CHAPTER 10
MACHINE SAFETY

Lecture material for TTK 4175 Instrumentation Systems and Safety at the Department of Engineering Cybernetics, Norwegian University of Science and Technology (NTNU).

Author: Professor Mary Ann Lundteigen, Department of Engineering Cybernetics

The essence of a safe machine?

Illustration generated by Microsoft Copilot (powered by OpenAI), July 2025

The content is updated regularly to improve precision and ensure relevance, which is reflected in the revision number. Please reach out to mary.a.lundteigen@ntnu.no if you have comments or suggestions for improvement.

Rev: 2.0/2026

Revision tracking (most recent)

Rev	Date	Modifications
2.0/26	01.07.2026	Revised with edits from the spring semester

Contents

10 Machine safety 3
10.1 Abbreviations 3
10.2 Regulations, EU directives, and standards 4
10.2.1 Systems covered by the MD 5
10.2.2 Harmonized standards for machinery 7
10.3 Application of the MD 8
10.3.1 Incorporate essential H&S requirements 8
10.3.2 Perform a risk assessment and propose risk-reduction measures 9
10.3.3 Prepare declaration of conformity and user manual 10
10.4 Risk assessment methods per ISO 12100 10
10.4.1 Define the machine limits 11
10.4.2 Identify hazards 12
10.4.3 Estimate and evaluate risk 13
10.4.4 Propose risk-reducing measures 14
10.5 Role of ISO 13849 and IEC 62061 15
10.5.1 Machinery safety functions 15
10.5.2 IEC 62061 vs ISO 13849 17
10.6 Application of ISO 13849 17
10.6.1 Determine the PL requirement, PL_r 18
10.6.2 Select architecture category based on PL_r 19
10.6.3 Case study 1: Adding SIF to a circular saw 22
10.6.4 Case study 2: An alternative architecture of the SIF 23
10.7 Application of IEC 62061 24
10.7.1 Determine the SIL requirement 25
10.7.2 Determine architectural constraints 26
10.7.3 Calculate PFH and compare with SIL 26
10.7.4 Choice of failure rate 27
10.7.5 Measures to avoid systematic faults 28
10.7.6 Case study 1 repeated: Door sensor system 28
10.7.7 Implication of interval T and SIL follow-up 29
10.8 Bibliography 31

10 Machine safety

Machines and assemblies of machines, collectively referred to as machinery, constitute a large product category used by both private consumers and industry. They have rotating and moving parts that can harm people operating them or those nearby unless safety precautions are made in the way the machines are designed and operated. Therefore, authorities provide laws and rules about safety requirements for design and use. This chapter explains some of the requirements that apply to safety functions implemented for machinery involving electrical, electronic, and programmable electronic (E/E/PE) systems. In other words, requirements ensure the functional safety of machinery. The main topics of the chapter are summarized in Fig. 1.

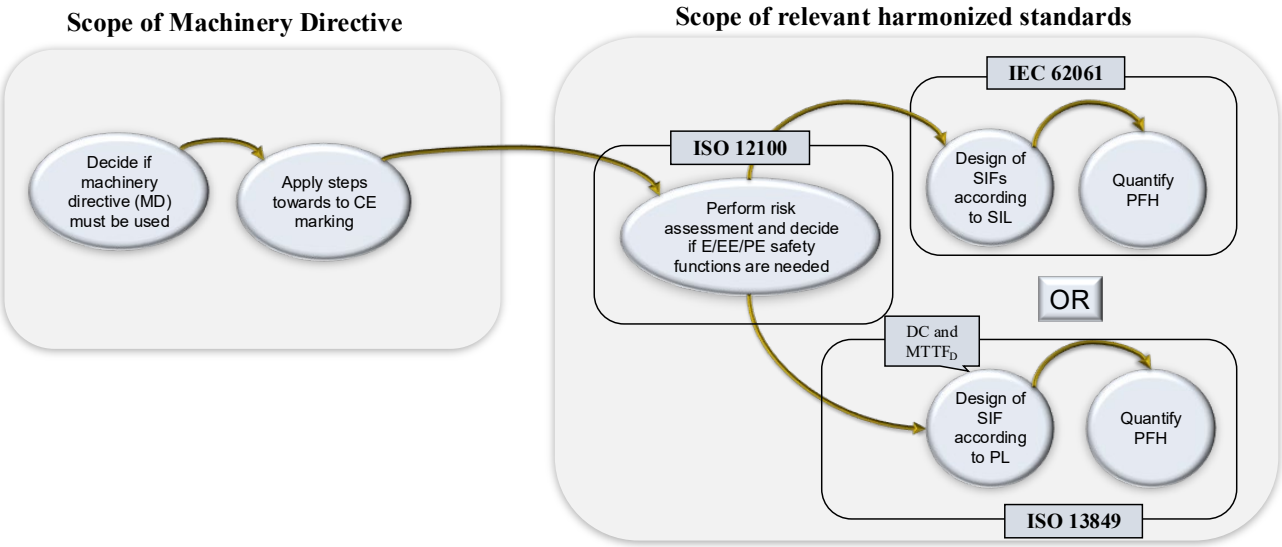

Fig. 1. Overview of topics in this chapter

We will start by defining what we mean by a machine in general and what types of machines are within the scope of the MD and implemented in the Norwegian regulation "Maskinforskriften". The MD is published by the European Commission (EC) and applies to all machinery products used in private and commercial settings within the EU market. As with most regulations, the MD provides high-level requirements, while the EC provides a list of international and European standards with more guidance on implementation. Among these, we are focusing on three standards: ISO 12100 (2010) covering procedure for risk assessment and the two standards on functional safety of machinery, IEC 62061 (2021) and ISO 13849 (2023).

10.1 Abbreviations

ALARP	As low as reasonably practicable (a way of defining risk acceptance criteria)
B10	The (expected or experienced) number of cycles until 10% of the component (of a population at test) fail (primarily as a result of wear)
$B10_D$	B10 value considering dangerous (D) failures only
CE	Conformité Européene
CCF	Common cause failure
DC	Diagnostic coverage
DD	Dangerous detected
DU	Dangerous undetected
FE	Final element
H&S	Health and Safety
HFT	Hardware fault tolerance
IE	Input element
LS	Logic solver

MD	Machinery Directive
MTTF	Mean time to failure
$MTTF_D$	Mean time to failure considering dangerous (D) failures only
OM	Other measures
PFD	Probability of failure on demand
PFH	Probability of having a dangerous failure per hour, alternatively, average frequency of dangerous failures over a given time (measured in hours)
PL	Performance level
S	Safe
SFF	Safe failure fraction
SIF	Safety instrumented function
SIL	Safety integrity level
SIS	Safety instrumented system
SRCS	Safety-related control system (SIS for machinery, IEC 62061)
SRP/CS	Safety-related parts of control systems (SIS for machinery, ISO 13849)

For abbreviations related to standardization organizations, such as CEN, CENELEC, IEC, and ISO, see Chapter 1.

10.2 Regulations, EU directives, and standards

Everyone who manufactures or sells machines in Norway must meet the Norwegian regulation "Forskrift om maskiner" requirements available from Lovdata. The content for the regulation is aligned with the European Machinery Directive 2006/42/EC (2006), from now on abbreviated as MD, a directive that Norway must follow under the European Economic Area (EEA) Agreement.

The MD applies to anyone involved in the manufacturing, rebuilding, or selling of machinery and machinery-related products in the EU market. The MD follows the organization and structure of the new approach for EU directives (see Chapter 1) so that it:

- Covers a large family of machinery products, i.e., what is defined as machines or machine-related equipment within the scope of the directive
- The directive focuses on general health and safety requirements that remain valid over time, even when technology develops. Requirements relate to:
    - Functions that must be in place to ensure safe behavior in operation and during maintenance
    - There is a need to carry out a risk assessment to find the specific risks of a machine and the corresponding need for risk-reducing measures. What is meant by risk-reducing measures is explained later.
- The directive is complemented by a list of harmonized standards with more detailed requirements about how the regulatory requirements can be met. The standards will be able to address more recent technological developments
- Preparing a user manual with the necessary safety instructions
- Filling out the declaration of conformity that explains:
    - Which directives and (harmonized) standards have been applied
    - The person responsible for signing the declaration
    - The codes naming the notified bodies involved in certifying or assessing the products
- Placing the CE marking on the machine

The European Commission has issued a new Machinery Regulation 2023/1230 (2023) to replace the 2020/42/EC MD. The new regulation enters into force on the 20th of January 2027, meaning that all manufacturers of machines must ensure that their products satisfy these requirements by this date. New rules address autonomous machines, human-machine collaboration, safe use of artificial intelligence (AI), and cybersecurity. The Norwegian Government has made a webpage to inform about the status and adoption of the new regulation.

The Norwegian regulation on machinery is anchored in the Norwegian act on product liability, called "Lov om produktansvar," which focuses on general aspects of consumer and user product safety. Employers of personnel who use and maintain machinery must follow the Norwegian regulation "Forskrift om utførelse av arbeid" concerning work execution, the use of work equipment, and associated technical requirements. The regulation mandates that employers take necessary protective measures to prevent personnel injuries. The regulation anchors itself in the Working Environment Act "Lov om arbeidsmiljø, arbeidstid og stillingsvern". Fig. 2 summarizes the relationships between the regulations, laws, and EU directives.

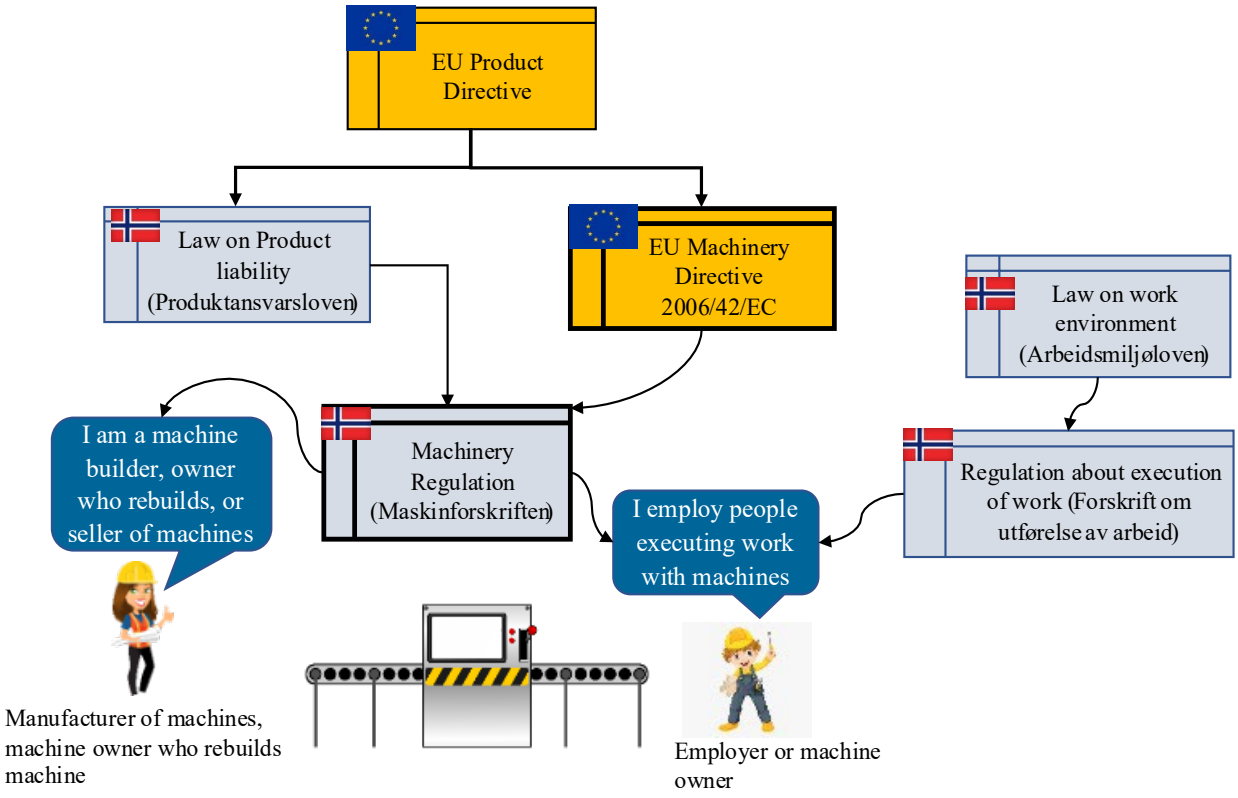

Fig. 2. Relationship between regulations, laws, and EU directives relevant to

The Machinery Directive (and the Norwegian machinery regulation) applies to machine builders. A machine builder is one who:

1. Builds machines (complete and partially completed) for commercial sale
2. Installs and assembles machines (complete and partially completed) of various origins (from different manufacturers)
3. Modifying an existing machine
4. Designing and building machines for one's own use

The user, i.e., the company that buys a machine for use, may therefore become a machine builder if it modifies some of the machine's functionality. The same happens to the company if they integrate several machines purchased individually.

