CHAPTER 9
FUNCTIONAL 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 enjoying functional safety standards?
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	Updated after spring semester

Contents

9 Functional safety

Many industries and infrastructure that provide necessary services and products to society pose risks of harm to people and the environment if those risks are not properly managed. This includes process plants, power generation and distribution plants, railway systems, ships, and fabrication that involve machinery and robotics.

Hazardous events and situations that can lead to accidents are prevented or mitigated by systems specifically designed to do so. It means either to withstand, avoid, or detect and act. Systems capable of detecting and acting will naturally rely on sensors, programmable controllers, and actuated devices that can intervene to restore the safe state. These systems were introduced in Chapter 6 as safety-instrumented systems (SIS).

In this chapter, attention is directed to how the SIS systems are designed and followed up in operation, in an effort to ensure that the systems are sufficiently reliable. In this context, sufficiently reliable means that the systems can guarantee, through the effort put into technology choices, tools, processes, practices, and people's competences, that the SIS systems will perform their safety functions when needed. The safety achieved by using SIS, in combination with other safety systems, is referred to as functional safety. The requirements, practises, and methods for achieving functional safety are covered in functional safety standards, the most important for this specific chapter being (IEC 61508, 2010) and (IEC 61511-1, 2016).

But why is it important to learn about functional safety? Many industries and societal infrastructures must provide evidence that their systems are safe and compliant with national, international, or European authorities; otherwise, products are denied market access or operations are mandated to stop. But safety is not ensured solely by regulations. Society expects it, and one major accident can put a company out of business and ban a sector, temporarily or permanently. Investing in safety is not always so easy to justify if one does not understand that the success of safety means that nothing (bad) happens. Some say that if you do not want to invest in safety, try an accident.

Standards on functional safety represent how regulatory requirements and industry best practices for managing safety assess the risk at hand. This chapter introduces some of the concepts, methods, and practices applied to SIS systems throughout the whole lifecycle of the systems, starting with hazards and risk analysis, through design and installation that involve integration with other systems, to operation, modifications, and maintenance. The principles addressed are generic, even if the examples are primarily from the process industry.

The chapter is closely linked to Chapter 6 on safety-instrumented systems, Chapter 8 on reliability analysis, and Chapter 10 on Machinery safety.

9.1 Abbreviations

CCF	Common cause failures
DC	Diagnostic coverage
DD	Dangerous detected
DU	Dangerous undetected
FTA	Fault tree analysis
IEC	International Electrotechnical Commission
IEV	International Electrotechnical Vocabulary
ISO	International Organization for Standardization
PFD	Average 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)
RBD	Reliability block diagram
S	Safe
SFF	Safe failure fraction
SIF	Safety instrumented function
SIS	Safety instrumented system

9.2 What is functional safety, and what is not?

Functional safety is a concept that can be a bit difficult to grasp, and many find the definitions in IEC 61508 and IEC 61511 somewhat difficult to apply. This is because the definition sets a wide and vague boundary, blurring the lines between functional safety and broader technical or overall safety measures. In this Chapter, we therefore use our own definition:

> **Functional safety:** The safety achieved by active safety systems in response to hazardous situations, specifically where electrical, electronic, and programmable electronic technologies are involved.

A couple of remarks are added for clarity:

Remark 1: The definition implies that functional safety focuses on safety systems activated only in hazardous situations, and not those that are more indirect.

Remark 2: Functional safety standards, like IEC 61508 and IEC 61511 are primarily focused on requirements for specification, design, and operation of electrical, electronic, and programmable technologies applied in safety applications. This is why our chosen (own-worded) definition was crafted to better reflect this alignment.

Safety, however, is a broader concept and achievement, with functional safety making some contributions. According to the Online Electropedia vocabulary by IEC (IEV), safety is defined as:

> **Safety:** Freedom from unacceptable risk [IEV 903-01-19].

The term "freedom" means keeping unwanted risks at a distance. The term "risk" is often expressed as a triplet of what can go wrong, its likelihood, and the severity of the outcomes. More recent definitions of risk have placed greater emphasis on assessing the degree of knowledge when decisions are made about how to manage the risk. The term "unacceptable" acknowledges that risk cannot be zero and that a decision must be made about what is acceptable and what is intolerable. Depending on the sector and application area, acceptance criteria are defined by authorities, companies, or society. An important aspect of safety is aligning efforts with the amount of risk reduction needed. Therefore, hazard and risk analysis serve as a key input to functional safety. Nonetheless, decisions and solutions do not rely solely on these analyses; they must also consider regulatory requirements and industry best practices. This makes the approach to functional safety risk-informed rather than purely risk-based.

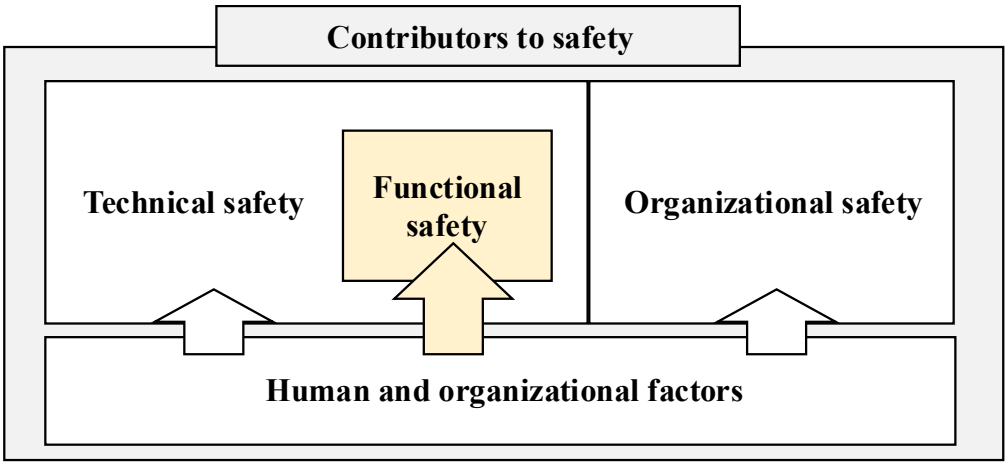


Fig. 1 Contributors to safety

9.2.1 Relationship with other contributors to safety

Functional safety is only one component needed to achieve safety, as illustrated in Fig. 1: It is often considered part of **technical safety**, a well-established discipline that encompasses all technical measures aimed at ensuring safety. In addition to active safety functions, technical safety includes passive measures such as safety margins in equipment design, physical separation of hazardous equipment, firewalls, dikes, spill containment systems,

and other engineered barriers. Therefore, technical safety is broader than functional safety, covering both active and passive risk-reducing measures.

Operational and organizational measures, collectively referred to as **organizational safety**, complement technical safety. Although not a standard term, it describes the safety achieved by personnel with established procedures and organization for managing hazardous situations. Examples include emergency operating procedures, alarm response procedures, emergency preparedness plans, response plans, evacuation procedures, and role assignments.

Human and organizational factors provide the foundation for achieving both organizational and technical safety, including functional safety, as indicated in Fig. 1. In functional safety, this means that many technical capabilities rely on people with the necessary competencies, that roles and responsibilities are clearly defined and adequate, and that established procedures and practices are followed.

Technical and organizational safety measures supplement the basic process control system and the inherent safety provided by facility and equipment design. In this context, “built on top” means that these measures are intended to manage hazardous situations that are not adequately controlled by normal process control functions or by the inherent safety margins of the facility and its equipment. If safety depends on control functions operating continuously during normal operation, as is the case for many machinery and railway signaling systems, these control functions fall within the scope of functional safety.

9.2.2 Functional safety in perspective

Before the 1980s, logic operations in SIS systems were implemented using simple electromechanical relays. When industrial programmable logic controllers (PLCs) and distributed control systems (DCS) arrived in the 80s, many automation and technical safety professionals questioned whether they could be used for safety purposes. Arguments against using PLC and DCS technologies were:

- Engineers were more familiar with hardwired relay systems, whose behavior was considered relatively transparent, easier to understand, and to verify.
- Software-based logic was perceived as less transparent and more difficult to verify, and software faults could remain hidden for long periods before being triggered by specific operating conditions.
- Software logic could more easily be subject to modifications than hardwired logic, creating concerns that changes and updates might inadvertently introduce new faults.
- Software engineering methods, development processes, verification techniques, and support tools were less mature than they are today, and there was no widely accepted best practice for the development of safety-critical software.

Since the 1990s, efforts have been made to find safe ways to implement PLC and DCS technologies for SIS, aiming to enhance safety with more flexible, digital systems. Despite the mentioned concerns, these technologies provide the capabilities of:

- Improved diagnostic capability to report faults and degradations
- More advanced sensor capabilities for detecting hazardous situations
- Capability to provide information for monitoring the performance of safety functions, for example, response times.
- Scalable solutions for safety logic to accommodate detecting and intervening in safety in larger and more complex operations, which would be nearly impossible to scale with traditionally hardwired systems
- Accommodate new ways of operating, like remote operations, where digital solutions, also for safety, are needed.

Coordinated by various organizations, including the IEC, industry actors joined forces to work on the first publication of IEC 61508 in 1998, titled "Functional safety of safety-related electrical/electronic/programmable electronic (E/E/PE) systems.' This standard provided, and still does, though in a newer version, the broad principles for technology safety. Today, it continues to serve as a generic framework for vendors certifying their systems and products for safety applications. In addition, the standard forms the foundation for developing industry-specific standards. One example is IEC 61511, developed for use by plant owners and systems integrators in the process industry.

9.2.3 Scope of functional safety standards

As mentioned, standards on functional safety are primarily focused on the specification, design, implementation, operation, and maintenance of E/E/PE technologies that are applied to safety-critical applications. Some of the activities, along with some central concepts required by the standards, are illustrated in Fig. 2, using the house metaphor.

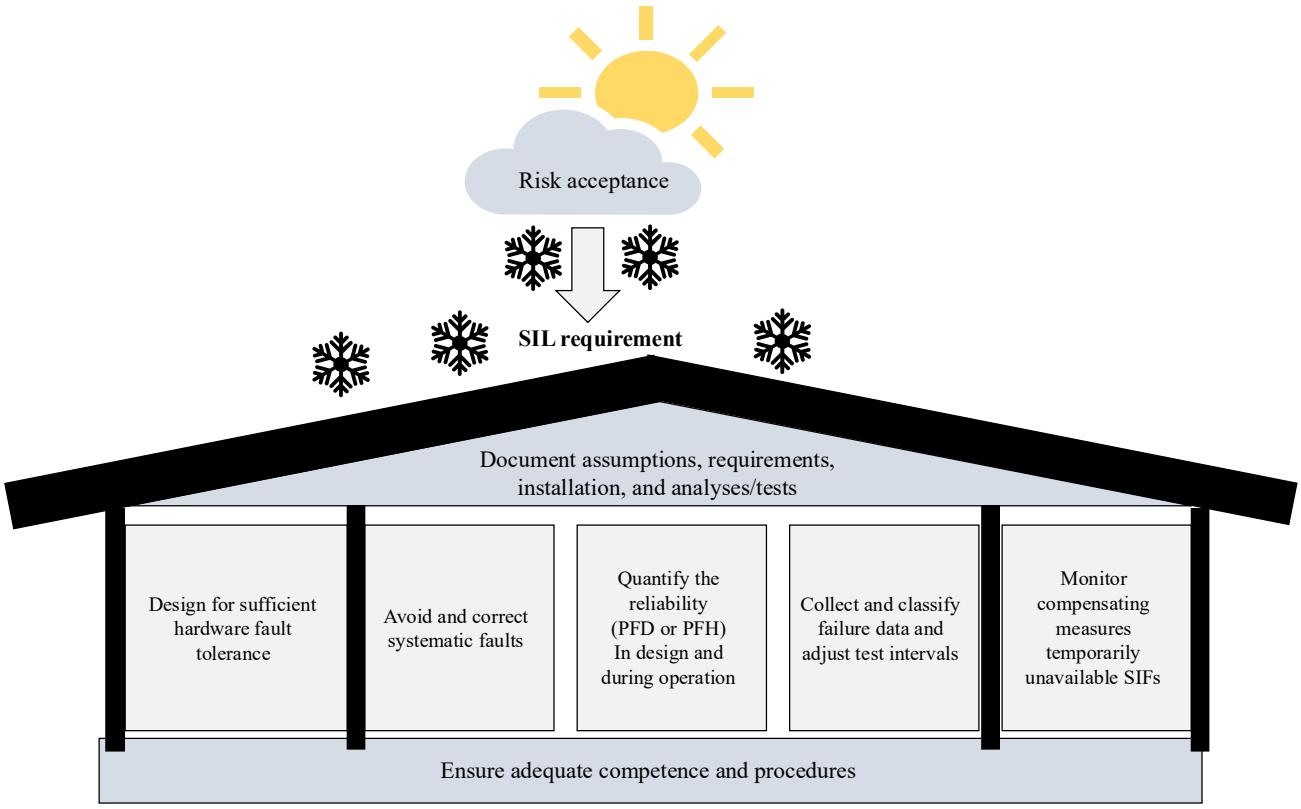


Fig. 2. House of functional safety

The starting point is that we are to build a house, i.e., an E/E/PE system, that can withstand weather and wear, i.e., the E/E/PE system must be reliable enough to achieve the required level of safety. The functional safety standards have introduced the concept of safety integrity level (SIL), split into four levels, SIL 1-4, for which the appropriate level is chosen by analysis of the risk at hand and the risk accepted. The SIL concept, applied to the house metaphor, could be the amount of snow the roof must withstand, depending on where in Norway the house is built.

The SIL requirement will result in some design and operational restrictions and demands, just as the snow load will call for the dimensioning of walls and structures and the choice of materials. In Fig. 2 , we have split them into two horizontal and five vertical activities. The vertical ones are about achieving a robust, reliable

design solution and ensuring reliability meets the expectations of the SIL requirement, not only as designed but also in operation.

More specifically, the individual safety functions are designed and realized so that they:

- Are equipped with sufficient hardware fault tolerance, considering the complexity of the devices, their documented performance, and the SIL requirements.
- Have a negligible impact of systematic faults, which are faults that are not always possible to incorporate in reliability assessments.
- Are sufficiently reliable as designed, considering the quantified reliability, using reliability measures like Probability of failure on demand (PFD) or failure frequency (PFH), which must be within a permitted range of the SIL requirement.
- Are continuing to be sufficiently reliable by analyzing faults from operation and, as needed, replacing unreliable equipment or performing inspection and testing more frequently.
- Are always compensated by other alternative measures if the safety functions are temporarily out of service, ensuring that these measures are always monitored.

The horizontal activities support and are relevant to all vertical activities, focusing on requirements about what to document, what procedures must be in place, and what level of competence is required for those involved.

9.2.4 IEC 61508 and related sector standards

IEC 61508 is an extensive standard that consists of 7 independent documents or parts, which are all applied worldwide by those designing and having on the market equipment for safety-critical applications:

1. IEC 61508 (2010): General requirements relating to each phase of the safety lifecycle of the safety system
2. IEC 61508-2 (2010): Requirements regarding the design of the hardware solution, the calculation of achieved reliability, and the integration of software and hardware
3. IEC 61508-3 (2010): Requirements for software development (process and choice of programming methods and development tools)
4. IEC 61508-4 (2010): Definitions of terms used in all parts of the standard
5. IEC 61508-5 (2010): Guide to specific activities described in Part 1 and Part 2. Examples are risk analysis methods for determining safety integrity level (SIL) requirements.
6. IEC 61508-6 (2010): Guide to methods for calculating the reliability of different hardware solutions.
7. IEC 61508-7 (2010): Guidance to the selection of other methods that can be used to meet requirements in Part 1, Part 2, and Part 3.

Parts 1-4 of IEC 61508 are mandatory, meaning they **must** be used to comply with the standard. The other parts are informative, providing examples and guidelines that can be replaced with other suitable methods.

In short, IEC 61508 covers:

- A lifecycle model that defines key phases of SIS design, development, and operation.
- A risk-based approach for identifying safety functions and their associated reliability requirements expressed by safety integrity level (SIL).

- Requirements and restrictions on design solutions and design methods for hardware and software.
- Process for verifying and validating that requirements have been met, in design as well as during operation.
- Requirements for follow-up of reliability in operation and to take necessary compensating measures.

When IEC 61508 was introduced, it was to serve two purposes:

- To be a reference standard that facilitates the development of product and application sector standards. The reference standard provides generic requirements that can be adopted for concepts, processes, and specific risks associated with the sector or product.
- Enable the development of E/E/PE technologies where product or application standards do not exist or where the same product is targeting several sectors and applications.

Sector standards may cover the full scope of IEC 61508 or parts of it. Most sector standards focus on system integration and use, assuming that products in use are already certified to IEC 61508 or have documented evidence of proven use. Manufacturers are therefore using IEC 61508 more often than the engineering companies and end users (plant owners and operators).

Fig. 3. Examples of IEC 61508 certificates

The certification process is usually conducted by a third-party (independent) company, which issues the certificate. Two internationally recognized third-party certification companies are TÜV and Exida. TÜV is not *a single company* but an association of several companies, including TÜV Rheinland, TÜV Süd, and TÜV Nord (all in Germany). Certificates for products that conform to IEC 61508 are called SIL certificates. Two examples of SIL certificates are shown in Fig. 3.

Fig. 4 gives examples of the most important sector standards developed on the basis of IEC 61508 (straight arrows) or that are relevant to it, even if not anchored in this standard (stippled lines).

Some remarks on the figure:

- Some sectors have more than one functional safety standard.
    - Machinery safety has two standards on functional safety, i.e. IEC 62061 (2021) and ISO 13849 (2023) where either of the two can be used at the user's choice. The reason for having two standards is that one of them, ISO 13849, had long existed and was widely used when IEC 62061, which aligns more closely with IEC 61508, was introduced.

- The railway sector in Europe, including Norway, applies three standards, originally published by CENELEC: EN 50126 addresses process requirements, while the other two parts address hardware (EN 50129) and software (EN 50128) requirements. The standards were later published by IEC as IEC 62278 (covering EN 50126), IEC 62279 (covering EN 50128), and IEC 62425 (covering EN 50129).

