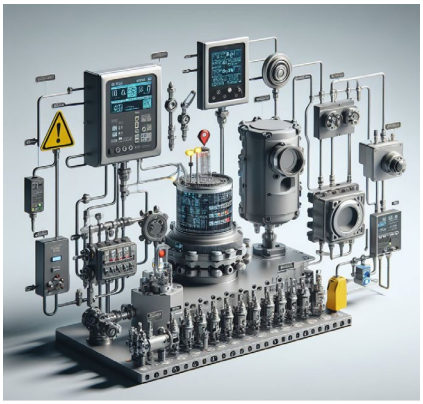
CHAPTER 6
SAFETY INSTRUMENTED SYSTEMS

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

Author: Professor Mary Ann Lundteigen, Department of Engineering Cybernetics



The essence of a safety-instrumented system?

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 the spring semester

Contents

6 Safety-instrumented systems

Safety, as defined by the IEC Encyclopedia, is freedom from unacceptable risk, where risk is related to potential harm to people, property, and livestock. Safety-instrumented systems (SIS) are systems that perform functions dedicated to ensuring that systems and facilities remain safe in hazardous situations.

The chapter explains selected aspects of the design of safety-instrumented systems (SIS). It first introduces general concepts, then reviews examples of regulatory requirements and design principles. The chapter concludes with a brief overview of the lifecycle phases of SIS design, implementation, operation, and maintenance. Measures to ensure the reliable design and operation of SIS, also referred to as functional safety, are covered in more detail in Chapter 9.

6.1 Abbreviations

(Some selected)

ALARP	As low as reasonably practicable
ERTMS	European railway traffic management system
ABS	Antilock braking system
CAP	Critical action panel
DSB	Directorate for Civil Protection
ESD	Emergency shutdown system
EUC	Equipment under control
F&G	Fire and Gas
HVAC	Heating, ventilation, and air conditioning (HVAC)
PCS	Process control system
PFD	Probability of failure on demand
PFH	Probability of having a dangerous failure per hour
PSA	Petroleum Safety Authority (to become “Havindustritilsynet” from 1.1.2024)
PSD	Process shutdown
SIL	Safety integrity level
SIF	Safety instrumented function
SIS	Safety instrumented system
SKF	Sikkerhetskritisk funksjon (railway)
SMR	Small modular reactor

6.2 Safety-instrumented system (SIS)

A control system can manage many types of disturbances without exceeding the normal operating boundary. However, in some cases, the disturbance becomes more significant, sudden, or intense, making the situation beyond the control system's capacity to manage. This disturbance can originate from another system, be caused by an external event, or result from a failure in the control system itself, in its hardware or software. If not managed, these events could escalate into hazardous situations and develop into severe accidents. In this case, we need systems to stop such events or mitigate the consequences. The measures can be technical, human (meaning that people take specific actions), organizational, or a combination of these. In this chapter, we will focus on safety-instrumented systems, a type of technical safety system that relies on sensors, controllers, and devices that interact with a physical system.

> A **safety-instrumented system (SIS)**: A system that relies on electrical, electronic, or programmable electronic technologies to detect and respond to hazardous events to achieve or maintain a safe state of the protected system.

The term SIS is borrowed from the process industry, where it serves as a generic designation for a safety system, and has been adopted for consistency with established industry terminology. Other terms with the same meaning

as SIS include safety-related E/E/PE systems, safety-related control systems (SRCS), and safety-related instrumentation and control (I&C) systems.

A simplified illustration of an SIS is shown in Fig. 1, and highlights that:

- The SIS is often split into three main subsystems: Initiators (or input elements), logic solver, and final (actuated) elements. Examples of equipment within each category are shown in the figure.
- Despite E/E/PE technologies being most central, the SIS also covers mechanical equipment that is operated directly or indirectly by logic solvers, like valves, motors, and pumps.
- There is an expectation that SIS devices have internal diagnostics, in particular, the logic solver and input elements. Diagnostics may be less applicable for mechanical and electromechanical devices.
- The SIS connects to relevant operator interfaces, such as screens and panels in the control room.

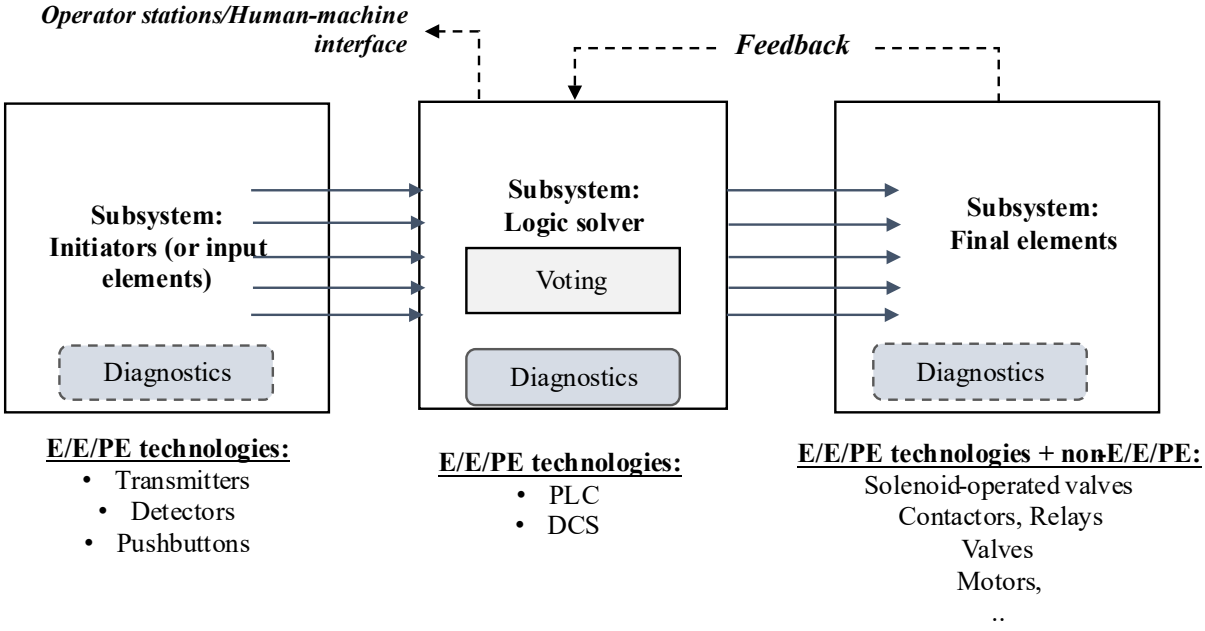


Fig. 1. Scope of SIS

Remark: Some standards use the term "input elements" in the same sense as "initiators".