The Norwegian regulation and the MD are identical in content, and for simplicity, we will refer only to the MD from now on.

10.2.1 Systems covered by the MD

The MD focuses on the safety of machinery and the requirements applicable to individual machines and their related components. According to the direction, a machine is a system that:

1. Has a drive system (but *not* from animals or humans)

2. Consists of several parts, at least one of which is movable
3. Performs a well-defined task that depends on force and movement.

In practice, there may be borderline cases in which it is difficult to decide whether equipment is a machine. One such example is a valve with an actuator. The actuator has moving parts, and the valve and actuator together perform a well-defined task (open or close). However, the MD does not regulate this system unless the actuator has a motor drive. It means that actuators operated by pressurized air or hydraulics are not considered machines.

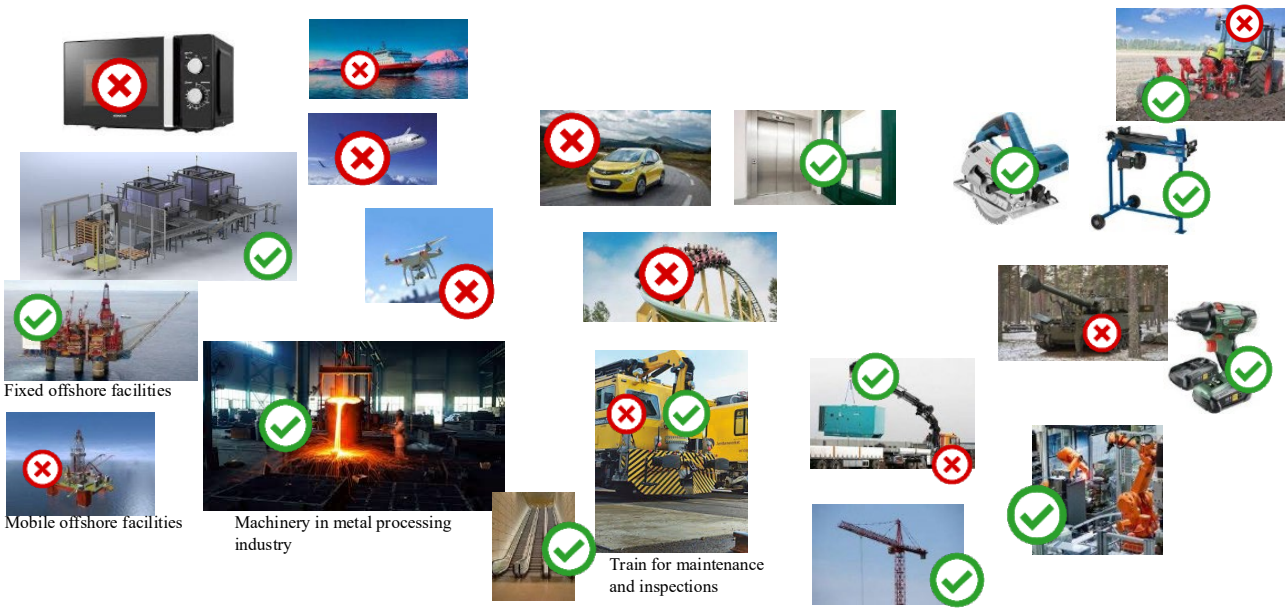

Fig. 3. Examples of what are covered by the Machinery Directive

The MD excludes specific machine types and industrial applications, as shown in Fig. 3. The explanation is that these sectors and applications have additional regulations that incorporate machine safety.

The MD extends beyond machines and covers equipment used with a machine:

- Interchangeable equipment
- Safety devices (also referred to as protective measures/devices)
- Lifting accessories
- Chains, ropes, and webbing
- Removable mechanical transmission devices
- Partly completed machinery

From the bullet list, interchangeable equipment means a component within the machine that is replaceable and, if replaced, could change the machine's function. A safety or protective device, on the other hand, is a technical device that:

- Fulfills a safety function added to make the machine safer
- It is independently placed and sold on the market (independent of the machine)
- Does not affect the operation of the machine itself

Examples of safety or protected devices, such as those in shown in Fig. 4. are:

- Sensors that can detect people close to the machine (such as light curtains)
- Safety PLC is independent of the machine's control system
- Emergency stop button
- Two-hand control that requires both hands to be involved to start and run the machine manually
- Switches operated to stop dangerous movements on machine

- Exhaust system to record emissions from machines
- Systems and facilities to reduce noise emissions and vibrations

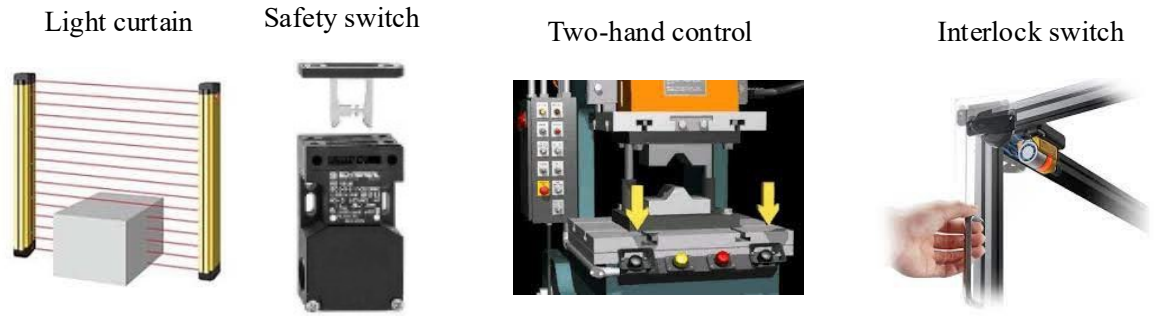

Fig. 4. Examples of safety (or protective) devices

10.2.2 Harmonized standards for machinery

The MD provides general and function-oriented requirements, such as that the machine shall not start suddenly if the user has stopped it. In addition, the European Commission publishes lists of European and international standards that can be used for detailed implementation; standards on these lists are called **harmonized standards**. Harmonized standards for electrical, electronic, and programmable systems are published by the European standardization organizations CEN and CENELEC.

A standard published by CEN or CENELEC always includes "EN" for European Norm in its title. However, CEN and CENELEC do not develop standards if international standardization bodies, such as the IEC and ISO, have already published standards on the same topics. If CEN or CENELEC adopts an existing ISO or IEC standard, it will simply add "EN" before "IEC" or "ISO" in the standard's name. For example, for functional safety, the two international standards IEC 62061 and ISO 13849 have been adopted by CEN and CENELEC as harmonized standards reflected by the coding EN IEC 62061 and EN ISO 13849. We will refer to the standards as IEC 62061 and ISO 13849 for simplicity.

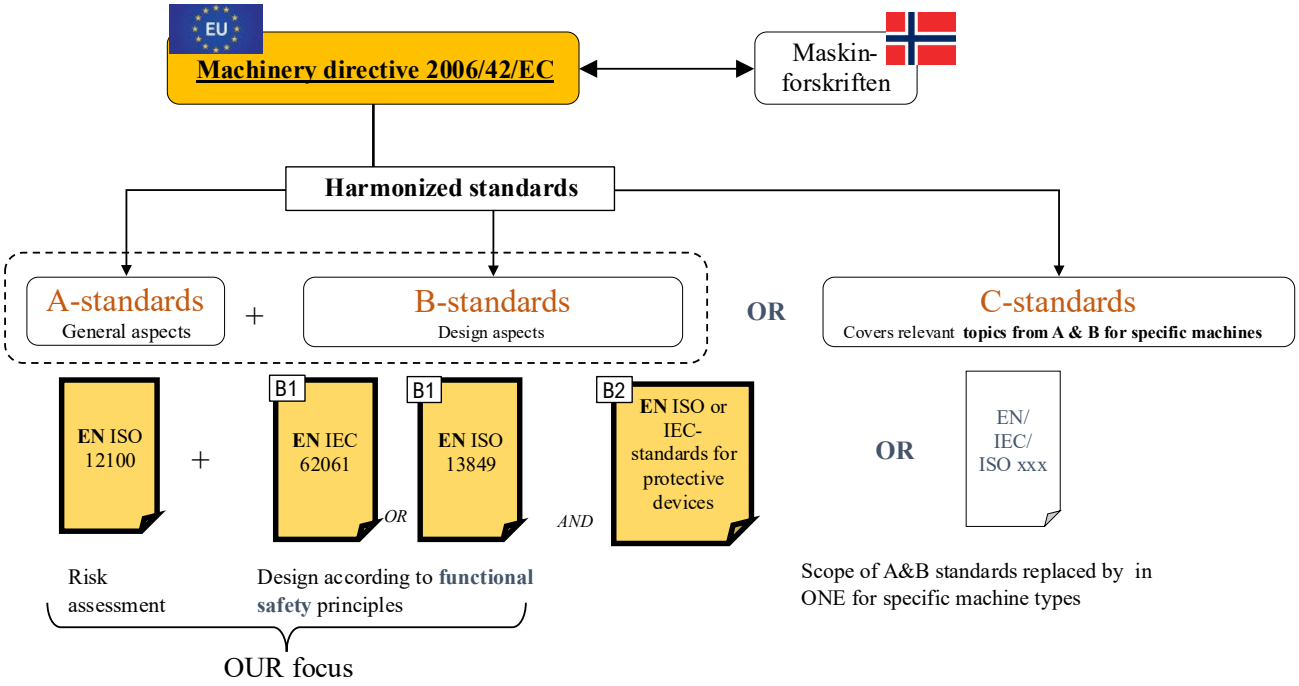

Fig. 5. Categories of harmonized standards for machinery

All harmonized standards associated with the MD can be found on the single market economy webpage. In total, there are several hundred harmonized standards organized into three main categories:

- Type A: Basic principles and concepts
- Type B: General standards covering one or more safety aspects
    - Type B1: Standards that address specific safety aspects, such as functional safety, as well as requirements for safe distances, temperature, vibration, noise, radiation, and ergonomics
    - Type B2: Covers device-oriented design requirements for safety devices/protective devices, like emergency stops, workstations/screens, ladders, guard rails, and instrumentation, like pressure-sensitive protective devices and positioning
- Type C: Standards targeting specific types of machines, and where type A and type B requirements have been applied in this context.

Examples of machines with a C-standard are paper machines, hydraulic presses, paper rollers, printers, and agricultural machinery. A manufacturer who wants to produce a new type of machine should first check whether a relevant C standard is available. Otherwise, it is necessary to search through all the standards within types A and B that will be used.

The most central standards for our use for functional safety are also summarized in Fig. 5, are:

- ISO 12100 (2010) about safety of machinery — General principles for design — Risk assessment and risk reduction (type A-standard)
- ISO 13849 (2023) about Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design (type B1 standard)
- IEC 62061 (2021) about the Safety of machinery - Functional safety of safety-related control systems (type B1 standard)

ISO 13849 and IEC 62061 overlap in scope and use, as explained in (IEC TR 62061, 2010), and the user can decide which one to use. IEC 62061 was developed as a sector variant of IEC 61508, while ISO 13849 was introduced long before IEC 61508, and many machine builders are more familiar with this standard. We will address some of the differences later, but for now, note that IEC 62061 uses the SIL concept, while ISO 13849 uses performance level (PL).