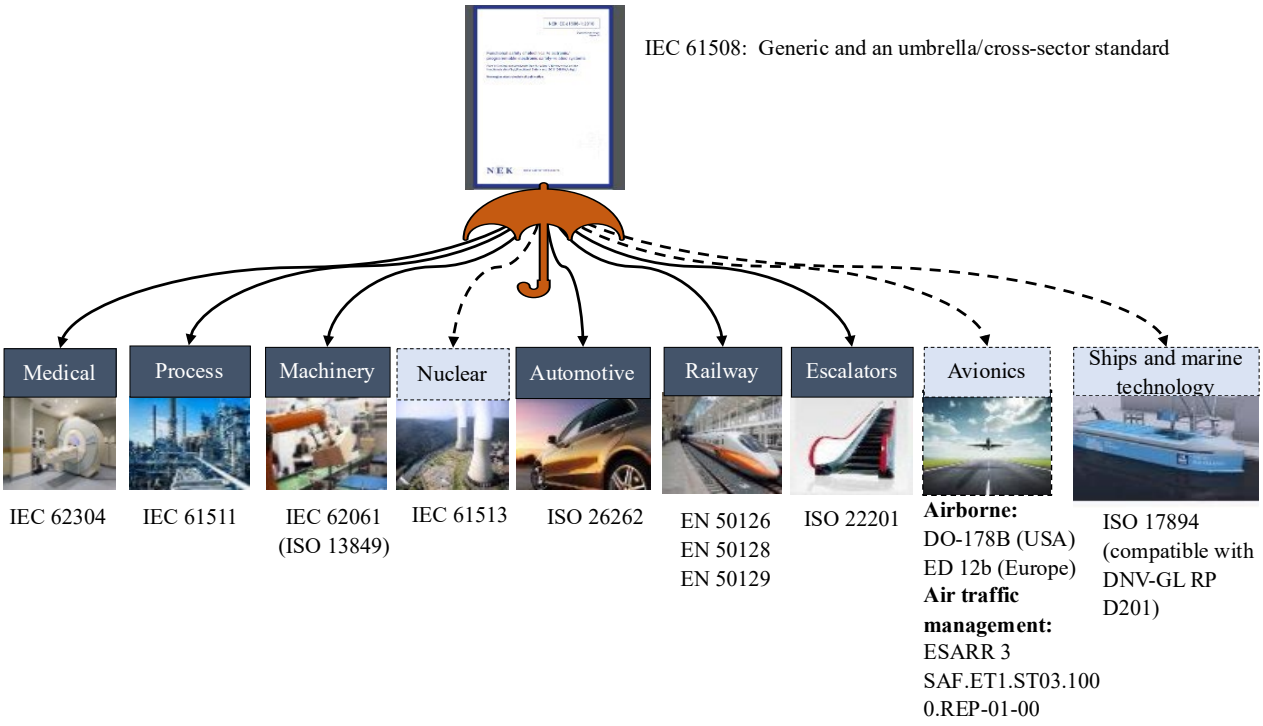


Fig. 4. IEC 61508 and sector standards

Manufacturers often use IEC 61508 for products that need to meet requirements across multiple sectors. For this reason, IEC 61508 is also called **the manufacturer's standard**.

IEC 61511-1 (2016) is used by asset or plant owners and engineering companies that design and integrate SIS using a product that is already SIL-certified or documented according to requirements for prior use. IEC 61511 is therefore referred to as the end users' standard. It is this standard that systematically uses the term SIS rather than the lengthier term "E/E/PE safety-related system" used in IEC 61508. A summary of the distinctions between IEC 61511 and IEC 61508 is shown in Fig. 5.

	Used *for*…	**Used *by*…**
 IEC 61508	• Product development • Certification • Basis for new sector standards	• Manufacturers • Expert groups (IEC, ISO,..) developing new standards
 IEC 61511	• Design and integration of SIL-certified systems • Operation and use	• Engineering companies • Facility owners • Manufacturers (for integrating and configuring already certified products)

Fig. 5. IEC 61511 vs IEC 61508

9.3 The SIL concept

We have already briefly mentioned the term SIL. As SIL is a central concept in IEC 61508 and in all sector standards based on this standard, it warrants more thorough attention.

Before defining SIL, we should introduce what we mean by safety integrity. Here, and for SIL, we rely on IEC 61511, as it aligns with the chosen terms "SIS" and "SIF" introduced in Chapter 6.

Safety integrity: Ability of the SIS to perform the required SIFD as and when required

The safety integrity level (SIL) is a concept that divides the ability into four distinct levels and is used to set a distinct expectation level (SIL requirement) for which evidence that it is met must be documented.

- **SIL:** discrete level (one out of four) allocated to SIF for specifying the safety integrity requirements to be achieved by the SIS.

SIL is always used in combination with specific SIFs, and not the SIS as such. This is following the same line of arguments as when we defined reliability in Chapter 8.

The term "ability" is also used in the definition of reliability (as shown in Chapter 8). Therefore, the functional safety standards have defined a link between each SIL level and reliability requirements, the latter formulated by a range with a max and minimum value of a chosen target failure measure as shown in Tab. 1. More specifically, we observe that:

- The table uses different target failure measures for low-demand and high demand/continuous demand, three terms explained in Chapter 6, but is repeated here as well:
    - Low-demand mode: The mode of operation where a safety function is subject to, on average, less than one demand per year
    - High demand: The mode of operation where a specific safety is subject to, on average, one demand per year or more
    - Continuous mode: The mode of operation where the safety function is executed as part of normal operation
    - The target failure measures are:
        - The average probability of failure on demand (PFD) (for low-demand)
        - The average probability of having a dangerous failure per hour (PFH), also referred to as the dangerous failure frequency, forhigh-demand and continuous demand.

      Both measures (PFD and PFH) were introduced in Chapter 8.
- The lowest PFD value in the SIL 4 range and the highest PFD value in the SIL 1 range define the boundary of what is achievable and acceptable for a safety function.
    - For example, if a SIF is allocated a PFD above 01E-1, it is below the SIL 1 range and therefore considered a SIF per IEC 61508.
    - If SIF is allocated a PFD below 1E-5, it is assumed to be unrealistic to achieve, and a redesign process and/or a new performance is performed. Some industries even exclude SIL 4 as an option because they find it unrealistic to build and operate a SIF at that performance level. Still, some industries rely on SIL 4 functions, as there are few other systems to allocate risk reduction to. For example, many SIFs used in railway signaling systems are SIL 4 compliant.

Tab. 1. SIL table in IEC 61508

SIL	Allowed failure probability (PFD) when low demand	Allowed failure rate of dangerous failures per hour (PFH) when high/continuous demand
4	1E-5 ≤ PFD < 1E-4	1E-9≤ PFH < 1E-8
3	1E-4 ≤ PFD < 1E-3	1E-8 ≤ PFH < 1E-7
2	1E-3 ≤ PFD < 1E-2	1E-7 ≤ PFH < 1E-6
1	1E-2 ≤ PFD < 1E-1	1E-6 ≤ PFH < 1E-5

The PFD value is sometimes expressed by its reciprocal, named the risk reduction factor (RRF). This relationship can be explained as follows:

- Assume that a SIF has a PFD requirement of 5E-3, meaning within the SIL 2 range
- With this requirement, the SIF cannot tolerate failing more than once out of 200 times the function is demanded.
- Assuming an initial demand rate (DR), say 1 per year, the rate of a hazardous event (HE) resulting from a SIF failure is 200 times lower, i.e.: $HR = DR \cdot PFD$
- RRF is an expression for how many times the initial event (demand) is reduced compared to the hazardous event following a SIF failure, naturally, the reciprocal of the PFD value:

$$RRF = \frac{DR}{HR} = \frac{1}{PFD}$$

We will later use the term RRF more broadly as the relationship between any hazardous event and the threshold for which risk is not acceptable.

It may be tempting to ask (and probably some do): Why use SIL complementary to PFD or PFH?

- One explanation is that SIL and PFD/PFH serve different purposes:
    - PFD and PFH are useful for translating risk reduction requirements into measures relevant for reliability analysis. However, these measures are not very useful for guiding engineers on which specific requirements apply to hardware architecture, software implementation, procedures and practices, and support tools. Also, PFD and PFH do not take all types of failures into account and are subject to several sources of uncertainty related to data, models, and assumptions about the effectiveness of testing and diagnostics.
    - SIL represents a way to differentiate the level of effort and requirements for hardware architecture, software implementation, procedures and practices, and support tools. It means that there are more and stricter requirements for a SIF and involved devices that have a SIL 3 requirement than for a SIF with a SIL 1 requirement.

9.4 The safety life cycle

The safety lifecycle is another central concept in the functional safety standards, as it defines all phases of an SIS, covering both design and operation. The standards also organize the requirements according to this model. The way the lifecycle is organized differs slightly among the functional safety standards, and we have chosen to rely on the one in IEC 61508 (part 1), which is perhaps the best-known. This model consists of a total of 16 phases, as shown in Fig. 6. Roughly, the 16 phases may be organized into four groups, as shown in the figure, and explained below.

Risk analysis and requirements identification phases (marked 1): The overall goal of these phases is to determine whether safety systems, including SIS, are needed and how reliable they need to be. The starting point is hazard and risk identification and analysis, grounded in the area or system under consideration, referred to as EUC.

Equipment under control (EUC): Equipment, machinery, apparatus, or plant used for manufacturing, processing, transportation, medical, or other activities.

Some of the foreseeable hazards and hazardous situations can be prevented and managed by the EUC control system.

EUC control system: A System that responds to input signals from the process and/or an operator and generates output signals that cause the EUC to operate in the desired manner.

However, a malfunction of the EUC control system can trigger a response from SIS or other safety systems. The risk analysis determines the EUC risk, meaning the risk of hazardous events arising within the EUC and its control system. A comparison with the risk acceptance criteria determines the risk reduction needs and the need for risk-reducing measures, including SIS. The SIL allocation process determines the amount of risk reduction to be covered by SIS, expressed as a SIL requirement for each SIF.

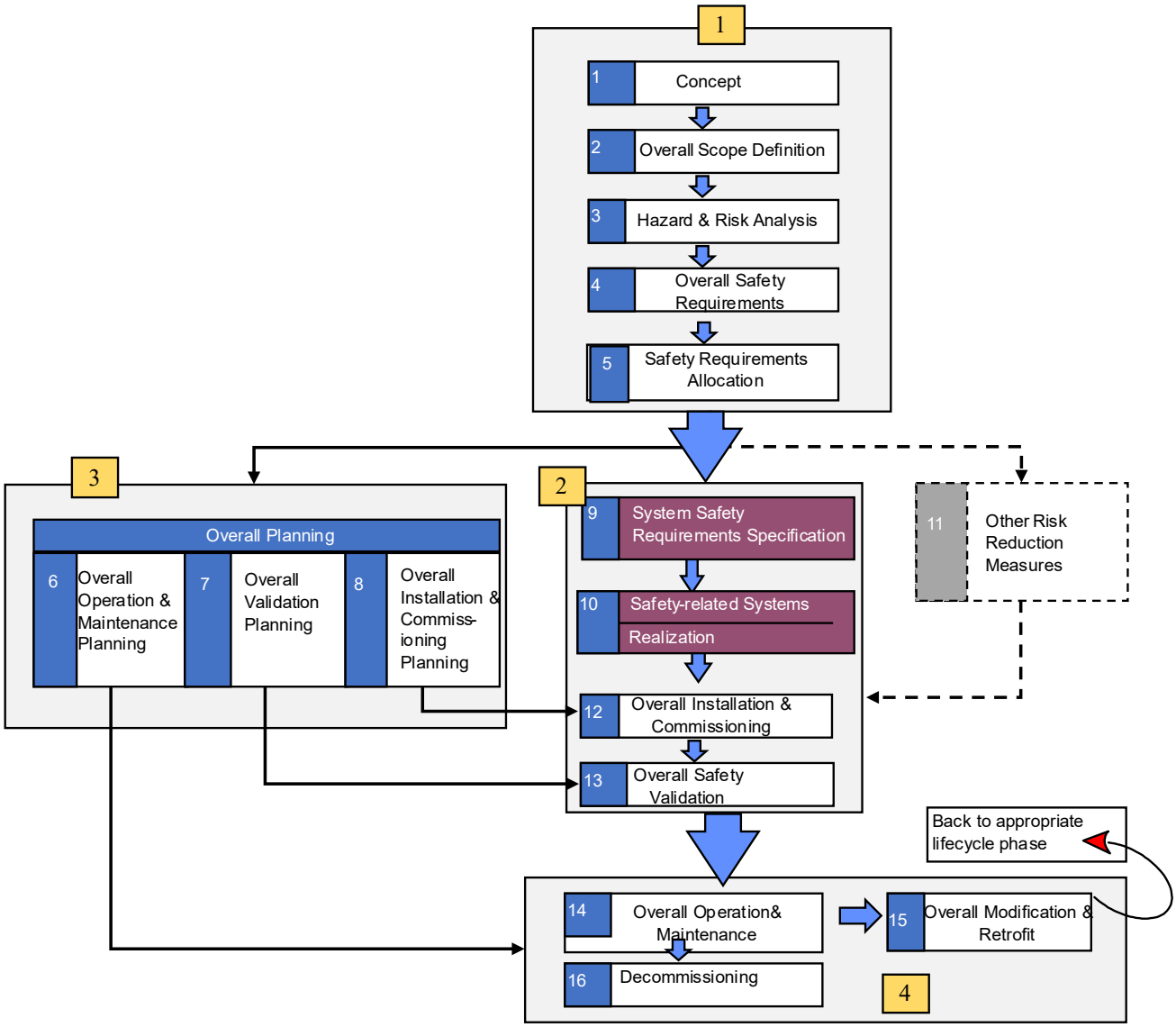


Fig. 6. Safety life cycle in IEC 61508

Design and implementation phases (marked 2) Design and implementation, including installation and overall validation. The Central goal here is to implement requirements from the hazards and risk analysis, including SIL requirements, in the design, analysis, and work process in the design and construction of SIS. A starting

point is to prepare the safety requirements specification (SRS) using input from the risk analysis and SIL allocation.

> **Safety requirements specification (SRS):** specification containing the requirements for the safety functions and their associated safety integrity levels.

The SRS is a mandatory document to prepare during the design phase, and it must be kept up to date throughout all lifecycle phases. Various verification activities, including reliability analyses, are conducted to confirm that the SIL requirements are met. The overall installation and commissioning concern the integration of SIS with other implemented risk-reducing measures, and the overall safety validation is confirmed at the facility, after extensive pre-startup testing, that the systems, in combination, can manage safety.

Planning phases (marked 3): These phases cover the preparation of procedures for installation, testing, commissioning, operation/maintenance, and handling of proposals for modifications/modifications.

Operation, maintenance, and modifications phases (marked 4): These phases cover what is sometimes referred to as SIL or SIS follow-up in operation. It includes activities maintenance and testing activities, failure registration and analysis, failure classification, and re-calculation of PFD (or PFH) to check if the SIL requirements are met such as failure data acquisition and classification to reveal dangerous failures where the SIF did not perform as required, evaluate corrective measures as needed, for example to replace equipment or modify test intervals, and monitoring and compensating for any temporary SIFs that are unavailable due to repair actions or operational situations.

Phases 9 and 10 are most important for manufacturers for their product development and certification. The facility owner is responsible for all phases but often contracts the work for phases 1-12 to a system integrator or engineering company. Phases 9 and 10 will then be focused on composing systems based on certified products. The facility owner is most directly involved in phases 14 and 15, a period that can range from 10 to 30 years, sometimes even more.

The following sections further detail the lifecycle phases.

9.5 Risk analysis and requirement identification (phases 1-5)

IEC 61508 takes a **risk-informed approach,** meaning hazard and risk analysis is important for determining which safety functions are needed and how reliable they must be. The reason for not using risk-based approaches, meaning that decisions are made solely from hazard and risk analyses, is that requirements relevant to identification and performance may also be influenced by regulatory requirements and national guidelines.

Before proceeding, we will introduce some important terms and concepts related to these phases, some of which have been explained more briefly earlier.

9.5.1 What is risk?

Before we describe what is included in a risk analysis, it is important to understand what we mean by the term **risk**. Risk is often expressed by answering three questions, first proposed by Kaplan and Garrick (1981):

1. What could go wrong?
2. How often does it happen?
3. What are the consequences?

The answer to "What can go wrong" is often defined as hazardous events and should be those that represent a significant deviation from regular operation and, if not acted upon, may develop into an accident. Each identified hazardous event is called a scenario, as it may have its own causes and consequences. The frequency or probability of the event can be expressed quantitatively (as a number) or qualitatively (on a scale). Answers about the consequences lead to a vector of possible outcomes, depending on the circumstances and the capabilities of the safety systems.

Therefore, risk is often expressed by the following formula:

$$Risk_i = F_i \times \underline{C}_i$$

Where $Risk_i$ is the risk associated with the hazardous event *i,* F_i is the associated frequency (or probability), and $\underline{C}_i$ is the vector of potential consequences. This vector is also called a consequence spectrum. When values, frequencies, or probability categories are not explicitly given, the more general term "likelihood," representing both, is used.

Newer definitions, like the one in ISO 31000 (2018)Focus more on uncertainty and the importance of determining and accounting for the degree of knowledge about the probability of outcomes, not only their estimated values.

Hazardous events arise from the presence of **hazards** in combination with initiating (triggering) events.

- **Hazard:** potential source of harm.

Hazards can be phenomena such as shocks, crushing, cutting, forces and speed, toxic material, flammable and explosive materials, and the like. Hazards do not directly lead to hazardous events unless someone or something is exposed to them. The triggers that lead to such exposures are called initiating events.

A hazardous event for a washing machine is the door opening while the machine is running. The hazards are the rotating drum and water, and the hazardous event occurs when someone opens the door. The consequences of opening the door can range from water on the floor to crushing or cutting of fingers if someone puts their hand into the drum.

Hazardous events can be any event along the trajectory from the loss of control with a hazard to an accident. However, in some analyses, for example, bow-tie analysis mentioned in Chapter 6, the term has a narrower meaning**:**

Hazardous event: A significant event that, if not stopped, may lead to an accident.

A bow-tie analysis places the hazardous event in the middle and refers to safety systems (or barriers) before as preventive and after as mitigative.

9.5.2 Risk analysis and risk assessment

A risk analysis is a structured process to identify the risks, meaning:

- The hazards and initiating events
- The hazardous events
- Possible consequences
- Risks associated with all of these

The first two items are part of hazard identification. Hazard identification is often conducted through a multidisciplinary review (e.g., a workshop) that uses checklists and guidelines to stimulate discussions on what can go wrong and why. The risk analysis assesses the risks of all identified hazardous events based on frequency and consequence. Risk matrices are sometimes used to support this process. Risk assessment is an overarching activity that determines whether the risks associated with dangerous incidents are acceptable. For this, risk-acceptance criteria are required. When the risk is unacceptable, risk-reducing measures must be proposed to make the risk ultimately acceptable. The term risk assessment is therefore more precise than risk analysis for the first five phases of the safety lifecycle.

9.5.3 Equipment under control (EUC)

IEC 61508 has introduced the term Equipment under control (EUC), as a generic term applied to a system or piece of equipment in which hazards are present and therefore likely to require protection.

EUC: Equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities

It is natural that the identification of EUC is the starting point for the safety lifecycle, as it determines the focus of the next phases, in particular the scope and focus of the hazard and risk assessment.

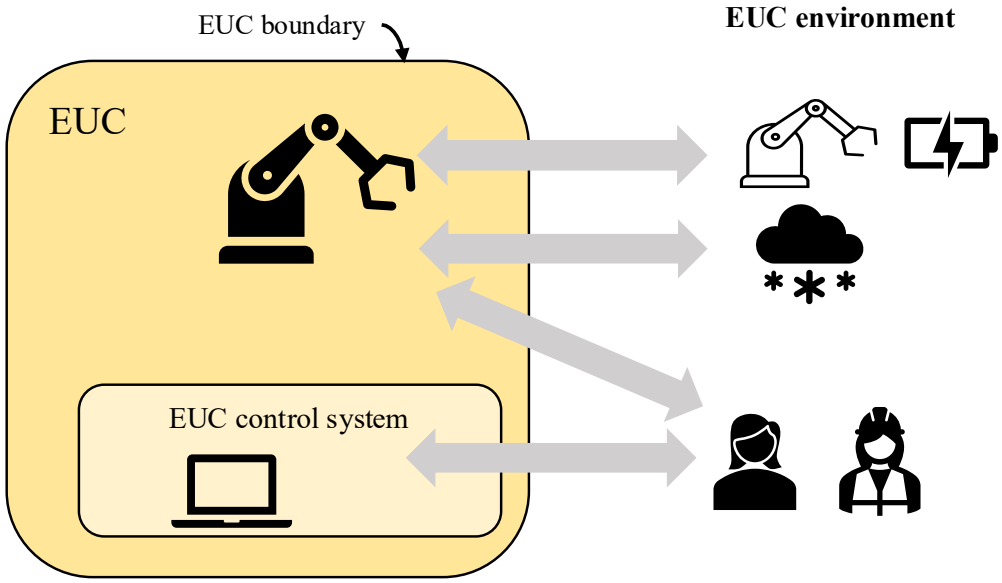


Fig. 7. EUC and related concepts

The EUC boundary can be the entire processing plant, a part of the plant, a specific machine, medical equipment, a car, a ship, a train, or a railway track section. In either case, it is essential to emphasize that the EUC ***does not*** include safety systems, as these are added after hazards are assessed and the required protection identified. Rules of thumb when defining the EUC:

- Larger systems, like ships, should be split into several EUCs as the risks associated with systems in these areas will differ. EUCs' boundaries can be limited to specific systems (e.g., a propulsion system) or to physical areas (e.g., the hull, deck, or storage room). Sometimes, both types of EUC are needed to cover system- and area-specific risks.
- The EUC should not be sliced into too small pieces, as this may lead to omitting the interaction of systems that are important for understanding the risks. For example, a ship's propeller constitutes a narrow boundary for EUC, as its interaction with engine systems is vital.