6.2.1 Examples of how SIS systems interact

Industries with major accident risks rely on various measures to prevent the escalation of critical scenarios, each with safety functions that must act independently to enable multiple layers of protection. To be independent, the systems must have their own input elements, logic solver, and final elements. Examples of SIS systems commonly present for industrial plants are:

- Process shutdown system (PSD) that collects all safety functions needed to protect process units and equipment. This system stops rotating equipment and closes applicable valves, but does not disconnect electrical power sources. The safety functions are often referred to as local functions because they operate locally on specific units and systems.
- Emergency shutdown system (ESD) that collects all safety functions that interact globally at the facility to manage more severe events. The safety functions include shutting down the main power, starting the emergency power generator, and disconnecting nonessential electrical systems during facility shutdown. An ESD is activated manually upon a few high-risk events in the process and upon confirmed fire and gas (F&G) detection, the latter being on input from the F&G system. For the most severe events, the ESD system will also perform a delayed disconnection of all remaining power supplies, such as uninterruptible power supplies (UPSs), leaving the facility completely powerless. An important

function of an ESD system is therefore the isolation of ignition sources, reducing the potential for electrical ignition of any release of flammable or dusty atmospheres.
- F&G system that collects all safety functions related to automatic and manual fire and gas manual activation and release of fire extinguishing systems, start of fire pumps, and stop/start of fans and closure of fire dampers. The F&G system shares confirmed fire and gas detection with the ESD system, enabling the ESD system to perform ignition source control.

Some plants may also have a high-integrity pressure protection system (HIPPS), a stand-alone SIS whose sole purpose is to protect process equipment that lacks the design margins to withstand the highest pressures that can occur. Such systems are sometimes introduced for older facilities that have been expanded and, as a result, face capacity constraints, or in cases where the highest-pressure scenarios are relevant for a shorter period, typically in the initial phase of plant operation, and will decline rapidly afterward.

A very simplified example of how the mentioned SIS systems act independently to a process upset and potential escalation is shown in Fig. 2. The assumption is that the process control system (PCS) controls pipeline pressure during normal operation, but it cannot efficiently handle all process upsets, such as a sudden restriction downstream (not shown) of the facility. In this case, the SIS systems interfere in the following way:

- The PSD system is the first SIS to act: The PSD system monitors the pressure in the same pipeline and commands relevant shutdown (S/D) valves to close if the pressure exceeds a preset threshold (setpoint) value. The PSD usually issues a command to the PCS system as well, even if this is not credited as the safety function.
- If the PSD system fails or does not respond quickly enough, pressure may continue to build. In this case, the emergency shutdown system (ESD) is activated. Activation can be performed manually from the operator screen, the stand-alone critical action panel (CAP), or pushbuttons located around the plant. The ESD system may be automatically activated upon command from the F&G system in the event of a gas leak or fire.
    - The illustration shows that the ESD shutdown is often divided into levels: For offshore oil and gas facilities, the levels, in order of authority, are the Abandoned Platform (APS) level, ESD1 level, and ESD2 level. The level activated depends on the severity of the situation at the facility. When APS is activated, personnel must muster and prepare to evacuate. A higher ESD level always activates the level below. For example, APS activates ESD1, which in turn activates ESD2. The lowest ESD level always activates PDS, meaning ESD2 in our example.
    - It is possible for the PSD and ESD systems to share some (but not all) shutdown valves, due to practical considerations and the total number of ESD and PSD valves across the facility. In this case, independence is only partial for these valves; the solenoid-operated valves must be separate and independent for the two systems.
- The F&G system receives input from fire and gas detectors in the area. If a gas or fire is confirmed, the F&G system performs several tasks in addition to sending a command to the ESD system, such as releasing extinguishing systems, shutting down heating, stopping ventilation, and closing fire dampers associated with the air conditioning (HVAC) systems.

It may be noted that not all hazardous situations requiring a response from SIS systems begin with a process upset. For example, leakage of flammable gases may occur during normal operation due to an undiscovered crack or fatigue, or a heavy load from a crane could fall onto process equipment, leading to loss of containment of the affected systems. In this case, the F&G and ESD systems are activated first, with the PSD activated as a secondary effect.

Having more than one SIS is also essential for reducing the impact of SIS failures. If all safety functions mentioned in the example above were placed into one SIS system, a failure of the logic solver, as a common component, could lead to a simultaneous loss of PSD, ESD, and F&G systems.

Therefore, regulatory and standards authorities relevant to SIS require that SIS systems be designed and operated to be *sufficiently* independent.

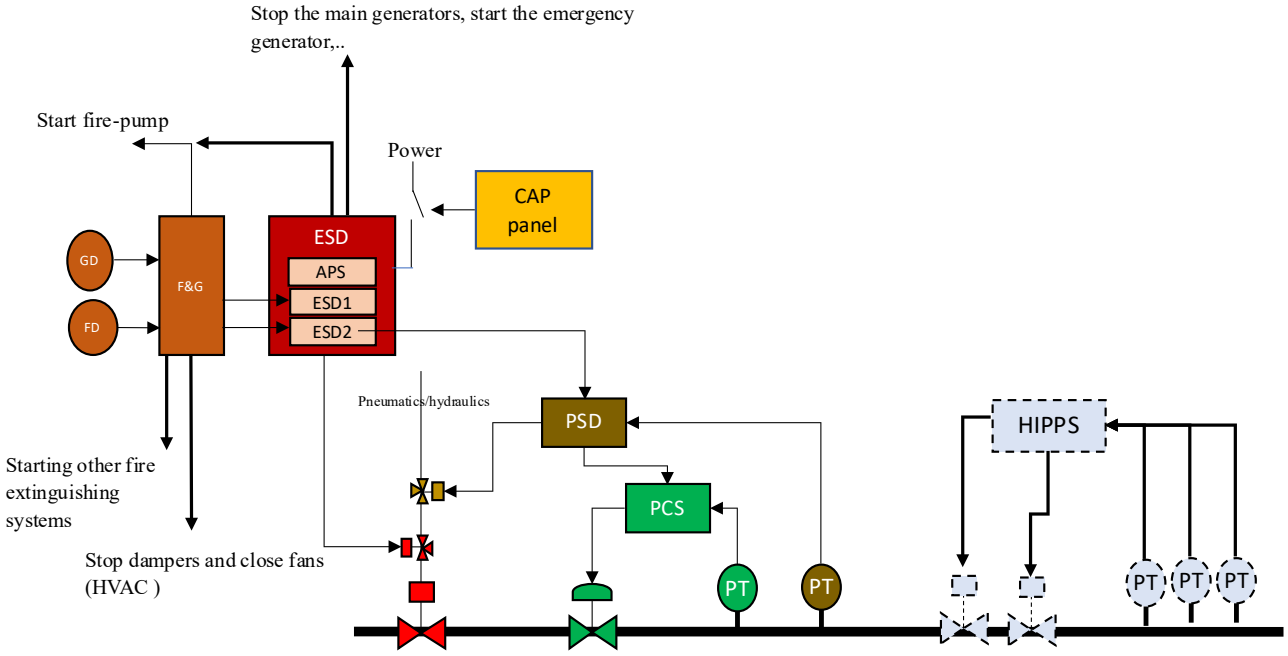


Fig. 2. Realization of PSD, ESD, and F&G detection

The above presentation of SIS has been biased by how the systems are applied in the process industry. However, in other sectors, such as railway signaling and machinery operation, there is no separate control system, and SIS functions are integrated into normal operations. Separating control from safety is not always possible if failure of any (normal) operation can immediately lead to a loss of safety. In this case, the SIS-control system is designed as an SIS, but it goes by other names, as SIS is a process-industry-specific term.