There are many B2 standards covering specific safety devices, such as ISO 13850 for emergency stop systems.

10.3 Application of the MD

The MD requires that those involved in the construction or modification of systems covered by the directive carry out the following tasks:

1. The **specification of control systems and safety/protection devices** should always incorporate the **essential health and safety (H&S) requirements**.
2. Perform a **risk assessment** to decide on ***specific*** risk-reducing measures for the machine
3. Build and operate systems following the requirements in relevant **harmonized standards**
4. Develop a **user manual** with all necessary information about safe installation and use
5. Fill out and issue a **Declaration of Conformity** («Samsvarserklæring»)
6. Add a **CE label** with the necessary codes and information

Manufacturers may use an independent third-party assessor to inspect the above-mentioned tasks. In this case, the CE label includes a code identifying the assessor.

10.3.1 Incorporate essential H&S requirements

The essential health and safety (H&S) requirements specify the functional requirements and constraints necessary to ensure safe behavior of the machine control system and related safety (protective) devices during start-up, regular operation, abnormal operation, and maintenance.

The machine control system will, from now on, be referred to as the safety-related control system (SRCS), a term introduced in IEC 62061 (2021), one of the harmonized standards. Some of the requirements that MD places on all machines are:

- The SRCS must withstand the required operating stresses and external influences.
- The loss of power supply or a failure of SRCS devices or software must not lead to hazardous situations.
- A reasonably foreseeable human error during operation shall not lead to hazardous situations.
- The machine must not start unexpectedly.
- The parameters of the machine must not change uncontrolled, where such a change may lead to hazardous situations.
- The machine must not be prevented from stopping if the command has already been given.
- Automatic or manual stopping of the moving parts, whatever they may be, must be unimpeded,
- The machine must be fitted with one or more emergency stop devices to enable actual or impending danger to be averted. The protective devices must remain fully effective or give a stop command,
- The control or operating mode selected must override all other control or operating modes except for the emergency stop.
- When using a wireless control device, automatic stopping shall be triggered when the correct control signal is not received, including when signal transmission is lost.

The listed requirements are general, independent of the specific application of the machine. However, different machines and their use pose different risks, and a risk assessment is therefore necessary to identify and detail the general and potential additional safety requirements that the machine and its safety (protective) devices must meet, specifically to the operating context.

10.3.2 Perform a risk assessment and propose risk-reduction measures

The MD outlines the following requirements for the execution of risk assessments:

- The machine builder shall ensure that a risk assessment is carried out to determine the requirements for protection against harm to life and health associated with the machine in question
- A risk assessment must not be carried out only once, but several times as the design is improved or re-developed.

The risk assessment shall:

- Reflect on the machine's limits, including its intended use and misuse that are reasonably foreseen.
- Identify the hazards the machine may cause and the hazardous situations that may arise with the use of the machine
- Use risk to rank hazards and hazardous events concerning the severity of possible harm to life and health, and the likelihood of the occurrence
- Determine, with a basis in the risk assessment, the need to further reduce the risk
- Suggest protective measures in order of priority of effectiveness (which is explained below)

Risk-reducing measures are technical, operational, or organizational measures added to the machine or in its vicinity to prevent harm to people. They can reduce the occurrence of dangerous situations, the probability of exposure, and the severity of harm if people are exposed.

The MD requires that highly effective measures be selected before those with lower effectiveness. ISO 12100 assigns a priority of risk-reducing measures ranked according to their efficiency:

1. **Apply inherently safe construction measures to the machine:** Modify the machine, either by physical layout and design, by introducing new functions in the machinery control system, or by enhancing reliability to prevent or reduce the likelihood of exposing people to hazards.
2. **Install safety (or protective) devices:** Add safety devices to reduce the risk of harm when the machine (as designed) cannot eliminate hazards. Examples include (additional) emergency stop buttons, light beams, and door locks that automatically stop the machine if people enter an area or space where the machine could pose a risk.

3. **Add user information, training, and personal protection:** Add warnings and signs (notice, flashing light, sound), and provide training and personal protection to reduce remaining risks not managed by 1. and 2.

Some measures, such as the emergency stop button, could be part of an inherently safe design principle if added by the machine builder and subject to a conformity assessment process, or added later as extra or complementary protective measures if not covered. One reason for not being covered yet could be that new (unanticipated) risks have arisen due to how the machine operates.

	Watch a video about the risk assessment of a machine on YouTube.

10.3.3 Prepare declaration of conformity and user manual

The declaration of conformity confirms that the machine has been built in accordance with relevant regulations and standards. All standards used must be listed in the declaration. In addition, a person authorized to have such responsibility with the company must sign the declaration of conformity. An example of a declaration of a chainsaw is shown in Fig. 6 (the left-hand side).

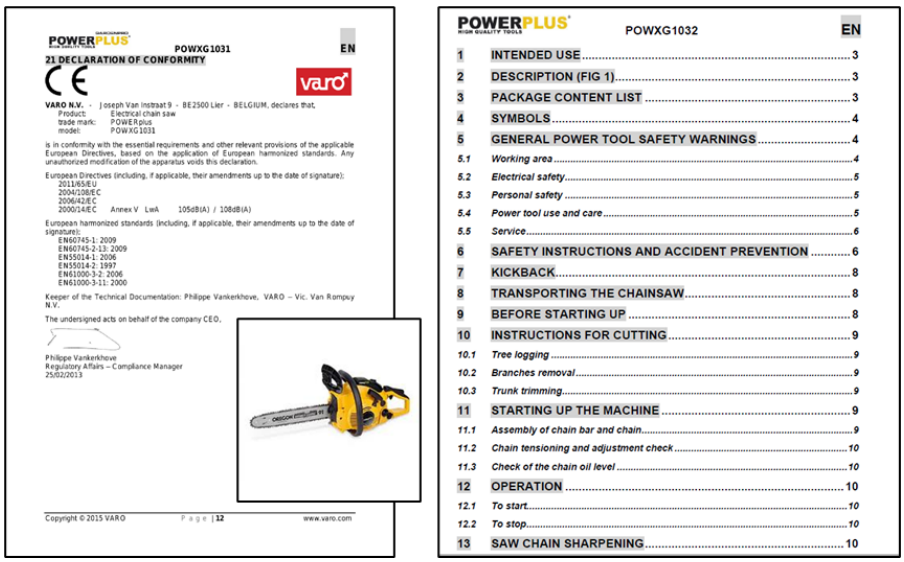

Fig. 6. Example of a declaration of conformity and content of a user manual

The user manual provided with the machine is comprehensive, and an example of topics covered for a chainsaw is shown in Fig. 6 (right-hand side).

10.4 Risk assessment methods per ISO 12100

ISO 12100 (2010) provides a structured approach to carrying out a risk assessment of a machine or machinery. A guideline supporting the standard, the ISO TR 14121-2 (2012)includes some examples of results from applying the approach.

The risk assessment is split into the following primary tasks:

1. Identify hazards associated with the machine and its use
2. Determine whether the risk is acceptable or not
3. Identify risk-reducing measures (in the listed order of priority):
   - Inherently safe design principles, covering layout/design of the machine or improving safe behavior with the machinery control system
   - Add safety (protective) devices and systems

- Add user information and apply personal protective equipment

The risk assessment steps are detailed further in Fig. 7. The figure also explains the relationship to two other harmonized standards, the functional safety standards IEC 62061 and ISO 13849, which apply risk reduction measures involving E/E/PE technologies. For example, the safety functions implemented in the machine control system must comply with ISO 13849 or IEC 62061, and the same applies to complementary safety functions, such as emergency stop. The functions to implement in the control system still need to fulfill the requirements listed in the MD.

The steps of the risk assessment process are explained in the following sections.

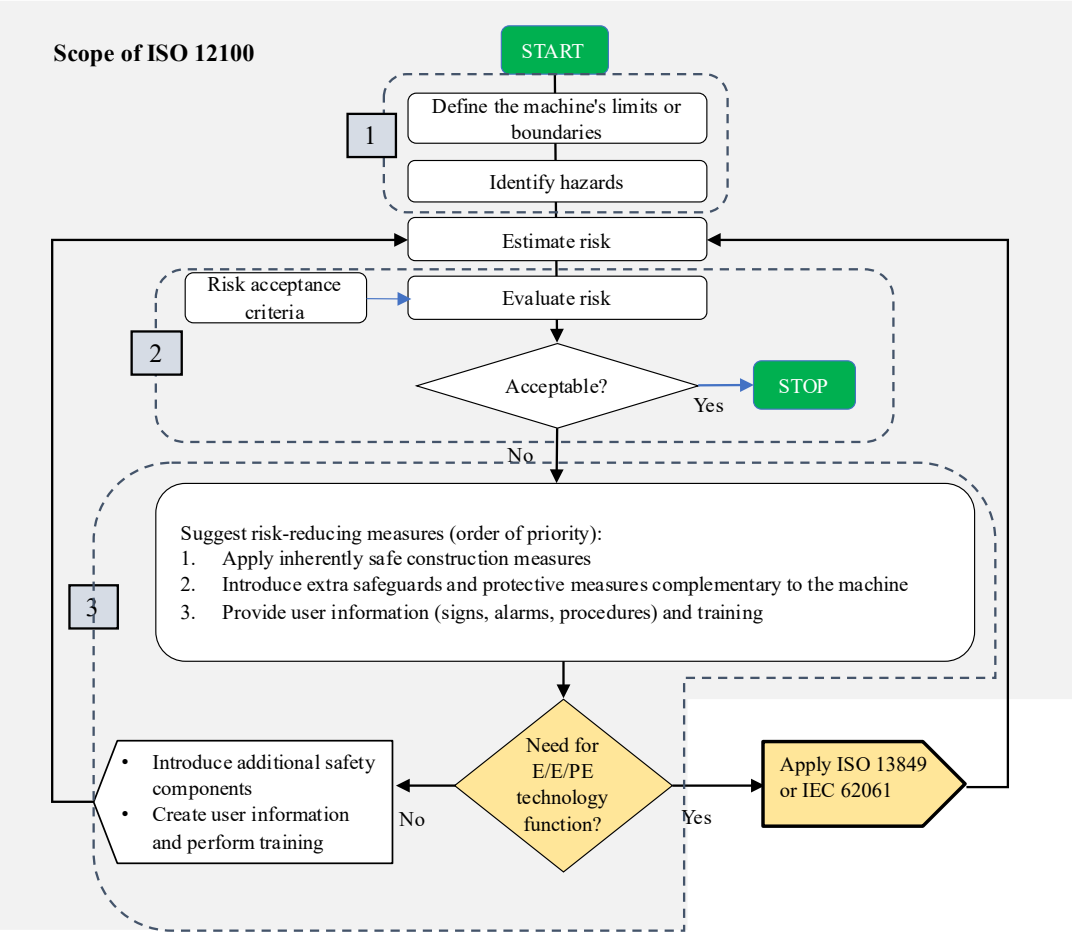

Fig. 7. Flow diagram of the risk assessment procedure (adopted from ISO 12100)

10.4.1 Define the machine limits

Defining machine limits defines the scope of the risk assessment and involves determining the physical and logical boundaries of the machine's operation, including intended and possible misuse. The following limits should be identified:

- Limits about use: Operating conditions, user interaction, expected level of knowledge/training of users, and possible exposure to people who do not operate the machine.
- Limits about location: The machine's range of motion and space where people must be present for operation and maintenance, including operator stations and interfaces to energy supply (electricity, fuel, hydraulics, etc.).
- Time limits: Machine life, device life, recommended service intervals.
- Other limits: Type of materials, cleaning, ambient conditions (temperature, humidity, dust).

The information above is added to the machine's user manual and, as needed, to operating procedures.