In general, selecting EUC and EUC boundaries can be done with the support of the following questions:

- What types of hazards are to be identified? To address risks in a processing facility, it is reasonable to select larger equipment for handling or storing hazardous fluids, such as larger tanks, compressors, and pipelines. To address fire hazards, it seems more sensible to choose an area and a room to cover all sources of fire risks simultaneously.
- What are the interacting systems relevant to hazards? In addition to a tank or a room, a more detailed boundary can identify interfaces with other systems that could influence hazards and should not be overlooked in the analysis. For example, which pipes in and out of the tank could be marked as critical? If a tank is connected to a heating circuit, it seems relevant that the pipes entering and existing the tank form a closed loop.

Complementary to the EUC are:

- The EUC control system, i.e., the programmable systems that control the EUC as part of regular operation.
- The EUC environment describes the exposures and events in the environment of relevance to the risks associated with the EUC.

The EUC control system is directly involved in the operation of EUC, while the EUC environment covers exposures of indirect relevance, as shown in Fig. 7.

9.5.4 Hazards and risk analysis methods

Hazards and risk analysis methods are structured approaches for identifying hazards, their associated hazardous events, and their triggers. The Hazards and Operability Study (HAZOP) is a well-known and widely applied method. HAZOP was originally developed to identify hazards in processing plants. However, the method is suitable for most processes that involve a flow of something, whether data, fluids, or activities/sequences. For example, HAZOP is used to detect programming errors in software logic (software HAZOP), work processes for e.g., logistics and manufacturing (process HAZOP), and control loops (Control HAZOP). For now, we will use the original HAZOP as the basis for the explanation.

HAZOPs are usually conducted in a workshop involving experts in equipment design, operation, and maintenance. In the workshop for a process HAZOP, the goal is to:

- Identify how hazardous events may occur if the current design is implemented
- Identify possible ways to either remove the possibility of having the hazardous event, reduce its occurrence, or limit its consequences
- Identify who is responsible for follow-up of identified action points.

HAZOP achieves a systematic approach to hazard identification by combining process parameters and keywords to direct attention in different directions:

- Process parameters: Process properties, such as flow, pressure, temperature, level, and composition.
- Guidewords: Such guiding words are not, none, more of, less of, instead of, in addition to, part of, opposite (direction), (for) early, (for) late, before, after, etc.

The process facility is divided into several sections, called nodes, which are analyzed sequentially. The most essential design document used in the workshop is the P&ID drawings. By combining process parameters and guidewords when examining a specific piece of equipment or process section, it is possible to detect potential deviations that could lead to a hazardous event.

System	Guideword	Deviation	Causes	Consequences	Existing barriers	Frequency	Severity	Additional risk-reducing measures	Responsible

The table columns are:

- Node: Short name or number that identifies the node
- Guide words: Combination of process parameters and guidewords
- Deviation: Identified hazardous event

- Possible causes, covering hazards and triggering events.
- Possible consequences: Written explanation or selection of relevant consequence category if these are defined
- Existing barriers: Listing of any measures already introduced as part of the planning and design to prevent the event or mitigate its consequences. It can relate to technical, human, or organizational measures.
- Frequency: A qualitative or quantitative expression of how frequently deviation will occur, considering the presence of existing barriers.
- Severity: A qualitative or quantitative expression of the worst-case consequence.
- Additional risk-reducing measures: New measures of relevance for reducing risk, covering operational procedures, human tasks, and technical systems.

Frequencies and severities may be given, e.g., as events per year or fatalities per event. Alternatively, the semi-quantitative frequency and severity statements listed below can be used.

Value	Description
5	Occurs frequently, typically from 1 to several times per year
4	Happens occasionally, typically less often than 1 time per 10 years
3	Rarely, in the sense that it is possible to imagine that it could happen, but has not yet been experienced
2	Very unlikely (remote) in the sense that this has never been experienced and seems very unlikely
1	Improbable in terms of this being extremely unlikely

Value	Description
5	Catastrophic, potentially causing the loss of multiple human lives, (almost) irreparable damage to the environment, and the loss of an entire facility with great social consequences.
4	Serious, meaning severe injuries, loss of one life, and damage to the environment and assets that are possible to restore within a certain time
3	Significant damage, meaning injuries to humans and temporary damage to the environment and/or the asset.
2	Damage, meaning some minor injuries and light or limited damage to the environment and/or the asset
1	Limited damage, meaning only minor injuries involving no or short unavailability and negligible damage to the environment and/or assets

Guidewords and deviations may be selected based on what is relevant to the system under analysis. Examples that may apply to a process section are:

Process parameters	Guidewords
Flow Pressure Temperature Level	No (not, none) More (more of, higher) Less (less of, lower) As well as (more than) Part of (partly executed) Reverse (opposite) Other than (replaced by other)

The application of the HAZOP method is shown for a vessel separating gas from liquids in Fig. 8. Here, we define the vessel as the EUC and the level control loop as the EUC control system. We assume that the two-phase flow entering the vessel is explosive if released to air, and that a control system ensures the level is optimal for separation. We may also expect other control loops installed for the vessel, but they were excluded for our simple example.

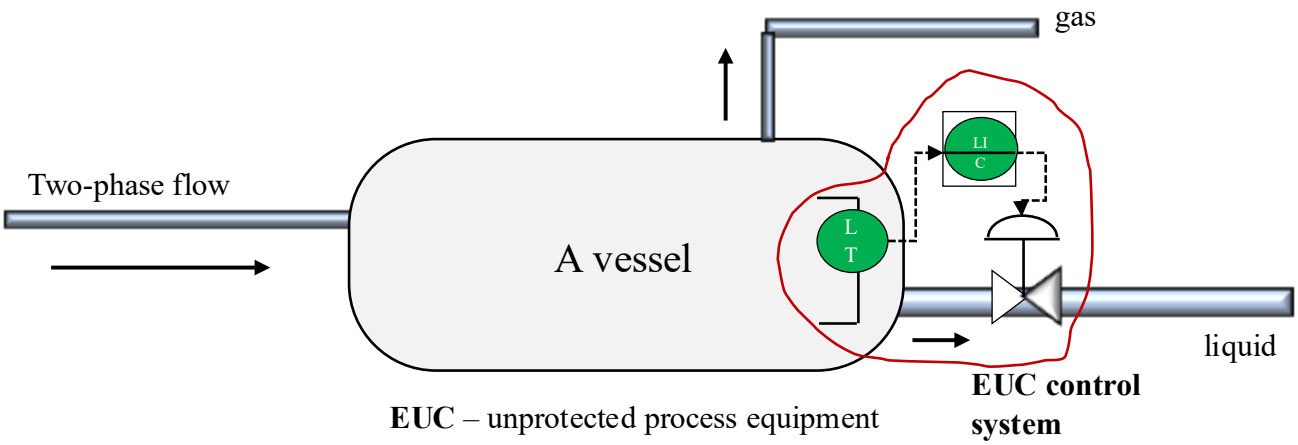


Fig. 8. Simplified P&ID with (HAZOP) nodes marked with color

The HAZOP workshop is organized and led by a HAZOP facilitator. It is the responsibility of the facilitator to ensure that the relevant experts are attending the workshop. During the workshop, there is usually a secretary, also called a scribe, who takes notes from the discussions. The notes added to the HAZOP table show one example of a deviation that may create a hazardous situation for the vessel.

System	Guideword	Deviation	Causes	Consequences	Existing barriers	Frequency	Severity	Additional risk reducing measures	Responsible
Vessel	Pressure	Too high	Spurious closure control valve outlet	*Over-pressuring of a separator leading to an explosion*	The control system is regulating the pressure using an outlet valve SIF1: PSD function closing inlet valve SF2: Pressure safety valve (mechanical)	5	5	Operator intervention upon alarm Do a LOPA to decide if additional measures are needed	Functional safety lead

9.5.5 Risk acceptance and risk matrix

A risk acceptance criterion (RAC) is the threshold or boundary beyond which risk mitigation is always required. The RAC can be expressed as e.g.,

- Risk matrix: A set of combinations of probabilities or frequencies and severity marked in a risk matrix
- Maximum tolerated frequency: The maximum frequency at which a major accident can occur at a facility caused by a specific hazardous event, like over-pressurization or fire. Such criteria can be incorporated into the risk matrix.
- Fatal accident rate (FAR): The expected number of fatalities per 100 million hours of exposure.
- IRPA: Individual risk per annum

We will use the first two mentioned, as they are most commonly used in relation to hazard and risk analysis for functional safety purposes. Applicable to all RACs is the difficulty of setting these thresholds in the first place, as doing so indirectly implies that some deaths or harm are acceptable, albeit seldom. The offshore oil and gas industry often uses the "1E-4 per year criterion" for loss of main safety functions, such as main support structures, control room, escape ways, and active fire/blast barriers, meaning that such loss is not tolerated more than once every 10,000 years. The individual hazardous events that could lead to such losses, for example, over-pressurization followed by a gas cloud ignited at a facility, may face the same or often stricter requirements, typically one decade lower (1E-5 per year).

Related to RAC is the "As low as reasonably practicable" (ALARP) principle, which widens from RAC as a point value to risk regions. It was first introduced in UK and (at a later stage) formally incorporated in the Health and Safety at Work etc Act 1974, and has been applied to nuclear as well process and offshore industry: The following principles are characteristics for ALARP:

- It suggests three distinct regions of risk: Unacceptable, tolerable ("the ALARP region"), and broadly acceptable.
    - Risk is always unacceptable in the unacceptable region and must therefore be reduced so that it escapes this region. Risk is always acceptable in the broadly acceptable region, and no risk reduction is required or expected.
    - Risk is always acceptable if in the broadly acceptable region: The threshold is often set well below the risk we face just by living an average life; alternatively, it may be set slightly higher for workplaces where third parties are not exposed, and workers are equipped and trained for handling accidental events.
    - The ALARP region is between the unacceptable and broadly acceptable regions, and risk is acceptable under the conditions in this region. The conditions involve cost-benefit analysis: it applies a gross proportionality principle, meaning that the cutoff for not implementing additional measures is when the cost is grossly disproportionate to the safety benefits. It is not always easy to decide what is grossly disproportionate; however, a rule of thumb is that you are expected to invest more in reducing risk when close to the unacceptable region than if you are close to the broadly acceptable region.

When RAC is applied to a risk matrix, it identifies, often by color-coding of table cells, the three regions as combinations of likelihood (probability or frequency) with severity of consequences, as shown in Fig. 9.

Without acceptance criteria

Likelihood	Consequence				
	Negligible	Minor	Moderate	Significant	Severe
Very unlikely			Hazardous event 1		
Unlikely					
Possible					Hazardous event 3
Likely				Hazardous event 2	
Very likely					

With acceptance criteria

Likelihood	Consequence				
	Negligible	Minor	Moderate	Significant	Severe
Very unlikely			Hazardous event 1		
Unlikely					
Possible					Hazardous event 3
Likely				Hazardous event 2	
Very likely					

Unacceptable risk | Conditional acceptable (ALARP) | Generally accepted risk

Fig. 9. Risk matrix with and without risk acceptance criteria

Why is it important to add these ALARP regions to the risk table? Assume that we have identified three hazardous events, numbered 1, 2, and 3. By inserting these three events into a matrix without the risk acceptance criteria, as done for the upper matrix in Fig. 9, it is difficult to judge if the risk is too high or not. By adding risk acceptance criteria zones, we can easily identify which events are unacceptable, conditional, and broadly acceptable.

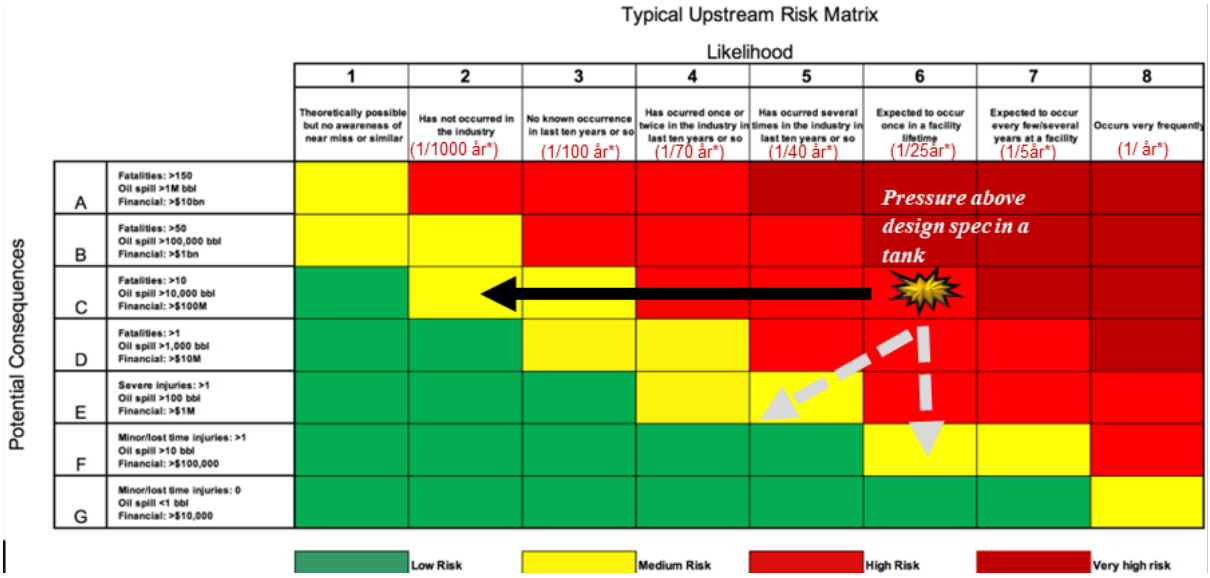


Fig. 10. Illustrating risk reduction in the risk

Risk matrices can be organized and scaled in several ways and sometimes add more regions than the three required by ALARP. For example, in Fig. 10, we can read out that:

1. The consequence categories can be further divided into more specific characterizations of losses related to fatalities, spills, and financial damage. If the evaluation yields different criticalities, the most severe is selected.
2. Likelihood categories can be complemented by threshold values for probabilities or frequencies, as shown with text in red (numbers only for illustrative purposes).
3. Additional regions can be added. This table contains two shades of red. As this distinction is not explained, we consider the entire red zone unacceptable, since it is not known what conditions were originally imposed on these zones.

A risk matrix is well-suited for illustrating what options we have for risk reduction, also illustrated in Fig. 10:

- Reduce the frequency (moving left horizontally)
- Reduce the severity (moving down vertically)
- Doing both (moving diagonally down towards the left)

Some red numbers have been added to the likelihood categories for use in a later calculation example; however, these numbers do not refer to any specific practice.

9.5.6 Risk reduction and risk reduction factor (RRF)

The term **risk reduction** refers to a reduction in risk achieved by lowering the likelihood (probability or frequency) or the severity of the consequence, or both.

Necessary or required risk reduction is the amount required to keep the risk below the tolerable level, defined by the risk acceptance criterion (RAC). Risk reduction is achieved by applying **risk-reducing measures,** for example, an SIS in combination with other systems, and relying on these systems being independent of each other so that a fault in one does not impact the others.

We have already introduced risk reduction factor (RRF) in relation to PFD. However, RRF can also be used more broadly, as the relationship between any initial risk and what is tolerable:

$$RRF = \frac{Risk_{Initial}}{Risk_{Tolerable}}$$

Fig. 11 illustrates the meaning of this formula.

- The risk of the event “Pressure above design spec in a tank” is clearly inside the unacceptable region
- The options for reducing risk into the ALARP region are illustrated
- If we assume that we introduce measures that reduce the likelihood from what it was initially (1/5 years) to 1/10000 years) the total need for risk reduction (expressed by RRF) is 2000:

$$RRF = \frac{R_{Initial}}{R_{Tolerable}} = \frac{F_{Initial}}{F_{Tolerable}} = \frac{1/5}{1/10000} = 2000$$

- This risk reduction could be allocated to a single SIF, meaning that it must have a PFD less than 5E-4 (or SIL 3), or one may introduce a SIF with a PFD less or equal to 1E-2 (SIL 2) in combination with another type of safety system with a failure probability (not necessarily calculated with PFD formulas) of less than or equal to 5E-2. This calculation does not account for additional margins to address uncertainties or a lack of knowledge.

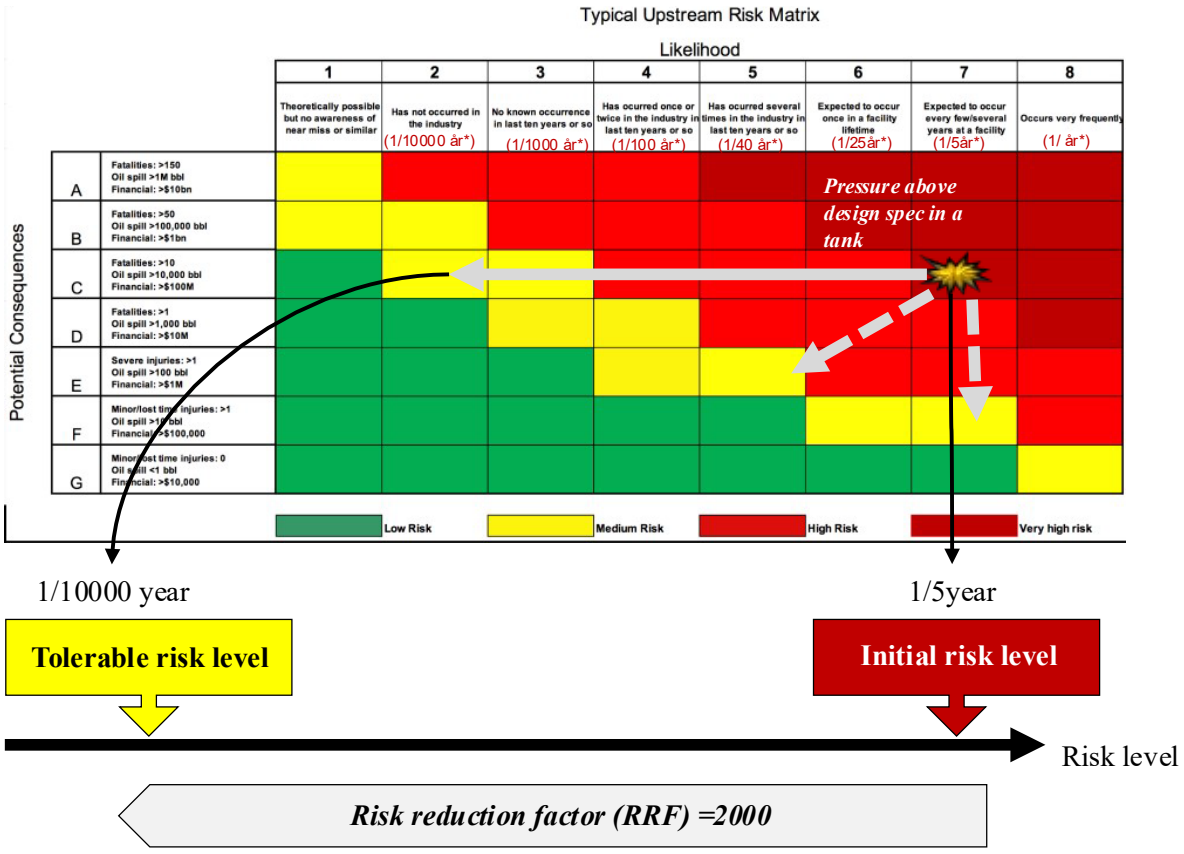


Fig. 11. Calculating the risk reduction factor

9.5.7 SIL allocation

SIL allocation involves assigning (or allocating) a proportion of the risk reduction, either as a SIL requirement or as a PFD or PFH value, to specific SIFs. The principle is explained with support of Fig. 12.