6.3 Safety-instrumented function (SIF)

A plant may implement several types of safety functions; not all are implemented in SIS. For example, some may be purely operational, meaning that an operator has to manually rotate an actuator wheel to close a valve, or that a mechanical pressure-release valve has an inbuilt opening mechanism that does not involve any SIS.

It is therefore common to introduce a specific term for SIS-implemented safety functions, which, according to IEC 61511-1 (2016)

> **SIF:** safety function to be implemented by a SIS.

The concept of SIF is of particular importance for requirements allocation and reliability analysis. Each SIF faces specific requirements for handling specific events, and a reliability analysis must demonstrate that the SIF is sufficiently reliable to meet those requirements.

Fig. 6 aims to clarify the relationship between SIS and SIF:

- A SIS generally has three types of subsystems: input devices, logic solvers, and final elements. A SIF is performed using specific devices within each of these subsystems, typically in all three or at least two.
- All SIFs implemented within the same SIS share the same controller or controller architecture. Therefore, the SIFs within the same SIS are not independent, but this is generally acceptable because each SIF responds to individual scenarios that are unlikely to occur simultaneously.

- The SIS collects SIFs that are either operating “all the time” or seldom, but not a mixture. This is because the design requirements for SIS systems differ, as the risk picture is different, leading to different technical solutions. For example, a railway signaling system uses different hardware and software architectures than those in the process industry, beyond the differences evident in handling entirely different types of operations.
- Within or at the boundary of the SIS are also interfaces to operator stations, servers, power supplies, and internal network topologies, but not all of these are explicitly addressed within the boundary of the SIF if they do not directly prevent the SIFs from being performed.

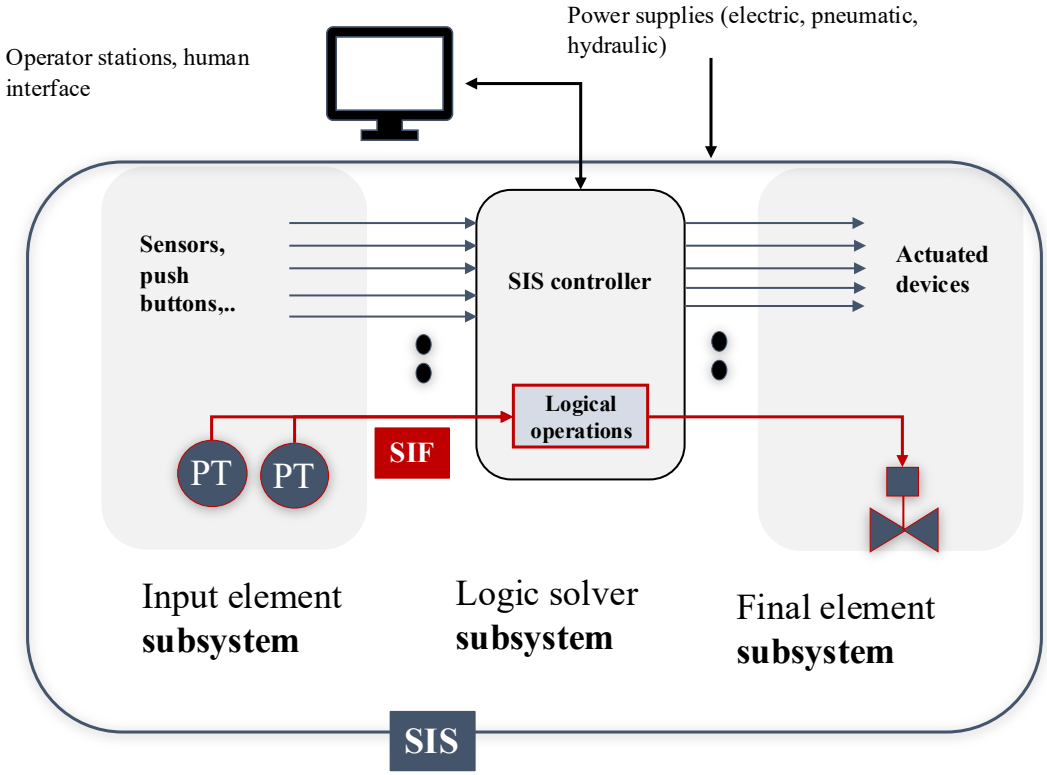


Fig. 3. SIS versus SIF

The Offshore Norway GL 070 (2026), a guideline on the application of IEC 61508 and IEC 61511 (the key SIS-related standards) provides valuable insights into typical SIF functions for PSD, ESD, and F&G. Fig. 3 shows one such SIF from the PSD system named PAHH:

- A dedicated pressure transmitter (PT) monitors the pressure in a tank and shares it with the logic solver (PSD logic
- The logic solver compares the received signal with the “high high” (HH) setpoint. The term “HH” typically refers to a trip or action threshold and has a higher value than the threshold labeled “H” for alarm purposes.
- When the HH level is exceeded, the SIF issues a command (often as an “off” signal) to the solenoid-operated valve, which switches position, closing the shutdown valve here named ESV 1.
- The example shows that the same valve is also used by the ESD system via a separate solenoid-operated valve. The fact that the valve is also used for ESD is probably why it is named ESV (emergency shutdown valve).