10.4.2 Identify hazards

To identify hazards means systematically identifying specific hazards, hazardous situations, and hazardous incidents that can cause harm to people, considering a specific machine's operating context, including regular operation, maintenance, fault-finding, start-up, and shutdown. Other relevant contexts to consider are transport, assembly, installation, commissioning, and assembly, and (at a later stage) disassembly and disposal.

Hazard identification should involve all relevant disciplines with knowledge and experience in machine operation and is therefore conducted in a meeting that invites these disciplines, often called a hazard identification workshop. To ensure that all possible hazards are identified, it is often helpful to structure discussions around a checklist that includes typical hazard types and examples. A checklist example, adapted from ISO 12100, is shown in Tab. 1.

Tab. 1. Examples of Hazards (adapted from ISO 12100)

Hazard category	Hazard example	Potential consequences
Mechanical hazards	• Moving parts • High energies • Speed • Cutting • Shearing • Falling objects • Sharp edges • Stored energy	• Crushing • Trapped/ drawn into • Run into • Suffocation • Internal injury • External injury
Material/ substance hazards	• High pressure • Release • Toxic • Dust • Explosive • Combustible	• Being hit • Burn • Damage to eyes and skin • Other injuries • Suffocation • Shock • Losing consciousness • Internal injury • External injury
Electrical hazards	• Arc • Overload • Electrostatic phenomena • Current passage • Live parts (when they should not be) • Short circuit • Fire/explosion	• Burn • Falling • Pushed /thrown away • Losing consciousness • Internal injury • External injury • Losing consciousness
Thermal hazards	• Low temperature • High temperature • Flame • Explosion • Hot surfaces • Radiation	• Burn • Dehydration • Discomfort • Frostbite • Internal injury • External injury • Scald
Noise hazards	• Gas leaking at high speed • Scraping surfaces • Unbalanced rotating parts • Whistling phenomena • Worn parts • Stamping, cutting • Release from exhaust systems • Cavitation phenomena	• Discomfort • Loss of awareness • Loss of hearing (temporary, permanent) • Stress • Tinnitus • Tiredness

		• Inability to hear alarms, essential messages, etc.
Ergonomic hazards	• Insufficient access • Design or location/distance to of indicators and visual displays • Design and location/distance to control devices • Flicker, dazzling, shadow, luminous level • Overload • Boredom, monotony • Repetitive activity • Visibility	• Discomfort • Fatigue • Musculoskeletal disorder • Stress
Environmental hazards	• Dust • Fog • Electromagnetic disturbance • Lightning • Moisture • Pollution • Snow • Temperature • Water • Wind/weather • Lack of oxygen	• Burn • Slipping falling • Suffocation • Losing consciousness • Internal injury • External injury • Frostbite • Drowning • Dehydration

This video provides a good overview of the hazards associated with operating a machine.

10.4.3 Estimate and evaluate risk

Risk estimation is about determining the risk level, typically by considering the combination of occurrence probability (or frequency) and severity. ISO 12100 explains that two parameters as follows:

- Probability of the injury occurring given that the hazardous situation or incident occurs.
- Severity (S): Severity of injury or harm associated with a dangerous situation/dangerous incident ("worst case outcome")

This probability of injury can be estimated directly, but more commonly by considering the three following factors:

- Frequency of exposure (F): The exposure of people to danger (likely that people are there when the situation arises)
- Probability of occurrence (P): The occurrence of the dangerous event or situation
- Possibility of avoidance (A): The technical and human possibilities for avoiding or limiting the damage

ISO 12100 provides a few generic methods for linking the above-mentioned factors to specific risk levels. For example, the decision tree shown in Fig. 8, referred to as a risk graph.

Determining the risk level using a risk graph analysis starts on the left side by considering a specific hazard identified for the machine. To determine the risk level, expressed in terms of 6 risk levels, it is necessary to follow the applicable path by choosing the relevant severity (S1 or S2), the exposure of personnel in the situation / during the incident (F1 or F2), the probability that the situation/incident occurs (O1, O2 or O3) and the possibility for personnel to avoid injury in the situation / during the incident (A1 or A2). This process is repeated for all identified hazards/hazardous situations/hazardous incidents, and the list can then be sorted by highest risk. At this stage, nothing has been said about the acceptable level of risk.

The risk graph itself does not identify which risk index is acceptable. However, risk acceptance criteria could be added using the as low as reasonably practicable (ALARP) principle (see Chapter 6), using color code green for generally acceptable (no further risk reduction needed), yellow (conditional acceptable, still expected to introduce additional measures if costs are not disproportionate to the effect on risk reduction), and red (not acceptable, risk reduction must be carried out).

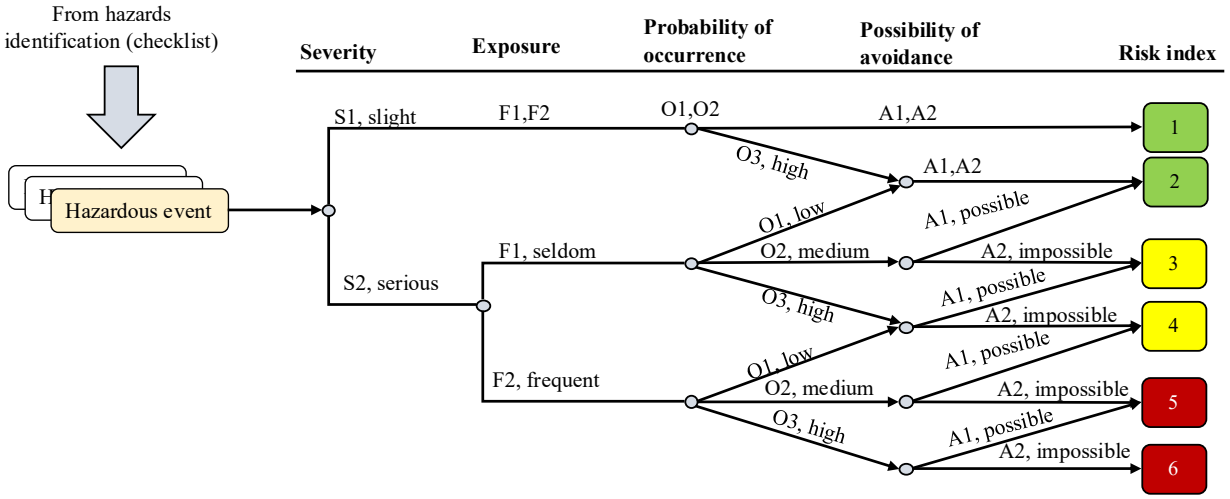

Fig. 8. Risk graph for risk estimation and evaluation (adapted from ISO 12100)

An alternative to the risk graph is the risk matrix in Fig. 9. Four risk parameters are considered: Se as severity, Fr as frequency of hazard, Pr as probability of occurrence of hazard, and Av as possibility of avoiding the hazard. The corresponding range of values for each parameter is also shown in the table. The need for risk reduction is evaluated by considering the Se and the class index CI, calculated as the sum of Fr, Pr, and Av. The risk acceptance criteria following ALARP are incorporated, with the darkest color indicating unacceptable risk, grey indicating conditionally acceptable, and white indicating generally accepted risk.

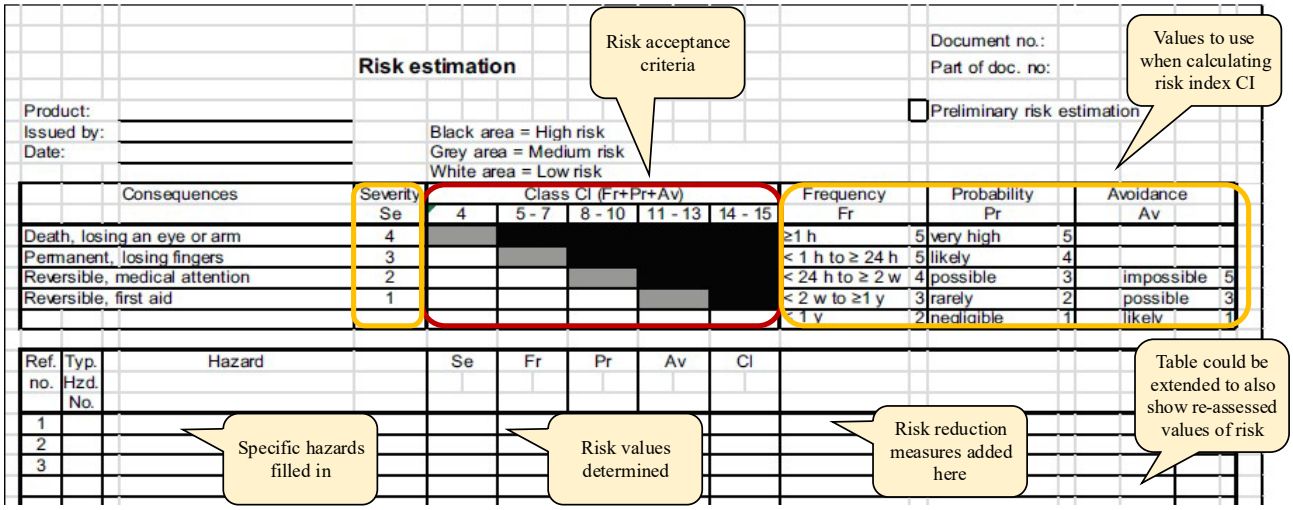

Fig. 9. Risk matrix for risk estimation and evaluation (adapted from ISO 12100)

The parameter value scales and acceptance criteria shown in Fig. 8 and Fig. 9 are generic, and the machine builders may have developed variants or their own versions of these risk assessment methods.

10.4.4 Propose risk-reducing measures

By comparing the risk level against the acceptance criteria, it is possible to identify hazardous circumstances that require risk reduction. The choice of measures shall follow the priority list explained earlier in chapter

10.3.2. Two of the risk reduction measure categories may be relevant to applying electrical, electronic, and/or programmable electronic (E/E/PE) technologies.

	Watch this video showing risk-reducing measures for a robot.

10.5 Role of ISO 13849 and IEC 62061

ISO 12100 refers to ISO 13849 and IEC 62061 for implementing safety requirements of machinery control systems and complementary (and independent) safety functions involving E/E/PE technologies.

- ISO 13849 was first published in 1999 and was based on the European Norm EN 954-1 from 1996. The standard targets simple safety systems that typically combine mechanical, pneumatic, electrical, and programmable devices.

As both standards are risk-based, the amount of risk reduction to be managed by the control system must be translated into a performance measure applicable to software and hardware design, such as the safety integrity level (SIL) per IEC 62061 or the performance level (PL) per ISO 13849. Both standards are harmonized, and it is up to the manufacturer to choose which one to use.

Examples of requirements in IEC 62061 and ISO 13849 are:

- Performance requirements shall be imposed on the programmable control system.
- Performance requirements must form the basis for software development, and the software shall not be possible to modify by the user/operator (only by an authorized person).
- Performance analysis must incorporate the effects of random hardware and systematic failures.
- Reliable devices must be used, and the need for redundancy must be assessed.
- Safety devices shall be used when the machinery control system alone cannot provide the assigned risk reduction.

IEC 62061 and ISO 13849 take slightly different approaches, and the standards are therefore presented separately. It is up to the machine builder to decide which one to use.

Fig. 10. Front page of IEC 62061 and ISO 13489

10.5.1 Machinery safety functions

Safety functions for machinery that involve E/E/PE technologies may be split into two types:

1. Safety functions implemented with the machine control system: Since these functions are part of the regular operation of the machine, e.g., ensuring that the speed does not increase in an uncontrolled way, the functions are always defined sd continuous mode.
2. Safety functions are implemented separately from the machine control system to act in case of a machine control system failure, e.g., for an emergency stop. These functions are often treated as high-demand; however, depending on how often they are needed, they may also be low-demand.