- A tank is equipped with a pressure control system. We assume that the hazards and risk assessment identified that a closure of the outlet control valve can result in a pressure build-up and that this occurs once per year. To protect the tank against overpressure, the hazards and risk analysis proposed SIF (SIF 1) in combination with a mechanical pressure relief/safety valve (PSV), referred to as safety function (SF) 2. Note that SF 2 is not SIF, as it involves no E/E/PE technologies.
- Assume that the total RRF requirement for over-pressuring the tank is 1000. A first allocation of this RRF to SIF1 and SF2 is shown in Fig. 13. Here, we have assumed that SIF 1 contributes an RRF of 100 times and SF2 an RRF of 10 times, yielding a total RRF of 1000 times. By applying the SIL tables, we can translate PFD=1/100 for SIF 1 (1E-2) into a SIL 2 requirement, choosing the most conservative option when the value is on the borderline between two SIL levels. The SIL allocation process ends by assigning a SIL 2 requirement to SIF1.
- Note that it is not relevant to assign a SIL 1 requirement to SF2, as standards on functional safety do not address the design of purely mechanical equipment.
- If the required RRF were 10,000, we would have to add more risk-reducing measures, like SIF2, or improve the reliability of, e.g., SIF1.

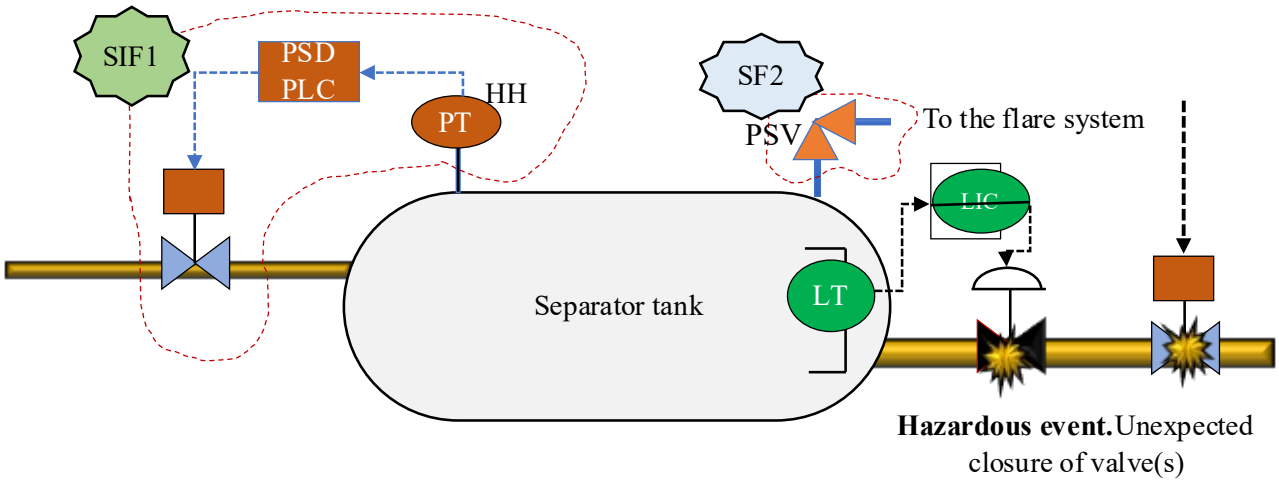


Fig. 12. Case study of a process control system and two safety functions SIF1 and SF2

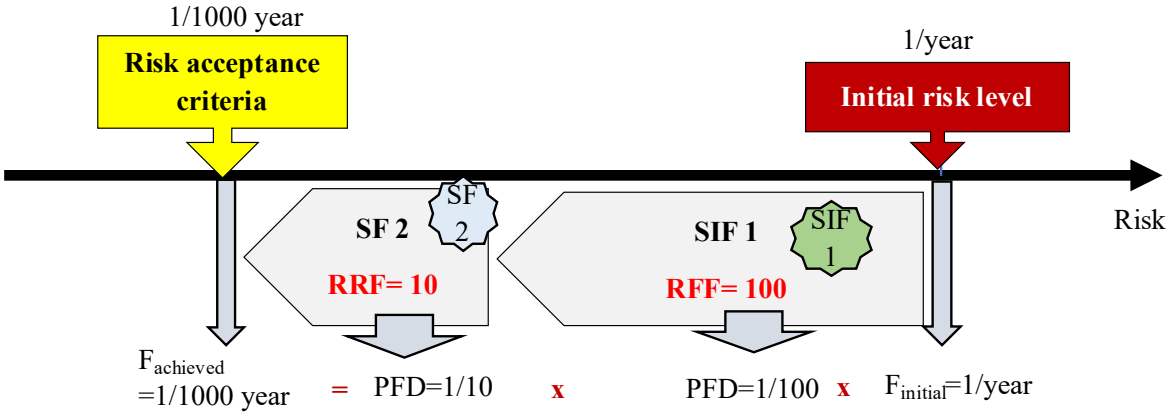


Fig. 13. Allocation of risk reduction

9.5.8 SIL allocation with LOPA

The risk reduction that was calculated in **Fig. 13** only considered one hazardous event with one specific consequence. However, a hazards and risk analysis, like HAZOP, identifies several hazardous events that may lead to the same consequence.

The layers of protection analysis (LOPA) is a method for calculating risk-reduction requirements (or expectancies) for specific SIFs, accounting for the effects of preventive barriers. LOPA was developed by the US Center for Chemical Process Safety and has since gained widespread popularity. The petroleum sector and, to some extent, land-based process industries in Norway have applied LOPA over the last 10-15 years.

- **LOPA** is a structured method to assess and calculate the effects of already identified SIFs against the need for risk reduction, and in case of an identified gap, to calculate the reliability requirement for a new SIF to be added.

LOPA is a semi-quantitative, table-based method that depends on expertise in facility design and operation. A key part of the process is the LOPA workshop, where specialists collaborate to determine the information to include in the table.

As preparation for the LOPA workshop, information from hazards and risk analysis, such as HAZOP (presented later in this chapter), is transferred to the LOPA table. The relevant information includes:

- Consequences with high severity
- The associated causes and hazardous events
- Their frequency of occurrence
- The already identified SIFs and other layers of protection

Supplementary information to identify can be the assumed reliability performance of the already identified SIFs and protection layers, considering regulatory requirements, standards, and operating experience.

The explanation of the LOPA method is made based on Fig. 12. We assume that the preparation and the workshop have provided the information in the LOPA table in Fig. 14.

			Independent protection layers (IPL)						New IPL	
Impact event	**Initiating event (IE)**	**IE frequency**	**PCS**	**SIF1**	**SF2**	**Modifying condition**	**Frequency impact event**	**Acceptance criteria**	**Additional SIF**	**Updated frequency impact event**
Ex: Over-pressuring of a separator leading to explosion	Spurious closure of outlet control valve	1/year	1 (= cannot be credited)	0.01	0.1	1	1/1000 years	1/10 000 years	0.05	1/16667 years
	Spurious closure of outlet ESD valve	1/10 years	1 (= cannot be credited)	0.01	0.1	1	1/10 000 years			
	Fire in process area	1/100 years	1 (= cannot be credited)	1 (= cannot be credited)	0.1	0.1	1/10 000 years			
						SUM:	1/833 years			

Fig. 14. LOPA table (example)

Prefilled information:

1. **Impact event:** This is the hazardous event that must be prevented. In our example, it is "tank overpressure, with risk of explosion". A LOPA table will include all hazardous events, but each hazardous event is analyzed separately.
2. **Initiating events:** Identifies triggers or causes for why hazardous events occur. For example, a malfunctioning control valve can be an initiating event. There are usually several initiating events for each hazardous event.
3. **Frequency of initiating event:** An estimate of how often the initiating event occurs. Many companies provide standardized values, based on their own expert judgment and operational experience. Data handbooks that provide device failure rates may also be used.

Information added in the LOPA workshop:

4. Ability of the process control system (PCS) to contribute to the reduction of risks. If the initiating event is not originating in the PCS and the PCS action is relevant, a maximum value of 0.1 can be added; otherwise, 1 (meaning that the PCS system is not being credited). The value of 0.1 is chosen as an upper value, as it is not possible to argue a PCS system more reliable than what is minimally expected for a SIF (the highest value of PFD for SIL 1).
5. PFD values for SIFs are already available or will be installed. Values are inserted only if SIF is relevant initiating event in question. As for PCS, it must always be evaluated if the specific SIFs are relevant, and if not, a “1” is added.
6. Failure probabilities of other on-demand functions, like PSVs, are to be added.

7. Modifying conditions can be justified conditions for additional risk reduction (by assigning a value <1). For example, the fire in the process area being discussed is less likely to escalate due to the availability of rescue teams.

8. Calculated frequency of impact event: The impact event frequency is calculated for each row by multiplying the IE frequency by all probabilities filled into the subsequent rows. The sum of all calculated values give the total frequency of the impact event that is being compared with the acceptance criteria 1/10 000 years.

9. In our example, the initial risk reduction, before considering additional SIFs, was below what is required. This is solved here by adding a new SIF, but the alternative could also be to improve the reliability of the other, already existing, or planned safety systems. It is not always possible to introduce additional functions, or the new functions can give unwanted complexity.

Here, we assume that a new SIF, SIF 3, is added as shown in Fig. 15. It will automatically open the flare valves to depressurize the tank contents into the flare system. As such, SIF 3 will have a similar function to SF2 but by another (diverse) technology (mechanical versus E/E/PE based).

From the LOPA table, we observe that the RRF can be reduced from 1/833 years to 1/16 667 years by introducing a new SIF 3 with PFD = 0.05. The PFD of the new SIF 3 falls within the SIL 1 range and will be designed in accordance with SIL 1 requirements.

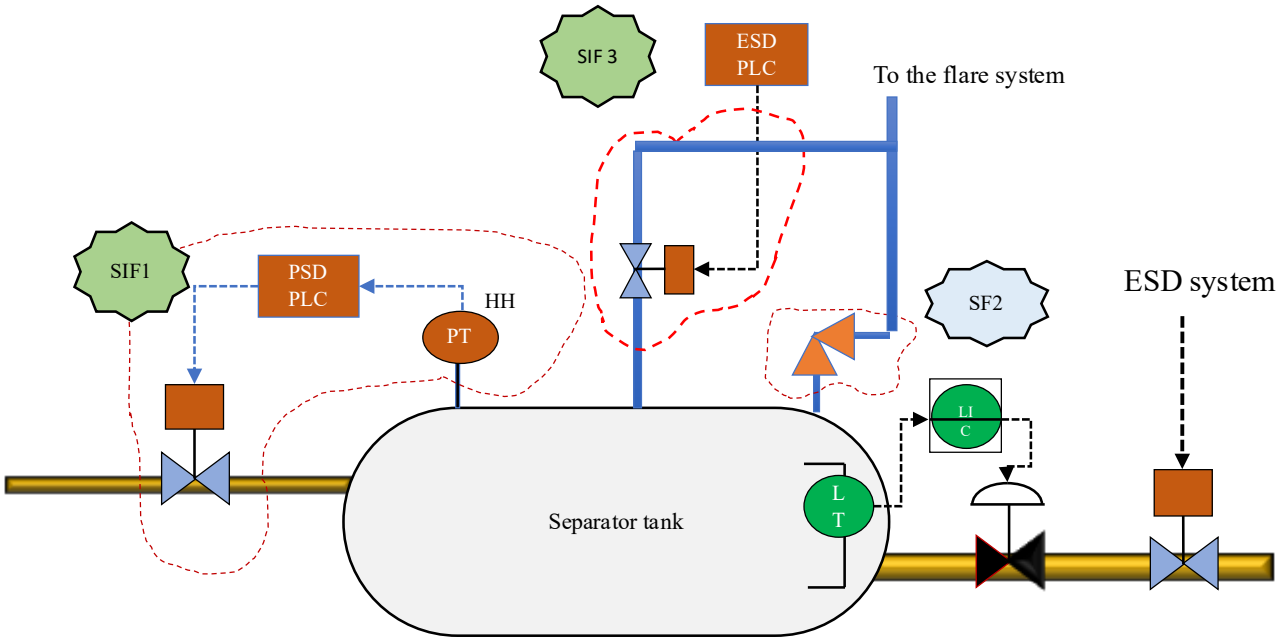


Fig. 15. Introducing a new SIF 3

9.5.9 Relationship LOPA and HAZOP

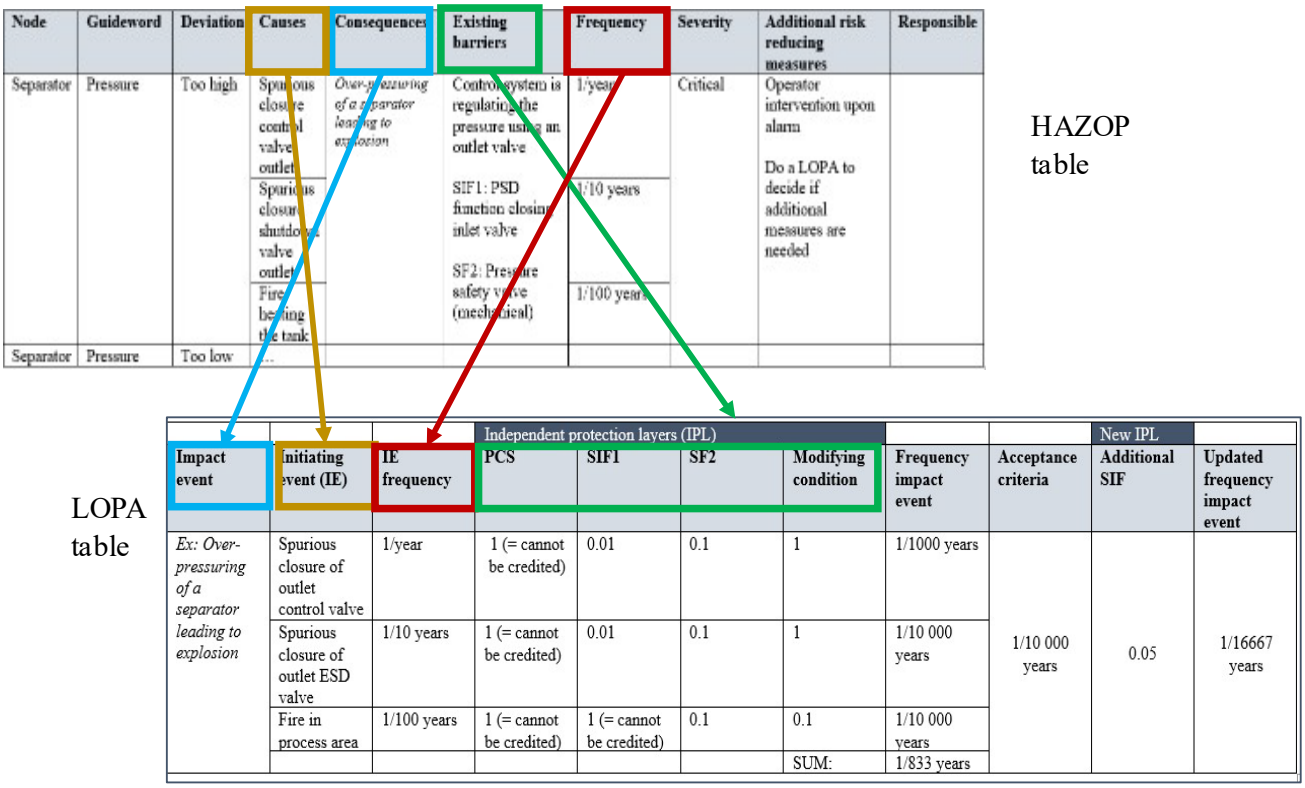
A LOPA analysis requires that a HAZOP or similar hazard and risk analysis has been carried out, as LOPA focuses on risk allocation rather than hazard and risk identification. The type of information transferred from a HAZOP into a LOPA table is illustrated in Fig. 16.

In this example, it has been assumed that a HAZOP analysis was carried out for the system in Fig. 12. From the illustration, we note that:

- The impact events are identified from the HAZOP column consequences. Of course, only severe consequences are entered into the LOPA table; less critical ones are omitted.

- The initiating events (IE) are identified from the causes. If the same consequence is listed several times in the HAZOP table, it is necessary to transfer all the corresponding causes into the LOPA table.
- Frequencies of causes are transferred to the IE frequency column. If HAZOP uses a scale (e.g., 1-5), additional work may be required to identify more precise frequencies for the LOPA analysis.
- Existing barriers that were noted in the HAZOP table are given one column each in the LOPA table.

The other columns of the LOPA table are filled in during the LOPA workshop. As part of the preparation, the facilitator will identify relevant data sets on probabilities and frequencies for review with the experts.



HAZOP table

Node	Guideword	Deviation	Causes	Consequences	Existing barriers	Frequency	Severity	Additional risk reducing measures	Responsible
Separator	Pressure	Too high	Spurious closure control valve outlet	*Over-pressuring of a separator leading to explosion*	Control system is regulating the pressure using an outlet valve SIF1: PSD function closing inlet valve SF2: Pressure safety valve (mechanical)	1/year	Critical	Operator intervention upon alarm Do a LOPA to decide if additional measures are needed	
			Spurious closure shutdown valve outlet			1/10 years			
			Fire heating the tank			1/100 years			
Separator	Pressure	Too low	...						

LOPA table

			Independent protection layers (IPL)						New IPL	
Impact event	**Initiating event (IE)**	**IE frequency**	**PCS**	**SIF1**	**SF2**	**Modifying condition**	**Frequency impact event**	**Acceptance criteria**	**Additional SIF**	**Updated frequency impact event**
Ex: Over-pressuring of a separator leading to explosion	Spurious closure of outlet control valve	1/year	1 (= cannot be credited)	0.01	0.1	1	1/1000 years	1/10 000 years	0.05	1/16667 years
	Spurious closure of outlet ESD valve	1/10 years	1 (= cannot be credited)	0.01	0.1	1	1/10 000 years			
	Fire in process area	1/100 years	1 (= cannot be credited)	1 (= cannot be credited)	0.1	0.1	1/10 000 years			
						SUM:	1/833 years			

Fig. 16. Transfer of information from HAZOP into a LOPA table

9.5.10 SIL allocation with event tree analysis (ETA)

Event tree analysis (ETA) is a graphical representation of how a hazardous event can evolve into a set of consequences, accounting for the impact of identified barriers or protection layers.