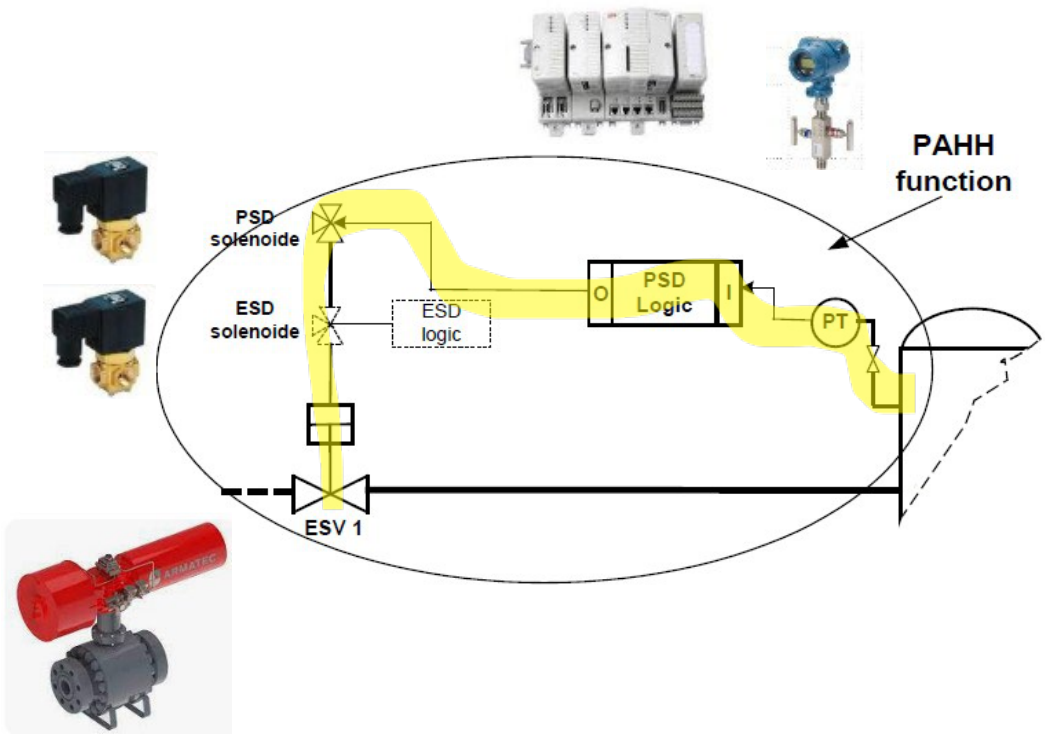


Fig. 4. Example of a PSD SIF (adapted from Offshore Norway GL 070)

The same GL070 identifies ESD and F&G SIF functions, either handling the input side (detection) or the output side (actuation), but not both.

The rationale is as follows: ESD and F&G are activated by events that can quickly escalate to larger areas, and therefore act globally. A single input, such as a confirmed gas leak or a manual activation, triggers numerous functions across the facility, including closing shutdown valves, shut down the main power supply, sounding alarms over loudspeakers, and starting fire pumps. It is more practical to describe each of these output functions separately. Therefore, as shown in Fig. 4, there is one ESD SIF for manual activation and one ESD SIF for electrical isolation, which stops the main power generators.

Similarly, Fig. 5 identifies one SIF for gas detection (in an area) and one SIF that handles the response function, the stop heat, ventilation, and air conditioning (HVAC) involving the closure of fire dampers and the stop of fans (with circuit breakers). The arrows in the middle indicate that the detection function can trigger multiple SIFs, not just one.

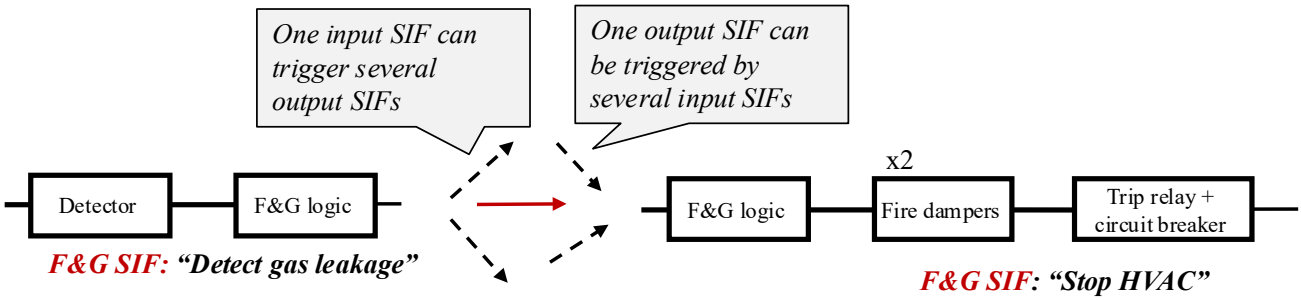


Fig. 5. ESD SIF for electrical isolation (From GL 070)

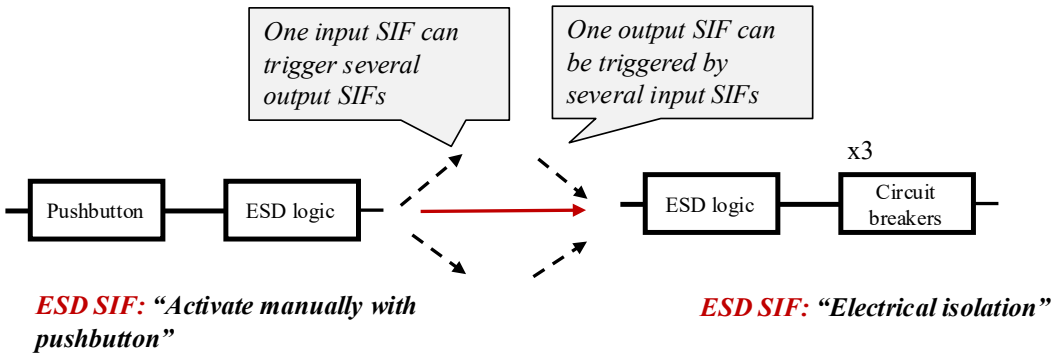


Fig. 6. Example of a F&G SIF split into two parts (From GL 070)

6.3.1 Demand and modes of operation

It was mentioned that a SIF may be required often or seldom, depending on how often (on average) an event that requires a response by the SIF occurs, and these events are referred to as demands.

> **Demand:** An event or circumstance where a response from a SIF is required in response to a hazardous situation.

The standards on functional safety IEC 61508 (2010) and IEC 61511-1 (2016) distinguished between two categories of on-demand modes of operation:

- **Low-demand mode:** When the average number of demands for SIF response is equal to or less than one per year. Examples include airbag systems, ESD, PSD, and F&G, which are SIFs.
- **High-demand mode:** When the average number of demands for SIF response exceeds one per year. Examples include emergency stops for machines and emergency brake systems

The choice to separate low- and high-demand modes at once each year is sometimes debated, and questions arise; the choice may have been made somewhat pragmatically.

A term related to, but not counted as, demands when classifying the mode of operation as unintended or spurious SIF activations, which can occur due to SIS-related faults. We will also learn in Chapter 8 that low-demand SIFs are subject to regular testing, but such activations are not defined as demands.