In either case, the safety function is defined end-to-end, from sensors to the devices that are activated. A safety function is therefore realized within the following three subsystems:

- Input device subsystem
- Logic controller subsystem
- Final (actuated) devices system

The two mentioned standards for the design of such safety functions apply the following terms for systems that implement safety functions:

- IEC 62061: Safety-related control system (SRCS)
- ISO 13849: Safety-related parts/control system (SRP/CS)

For the remainder of this chapter, we will replace the term "safety function (end-to-end)" with "safety-instrumented function" (SIF) to align with IEC 61508 (Chapters 8 and 9) and IEC 62061 terminology (Chapter 10).

Related to SIF, some key concepts are helpful to introduce at the start of the chapter: the channel and the safety-related parts of the control system (SRP/CS).

The term "channel" by ISO 13489 is defined as an element or group of elements that independently implements a safety function and is central for some of the reliability measures calculated according to this standard. The definition. The channel concept applied to a system with redundant logic is shown in Fig. 11. A channel is therefore not defined separately for each subsystem, such as the controller, but includes selected devices from all subsystems. A channel, therefore, is an individual path set in a reliability block diagram.

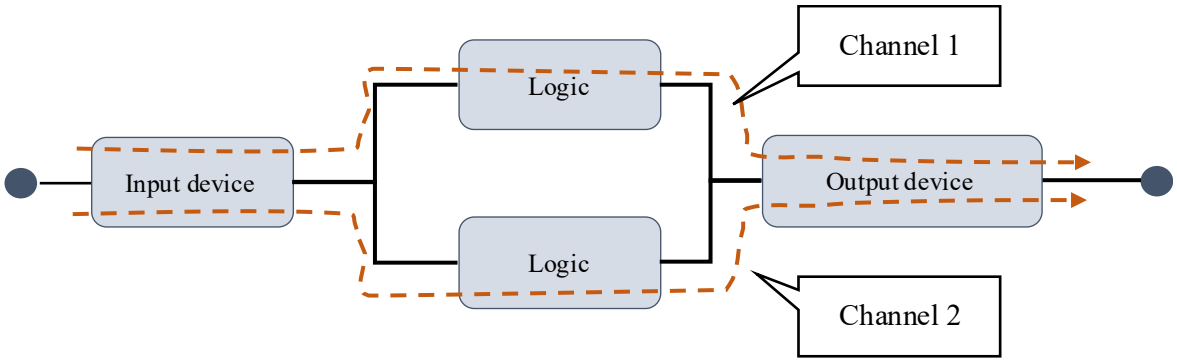

Fig. 11. Interpretation of the term "channel"

The logic part of the safety function is called "safety-related parts of the control system (SRP/CS)" and can be an integral part of the machine's control system or separate. As an integral part of the whole machine control system, ISO 13489 requires demonstrating that the safety functions are not affected, e.g., by being blocked or delayed, by non-safety functions under normal and faulty conditions. Means to ensure sufficient separation (and thereby less likelihood for negative impacts by non-safety functions) are, e.g.:

- Physical and logical separation, using e.g., certified safety cores or dual processors (one for non-safety and one for safety). Several manufacturers offer PLCs with this capability.

- Follow requirements in ISO 13489 regarding software specification and realization for safety functions, e.g., by applying modularized certified function blocks that are configured using rules and restrictions for avoidance of systematic faults.

The reliability of SIF is calculated by the average frequency of dangerous failures per hour (PFH). While IEC 62061 relates PFH ranges to safety integrity levels (SIL 1-SIL 4), ISO 13849 relates it to performance level (PL), ranging from PL a to PL e, where PL a is the least reliable, and PL e is the most reliable. To clearly distinguish what reliability is required from what is achieved, ISO 13849 adds the notation (r) to PL, i.e., PL_r, when it denotes a requirement and the notation (a), i.e., PL_a, when it denotes what has been achieved after implementation. PL (PL_r as well as Pl_a) applies to the whole safety function (end-to-end).

10.5.2 IEC 62061 vs ISO 13849

The technical report IEC TR 62061 (2010), now withdrawn, made a comparison of IEC 62061 and ISO 13849. This report concludes that one should use the standard with which one has the most knowledge and experience. Both are considered harmonized standards for the MD. After the new version of ISO 13849, which aligns with IEC 62061, was published in 2021, the technical report was no longer needed. Here, it is allowed to follow the traditional steps of ISO 13489 or apply the steps according to IEC 62061. Both standards are common in that they apply to a high-demand (and continuous) mode of operation.

However, some differences between the standards that can be highlighted are:

1. ISO 13849 requires that the architecture of SIF is restricted to one of five pre-defined categories. In contrast, IEC 62061 provides greater freedom in selecting the architecture for each subsystem, provided the requirements for minimum hardware fault tolerance are met.
2. ISO 13849 uses performance level (PL) as a measure of reliability for being able to perform the safety function, whereas IEC 62061 uses safety integrity level (SIL).

ISO 13489 explains the relationship between PFH values, PL, and SIL as shown in Tab. 2. As long as the PFH is calculated, it is possible to determine both the achieved SIL and the achieved PL.

Tab. 2. PL vs SIL

ISO 13849: PL	Selected values: PFH (per hour)	IEC 62061: SIL
a	1E-5 ≤PFH < 1E-4	-
b	3E-6 ≤ PFH <1E-5	SIL 1
c	1E-6 ≤ PFH <3E-6	SIL 1
d	1E-7 ≤ PFH < 1E-6	SIL 2
e	1E-8 ≤ PFH < 1E-7	SIL 3

10.6 Application of ISO 13849

ISO 13849 uses a risk-based approach to the specification and design of SIFs, meaning that a risk assessment must be carried out to determine the risk level and the need for risk reduction measures, and that risk level influences how the safety function is designed.

For this process, ISO 13489 includes the following steps:

1. **Determine** the **required performance PL_r level:**
   - ISO 13489 suggests similar methods as in ISO 12100, however, with the exception that the identified risk reduction is translated to a PL_r level.

2. **Decide on a sufficiently reliable architecture of SIF:**
   The standard restricts the choice of architecture for the safety function to one of the five available architecture categories (named B, 1,2,3, and 4):
   - The category is selected based on the PLr level and the value of the following two parameters:
     - Average diagnostic coverage (DC_{avg})
     - The mean time to failure for dangerous failures for one channel ($MTTF_D$)
   - The standard suggests formulas for determining DC_{avg} and $MTTF_D$ for individual channels of the safety function (end-to-end). A separate formula is available to compute the average of the two channel values for each parameter.
3. **Verify that PL_a level ≥ PL_r level:**
   Determine the achieved PL_a level by first calculating the dangerous failures (PFH) of the safety function and verifying that PL_a level ≥ PL_r level
   - Select devices that meet the requirements for DCavg and MTTFD for the selected architecture category
   - Appropriate methods to calculate PFH may be selected, e.g., from IEC 62061 and IEC 61508.
   - It is required to incorporate the effects of common cause failures (CCF)
   - Determine the SIF architecture following architectural constraints similar to what is done in IEC 61508

An overall view of the process, including the relationship with ISO 12100, is illustrated in Fig. 12.

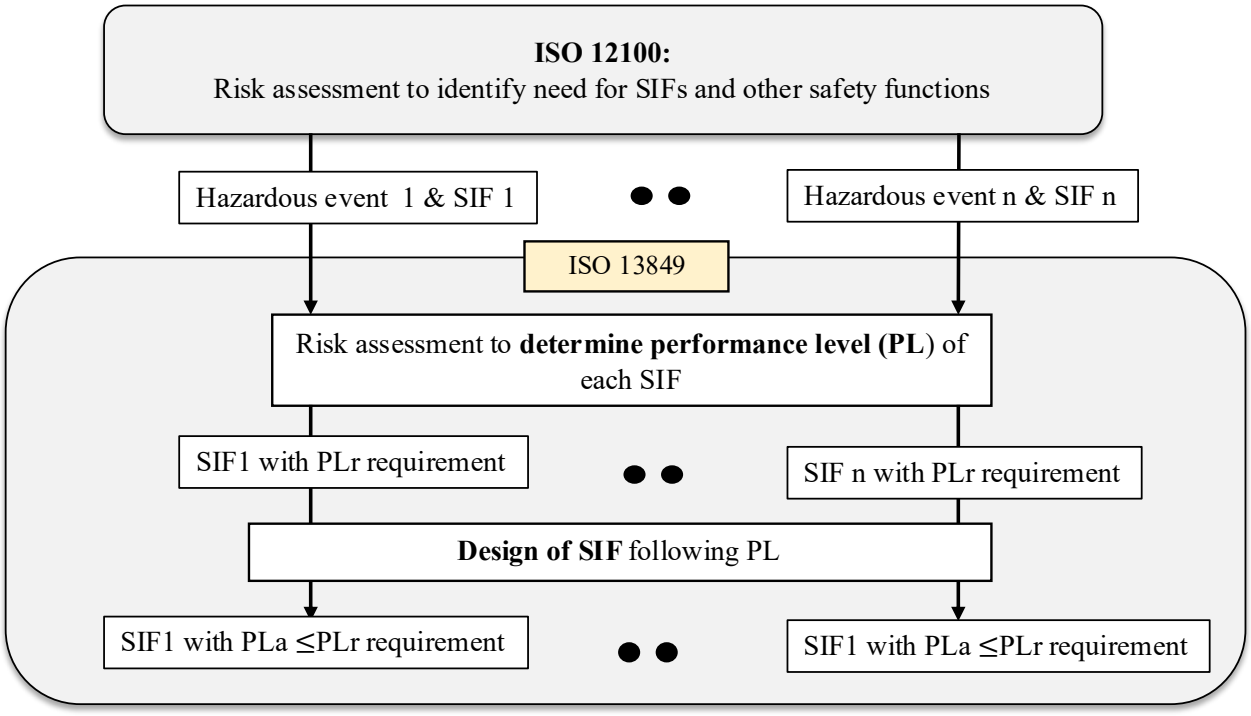

Fig. 12. ISO 12100 vs ISO 13489 activities

10.6.1 Determine the PL requirement, PL_r

The first step in ISO 13849 is to determine the PLr for each safety function (SIF) identified in the risk assessment per ISO 12100 for which E/E/PE technology is needed. ISO 13489 suggests similar risk estimation and evaluation methods as in ISO 12100, but does, unlike ISO 12100, relate the results to PL as shown with a risk graph in Fig. 13.

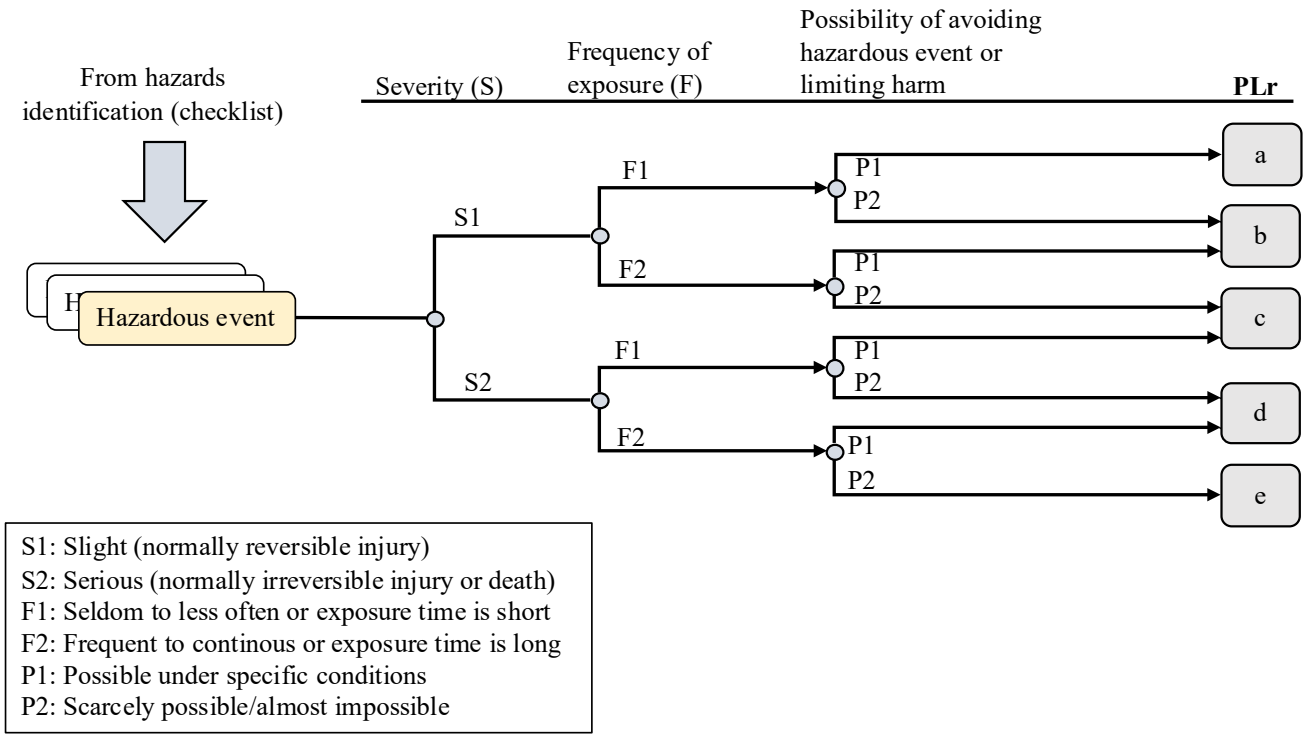

Fig. 13. Risk graph in ISO 13849

The first step is therefore to calculate the values of the associated probability, exposure, and severity parameters, and note down the corresponding required PL (PL_r) in the range of level a to level e. The results are added to the safety requirements specification, along with other information relevant to the safety function's required behavior.