Because the hazardous event is the starting point, the method is well-suited to developing requirements to mitigate barriers.

An event tree is drawn up by following a few set rules, which are illustrated in Fig. 17:

1. The left side starts with the hazardous event
2. The barriers that are relevant for mitigating the consequences of the hazardous event are listed.
3. A decision tree is drawn from left to right, identifying the role of each barrier. The barrier's naming must ensure that the branches' directions are consistent. For example, the way the barriers are named indicates that all Yes-branches worsen the situation, whereas the No-branches reduce it.

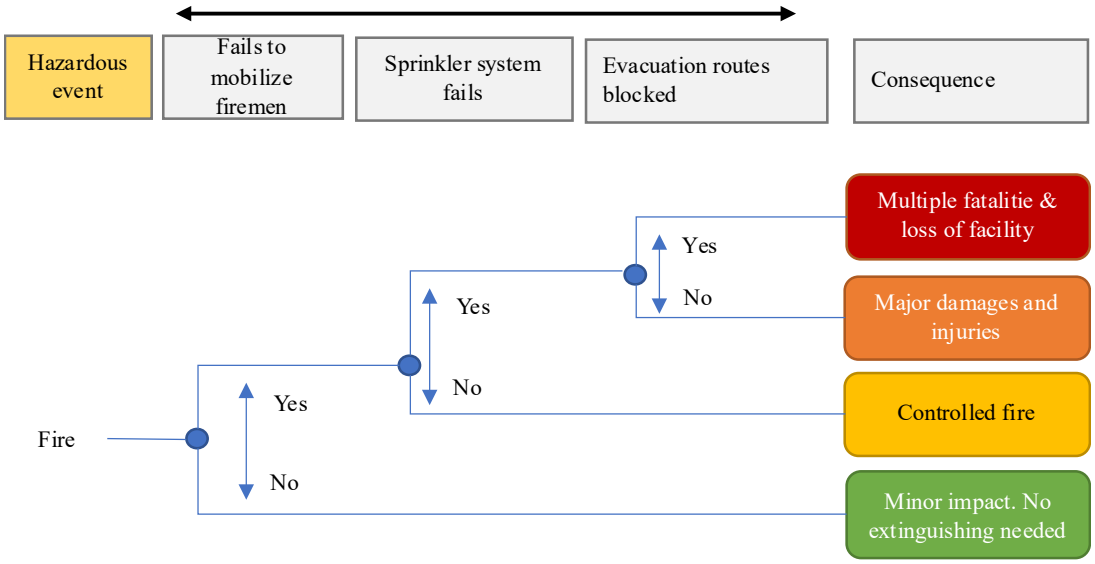


Fig. 17. Event tree analysis

The ETA can be a purely qualitative analysis focusing on the possible outcomes given the status of barriers. However, by adding probabilistic information, such as the frequency of hazardous events and the probabilities of success or failure for each barrier, it is also possible to calculate the frequencies of different outcomes. The event tree from Fig. 17 with such information added is shown in Fig. 18.

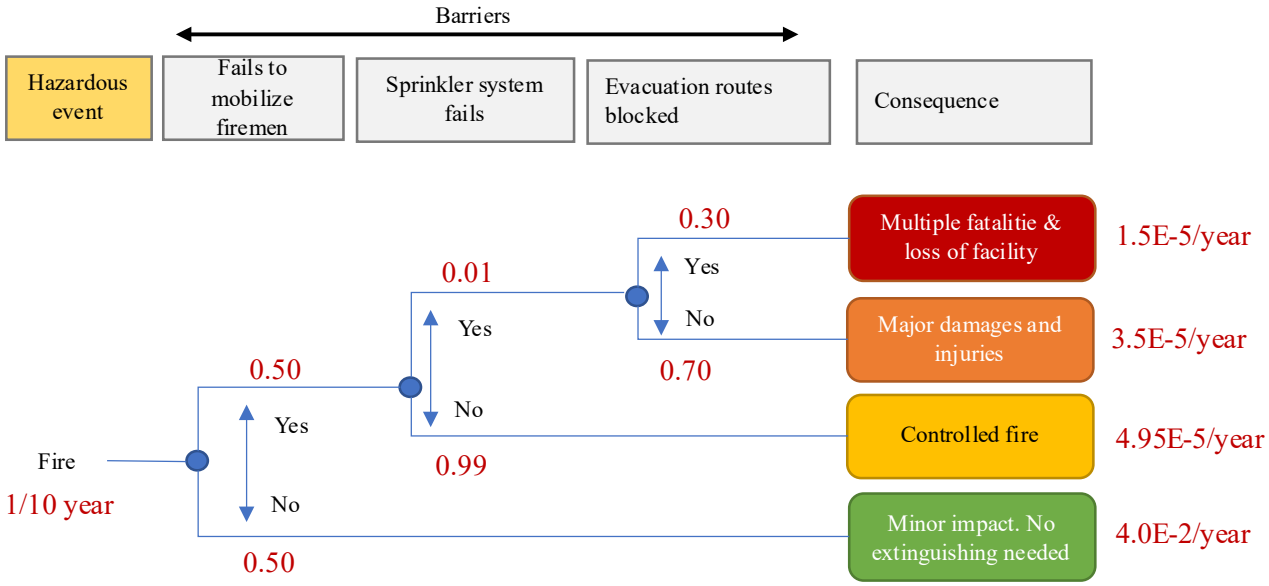


Fig. 18. Event tree analysis with probabilistic data included

Assuming the barriers are fully independent allows us to multiply the frequency of hazardous events by the probabilities along the different paths to the consequence. The resulting frequencies of the various consequence categories are listed on the right side of the figure.

The probabilities assigned to the branches are conditional, meaning they depend on the state of the system up to the point where the branch is located. In Fig. 19, the event tree has been expanded to illustrate the impact of conditional probabilities. A fire detection system has been added to notify firefighters and enable earlier intervention. If the fire detection system fails, we assume a 50:50 chance of extinguishing the fire. However, if the fire detection system works, we assume a 90:10 chance that firefighters will extinguish the fire. The calculation of results is listed on the right-hand side of Fig. 19 is shown in Tab. 2.

Now, we want to demonstrate how ETA can be used for SIL allocation. Two of the barriers, marked with blue boxes, are SIFs. The probabilities of failure (following the "yes" branch) could be used as initially selected PFD requirements. For example, both systems are assumed to have a PFD of 0.01 or less, which corresponds to a SIL 2 requirement. By inserting the branch values, including our initial assumption for the PFD of the two SIFs, we obtain the results shown in Tab. 2.

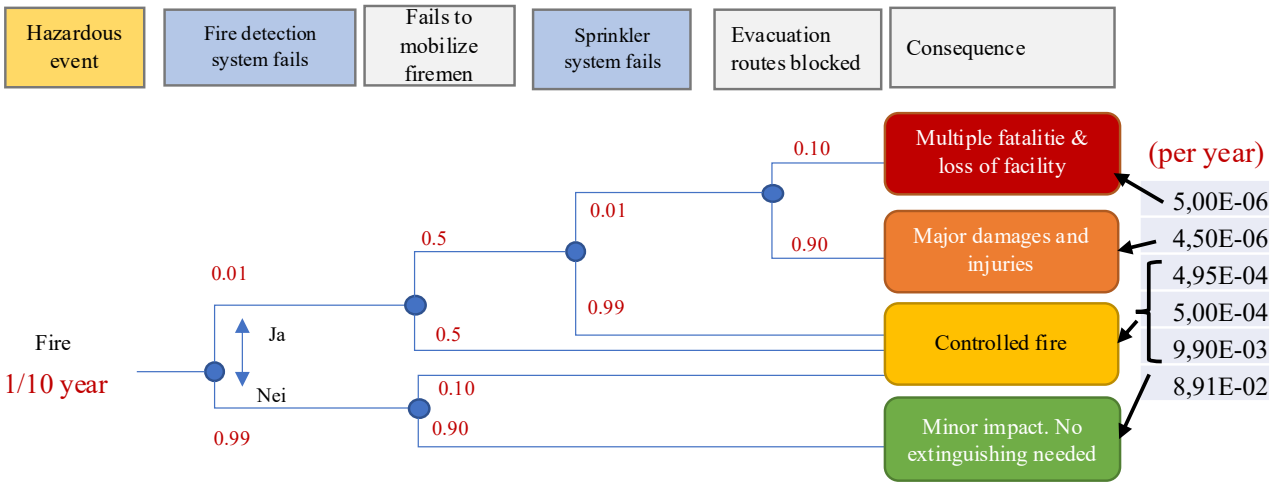


Fig. 19. Modified event tree analysis

If we assume that the worst-case consequence (red) is 1E-5/year, we observe from Tab. 2 that the chosen PFD values of SIF 1 and SIF 2 are sufficiently low (with some margin). These values could, of course, be optimized. If orange and yellow consequences are accepted, the criteria are adjusted by 1 decade each (i.e., 1E-4/year and 1E-3 years), and we observe that these requirements are also met. If the acceptance criteria are not met, we could modify the PFD values for one or both SIFs and, as a result, assign new SIL requirements. If it is not possible to build the SIFs to meet these requirements, we would need to modify the other parameters by redesigning or adding a third SIF or another safety function.

Tab. 2. Calculations for the event tree

Fire frequency	Fire detection fails	Fails to mobilize firemen	Sprinkler system fails	Evacuation routes blocked	Frequency of consequences	Consequence category
0,1	0,1	0,5	0,01	0,1	5,00E-06	
0,1	0,01	0,5	0,01	0,9	4,50E-06	
0,1	0,01	0,5	0,99	1	4,95E-04	
0,1	0,01	0,5	1	1	5,00E-04	
0,1	0,99	0,1	1	1	9,90E-03	
0,1	0,99	0,9	1	1	8,91E-02	

From the results, we observe that category four occurs (on average) 1 time per 1,000,000 years, which meets the acceptance criterion of 10% of the 10E-4 per year criterion. As such, a SIL 2 requirement becomes sufficient for both SIFs.

9.5.11 Relationship between LOPA and ETA

The bowtie model was introduced in Chapter 6. LOPA and ETA are applicable methods for being applied with a bowtie, as shown in Fig. 20.

- For example, LOPA, which primarily focuses on identifying requirements for preventive barriers, can be used to identify information about the safety barriers on the left side of the bowtie diagram.

- In contrast, the ETA, which focuses on mitigative barriers, models the information needed on the right side.
- Another method suitable for modeling the left side of the bowtie model is fault tree analysis (FTA).

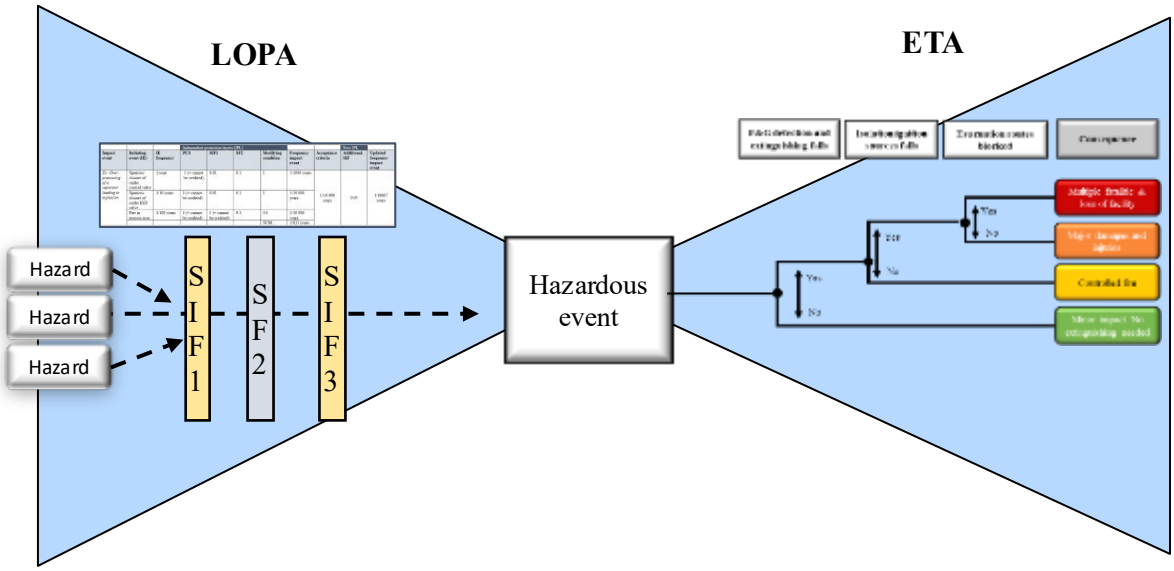


Fig. 20. Bowtie with LOPA and ETA

9.6 Safety requirements specifications (SRS) (phase 4-5)

The safety requirements specification (SRS) is one of the key documents that integrates the results of the SIL allocation process into a more detailed design specification for the SIFs. Most functional safety standards, including IEC 61508, require that this document be established after the SIL allocation process is complete and before detailed design of the SIS begins.

9.6.1 Safety requirements specification (SRS)

The safety requirements specification (SRS) collects all information relevant to the design of a SIS and its related SIFs, often in a single document. With more than one SIS, for example, PSD, and F&G systems, the SRSs are usually in separate documents. Although the document is established in the design phase, it must be kept up to date throughout the SIS life cycle.

The objective of the SRS is to provide a single source to reference SIS and SIF requirements. The SRS content is often split into two main parts: first, the general requirements that apply to the SIS as a whole, and second, the requirements that are specific to each SIF. Overall, the SRS must cover all requirements listed in IEC 61508 or IEC 61511 (in total 27), which have been reproduced in Tab. 3.

Tab. 3. Example of the required content of an SRS

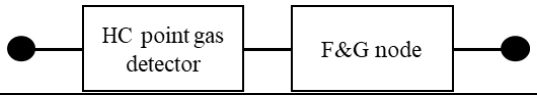
ID	Reference, IEC 61511, cl. 10.3
a)	Description of all the necessary instrumented functions to achieve the required functional safety
b)	A list of the plant input and output devices related to each SIF which is clearly identified by the plant means of equipment identification (e.g., field tag list)
c)	Requirements to identify and take account of common cause failures
d)	Definition of the safe state of the process for each identified safety instrumented function
e)	Definition of any individually safe process states which, when occurring concurrently, create a separate hazard
f)	Assumed sources of demand and demand rate of the safety instrumented function
g)	Requirement of proof test intervals

ID	Reference, IEC 61511, cl. 10.3
h)	Requirements related to proof test implementation
i)	Response time requirement for the SIS to bring the process to a safe state
j)	Safety integrity level and mode of operation (demand/continuous) for each SIF
k)	Description of SIS process measurements and their trip points
l)	Description of SIS process output actions and the criteria for successful operation, e.g. leakage rate for valves.
m)	Functional relationship between process inputs and outputs, including logic, mathematical functions
n)	Requirements for manual shutdowns
o)	Requirement related to energize or de-energize to trip
p)	Requirements for resetting each SIF after a shutdown (e.g., requirements for manual, semi-automatic, or automatic final element reset after trips).
q)	Maximum allowable spurious trip rate for each SIF; Failure modes and desired response of the SIS
r)	Any specific requirements related to the procedure for starting up and restarting the SIS
s)	All interfaces between the SIS and any other system
t)	Description of the modes of operation of the plant and requirements relating to SIF operation within each mode
u)	The application program safety requirements (Ref 61511, section 12.2.2)
v)	Requirements for overrides/ inhibits/ bypasses including how they will be cleared
w)	Specification of any action necessary to achieve a safe state in the event of faults being detected by the SIS. Any such action shall be determined taking account of all relevant human factors
x)	The mean repair time, which is feasible for the SIS, considering the travel time, location, spares holding, service contracts, environmental constraints.
y)	The mean down time due to routine maintenance
z)	Dangerous combinations of output states of the SIS shall be addressed
aa)	The extremes of all environmental conditions that are likely to be encountered by the SIS shall be identified. This may require consideration of the following: temperature, humidity, contaminants, grounding, electromagnetic interference, etc. (see IEC 61511, cl. 10.3)
bb)	Identification to normal and abnormal modes for both the plant as whole and individual plant operational procedures (for example, equipment maintenance, sensor calibration and/or repair). Additional safety instrumented functions may be required to support these modes of operation.
cc)	Definition of the requirement for any safety instrumented function necessary to survive a major accident event, for example, time required for a valve to remain operational in the event of a fire.

The specific SIF requirements are often presented in a SIF table. It can be for a specific SIF or a type of SIFs (SIF typical). An example of a SIF typical for hydrocarbon (HC) point gas detection is shown in Tab. 4. This example is a global SIF type, meaning that a detection triggers multiple actions across the facility. For convenience, global SIFs are split into two: the detection part (shown in Tab. 4) and actuation part with F&G node and the devices being actuated, for example, release of extinguishing medium, start of fire pumps, initiate emergency shutdown, and so on.

Tab. 4. Extract of a SIF table within an SRS

Field	Content
SIF (typical)	SIF-SFC-FG-C-03a
Title	Hydrocarbon (HC) point gas detection
Signal Code – Cause	1–9, 78, 82 (Specific cause number/ID used in Company C&E-matrix)
SIL requirement	SIL 2 (PFD < 10^{-2}), according to Guideline 070, Appendix A.
Function description	The safety function starts when the detector is exposed to gas and ends when the F&G node converts the measurement into an alarm or trip command.
Included components	Input elements: HC point gas detectors Logic elements: F&G node

	Final elements: N/A
EUC	Areas listed in the Fire Area report (ref).
Tag numbers	Specific tag numbers covered by this safety function are listed in the SIF Identification Report (ref)
Reliability block diagram	
Safe state	Safe state is when the alarm signal is generated, processed, and action/alarm signals are transmitted from the F&G node.
Failure Modes	Dangerous Undetected (examples, not an exhaustive list): detector fails to transmit information; no output from detector; node fails to generate action signal.
Operational mode	This safety function will operate in the low-demand mode.
Demand rate / Sources	Demand rate: < 1/year Sources of demand: Process leakages, other gas releases or dispersion.
Alarm limit	• Low alarm limit for point detectors is a maximum 20% LEL. • High alarm limit for point detectors is a maximum 30% LEL. • Low alarm limit for point gas detectors is a maximum 20% LEL in air intakes. • High alarm limit for point gas detectors is a maximum 30% LEL in air intakes. • Low alarm limit for point gas detectors is a maximum 10% LEL in turbines. • High alarm limit for point gas detectors is a maximum 15% LEL in turbines.
Response time	• Gas detector (Methane and Methanol): IR detector response time (T90) should be less than 5 seconds for general area applications. • Upon gas exposure, the time from when the detector alarm limit is exceeded until the alarm is presented/tagged on the operator station should be less than 2 seconds.

9.6.2 Software SRS

The Software Safety Requirements Specification (Software SRS) describes the required behaviour of the safety-related software and which must be documented as fulfilled during software design and implementation. It specifies what the software shall do, how it shall respond to faults and hazardous situations, and the constraints it must satisfy in order to meet the required safety integrity level. As such, it acts as the contract between the system requirements and the software design. An example of content to be addressed in a software SRS is shown in Tab. 5.