A third mode of operation is applied for SIS systems that operate as part of normal operation and therefore are continuous:

- **Continuous mode:** The mode of operation where the SIF retains the process in a safe state as part of normal operation. Examples include machinery control systems and train signaling systems.

For most practical purposes, high-demand and continuous modes of operation share the same general design requirements and reliability performance measures.

6.3.2 Safe state and fail-safe

The term safe state is often used in two contexts: the safe state of a system that can pose risks to someone or something, often referred to as equipment under control (EUC), and the safe state of SIS devices as part of an SIF. While the two are different, they are related: The safe state of what is to be protected influences what is the required safe state of the SIS devices. We can therefore introduce:

- **Safe state of EUC:** The state of the EUC where the risk of harm is sufficiently reduced or eliminated.
- **Safe state of SIS device:** The state when the SIS device contributes to acquiring or maintaining the EUC safe state.

The safe state of the EUC depends heavily on what the EUC is and on its operational situation. For example, the EUC can be an aircraft, a medical device, a ship, a processing facility, or a subpart of any of these. Examples include:

- To continue its mission or operation
- To continue, but in a degraded mode of operation
- To stop
- To start

Different plants and systems may have different safe states. Examples of typical safe states are:

- Oil and gas facilities: to shut down, as many hazardous situations can escalate rapidly if not stopped.
- Chemical plants: shut down or (for some processes) continue to operate until a specific chemical reaction is complete to avoid a runaway reaction.
- Nuclear power plants: Maintain the cooling water system in operation to prevent rapid temperature increases in the event of a loss of the reactor.
- Aircraft: Continue flying to the nearest defined airport.
- Ship: To drop anchor or drive with reduced engine capacity to the nearest port.
- Car airbag system: Release

A transition to the safe state can, for some of the listed states above, create dangerous situations. For example, deploying the airbag while driving can cause the driver to lose control. Such a dilemma cannot be easily resolved; however, it indicates that spurious activations (false demands) can be dangerous in some cases. Therefore, when no single state is safe across all relevant scenarios, the priority is to select the safe state for the most critical operating mode.

SIS devices must be designed or selected so that their safe state matches the safe state of the EUC for which they are to be used. By safety standards, it is common to require SIS devices to be capable of entering the safe state even in the presence of certain highly foreseeable faults. Examples of such faults include electrical power failure, communication faults, and loss of pneumatic (pressurized air) and hydraulic energy supplies. This leads to the requirement that SIS devices be designed as fail-safe, meaning that upon the occurrence of these faults, they will automatically enter their safe state.

> **Fail-safe** refers to the ability of SIS devices to enter their safe state upon specific fault conditions, such as a loss of power supply or a loss of sensor signal.

If fail-safe capability cannot be built into the device itself, it is necessary to incorporate additional redundancies in electrical power supplies, communication systems, or other energy sources to ensure they remain available even in hazardous scenarios. Such measures can be the availability of local battery supplies, accumulators, or diverse means of communication.

For example, a shutdown valve may be designed to automatically enter a safe state upon loss of power by incorporating a compressible spring that, when released, causes the valve seat to seal. Similarly, a transmitter may, upon detecting an internal fault, force its output to zero or to a predefined reading outside the valid measurement range, indicating that the measurement cannot be trusted.

The consequence of devices being fail-safe can be unscheduled stops or interruptions in facility operation if the same fault conditions occur during regular operation. Fail-safe devices may therefore lead to higher spurious trip rates. This is one of the consequences of prioritizing safety over production availability.

6.3.3 Safety integrity level (SIL)

Safety is often defined as freedom from unacceptable risk, and functional safety refers to the level of safety provided by the SIS. IEC 61508 (2010) provides the general requirements and best practices for designing, building, operating, and maintaining an SIS. Various sectors have made their own variant of this standard to align with their practices and terminologies, e.g., IEC 61511-1 (2016) for the process industry, IEC 61513 (2011) for nuclear power plants, ISO 26262-1 (2018) for automotive, EN 50129 (2018) for the railway, and IEC 62061 (2021) for machinery. IEC 61508 and related standards employ a risk-based approach to determine

whether a Safety Instrumented System (SIS) is required and to specify the corresponding performance requirements. Some performance requirements are placed on the SIS, while others are placed on the individual SIFs.

One of the most central performance requirements placed on the SIS is:

- The SIS must be sufficiently independent of other systems in a way that a fault in another system should not prevent the SIS from performing its functions.

Examples of performance requirements allocated to the individual SIFs are:

- Definition of the primary safety function: What is the main task of the SIF
- Definition of the fail-safe function: The state that the SIF must enter in the presence of faults like power loss, loss of communication, and individual component failures
- Triggering event (demand) and mode of operation: The phenomena or situations that will trigger the activation of the SIF (referred to as a demand) and how often the SIF is expected to be demanded (the demand mode of operation).
- Reliability: How reliable must the SIF be once demanded, often expressed in terms of a maximum tolerated failure probability or failure frequency
- Response time: How fast SIF must complete its task to be effective.
- Robustness: The types of exposures the SIF or some of its components must withstand during demand, and for how long the SIF must remain effective, for example, fire and heat resistance, and the tightness of valves.
- Human interaction: If necessary, the operator must interact with the SIF during its execution to maintain the safe state of the SIF and to reset it during the restoration and start-up of the plant or system being protected.

The reliability requirement is converted to a safety integrity level (SIL). Safety integrity is defined as the ability of a Safety Instrumented Function (SIF) to perform its required function. It is pragmatically categorized into four safety integrity levels (SIL 1 to SIL 4), with SIL 4 the highest and SIL 1 the lowest.

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

IEC 61508 defines the relationship between PFD/PFH values and the four SIL levels as seen in Tab. 1.

Tab. 1. SIL table in IEC 61508

SIL	Allowed failure probability (PFD)	Allowed failure rate of dangerous failures per hour (PFH)
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 information in the table should be extended with the following meaning:

- The SIL table also defines the limits of what is achievable and allowed for SIFs.
- The lowest SIL (1) sets the lowest reliability accepted for an SIF, and the highest SIL (4) is the limit of reliability that is believed to be achievable.

6.4 Equipment under control (EUC)

SIS systems are introduced to protect something – it can be a system, a process, a human, or a location. IEC 61508 (2010) refers to such a system as equipment under control (EUC), defined as:

> **EUC**: equipment, machinery, apparatus, or plant used for manufacturing, process, transportation, medical, or other activities.

Although not evident from the definition, the EUC is regarded as the system for which hazards may arise before any safety protection measures have been added. An EUC can be process equipment, for example, a pressurized vessel, as shown in

OBJ

. In other sectors, we can find parallel examples. A transport ship may define areas such as the control bridge, engine room, cabin areas, and storage rooms as individual EUCs. A medical device may be an EUC itself or regard the human as the EUC. A track section, or the distance between two stations, can also be an EUC. EUC.