10.6.2 Select architecture category based on PL_r

ISO 13849 specifies five permitted hardware architectures B, 1, 2, 3, and 3, all illustrated in Fig. 14 and detailed in Tab. 3.

Tab. 3 mentions three terms that have a specific meaning and are explained by examples in ISO 13849-2 (2012):

1. Basic safety principle
2. Well-tried safety principle
3. Well-tried components

Tab. 3. Description of each category (adapted from ISO 13849, table 5)

Cat.	Requirement	Fault tolerance	$MTTF_D$ (channel)	DC_{avg} (channel)	Prevention of CCFs
B	• Design and implementation according to relevant standards to withstand operating stresses, processed material, and external influences • Apply basic safety principles	0	Low to medium	None	Not relevant
1	As for type B. In addition: • Apply well-tried safety principles • Use of well-tried (proven) components	0	High	None	Not relevant

2	As for type B. In addition: • Apply well-tried safety principles • Testing at suitable intervals	0	Low to high	Low to medium	Apply CCF checklist (Appendix F)
3	As for type B. In addition: • Apply well-tried safety principles • Tolerate single faults • Apply diagnostics to detect faults	1	Low to high	Low to medium	Apply CCF checklist (Appendix F)
4	As for type B. In addition: • Apply well-tried safety principles • Tolerate single faults • Apply diagnostics to detect faults • Special attention to keep a low likelihood of having accumulated faults	1	High	High (also for the detection of accumulated faults)	Apply CCF checklist (Appendix F)

Tab. 4 identifies the maximum PL achievable for each category, given the values of DC_{avg} and $MTTF_D$. The value ranges of DCavg and MTTFD can be applied as requirements for individual channels or calculated once a choice of devices has been made.

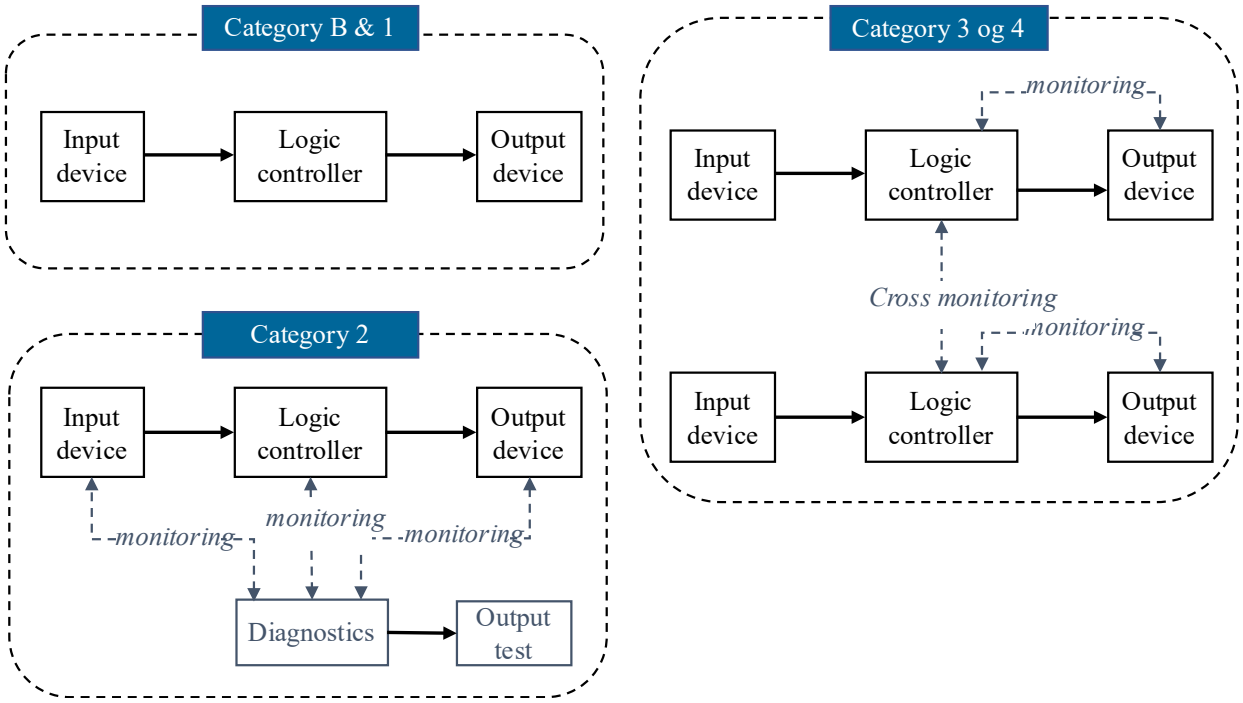

Fig. 14. Architectures for categories B and 1-4

Tab. 4. Requirements to PL, DC_{avg}, and $MTTF_D$ for each category

Category	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC_{avg} category	None	None	Low	Medium	Low	Medium	High
Corresponding DC_{avg} values	<60%	<60%	60% ≤ DC <90%	90% ≤ DC <99%	60% ≤ DC <90%	90% ≤ DC <99%	>99%

$MTTF_D$ (per channel)							
Low: 3 years ≤ $MTTF_D$ <10 years	PL a	N/A	PL a	PL b	PL b	PL c	N/A
Medium: 10 years ≤ $MTTF_D$ <30years	PL b	N/A	PL b	PL c	PL c	PL d	N/A
High: 30 years ≤ $MTTF_D$ <100 years	N/A	PL c	PL c	PL d	PL d	PL d	PL e

10.6.2.1 Formula for DC_{avg}

The DC_{avg} is calculated as a weighted average for all devices in one channel (as opposed to per component), with values of DC for inputs, logic, and outputs:

$$DC_{avg} = \frac{\lambda_{DD,avg}}{\lambda_{D,avg}} = \frac{DC_I\lambda_{D,I} + DC_L\lambda_{D,L} + DC_O\lambda_{D,O}}{\lambda_{D,I} + \lambda_{D,L} + \lambda_{D,O}}$$

Here, $\lambda_{D,I}$ is the dangerous failure rate of the sensor system (I = input device), $\lambda_{D,L}$ is the dangerous failure rate of the logic (L = logic device), and $\lambda_{D,O}$ is the dangerous failure rate of the actuated devices (O = output device).
ISO 13849 does explain how DC_{avg} is calculated with redundant channels. An interpretation is that each channel needs to meet the DC_{avg} requirement.

10.6.2.2 Formula for $MTTF_D$

The $MTTF_D$ is calculated for each *individual* channel using the following formula:

$$MTTF_D = \frac{1}{\frac{1}{MTTF_{D,I}} + \frac{1}{MTTF_{D,L}} + \frac{1}{MTTF_{D,O}}} = \frac{1}{\lambda_{D,I} + \lambda_{D,L} + \lambda_{D,O}} = \frac{1}{\lambda_D}$$

The formula shows that the $MTTF_D$ is the reciprocal of the channel's dangerous failure rate and $MTTF_{D,i}$ the reciprocal of the failure rate for a device *i.*

ISO 13849 suggests an additional formula to calculate the average MTTFD for two channels for categories 3 and 4. The formulas have not been included here.

10.6.2.3 Determine device failure rates

The device failure rate may be assumed constant, regardless of how often the device is operated. For example, a logic solver may be independent of the operations, whereas an input or output device that uses a switch may degrade more quickly with more frequent use.

When the number of operations has an influence, ISO 13489 provides the following formula to calculate the channel $MTTF_D$ of device *i*:

$$MTTF_{D,i} = \frac{1}{\lambda_{D,i}} = \frac{B_{10D,i}}{0.1 \cdot n_{op,i}}, i = I, L, O$$

Here, η_{op} is the mean number of annual operations, meaning that the calculated failure rate λ_D is expressed per year unless divided by 8760 to convert to per hour. Failure rates not influenced by the number of operations may be found in the products' certificates, user manuals, or reliability data handbooks. For components whose reliability is highly dependent on the annual number of operations, ISO 13849 proposes an indirect method to determine $MTTF_D$ using the $B10_D$ factor. Here, B10D is the number of cycles at which 10% of a component

population has failed dangerously. With $B10_D$ given from the certificate and the number of cycles per year expected for this type of device in operation, the $MTTF_D$ of the device becomes:

10.6.3 Case study 1: Adding SIF to a circular saw

We assume a control system with a door sensor that will disconnect a circular saw with a rotating blade if an operator/user comes too close to the machine's moving parts (protected by a cover and door).

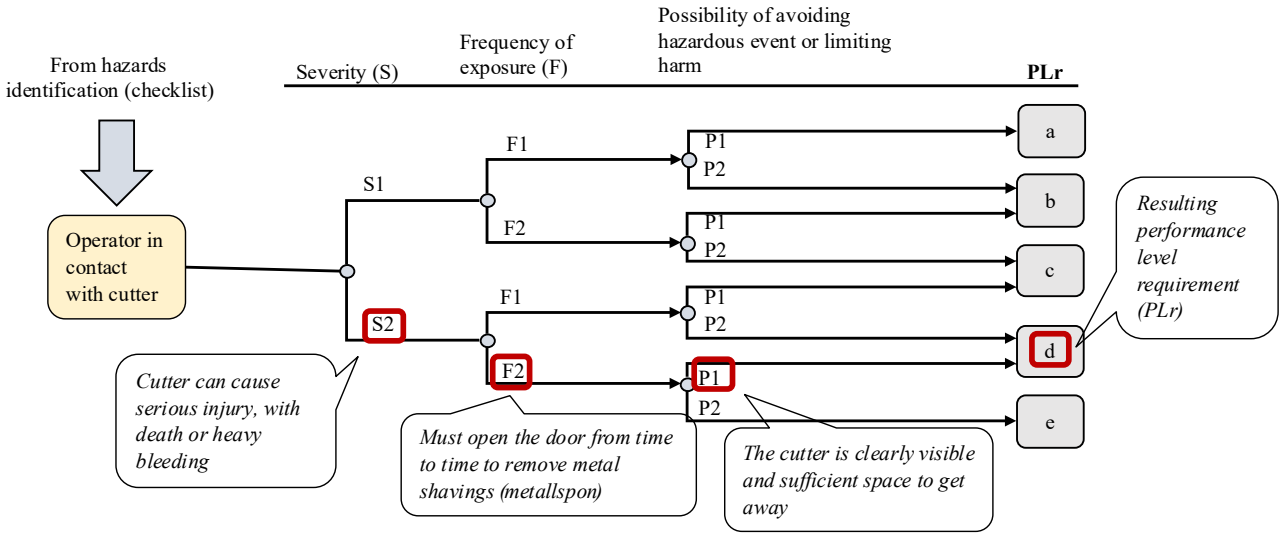

Fig. 15. Applying risk graph in ISO 13849

The hazards identification has found that a serious injury may result if the cutter continues to run after the operator has opened the door in front. The question is: What PL would be required for such a safety function? What architecture category must be selected?