Tab. 5. Example of content in a software SRS (assisted by Copilot)

Section	Typical requirement content	Example
Safety functions	Definition of all software safety functions and the conditions under which they shall be executed.	The software shall trip the reactor on high pressure.
Functional behavior	Requirements specifying how the software shall process inputs, perform logic, and generate outputs.	The software shall use 2oo3 voting on redundant pressure transmitters.
Operating modes	Behavior the software shall exhibit during normal operation, start-up, shutdown, maintenance, and degraded operation.	During maintenance mode, shutdown outputs shall remain active.
Safe state	Definition of the safe state and requirements for how the software shall achieve or maintain it.	Loss of controller power shall de-energize the shutdown valves.
Interfaces	Requirements for interfaces to sensors, actuators, operators, communication systems, and other software.	The software shall receive valve status from the safety network every second.

Response times	Maximum permissible times within which the software shall detect, process, and respond to events.	A high-pressure trip shall be executed within 500 ms.
Diagnostic functions	Requirements for fault detection, self-tests, diagnostics, and fault reporting.	The software shall detect input channel failures and generate an alarm.
Failure response	Actions the software shall perform following detected faults, communication failures, or invalid inputs.	An invalid pressure signal shall place the system in a predefined safe state.
Data and configuration	Requirements for data storage, validation, initialization, retention, and configuration management.	Configuration changes shall be password protected and logged.
Safety integrity requirements	Requirements derived from the allocated SIL, including integrity constraints and systematic capability measures.	The software shall satisfy the requirements allocated to SIL 2.
Security constraints	Requirements intended to prevent unauthorized changes that could affect safety functions.	Only authorized personnel shall modify safety parameters.
Verification requirements	Criteria that shall be satisfied during reviews, testing, and validation activities.	All safety functions shall pass factory acceptance testing.
Assumptions and constraints	Conditions, limitations, and assumptions on which the requirements are based.	The specification assumes valid measurements from certified transmitters.

9.7 Designing SIS according to SIL (phase 9-10)

The SIL requirement imposes restrictions on the SIF level, at the device level, and on equipment common to several SIFs, such as power supplies and operator screens. Fig. 21 gives an overview of these requirements, which are explained separately. We will address each of the three categories of requirements in the following sections.

A SIL requirement triggers, for example:

- Requirements relating to hardware safety integrity covering:
    - Architectural constraints on each SIF subsystem, as a minimum fault tolerance for each of these.
    - Demonstration, by reliability analysis, that the calculated PFD or PFH of the SIF, end-to-end, obtains a value within the SIL requirement
- Requirements relating to systematic (and software) safety integrity, covering:
    - Restrictions on the work methodology and quality assurance so that systematic failures, which are to a certain extent covered by PFD/PFH, are kept at a level where they have a negligible impact. Systematic failures can stem from specification errors, design errors, installation errors, and usage errors.
    - Software tools, methods, and development processes, including verification and validation.

It is important to note that the selection of devices must *first* consider the appropriate detection or measurement principle, given the operating and environmental conditions under which they are installed.

- A perfectly reliable device, not fit for the purpose, will not be safe. For example, there are several level measurement principles, but only one or two may reliably measure the true level.

- For level measurements in specific areas, the mounting solution is critical, as incorrect nozzle placement or sizing can hinder accurate measurements.
- Another example is the choice of actuator capacity sizing and fail-safe design for shutdown valves. Insufficient capacity, caused by constraints in the pneumatic or hydraulic utility system, spring sizing, or, if an electrical actuator is used, power availability under demand conditions, may prevent the valve from closing or opening as needed and within the given time constraints.

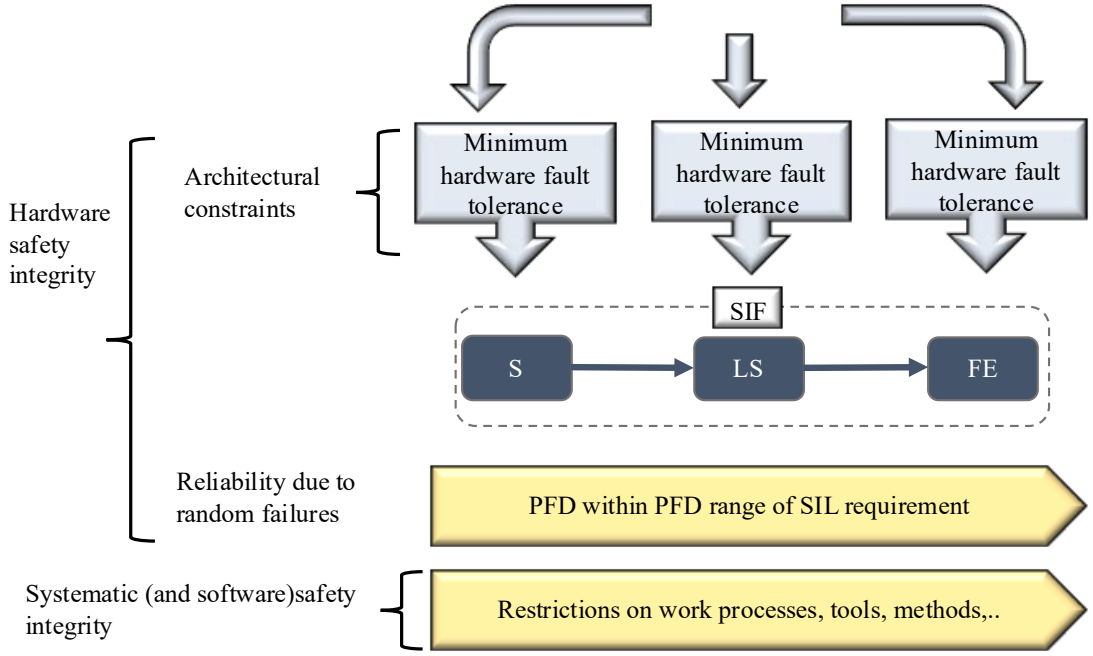


Fig. 21. Design implications of a SIL

9.7.1 Architectural constraints

Architectural constraints define the minimum hardware fault tolerance of SIF subsystems, based on the SIL requirement. Hardware fault tolerance is the number of dangerous faults a SIF subsystem can tolerate before failing. For example, a 2oo3-voted subsystem tolerates one fault, while a 1oo3-voted subsystem tolerates two faults. The minimum hardware fault tolerance (HFT) specifies the required level.

We may wonder why the architectural constraints have been introduced. It is already required to calculate the PFDs and verify that the results are within the SIL range. The most straightforward answer is that the industry recognizes the need for some "brake pads" when assessing how much to trust the PFD calculations. Using optimistic (i.e., low) failure rates can result in a PFD that is too low (compared to what will be experienced), leading to a too simplistic design that may require modifications later.

IEC 61508-2 (2010) identifies two routes or ways to determine architectural constraints:

- **Route 1H,** which is the approach focused on in this chapter. Here, the safe failure fraction (SFF) and the type A/B categories are inputs used to determine the minimum HFT.
- **Route 2H,** which is the alternative approach for min HFT without considering type A/B and SFF. This route applies only if the manufacturer can document an extensive operational history of failure types and statistics.

IEC 61511 has a simpler approach, which is easily understood when familiar with IEC 61508's route 1H.

9.7.1.1 Route 1H: Subsystems of identical devices

Redundancy is often introduced by using identical devices. The following procedure is described in IEC 61508-2 for such a system. The following steps are applied:

- **Step 1:** Determine whether the type of device(s) included in the subsystem is type A or type B
- **Step2:** Calculate safe failure fraction (SFF) or identify SFF from the product's SIL certificate
- **Step 3:** Determine minimum fault tolerance based on the tables provided in IEC 61508 and the results from steps 1 and 2.

The process is repeated for all three SIF subsystems.

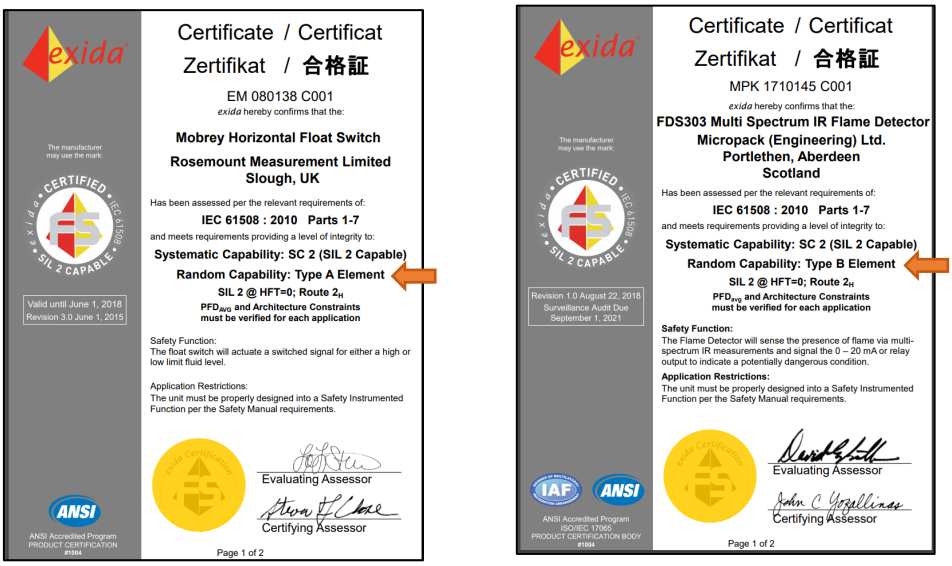


Fig. 22. Examples of SIL certificates

Step 1: Classify device(s) as type A versus type B: This is a relatively pragmatic, simple classification of SIS equipment into one of two predefined categories, A and B. IEC 61508 defines type A and B as follows:

Type A (simple product with well-proven and foreseeable behavior)
- Failure modes of all devices are well known
- The behavior of the device upon failure is known (and predictable)
- Sufficient failure data (systematic collection/reporting)

Type B (some lack thereof)
- One or more type A conditions are not met

Product certificates often specifiy the type of category, as shown in Fig. 22. There are also some rules of thumb for what is an A and what is a B category of equipment:

- Controllers (CPU + I/O card) are usually type B because of the complexity of a controller, including software, which makes it impossible with certainty to determine all failure modes and how the system behaves in all kinds of situations.
- Smart sensors will usually be type B, especially if they are connected in a bus network, where you become dependent on processors and logic to send and receive messages.
- Sensors that use 4-20mA and have been in extensive use may be classified as type A, as their behavior is more predictable and fail-safe.

- Switches, valves, and electromechanical devices with no programmed logic are generally type A due to their simple design and well-proven performance.

Step 2: Determine safe failure fraction (SFF): The SFF is a parameter that specifies the probability that, if the device fails, it will transition to a safe state. The SFF is determined separately for each device using the formula:

$$SFF = \frac{(\lambda_{DD} + \lambda_S)}{\lambda_{DU} + \lambda_{DD} + \lambda_S} \cdot 100\%$$

The formula suggests two alternative interpretations of SFF:

- SFF is the proportion of faults that are "safe", meaning safe (S) by definition or detected as dangerous (DD).
- SFF is the conditional probability that a fault is detected as safe or dangerous (DD), given that a failure has occurred.

Who important restrictions apply to which S and DD failures being credited:

- DD failures: Only those that are resolved within a short time compared to the time available to respond and resolve a hazardous event, alternatively, DD failures that result in a forced transition to the safe state
- Safe failures: Only the safe failures resulting in a transition to the safe state (as spurious trips" can be credited. It means that SU failures are included, while SD and failures classified as no part/no effect are excluded.

Step 3: Find minimum hardware fault tolerance: The minimum hardware fault tolerance can be derived from tables provided by IEC 61508-2 as shown in Tab. 6. There is one table for type A devices and another for type B.

Tab. 6. Minimum HFT table

SFF	Minimum HFT (type A)		
	0	1	2
<60%	SIL 1	SIL 2	SIL 3
60%-90%	SIL 2	SIL 3	SIL 4
90%-99%	SIL 3	SIL 4	SIL 4
>99%	SIL 3	SIL 4	SIL 4
SFF	Minimum HFT (type B)		
	0	1	2
<60%	Not allowed	SIL 1	SIL 2
60%-90%	SIL 1	SIL 2	SIL 3
90%-99%	SIL 2	SIL 3	SIL 4
>99%	SIL 3	SIL 4	SIL 4

9.7.1.2 Example 1 (Route 1H) Applied to one subsystem

Assume that a SIL 2 requirement has been specified for an SIF. The input element subsystem is for pressure measurement, and a pressure-transmitter type has been proposed. The question is whether the transmitter can be used as a single element or requires redundancy. We assume the pressure transmitter certificate shows SFF = 75% and that it is a type A device. The table indicates a minimum hardware fault tolerance of 0, meaning the transmitter can be used as a single (1oo1).

9.7.1.3 Example 2 (Route 1H): Min HFT for SIF 1

We now want to check if the SIF, as shown in Fig. 12 has sufficient fault tolerance given a SIL 2 requirement. In this example, we propose a single element for all three subsystems. We assume the following data have been provided for the category and SFF.

The analysis shows that a single valve and logic solver are allowed, but a minimum fault tolerance of 1 is required for the transmitters. A new pressure transmitter is therefore added as shown in Fig. 23.

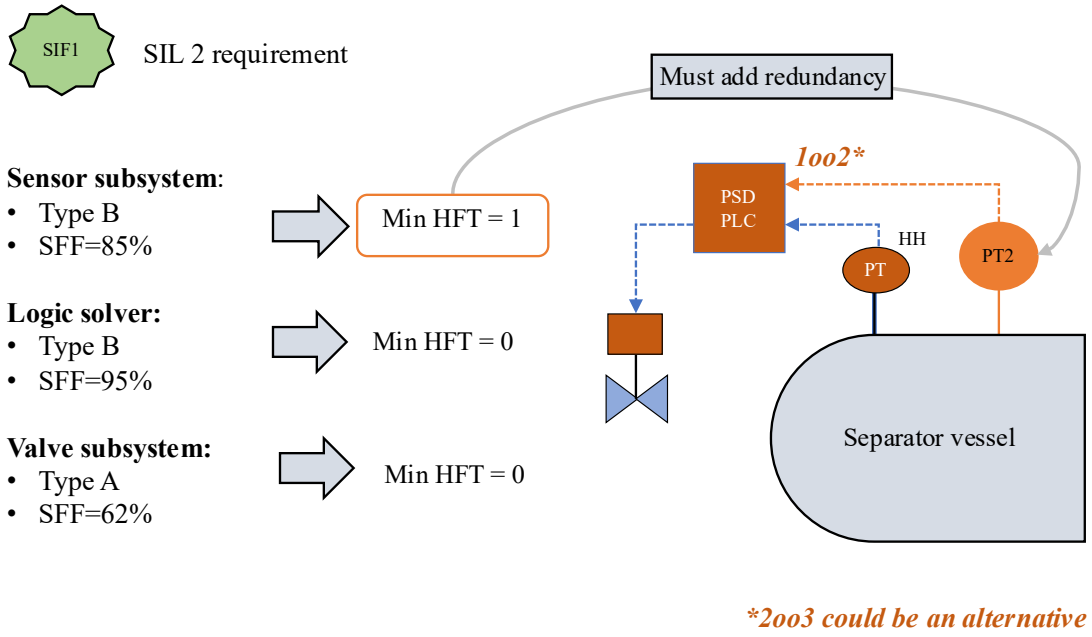


Fig. 23. Example on structural requirements for SIF 1

9.7.1.4 Subsystems consisting of non-identical devices

Some SIFs may have subsystems that rely on different sensors or actuator types. A subsystem may, for example, require a pressure transmitter and a level transmitter to trigger the valve to close. In this case, two practical problems arise:

- The devices may not have the same category, type A or type B
- The devices will have different SFF

The consequence is that Tab. 6 cannot be applied directly. Instead, we go step by step, following some merging rules. The principle is described in Fig. 24 where a subsystem comprises four devices distributed across three channels. The SFF of each device is shown. In this case, we want to determine the SIL level that such architecture can achieve. The procedure is as follows:

1. Determine the SIL level of each device individually as if it were 1oo1. For simplicity, we assume that all devices are of type B.

   Result:

   Device 1: With SFF = 75% & type B, the device achieves SIL 1 level
   Device 2: With SFF = 85% & type B, the device achieves SIL 1 level
   Device 3: With SFF = 92% & type B, the device achieves SIL 2 level
   Device 4: With SFF = 95% & type B, the device achieves SIL 2 level

2. Determine the SIL level per channel. If a channel comprises more than one device, the lowest achieved SIL level applies (the principle that no link is stronger than the weakest element).

Result :

Channel 1: Device 1 & 4: min (SIL 1, SIL 2)→ SIL 1
Channel 2: Device 2: → SIL 1
Channel 3: Device 3:→SIL 2

3. Determine the SIL level for the entire structure, that is, collectively for the parallel channels. Here, the following rules apply:

   SIL level obtained for the structure of parallel channels is equal to the highest SIL level of the channels *plus* the HFT of the structure.

   Result:
   This rule implies:
   Max SIL (channel 1, Channel 2, Channel 3) → SIL 2
   Three channels mean 1oo3, which again means that HFT = 2.
   The SIL level for the entire structure, therefore, becomes SIL 2 + 2 → SIL 4.

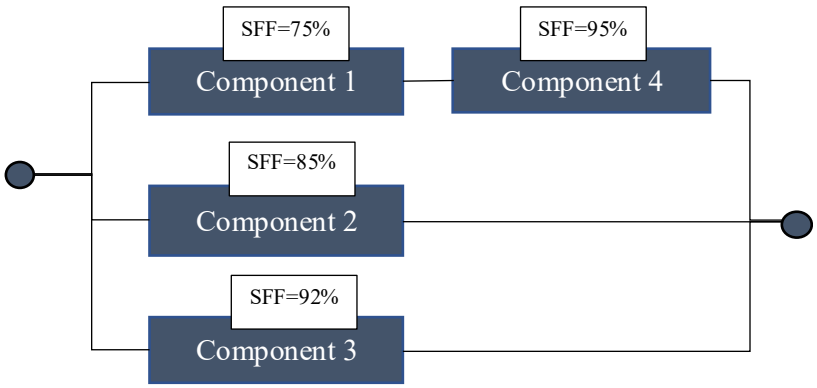


Fig. 24. "Merging" of subsystems for determining achieved SIL

This architecture achieves a SIL 4 level. If channel one or channel two is removed, SIL 3 would be achieved. If channel three is removed, a SIL 2 would be achieved.

9.7.1.5 Route 2H: Applying rules of thumb

Route 2H suggests the following rules of thumb for min HFT of subsystems, see Tab. 7.

Tab. 7. Min HFT for Route 2H

SIL requirement	Min HFT
SIL 4	2
SIL 3	1
SIL 2 (low demand)	0
SIL 2 (high demand)	1
SIL 1	0

If route 2H is selected, the calculation of the PFD of the SIF afterward *must* be based on:

- Failure rates calculated based on operational experience for similar devices in similar environments. There is no standard agreement on what constitutes sufficient operational experience, but, e.g., Exida, a recognized organization for SIL certification, suggests 30,000,000 hours across at least 10 different applications in its white paper “What does proven-in-use imply?” (Exida, 2020). If there are 1000

products of a specific kind on the market, it would take 3.4 years to collect data on them, and the manufacturer would face practical challenges in obtaining such data from end users with the required quality and completeness.

- Assured quality and completeness of data collection when collecting data from field experience, by using, e.g. ISO 14224 (2016) or IEC 60300-3-2 (2004). A manufacturer may need to rely on its customers to perform the actual data collection, which imposes requirements on the manufacturer.
- The PFD (or PFH) incorporates the uncertainty level by applying failure rates expressed with their uncertainty level (e.g., 90% confidence interval or probability distribution). Monte Carlo simulations are often used to draw parameters from a distribution. The PFD can be presented as a distribution or as a point value that satisfies a criterion Pr (PFD ≤ PFDmax) ≤ x, with x, e.g., 90%, determined from the cumulative distribution function.