The EUC usually includes an EUC control system that manages normal operation. IEC 61508 defined the term as:

> **EUC control system**: a system that responds to input signals from the process and/or from an operator and generates output signals causing the EUC to operate in the desired manner.

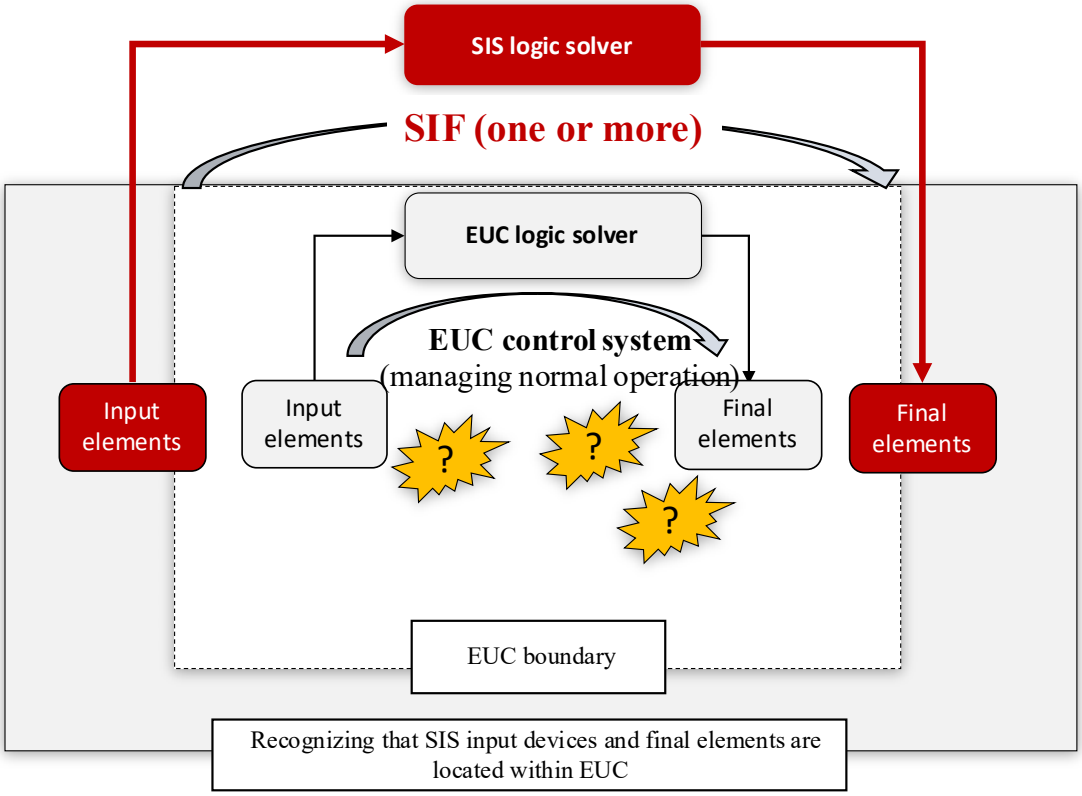


Fig. 7. Example of an EUC and EUC control system, and its relation to SIFs

The EUC control system, therefore, handles normal operations by the way it is designed and the use of a control system that manages the scenarios during normal operation, as shown in Fig. 7. The navigation system on a ship is another example.

EUC, with its EUC control systems, is the starting point for a hazard and risk analysis to determine whether protection is needed. Any protection measure that needs to be added, including those performed by SIS, is defined as complementary rather than part of the EUE and EUC control system. This can be somewhat confusing, as the SIS devices are located within the EUC boundaries. However, separation is made to distinguish clearly between what to protect and how to protect.

A special case is when the EUC control system itself is defined as safety-critical, meaning that safety functions are performed as part of normal operation in continuous mode.

6.5 SIS safety lifecycle

Key standards used for design, operation, and maintenance of SIS are IEC 61511-1 (2016) for process industry, IEC 62061 (2021) for machinery, and IEC 61508 (2010) being generic and often used by vendors that certify their products and systems for use in safety-critical applications. The standards are covered in more detail in Chapters 9 and 10; for now, we will introduce a few concepts.