Solution: We apply the risk graph in Fig. 15. By assessing the severity, frequency, and possibility of avoiding the injury from the information provided in the thesis, a performance requirement PL_r =d is derived.

With performance requirements, PL_r=d, can choose between categories 2 and 3 (and 4) architectures.

We start by selecting category 2 for the safety function, and for simplicity, we assume it consists of only one (mechanical) proximity detector/switch (N) that opens a contactor K, as shown in Fig. 16. We further assume that the safety function is activated on average once per day, i.e., 365 activations per year.

We assume the following data for these devices:

Device	**B_{10D}**	**N_{op} (per year)**	**$MTTF_d$ (years)**	**λ_D (per hour)**
Proximity switch (PS)	20 000 000	365	$MTTF_{D,PS} = \frac{20000000}{0.1 \cdot 365} \approx 547945$	$\lambda_{D,PS} = \frac{1}{8760 \cdot MTTF_D} \approx 2.1E-10$
Contactor (C)	2 000 000	365	$MTTF_{D,C} = \frac{2000000}{0.1 \cdot 365} \approx 54795$	$\lambda_{D,C} = \frac{1}{8760 \cdot MTTF_D} \approx 2.1E-9$

The $MTTF_D$ for the channel becomes:

$$MTTF_D = \frac{1}{1/MTTF_{D,PS} + 1/MTTF_{D,C}} = \frac{1}{1/547945 + 1/54795} \approx 49814 \text{ (years)}$$

The $MTTF_D$ becomes significantly longer than what is required, as it is actually beyond the high range. Category 2 can therefore be selected.

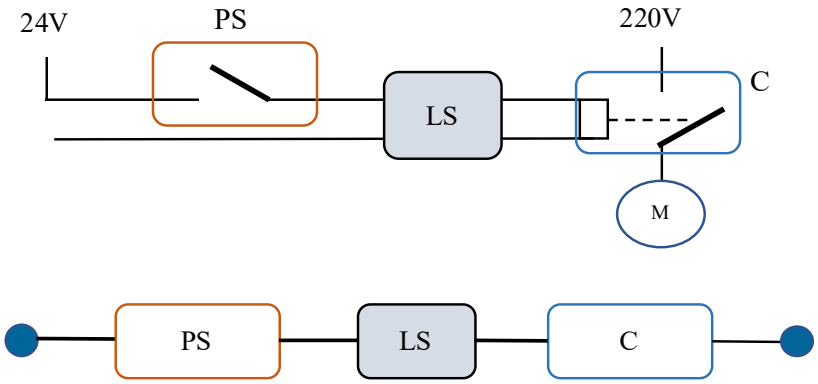

Fig. 16. Door sensor system with proximity switch and contactor

If instead we assume (a bit unrealistically) that the door must be opened even more frequently, for example, once every minute during a 16-hour shift, we have 1 x 60 x 16 x 365 cycles per year, corresponding to 350,400 cycles per year. The updated calculations become:

Device	$B10_D$	N_{op} (per år)	$MTTF_d$ (years)	λ_D (per hour)
Proximity switch (PS)	20 000 000	350 400	$MTTF_{D,PS} = \frac{20000000}{0.1 \cdot 350400} \approx 571$	$\lambda_{D,PS} = \frac{1}{8760 \cdot MTTF_D} \approx 2.0E-7$
Contactor (C)	2 000 000	350 400	$MTTF_{D,C} = \frac{2000000}{0.1 \cdot 350400} \approx 57$	$\lambda_{D,C} = \frac{1}{8760 \cdot MTTF_D} \approx 2.0E-6$

The $MTTF_D$ of the channel becomes:

$$MTTF_D = \frac{1}{1/MTTF_{D,PS} + 1/MTTF_{D,C}} = \frac{1}{1/571 + 1/57} \approx 52 \text{ (years)}$$

The calculated value remains within the "high" range, so we may still apply Category 2. If we assume that the proximity switch has a DC=60% and the contactor has a DC=75%, the average DC for the channel becomes:

$$DC_{avg} = \frac{DC_{PS}\lambda_{D,PS} + DC_C\lambda_{D,C}}{\lambda_{D,PS} + \lambda_{D,C}} = \frac{60\% \cdot (1/571) + 75\% \cdot (1/57)}{(1/571) + (1/57)} = 73.6\%$$

The calculated DCavg is in the medium range, and category 2 may, therefore, with high certainty, be applied with a single proximity switch and a single contactor.

10.6.4 Case study 2: An alternative architecture of the SIF

Suppose one wants to improve the design by introducing two contactors in parallel instead of a single contactor, as illustrated in Fig. 17.

Unfortunately, this architecture does not fit the five categories B, 1, 2, 3, and 4. The solution is to use IEC 62061, which offers more flexible methods for determining architectural constraints and calculating the SIL level.

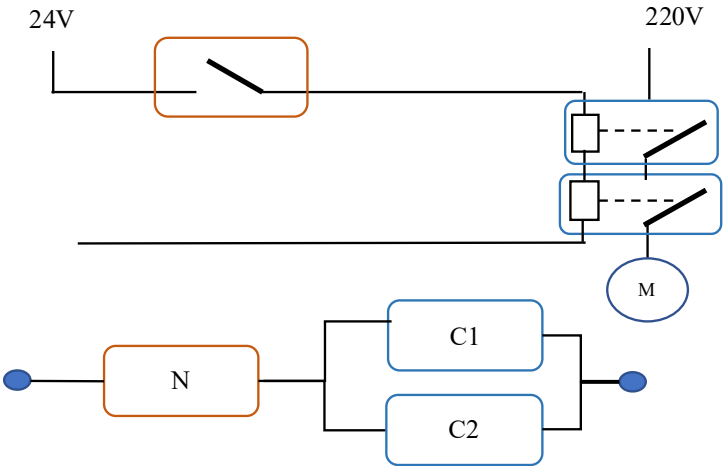

Fig. 17. Introducing redundancy

10.7 Application of IEC 62061

Compared to ISO 13849, IEC 62061 is relatively new, first published in the 2000s, just a few years after the first version of IEC 61508 became available. IEC 62061 has adopted terminologies and concepts from IEC 61508 that are relevant for machinery. For example, IEC 62061 considers only high-demand/continuous-mode functions, as most functions performed by machinery control systems (and add-on protection systems) fall into this category.

IEC 62061 uses the term safety-related control system (SCRS) for what ISO 13489 named SPR/CS, while both standards use the term safety function (which we refer to as an SIF to be consistent with Chapters 8 and 9).

Tab. 5. SIL table in IEC 62061

SIL	PFH (per hour)
SIL 1	1E-6 ≤ PFH <1E-5
SIL 2	1E-7 ≤ PFH <1E-6
SIL 3	1E-8 ≤ PFH <1E-7
SIL 4	--- Not allowed ---

The main steps in IEC 62061 involve:

1. Determine the SIL requirement of the SIF based on risk analysis
2. Design and verify the SIF according to the SIL requirement, including:
   - Architectural constraints
   - Measures to avoid systematic faults, including software faults (here, ISO 62061 refers to IEC 61508)
   - Calculate PFH and compare with the range allowed by the SIL requirement
3. Possibly redesign the function or choose other equipment if the SIL requirement is unmet.

While IEC 61508 distinguishes between four SIL levels, i.e., from SIL 1 to SIL 4, IEC 62061 is limited to three, i.e., SIL 1 to SIL 3, as shown in Tab. 5. The PFH ranges for the different SIL levels are consistent with IEC 61508.

A likely reason for excluding SIL 4 is that the machine requires a level of operator interaction that would be challenging to maintain at SIL 4. For systematic faults to be negligible for a SIL 4 system, less than one dangerous fault can be introduced by human error per (approximately) 1E-8 hours (approximately 100,000 years). Therefore, achieving SIL 4 performance will be difficult, primarily because of the risk of systematic failure.

10.7.1 Determine the SIL requirement

The procedure for determining SIL requirements in IEC 62061 is like that for determining PL_r requirements in ISO 13849. You start with a hazardous event or circumstance identified in the risk assessment per ISO 12100, where a need for risk reduction has been identified and allocated to the machinery control system or an add-on safety function involving E/E/PE technologies.

For each identified hazardous event of this kind, the following process is followed:

1. Se (Severity) – severity of injury caused by a hazardous situation or incident (worst case outcome)
2. Pr (Probability of occurrence) – probability of the hazardous situation occurring
3. Fr (Frequency and duration of exposure) – frequency for personnel being exposed in the hazardous area (where the event takes place). Two durations of exposure are considered.
4. Possibility for person(s) to avoid or limit the harm

Tab. 6. Risk influencing factors (adopted from IEC 62061)

Consequence (worst case) by hazardous event	**Se**			**Probability of the hazardous event**	**Pr**
Irreversible: Death, losing an eye or arm.	4			Very high	5
Irreversible: Broken limb(s) and losing a finger(s)	3			Likely	4
Reversible: attention from a medical practitioner	2			Possible	3
Reversible: First aid required	1			Rarely	2
				Negligible	1
Personnel exposure in the hazardous area	**Fr**			**Probability of avoiding or limiting harm**	**Av**
	Duration ≥ 10 min)	**Duration < 10 min)**			
Fr ≥ 1 per hour	5	5		Impossible	5
1 per hour < Fr ≤ 1 per hour	5	4		Rarely	3
1 per day < Fr ≤ 1 per two weeks	4	3		Probable	1
1 per two weeks < Fr ≤ 1 per year	3	2			
1 per year < Fr	2	1			

Each factor is to be determined independently of the others and with the worst-case outcome for the hazardous situation in question. This approach is, therefore, somewhat different from that of ISO 12100 and ISO 13489, where the risk graph approach makes Pr, Fr, and Av conditional on one another by the sequence in which they are listed.

IEC 62061 proposes categories for each of the four risk-influencing factors listed above in Tab. 6, together with a risk matrix shown in Tab. 6.

The values of Fr, Pr, and Av are summed to produce a risk level named class (Cl) of probability of harm. The corresponding need for risk reduction is reflected in a SIL requirement for the associated safety function, as

shown in Tab. 7. Cells marked "OM" mean "other measures." For such measures, the risk reduction requirement is so low that it is unnecessary to design the function in accordance with IEC 62061. Empty cells mean no need for a safety function.

The relationship between the SIL requirement and the PFH for high-demand SIFs is shown in Tab. 5. A SIL 2 requirement means that the PFH is lower than 1E-6/hour (but does not need to be less than 1E-7/hour).

Tab. 7. Matrix for assigning SIL requirement (adopted from IEC 62061)

Se	Class (risk of harm)				
	3-4	5-7	8-10	11-13	14-15
4	SIL 1	SIL 2	SIL 2	SIL 3	SIL 3
3		(OM)	SIL 1	SIL 2	SIL 3
2			(OM)	SIL 1	SIL 2
1				(OM)	SIL1

10.7.2 Determine architectural constraints

IEC 62061 adopts the approach of IEC 61508 to determine structural requirements and assigns a minimum fault-tolerance for hardware. However, some adjustments have been made:

1. Values for minimum fault tolerance always assume type B devices.
2. SIL 4 is not allowed.
3. Devices with SFF < 60% are allowed in architectures if hardware fault tolerance is ≥ 1, if the devices are proven in use. Proven in use indicates considerable operational experience and confirms that the device is safe for this application. In practice, this means that the devices are type A.