The calculated PFD is therefore *not* based on mean values of a constant failure rate. Instead, the calculated PFD will increase with the uncertainty in the failure rates. A practical challenge with this approach is that software or hardware upgrades can render field-experience data invalid.

An independent body, such as Exida or TUV, is often used to verify whether route 2H can be selected.

9.7.1.6 Example 1 revisited: Application of Route 2H

Given the SIL 2 requirement for SIF 1, all subsystems must meet SIL 2 for route 2H. As SIF is operating in low-demand mode, each subsystem can be implemented without redundancy (e.g., with a 1oo1 voting). Some observations:

- While the application of Route 1H to SIF 1 in chapter 9.7.1.3 required redundant transmitters with min HFT=1; we do not need redundant transmitters with Route 2H.
- From the cost perspective, route 2H gives a simpler and therefore less costly solution.
- At the same time, it is necessary to document that failure rates used for the calculation of PFD are based on field experience and data collection following recognized international (IEC and ISO) standards.

The last bullet most likely yields a PFD value higher than that obtained using constant failure rates. Ultimately, one may need to add more redundancy to satisfy the SIL requirement, but this time with a basis in the need to reduce the PFD. However, when PFD is the decision parameter, an alternative approach to reduce it, if operationally acceptable, is to test more frequently with a shorter functional test interval.

9.7.2 Calculation of PFD

Once SIF has been updated with the required minimum HFT of each subsystem and the selected devices, PFD or PFH must be calculated using reliability analysis methods. Measures, including possible redesign, must be taken if the PFD (or PFH) does not meet the SIL requirement. The topic of PFD/PFH calculations was covered in Chapter 7 and is not repeated here.

9.7.3 Requirements for work processes and tools

IEC 61508 Part 1 provides general requirements for work processes across all life-cycle phases, while Part 2 focuses on hardware design processes and Part 3 on software development and related tools for implementation. For programmable controllers, it is also useful to consult IEC 61131-6 (2012). The overall objective of imposing restrictions and requirements on work processes is to ensure that the impact of systematic faults, which could be introduced at any stage of the safety lifecycle, remains negligible relative to the SIL requirement.

9.7.3.1 General requirements for work process (samples)

IEC 61511 contains general requirements like those in IEC 61508, but it is tailored to the process industry and to the use of pre-certified devices. Some examples of requirements from this standard are:

1. Requirement about making a “Management of functional safety plan”, where all activities related to the design and operational follow-up of an instrumented safety system are defined. This includes the analyses and tests to be carried out, their timing, and who is responsible.
2. Identify how to conduct independent reviews called functional safety assessments (FSAs). FSAs are typically performed shortly after the SIL allocation, when the first SRS version is available. In contrast, other FSAs can be carried out after the detailed design is completed and before start-up (after installation and commissioning). The standard also specifies the need to carry out FSAs at regular intervals during the operation phase.
3. Ensure coordination with cybersecurity analyses to uncover possible vulnerabilities in connection with the solution chosen for the SIS.
4. Impose necessary restrictions for the use of the equipment as described in the product’s user manual to avoid incorrect configuration of field equipment.
5. Ensure that the control system manufacturer has equipment, development tools, and quality assurance around its software development that meets the SIL level provided by SIF, with the highest SIL requirements
6. Enforce and continuously improve test and maintenance procedures
7. Enforce recording of failures, failure classification, and failure analysis that can be used to update the failure rates of SIF devices with real data.
8. Recalculate the PFD / PFH at regular intervals based on updated (experienced) failure rates, and initiate, as needed, improvement measures if the performance does not meet the SIL requirement. Improvement measures can include replacing equipment, implementing stronger environmental controls to reduce exposure, improving testing and inspection procedures, or reducing the regular functional test interval.
9. Implement regular training of personnel involved in SIS related activities (support, upgrades, maintenance, operation...) at the level needed to serve their tasks

All these requirements apply regardless of the SIL level specified for each SIF.

9.7.3.2 SIL dependent requirements

Higher SIL levels require more effort to achieve the specified reliability, also considering the avoidance of systematic faults. Tab. 8 reproduces the content of one of many tables that align design requirements with SIL levels.

From Tab. 8, we note that a design measure can be either:

- Mandatory (M): The measure shall be used.
- Highly recommended (HR): The measure is strongly advocated, and if not applied, the rationale for not doing so must be explained.
- Recommended(R): The measure is recommended, but other measures with similar capabilities can be selected without justification.
- -: No specific recommendation has been made regarding this measure.
- Not recommended (NR): The measure is strongly recommended against. If still applied, it should be justified.

The required effectiveness of a design measure, meaning how efficient the measure must be to prevent and reveal systematic faults, is also specified. Three levels are used: low, medium, and high. The IEC 61508 standard provides examples of tools and methods that are suitable for achieving the different levels.

Tab. 8. Techniques and measures to avoid introducing faults during design and development (based on table B.2 in IEC 61508-2).

REQUIRED TECHNIQUE/MEASURE	SIL 1	SIL2	SIL 3	SIL 4
Adaptation of sector-specific guidelines and standards	M high	M high	M high	M high
Project management with organizational rules and measures for development and testing	M low	M low	M medium	M high
Documentation of each step during development	M low	M low	M medium	M high
Create a hierarchical structure of partial requirements for hardware and software	HR low	HR low	HR medium	HR high
Modularization of subsystems with restricted size and well-defined interfaces	HR low	HR low	HR medium	HR high
SELECT ALSO AT LEAST *ONE* OF THE FOLLOWING MEASURES:				
• Choice of well-tried components, when applicable	R low	R low	R medium	R high
• Use of semi-formal methods like logic/function diagrams, data flow diagrams, sequence diagrams etc.	- low	R low	R medium	R high
• Use of checklists to ensure coverage of requirements, e.g., for internal and third-party verification and validation	- low	R low	R medium	R high
• Use of simulations to confirm functional performance of electronic and programmed components.	- low	R low	R medium	R high
• Use of inspections and walk-throughs to reveal discrepancies between the specification and implementation	- low	R low	R medium	R high
• Use of formal methods with mathematical formulation of specifications and implementations	- low	R low	R medium	R high

Manufacturers of new or modified E/E/PE devices to be used in SIFs with SIL 3 requirements must provide arguments and documentation of why the methods were selected and how they were used. This is done "from scratch" for each unique delivery because it would be costly. Instead, manufacturers have developed manuals with instructions and methods most suited for their products. A third-party assessor is often used to confirm and SIL-certify that these manuals meet the requirements of IEC 61508.

9.7.3.3 Functional safety assessment (FSA)

The functional safety assessment (FSA) is an independent review conducted during the SIS lifecycle to determine whether the requirements relevant at the time, as specified in IEC 61508 or IEC 61511, have been met.

The FSA is an integral part of the quality assurance for the implementation of the IEC 61508 and IEC 61511 standards, and is often carried out by an external company, called a third party, that is not involved in the design project. An FSA involves a thorough, in-depth review of how the various phases have been implemented: whether the chosen methods are appropriate and aligned with the requirements of the standards, whether the technical solution is appropriate and safe for the destination system, and whether anything has been overlooked.

An FSA will not review all documents produced, but will focus on spot-checking primary documents such as the Management of Functional Safety Plan, HAZOP, LOPA analysis, the SRS, SIL analysis, and the training

provided to involved personnel. IEC 61511 proposes a total of 5 times an FSA should be implemented, referred to as stages:

- Stage 1 and Stage 2 refer to the FSA carried out for the design basis, before the actual installation starts. The two stages are not mandatory but are often recommended, as the costs of discovering critical design errors later may be high.
- Stage 3 is the only FSA that is mandatory before start-up and is the last resort to have an audit before the SIS is put into operation.
- Stage 4 represents FSA performed at regular intervals, for example, every five years, during operational life, and this stage is also mandatory.
- Stage 5 FSA focuses on the preparation for the dismantling of SIS to ensure that all aspects of safety during commissioning are ensured.

The FSA is conducted through a combination of document review and questioning in a workshop or through selected interviews.

The most important references are the IEC 61508 and IEC 61511 standards (depending on which one is used) and the company's own internal practices and procedures established for their use. The audit team often creates a checklist, for example, as shown in Tab. 9. An FSA typically requires a few days to prepare for 1-2 people and 1-2 days to conduct the actual visit and interviews. Companies that act as third-party FSA assessors have developed their own templates and checklists for the FSA.

Tab. 9. Extract of an FSA table

Item	Completion Measure	Evidence
SIS Design and Engineering		
1	Have requirements for segregation of SIF and non-SIF functions been applied in the segregation of software and hardware design?	
2	Does the system reset philosophy ensure that SIS outputs remain in a safe state until a reset is performed?	
3	Where voting groups exist, have they been designed to minimize common-cause failures, such as by allocating them to independent cards?	
4	Have safety manual been applied for configuration and testing?	
5	Does the application program shut down the system automatically after a fault if the fault is not resolved within the required mean time to restoration?	
6	If fault action on a safety-critical input is not set to trip the system, has the fault alarm been designed as a safety-critical alarm with operator action clearly defined in the operator's procedures?	
7	Has the systematic capability of system design been assessed, including measures to prevent failures and to control failures?	
8	Have the hardware fault tolerance and architecture requirements for the SIL been met by the proposed design?	
9	Has the response time to resolve various hazardous events been calculated, and requirements allocated to the applicable SIFs?	
10	Has the verification confirmed that the safety functions are fully testable for both validation and regular proof testing, and that they are accessible for inspection and maintenance?	
Application program		
11	Does the application program contain comments to explain complex functionality and cross-reference SIFs?	
12	Does the functional design specification contain a detailed description of application-specific user-defined function blocks?	

The result of the FSA is a report with findings and the responsible parties for follow-up.

9.7.4 Application (software) requirements and development process

There is some overlap between this section and a similar section in Chapter 4 on hardware and software logic.

IEC 61131-3 (2013) specifies requirements for software development, including limitations on the choice of programming languages and on the functionality of development tools, when pre-existing, certified software functions are not yet available. IEC 61131-6 (2012) provides more specific details relating to various safety design aspects of programmable controllers, but its content is not reflected here. The steps can be visualized in a V-model as illustrated in Fig. 25. The starting point for the V-model for software development is the more detailed SIS system specification. The SIS system specification details the technical implementation of the safety functions specified in the safety requirements specification (SRS).

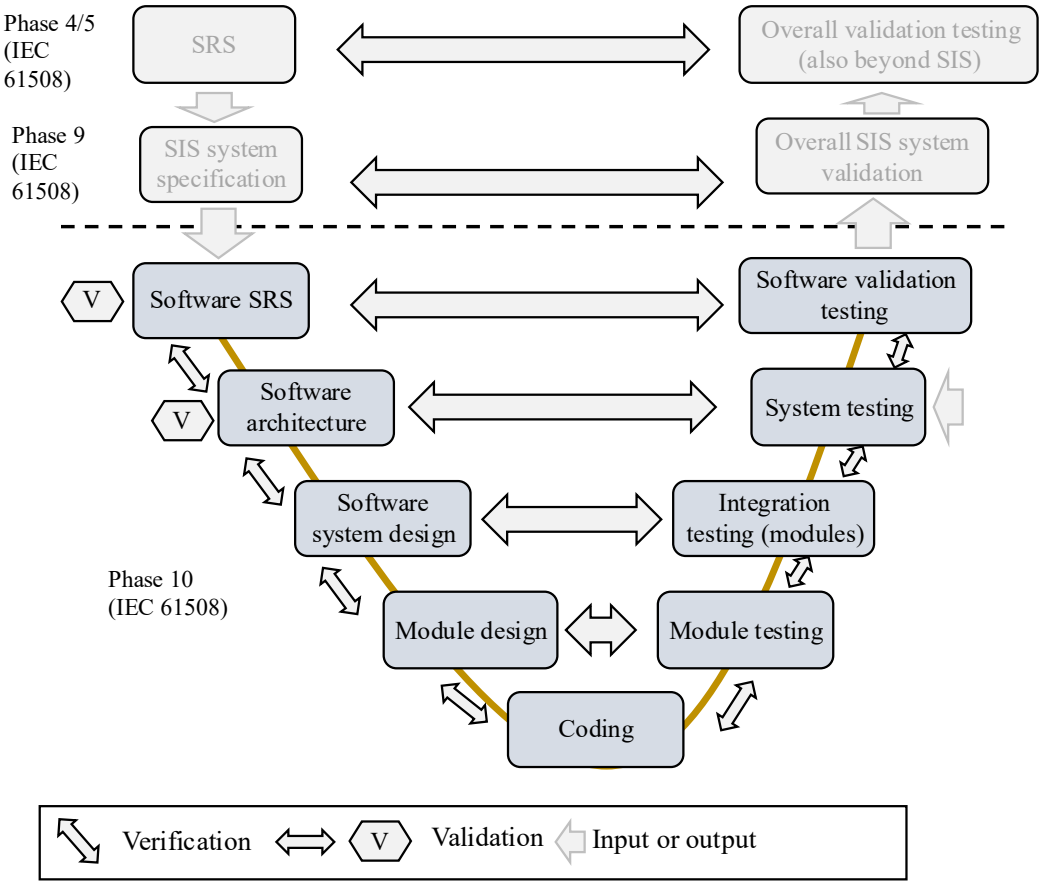


Fig. 25. The V (or waterfall) model for software design and development lifecycle

The phases of the V-model include:

- Development of software SRS: This phase involves the development of the high-level specifications of the software implemented functions, e.g., logical operations performed by each SIF.
- Software architecture: This phase involves the application of tools or modeling languages, like UML, to describe in more detail the classes, properties, interactions, and behavior that are needed to detail the software functions. Software development based on functions available in a pre-existing library may, for this step, focus on which library functions to apply and what new functions are needed.

- Software system design: This phase focuses on how to partition the software into manageable modules and their relationships. Software development based on pre-existing library functions may focus on configuring them.
- Module design: This phase focuses on how to implement each module, considering programming language, tools, and practices. Software development based on pre-existing library functions may focus on configuring the modules.
- Coding: This phase involves the programming of the modules. Software development using pre-existing libraries will focus on configuring them.
- Verification and validation: Verification is carried out along the legs to compare the output of the phase with what was specified as input. Validation is primarily indicated as horizontal activities that assess how well the software achieves the required performance. Validation is also suggested early to determine whether the specification and software architecture are sufficient and suitable for the intended purpose.

We have already introduced an example of a requirement that may be included in a software SRS. An example of the detailing of one such requirement in the specification for system architecture and software system design is shown in Tab. 10.

Tab. 10. Detailing of Software SRS requirements (with the assistance of Copilot)

Software SRS requirement:	*The software shall trip the reactor on high pressure*
Software architecture design specification	• Pressure measurements are acquired through the safety input module. • Shutdown logic is executed in safety PLC A. • Trip commands are transmitted via the safety network. • Valve commands are generated by the safety output module
Detailed software design specification	Pressure measurement: • PT-101 • Node: 3 • Rack: 1 • AI Card: 2 • Channel: 5 Output commands: • XV-101 • Node: 3 • Rack: 1 • DO Card: 4 • Channel: 2 Logic specification: • Could rely on system control diagram (SCDs) introduced in chapter 3 or e.g., structured text per IEC 61131-3.

IEC 61508-3 provides more thorough insights to the requirements for each phase of the V-model.

- Some requirements are general to application program development and coding and apply regardless of the SIL level to be achieved, while others vary by SIL level.

- For example, if an application program is developed “from scratch”, for example, when pre-existing libraries are not available, or a new software function is to be developed for a pre-existing library, the following requirements apply to the choice of programming language shown in Tab. 11.

Tab. 11. Adapted from table A.3 in IEC 61508-3 on support tools and programming language

REQUIRED TECHNIQUE/MEASURE	SIL 1	SIL2	SIL 3	SIL 4
Suitable programming language that provides block structure, translation time checking, and run-time type and array bound checking: Avoid features difficult to verify such as unconditional jumps, recursion, pointers, interrupts at source code level, and implicit variable initialization or declaration.	HR	HR	HR	HR
Strongly typed programming language where compiler can do extensive checking, e.g., on how variable types are used in e.g., procedure calls and external data access.	HR	HR	HR	HR
Systematic or computer-aided checking (static analysis) of language subsets that are error-prone or difficult to analyze	--	--	HR	HR
Use of certified tools and certified translators	HR	HR	HR	HR
Verify that the compiler has adequate performance	HR	HR	HR	HR

Most companies will develop their own tools, such as compilers and manuals with procedures for software development and configuration that align with IEC 61508 requirements. The tools and procedures are often subject to IEC 61508 certification by a third-party company. The configuration of an application program that utilizes function blocks from a library of certified functions often follows sector standards, such as IEC 61508, that are less detailed than IEC 61508-3. The procedures the companies develop are included in their products’ safety manuals.

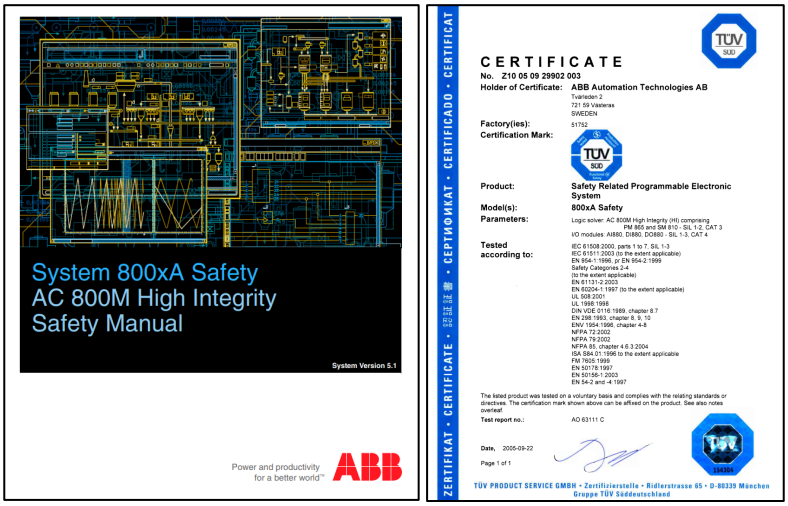


Fig. 26. Safety manual and TUV SUD certificate for ABB

9.7.4.1 Example: ABB controller and programming editor

ABB delivers a safety manual with its DCS controller, AC 800M, for high-integrity applications. Here, we can find information relevant to software development, like:

- 800xA's DCS product family has an object-oriented engineering environment with SIL-compliant function libraries that support the entire safety lifecycle.
- Specifically, System 800xA provides the following additional measures for safety system engineering:
  - IEC61131-3 language usage
  - Access control and override (force) control

- Application change report
- Application libraries and solutions

ABB provides the following advice on the selection of software languages (same source as above):

- **Function Block Diagram (allowed for non-SIL and SIL1-3)**

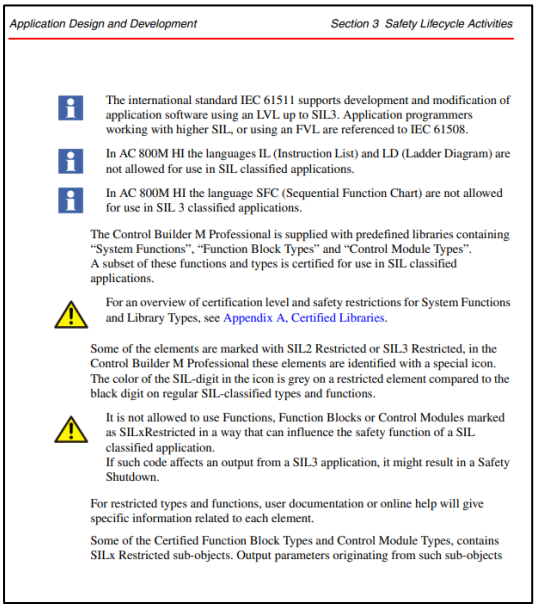
  Function Block is a graphical language for modeling logic elements and their interactions using library-stored software elements and interconnections. Function block programs are easy to develop and, thanks to the resulting graphical diagrams, also easy to read.