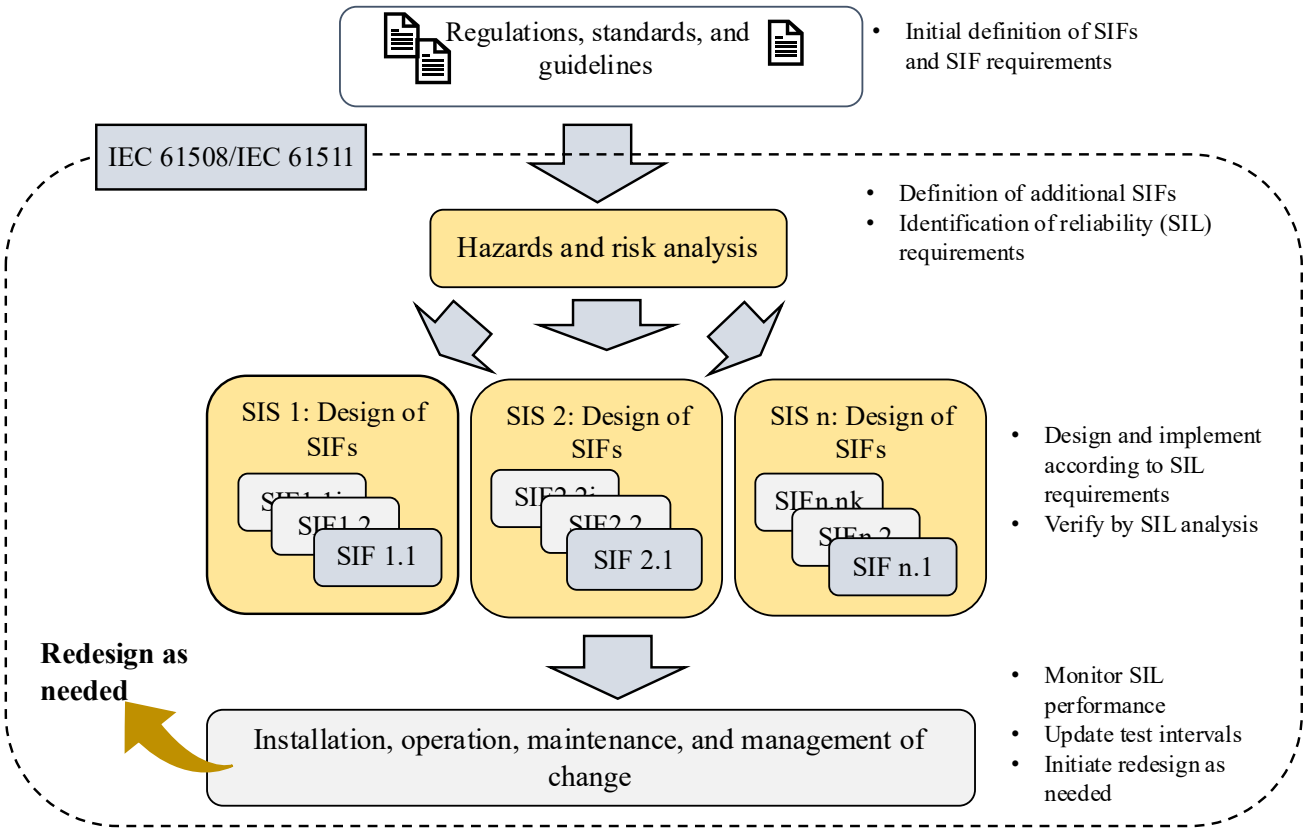


Fig. 8. Simplified lifecycle model for SIS

The first is the SIS lifecycle model, which identifies all the required phases from the SIS "cradle to grave". Fig. 8, is a simplified presentation of the SIS lifecycle emphasizing the following:

- SIS design is risk-informed: A hazards and risk assessment is conducted to identify which SIFs are needed, the amount of risk reduction allocated to these SIFs, and the corresponding SIL requirements. Along with other important framing conditions, such as regulations, national guidelines, and internal company practices, this forms the starting point for specifying requirements.
- Safety-integrity levels (SIL) are applied to translate risk reduction requirements into design and performance requirements for SIF: The SIL requirement is used to select design principles, tools, and methods for work processes to achieve a SIF with a performance that can meet the SIL requirement. The work processes aim to prevent systematic errors.
- Reliability analyses play a key role: Reliability analyses are conducted in design as well as throughout the operational phase to check if the SIF continues to meet the SIL requirements.
- Reliability analysis depends on access to operational and failure data: Monitoring, testing, and inspection are conducted regularly to collect data on the SIFs' performance. Corrective measures are implemented if performance deviates from the SIL requirements.

The following sections elaborate on some parts of Fig. 8. More details about the SIS lifecycle are covered in Chapter 9, which focuses on functional safety and IEC 61508. How to calculate PFD and PFH of a SIF is covered in Chapter 8, "Reliability Analysis."

6.5.1 Hazards and risk analysis

A hazard and risk assessment is a systematic identification and analysis of the risks. But what do we mean by risk? IEC Electropedia at https://www.electropedia.org/, which gathers many of the definitions used in IEC standards, defines risk as:

> **Risk:** The combination of the probability of harm and the severity of that harm.

The most common approach to defining the risk is, therefore, to answer the following questions:

- What can go wrong? (may cause harm)
- How often can it happen? (probability)
- What are the consequences? (severity)

It may be noted that newer definitions of risk place greater emphasis on the degree of knowledge about events, and that this knowledge must be documented alongside the best estimates of event frequencies or probabilities and possible outcomes.

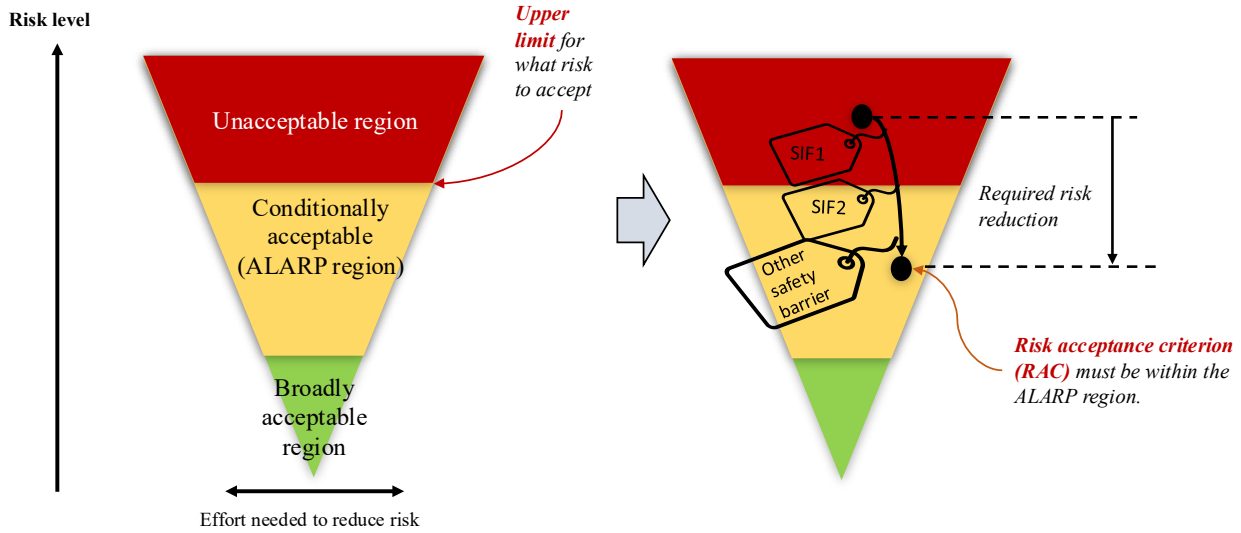


Fig. 9. The regions of the ALARP principle

The outcome of these questions is a list of hazardous events, which IEC Electropedia defines as:

> **Hazardous event:** An Event that can cause harm.

It is necessary to determine whether the risk of each hazardous event, or of a group of hazardous events, is too high. A widely accepted principle for risk reduction is the 'as low as reasonably practicable' (ALARP) principle, first introduced by the UK Health and Safety Executive (HSE) to prevent major accidents in industries with a high potential for them. ALARP identifies three central regions of risk, as shown in Fig. 9:

- Unacceptable risk region, meaning a region where activities are not allowed.
- Conditionally acceptable region, also called the ALARP region, where the activities may be conducted *if* additional measures are implemented to reduce the risk even further. The willingness to spend money to reduce the risk must be proportional to the risk level, meaning that you (or your organization) are required to spend more money on risk reduction efforts if you are in the upper part of the ALARP region

compared to the lower region. A cost-benefit analysis for safety may be conducted to support decision-making, an activity that is sometimes controversial, as the value of a human life must be quantified.
- Broadly acceptable region, meaning the region where the risk is insignificant in the sense that it corresponds to what the public accepts as part of daily life (excluding work).