Tab. 8. HFT table (adopted from IEC 62061)

Safe failure fraction (SFF)	Minimum hardware fault tolerance (HFT)		
	0	1	2
< 60%	Not allowed	SIL 1	SIL 2
60% to < 90%	SIL 1	SIL 2	SIL 3
90% to < 99%	SIL 2	SIL 2	SIL 3
≥ 99%	SIL 3	SIL 3	SIL 3

10.7.3 Calculate PFH and compare with SIL

IEC 62061 provides formulas for calculating PFH based on formulas in IEC 61508-6, but with slightly different notations. We have adopted simplified formulas for PFH without considering dangerous detected (DD) failures; if DD failures result in a safe state, they will automatically be redefined as DU failures.

Formulas

For example, for a subsystem consisting of a single element, PFH, we can use the following simplified formula:

$$PFH^{1oo1} = \lambda_{DU}$$

where λ_{DU} is the dangerous undetected (DU) failure rate. The dangerous detected (DD) failures are not included because they are assumed to trigger an automatic transition to the safe state, for example, by stopping the machine. Dangerous failures detected by diagnostics that do not fulfill this criterion are reclassified as DU failures.

The general formula for a *koon* system where the n devices fail independently, i.e., when excluding common cause failures (CCFs), is:

$$PFH = \binom{n}{n-k+1} \lambda_{DU}^{n-k+1} T^{n-k}$$

Here, T denotes the interval between regular inspections and, as needed, the repair and renewal of all devices in the koon system. The formula is explained in more detail in Chapter 8 on reliability analysis.

For a subsystem of two devices voted 1oo2, the PFH is:

$$PFH^{1oo2} = \lambda_{DU}{}^{2} T$$

It is necessary to incorporate the effects of CCFs in redundancy subsystems. IEC 62061 recommends using the standard beta factor model. The values of the parameter β can be found in data handbooks, in manufacturer documentation, or in the checklist in IEC 62061.

For a subsystem of two devices voted 1oo2, the PFH becomes:

$$PFH^{1oo2} = ((1-\beta)\lambda_{DU})^2 T + \beta\lambda_{DU}$$

The PFH formulas may be modified to align with the PDS method for including CCFs, following the arguments explained in Chapter 8 (on Failure classification and Reliability).

The total PFH of the SIF is calculated by adding the SIF of each subsystem in series:

$$PFH_{SIF} = PFH_{IE} + PFH_{LS} + PFH_{FE}$$

where IE refers to input elements like sensors, LS to the logic solver subsystem, and FE to the final element subsystem. The PFH of the SIF is compared with the range permitted by the SIL requirement.

10.7.4 Choice of failure rate

In high-demand or continuous-operation modes, it is reasonable to expect that the reliability of electrical and some electronic devices (such as switches and contactors) is influenced by their operating frequency. This assumption may not necessarily apply to a programmable electronic controller (PLC) with no moving parts.

IEC 62061 adopts the same approach as ISO 13849, in which λ_{DU} is calculated using the B10D factor and the average number of cycles per year, η_{OP}. Recalling that $B10_D$ factor is the number of expected or experienced cycles where 10% of a component population have failed dangerously, we can calculate the DU failure rate as follows:

$$\lambda_{DU} = (1-DC)\cdot\frac{1}{MTTF_D} = (1-DC)\cdot\frac{0.1\cdot n_{op}}{B_{10D}} \text{ (per year)}$$

Here, DC is the diagnostic coverage given as $DC = \frac{\lambda_{DD}}{\lambda_D}$.

To express the DU failure rate per hour, the formula becomes:

$$\lambda_{DU} = (1-DC)\cdot\frac{1}{MTTF_D} = (1-DC)\cdot\frac{0.1\cdot n_{op}}{B_{10D}\cdot 8760} \text{ (per hour)}$$

For all the formulas mentioned, the following assumption applies: If it cannot be assumed that there is a transition to the safe state upon a dangerously detected (DD) failure or there is no time available to repair it before the next demand, we need to replace λ_{DU} with the sum of DD and DU failure rates, i.e., $\lambda_{D,}$ in the formulas above.

10.7.5 Measures to avoid systematic faults

IEC 62061 has several general requirements for both revealing and avoiding systematic faults. For software, IEC 62061 has introduced "SW level" 1 to 3, which have the following meanings:

- SW level 1: Can achieve maximum SIL 3 by following the principles of SW level 1 in IEC 62061
- SW level 2: Can achieve maximum SIL 2 by following the principles of SW level 2 in IEC 62061
- SW level 3: Not covered by IEC 62061; reference is made here to IEC 61508 for software development.

IEC 62061 sets out specific requirements for software SW level 1 and level 2, such as:

1. Development steps/process
2. What requirements must be established for the software
3. Requirements to tools for programming and compilation
4. Modular design
5. Programming/Encoding
6. Testing
7. Documentation
8. Change management and configuration

Compared with IEC 61508-3, IEC 61062 provides fewer, more practical pieces of advice and is thus easier to use.

10.7.6 Case study 1 repeated: Door sensor system

Assume the same door lock safety feature mentioned previously, analyzed with ISO 13849. An assessment of the same hazardous event results in the following values for the parameters that determine the risk level:

- Se: 4 (Death, loss of arm)
- Fr: 4 (at least once in 2 weeks)
- Pr: 3 (Possible)
- Av: 3 (Rarely)

Summing Fr, Pr, and Av yields CI = 10, which corresponds to a SIL 2 requirement for this safety feature. This aligns with the PLr d requirement obtained for the same case study using ISO 13489.

IEC 62061 uses a minimum hardware fault tolerance (HFT) table to determine the required fault tolerance for each subsystem. For our case study, we have assumed:

- We assume for our case study that the sensor has an SFF equal to 92% and the contactor has an SFF equal to 85%.
- From Tab. 8, we find that the minimum HFT is 0 for the sensor and 1 for the contactors. A minimum HFT of 1 means we can choose between, e.g., 1oo2 and 2oo3 (the most typical options). We will therefore modify the SIF to meet the architectural constraints as a next step and check again whether the PFH meets the SIL 2 requirement by choosing 1oo2 for the contactors.

Tab. 9. Input data

D failure rate	(per hour)	DC	DU failure rate	(per hour)	Common cause failures (CCF)
$\lambda_{D,PS}$	2,00E-07	60%	$\lambda_{DU,PS}$	8.0E-08	
$\lambda_{D,C}$	2,00E-06	75%	$\lambda_{DU,C}$	5.0E-07	β_C =10%.

The corresponding reliability block diagram for this SIF is shown in Fig. 18. The logic solver has been excluded to ensure the result is comparable to the previous analysis using ISO 13849.

To check if the PFH is within the SIL 2 requirement, we apply the same failure rates for the sensor and the contactor type with 350 400 cycles per year, i.e., as shown in Tab. 9. The formula to calculate the PFH of the SIF (see Chapter 8) becomes:

$$PFH_{SIF} = PFH_{PS} + PFH_C = \lambda_{DU,PS} + \left[(1-\beta_C)\lambda_{DU,C}\right]^2 T + \beta\lambda_{DU,C}$$

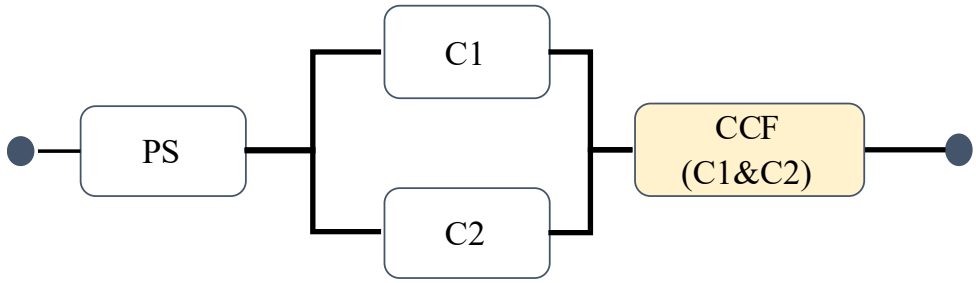

Fig. 18. RBD for a door sensor system

$$PFH_{SIF} = 8.0E-8 + 5.18E-8 = 1.32E-7$$

The result shows that the calculated PFH of the SIF falls within the SIL 2 requirement, and we have obtained an alternative architecture not permitted per ISO 13849, but still meets the PFH requirement for a PL d.

10.7.7 Implication of interval T and SIL follow-up

PFH is not strongly influenced by the value of the regular inspection and testing interval T, particularly when CCFs are included and for single devices, where T is excluded entirely from the formulas. In the low-demand mode, it is assumed that at each interval T, the SIF devices undergo a regular test, with complete renewal to regain an as-good-as-new state. However, regular tests are not the primary means of detecting DU failures in the high-demand and continuous mode:

- In the high-demand mode, most DU failures are revealed by demand rather than by regular scheduled tests, since performing more frequent testing than demand is practically impossible.
- In the continuous mode, DU failures are revealed as part of normal actions.

Despite frequent activations, the purpose of the interval T is to ensure that a renewal occurs after some time to reveal any remaining hidden DU failures and replace devices that are reaching the end of their useful life period. But what influences the choice of T when it is not impacting the calculated PFH? One suggestion is to look into the assumptions underlying the simplified PFH formulas:

- PFH formulas assume that T is chosen so that no more than one failure of a SIF subsystem is experienced in the period. (The influence of independent double, triple, etc., failures is excluded).
- The formulas also assume that $1-e^{-\lambda_{DU}T} \approx \lambda_{DU}T$, which means that $\lambda_{DU}T \leq 0.1$. If λ_{DU} is in the range of 1E-6 per hour (approximately once every 100 years), then T must be less than or equal to 10 years.
- Some restrictions may be specified in the device's safety (user) manual, which outlines the type of routine maintenance needed to ensure that the DU failure rate remains constant. As mentioned, demand does not trigger any inspection or maintenance unless it reveals that the SIF is failing to perform, unlike regular tests in low-demand mode, where inspections and maintenance are always carried out. The inspection and maintenance intervals specified in the safety manual may range from 5-15 years to annually, depending on the type of device.

- While demands may reveal DU failures efficiently for SIF subsystems that comprise only single devices, the same is not necessarily the case for SIF subsystems with redundancy. Here, SIF will still perform its functions in response to demand even if a redundant channel experiences a DU failure, and, given the nature of a DU failure, it is not clear unless the status of each subsystem is monitored.
- Some restrictions may follow from modifications that have been performed while in operation, like changes made to the software, replacing failed devices, introducing new network interfaces, and so on. While such activities are not regularly scheduled, they may, on the one hand, introduce the possibility of new types of DU failures if testing before restart is incomplete. Most likely, such faults will be revealed during the next demand.

To conclude:

- Some regular renewal over the life of a high-demand/continuous-mode SIF is needed, even if DU failures are primarily revealed during demands (high-demand mode) or activations that are part of normal operation (continuous mode)
- Overall, with a basis in assumptions underlying PFH formulas, a regular scheduled renewal may be needed around every 10 years.
- Depending on the type of device, the manufacturers' safety (user) manual can provide instructions for more frequent inspections and maintenance, so that the failure rate estimates remain valid. Some products may, for example, request intervals of 5 years rather than every 10 years.

10.8 Bibliography

IEC 62061. (2021). *Safety of machinery - Functional safety of safety-related control systems*. International Electrotechnical Commission.

IEC TR 62061. (2010). *Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery*. International Organization for Standardization.

ISO 12100. (2010). *Safety of machinery — General principles for design — Risk assessment and risk reduction*. International Organization for Standardization.

ISO 13849. (2023). *Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design*. International Organization for Standardization.

ISO 13849-2. (2012). *Safety of machinery — Safety-related parts of control systems — Part 2: Validation*. International Organization for Standardization.

ISO TR 14121-2. (2012). *Safety of machinery — Risk assessment — Part 2: Practical guidance and examples of methods*. International Organization for Standardization.

Machinery Directive 2006/42/EC. (2006). *Directive 2006/42/EC of the European parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC*. European Commission.

Machinery Regulation 2023/1230. (2023). *Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC (Text with EEA relevance)*. European Commission.