- **Structured Text (allowed for non-SIL and SIL1-3)**

  Structured text (ST) is a high-level programming language constrained by the software development environment. It provides a comprehensive set of constructs for assignments, function calls, expressions, conditional statements, and loops. The use of ST in SIL applications is subject to additional restrictions per IEC 61131-3 (2013) (Loops, parallel execution, and Returns are not allowed).

- **Sequential Function Chart (allowed for non-SIL and SIL1-2)**

  A sequential function chart (SFC) is a graphical language for depicting the sequential behavior of a control system. It is used for defining time- and event-driven control sequences. A sequence is shown in flow-chart form, using steps, transitions, and selection nodes. The language is well-suited to handling control tasks that are sequential in nature, i.e., consisting of several distinct steps, each requiring several enabling inputs, with the completion of the previous step, usually one of them.



Application Design and Development — *Section 3 Safety Lifecycle Activities*

The international standard IEC 61511 supports development and modification of application software using an LVL up to SIL3. Application programmers working with higher SIL, or using an FVL are referenced to IEC 61508.

In AC 800M HI the languages IL (Instruction List) and LD (Ladder Diagram) are not allowed for use in SIL classified applications.

In AC 800M HI the language SFC (Sequential Function Chart) are not allowed for use in SIL 3 classified applications.

The Control Builder M Professional is supplied with predefined libraries containing "System Functions", "Function Block Types" and "Control Module Types". A subset of these functions and types is certified for use in SIL classified applications.

For an overview of certification level and safety restrictions for System Functions and Library Types, see Appendix A, Certified Libraries.

Some of the elements are marked with SIL2 Restricted or SIL3 Restricted, in the Control Builder M Professional these elements are identified with a special icon. The color of the SIL-digit in the icon is grey on a restricted element compared to the black digit on regular SIL-classified types and functions.

It is not allowed to use Functions, Function Blocks or Control Modules marked as SILxRestricted in a way that can influence the safety function of a SIL classified application.
If such code affects an output from a SIL3 application, it might result in a Safety Shutdown.

For restricted types and functions, user documentation or online help will give specific information related to each element.

Some of the Certified Function Block Types and Control Module Types, contains SILx Restricted sub-objects. Output parameters originating from such sub-objects

Table 2. Compiler Switches

Switch	Description	Global (Non-SIL)	SIL 1 - 2	SIL 3
Simultaneous Execution in SFC(1)	Simultaneous sequences in SFC	**A**/E/W	E	E
Loops In ST	Loops in Structured Text (FOR, WHILE, REPEAT and EXIT)	**A**/E/W	E	E
Nested If or Case	Nested IF and CASE statements in ST	**A**/E/W	**A**/E/W	**A**/E/W
Implicit Cast(2)	Automatic conversion of data types (e.g. int. to real)	**A**/E/W	A/**E**/W	A/**E**/W
Instruction List language	Instruction List	**A**/E/W	E	E
Ladder Diagram language	Ladder Diagram	**A**/E/W	E	E
SFC Language	Sequential Function Chart	**A**/E/W	**A**/E/W	E
Loops in Control Modules(3)	Code sorting loops	A/**E**/W	A/**E**/W	A/**E**/W

Switch	Description	Global (Non-SIL)	SIL 1 - 2	SIL 3
Force I/O from code	Restricts the possibility to change the "Forced" component of IO Variables	**A**/E/W	E	E
Multiple calls to the same Function Block	Checks for multiple calls to the same FB instance within a POU	A/E/**W**	A/E/**W**	A/**E**/W
None or multiple calls to ExecuteControlModules	Checks for correct use of this function.	A/E/**W**	A/E/**W**	A/**E**/W

Fig. 27. Restrictions posed by SIL requirement for configuration of ABB

The 800xA safety DCS controller has been certified by TUV SUD, with the certificate retrieved from the shown in Fig. 26. The certification includes product reliability for SIL performance, and the work processes are documented in the safety manual. It is assumed that the safety manual is complemented by ABB's internal procedures for programming and configuration. This controller is primarily developed for use in the process industry, and therefore, the certification covers both IEC 61508 (generic) and IEC 61511 (process industry).

Some examples of how SIL requirements impact software development, according to the ABB safety manual for 800xA safety controllers, are shown in Fig. 27. In the tables they provide, the meaning of letters A, W, and E is as follows:

- A: Allowed. Checking that the rule is not activated
- W: Gives a warning if the rule is violated, and acknowledgment must be made before downloading to the controller from the engineering workstation (EWS) is allowed.
- E: Gives an error if the rule is violated and download is blocked

9.7.5 What about artificial intelligence?

The current (2010 version) of IEC 61508 does not permit the use of artificial intelligence (AI). IEC 61508-3 (table C.2, page 70) identifies examples that are difficult to achieve if AI is involved, with the author's reflection on why:

- Correctness of software specification: A specification of an AI system is implicitly given through the data used for training and not given explicitly. Specifications for AI systems are therefore vaguer than for conventional safety systems.
- Freedom from intrinsic design faults: The functionality of an AI-trained system is more complex and less specified, and the software code cannot be reviewed and checked in the same way as for conventional systems.
- Simplicity and understandability: IEC 61508 places many restrictions on what is allowed to be implemented for safety systems compared to, e.g., control systems. These restrictions are in place to ensure the system is simple and understandable enough for the functions to be fully verified. The functionality within AI-trained systems is not particularly transparent or explainable.
- Predictability of behavior: A safety system shall perform as specified each time it is demanded, and unexpected behavior can cause confusion and escalate a dangerous situation. AI systems may, on the one hand, be trained to cover more situations than those initially encountered, thereby contributing to greater safety. However, unexpected behavior may occur if the AI system's performance degrades over time or if it is trained on incomplete or insufficient data.

However, a recently published technical specification ISO/IEC TR 5469 (2024) developed by IEC and ISO, identifies some ways forward for using artificial intelligence in system development, diagnosis, and execution of safety functions. Work is already in progress to develop this technical specification into a formal IEC and ISO standard.

9.8 SIL follow-up in operation (phase 14-15)

SIL (or SIS) follow-up is required by IEC 61508 and IEC 61511.

> **SIL follow-up:** The tasks, resources, and competencies necessary to monitor and maintain SIS performance in accordance with SRS and SIL requirements throughout the entire operational life.

This section builds on a practical guideline on SIL follow-up that has been developed by Håbrekke et al. (2023) from SINTEF and NTNU. The guideline identifies the SIL follow-up activities as shown in Fig. 28.

The activities are:

- **Management of functional safety:** Covers management of procedures and personnel, for example, development and updating of operation and maintenance, ensuring that someone has the overall responsibility for SIS- and SIL-related activities, ensuring that people involved in SIS operation and maintenance have received necessary training, ensuring that regular audits are made to review practices, and so on.
- **SIS operation:** Covers day-to-day interaction with the SIS, including monitoring alarms, the status of temporarily inhibited SIF functions, following up on detected faults, and ensuring that compensating

measures are implemented. Failures identified during normal operation must be recorded in the maintenance management system for follow-up as part of the SIS maintenance.

- **SIS maintenance:** Covers scheduled maintenance, such as regular inspections and testing of SIF functions and devices, as well as unscheduled corrective maintenance and repairs triggered by failures revealed during scheduled activities, diagnostic alarms, and condition-monitoring systems. Failures are recorded in the maintenance management system, along with updated information on the causes and the status of repairs or replacements.

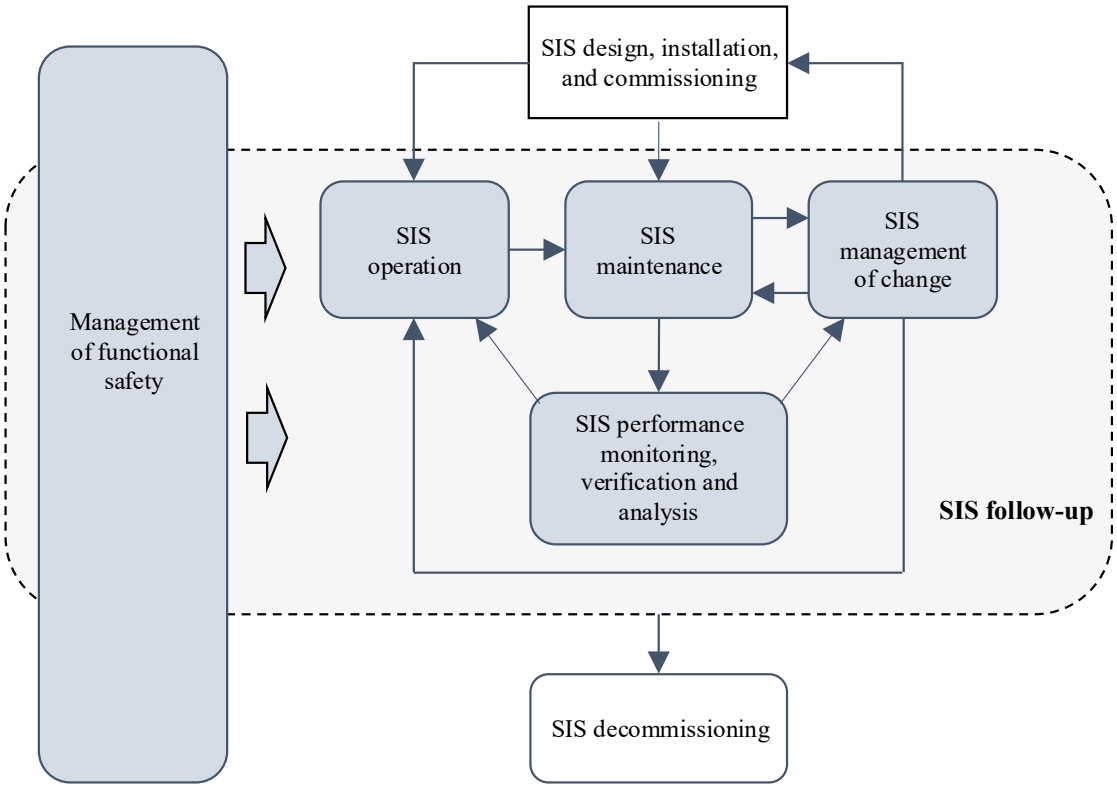


Fig. 28. SIL follow-up activities

- **SIS performance monitoring, verification, and analysis:** Covers all the necessary tasks for monitoring SIL performance and making necessary suggestions in case of performance deviations. More specifically:

  - Includes analysis of failures registered in the maintenance management system and through the SIS information management system. The SIS information management system collects data on when SIF actions are triggered, feedback (e.g., valve positions), and valve response times.

  - The failure data are classified according to IEC 61508/IEC61511 into dangerous undetected (DU), dangerous detected (DD), safe (S), and other failures (non-critical). At regular intervals, the failure rates for DU failures are recalculated and used as input in new updated SIL (i.e., PFD) calculations.

  - If the updated PFD exceeds the SIL requirement, it is necessary to reduce the proof (function) test interval. Likewise, if the updated PFD is below the SIL requirement, the test interval can be increased. Reducing the functional test interval can reduce PFD if needed. A PFD that is already below the SIL requirement allows the test interval to be extended, thereby reducing costs.

  - A reduction of the function test intervals does not make equipment more reliable but compensates for a lack of sufficient reliability. Therefore, it is also necessary to consider possible modifications

or replacements of SIS equipment that, over time, have proven to have lower-than-expected reliability (i.e., reliability lower than required).

Discover failures

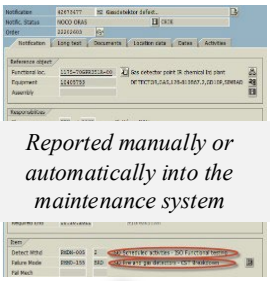
The equipment comes in with an alarm on display in the control room

Faults are revealed during functional test

Faults are discovered by casual observation during other types of work

Faults or degradations identified by condition monitoring systems

Registration



Reported manually or automatically into the maintenance system

Reported automatically via the control and safety systems

Classification

- Severity (dangerous, safe, other)
- Failure cause (random, systematic)
- Detection method (detected/undetected)
- Partly manual and partly automatic

Creating statistics

- Number of DU failures and DD failures during an observation period
- Trends from one period to the next
- Recalculation of failure rates
- Recalculation of PFD

Fig. 29 Process for failure discovery, registration, classification, and creation of statistics

- **SIS management of change:** The primary goal of this activity is to assess whether the proposed change could compromise safety. This means to reveal any reason the change *should not be made*. Covers the systematic evaluation of change requests related to SIS, covering:
  - Software changes, such as proposed changes in logic, like voting and values of setpoints, or upgrades of firmware and operating systems.
  - Hardware (new versions of controllers, new field devices, modifications of field devices,
  - Operating and maintenance procedures, including new test intervals

If no negative impacts are identified, the change management team determines how the modification will be handled. Often, it is necessary to revert to an earlier phase in the SIS lifecycle. For example, changing a setpoint value or replacing a transmitter with one with a different measurement range may require revising the previous hazards and risk assessment.

Fig. 29 shows a practical example of how failures are discovered, recorded in the maintenance system, and later classified and analyzed by an expert on SIL performance. We note that the discovery of failures relies on both people and systems. There is a trend toward using condition monitoring as widely as possible, but not all types of failures are yet covered by such systems.

A tool for failure rate and test interval calculation based on experience data has been provided with the guideline at https://mobilitet.sintef.no/pds/, and examples of the interface are shown in Fig. 30. The formulas are found in Håbrekke et al. (2023).

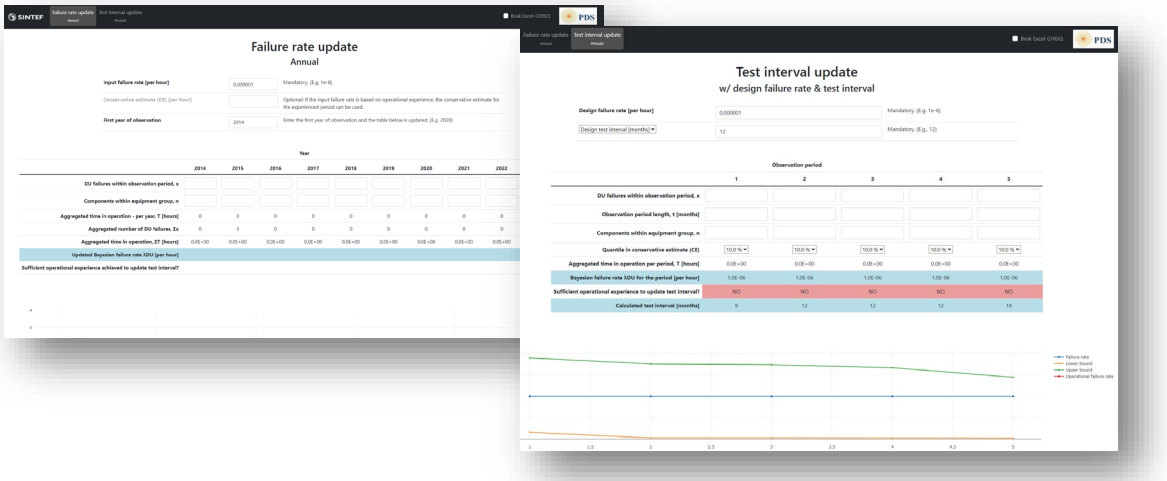


Fig. 30. PDS tool for failure rate and test interval updates

9.9 Concluding remarks, including further reading

This chapter covers only a selection of topics from IEC 61508. However, the overview is sufficient to convey how functional safety standards affect SIS design. A brief description of the implications for the operational phase has also been added.

Practitioners and industry experts have written several books on functional safety and SIS. For example:

- Rausand (2014): Reliability of Safety-Critical Systems: Theory and Applications

For practical insight into the use of IEC 61508 and IEC 61511, with primary focus on the petroleum industry in Norway, the following additional resources are relevant:

- Offshore Norway GL 070 (2026) on the application of IEC 61508 and IEC 61511 for the petroleum industry.
- Solfrid Håbrekke et al. (2021) on recommended guideline on the SIS follow-up in the operational phase.
- PDS method handbook and PDS data handbook, which some may acquire by purchase or by membership in the PDS forum.

9.10 Bibliography

Exida. (2020). *What does Proven In Use imply? White Paper*. Exida.

Håbrekke, S., Hauge, S., & Lundteigen, M. A. (2023). *Guideline for follow-up of safety instrumented systems (SIS) in the operational phase. An APOS project report*. SINTEF.

IEC 60300-3-2. (2004). *Dependability management - Part 3-2: Application guide - Collection of dependability data from the field*. International Electrotechnical Commission.

IEC 61131-3. (2013). *Programmable controllers - Part 3: Programming languages*. International Electrotechnical Commission.

IEC 61131-6. (2012). *Programmable controllers. Part 6: Functional safety*. International Electrotechnical Commission.

IEC 61508. (2010). *Functional safety of electrical/electronic/programmable electronic safety-related systems (Seven parts)*. International Electrotechnical Commission.

IEC 61508-2. (2010). *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety related systems*. International Electrotechnical Commission.

IEC 61508-3. (2010). *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*. International Electrotechnical Commission.

IEC 61508-4. (2010). *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*. International Electrotechnical Commission.

IEC 61508-5. (2010). *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels*. International Electrotechnical Commission.

IEC 61508-6. (2010). *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3* International Electrotechnical Commission.

IEC 61508-7. (2010). *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and measures* International Electrotechnical Commission.

IEC 61511-1. (2016). *Functional safety - Safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware and application programming requirements*. International Electrotechnical Commission.

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

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

ISO 14224. (2016). *Petroleum, petrochemical and natural gas industries — Collection and exchange of reliability and maintenance data for equipment*. International Organization for Standardization.

ISO 31000. (2018). *Risk management — Guidelines*. International Organization for Standardization.

ISO/IEC TR 5469. (2024). *Artificial intelligence - Functional safety and AI systems*. International Electrotechnical Commission, International Organization for Standardization.

Kaplan, S., & Garrick, B. J. (1981). On The Quantitative Definition of Risk. *Risk Analysis*, 11–27.

Offshore Norway GL 070. (2026). *Application of IEC 61508 and IEC 61511 in the Norwegian Oil and Gas Industry (ed.7)*. Offshore Norge. https://doi.org/https://offshorenorge.no/retningslinjer/arkiv/helse-arbeidsmiljo-og-sikkerhet/teknisk-sikkerhet/070-guidelines-for-the-application-of-iec-61508-and-iec-61511-in-the-petroleum-activities-on-the-continental-shelf/

Rausand, M. (2014). *Reliability of Safety-Critical Systems: Theory and Applications*. Wiley.

Solfrid Håbrekke, Stein Hauge, & Lundteigen, M. A. (2021). *Guideline for follow-up of Safety Instrumented Systems (SIS) in the operating phase*. SINTEF.