly, or indirectly as a result of damage to property or to the environment.

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.

Sub-system
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 sub-systems fail, the whole safety function fails.

Contact us

www.abb.com/drives
www.abb.com/lowvoltage
www.abb.com/motors&generators
www.abb.com/plc

www.abb.com

Power and productivity
for a better world™