The border between the unacceptable risk and the ALARP region defines the upper limit of the risk acceptance criteria, the risk formulated by a measure with a maximum tolerated value. There are several types of risk measures, for example, the individual risk per annum (IRPA), the fatal accident rate (FAR), the FN-curve (also known as the Farmer diagram), and the risk matrix. The risk matrix is the focus here, as it combines different levels of likelihood (e.g., rows) and consequences (e.g., columns) in a matrix format.

The application of the risk matrix is covered in more detail in Chapter 9, which focuses on functional safety and IEC 61508. For now, we conclude that the SIFs are measures to use to reduce the risk from a region where the risk is unacceptable and into the acceptable regions, ALARP and below, as shown in Fig. 9 (to the right). Each SIF, or a combination of SIFs and other safety barriers, must cover the amount or required risk reduction, meaning the distance from a point in the unacceptable region to a point in the regions below. The ALARP principle requires that the risk be reduced to below the unacceptable level and, if cost-effective, further into the ALARP region.

The amount of risk reduction allocated (meaning required to be managed) by each SIF can be converted into a reliability requirement that the SIF must fulfill. Refer to Chapter 9 for a more detailed explanation of functional safety. This reliability requirement is expressed as the maximum probability of failure on demand (PFD) for SIFs operating in low-demand mode and the probability of dangerous failure per hour (PFH) for SIFs operating in high-demand or continuous mode. As shown in Tab. 1, four distinct ranges of PFD and PFH values are defined and categorized as SIL 1 to SIL 4.

6.5.2 Design and SIL analysis of SIFs

In the design phase, the SIL requirement provides a set of rules and limitations in the freedom to choose a technical solution. This topic is covered in more detail in Chapter 9. For now, we are highlighting the following messages:

- "The higher SIL level does not always mean more safety:
  - Higher SIL requirements often result in a more complex and expensive solution that can be challenging to maintain in operation.
  - For example, a SIL 4 system may have a higher tendency to stop production, and this can have other adverse side effects. The process industry typically employs the layers-of-protection approach, using multiple Safety Instrumented Systems (SISs). In this context, it is often sufficient to have SIL levels of 1 and 2 (and, more rarely, 3).
  - Railway signaling systems have SIL 4 requirements, as this system alone is responsible for critical operations, such as setting the green (go) light and changing the position of rail switches.
- The manufacturers usually certify their SIS products (controllers, sensors, solenoid valves, etc.) to IEC 61508. For example, the HIMA controller used in the lab has a SIL certificate stating that it is approved for SIL 3 functions.

The design constraints eventually result in a list of SIFs that comprise some selected components, which may implement redundancy. Before the SIS (with its SIFs) is installed, it is necessary to perform a SIL analysis where the reliability of the SIFs is calculated and compared with the SIL requirements. The SIL analysis also verifies requirements in IEC 61508 related to fault tolerance and the selection of design measures. If the SIL analysis reveals that some SIFs do not meet the SIL requirement, the solution must be redesigned.

6.5.3 Operational phase

SIS systems may have an operational life of 15-30 years, with some upgrades during this period. Throughout their lifetimes, it is necessary to regularly verify that the SIL requirement for the SIFs is met, as many dangerous faults cannot be detected during normal operation. Verifying SIL performance, therefore, relies on regular

function tests, analysis of reported faults, and calculation of PFD (alternatively, PFH) based on recalculated failure rates.

The complete (end-to-end) SIF is not typically tested simultaneously due to operational considerations. It can be more practical to test multiple pressure transmitters in a single testing campaign, thereby avoiding interference with production. An example of a function test of a pressure transmitter is shown in Fig. 10. The steps are as follows:

1. The pressure transmitter is isolated from the process by operating a manual valve
2. The operators in the control room inhibit the output of SIF, where this pressure transmitter is included, to avoid a stop of production
3. An accumulator is connected to pressurize the tubing of the pressure transmitter up to the given setpoint set in the logic solver
4. The operators in the control room verify that the logic solver registers the correct measurement and that the output signal is set, depending on whether the pressure transmitter is part of a voted configuration or not.

If the performance is below the requirement, it is necessary to consider design modifications, replace unreliable devices, or test the functions more often.

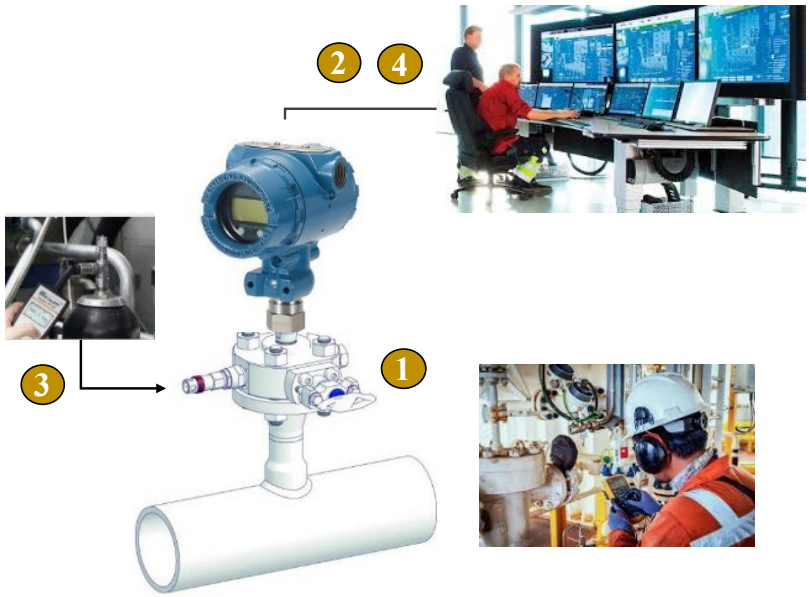


Fig. 10. Testing of pressure transmitter

SIFs taken out of service may be unavailable if a hazardous situation occurs. IEC 61508 therefore requires online monitoring of all temporary outages (bypasses, inhibits) of SIFs or SIF components due to maintenance and other activities at the facilities. The operators must ensure that the outage time is not exceeded and that compensatory measures are efficient throughout the entire period.

Industry guidelines for SIS follow-up in Norway, which are also used internationally by Norwegian energy companies, are:

- SINTEF/PDS forum guideline on the Guideline for follow-up of Safety Instrumented Systems (SIS) in the operating phase (Solfrid Håbrekke et al., 2021)
- Offshore Norway guideline on the application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry (Offshore Norway GL 070, 2026)

6.6 SIS as Barriers

We already mentioned that SIFs carried out by SIS are only one type of safety function, meaning there are several types of safety systems besides SIS. Some sectors have adopted the term "safety barriers" (or just "barriers") and the associated barrier functions. Barriers are useful as many concepts and ways to analyze barriers are well established.

6.6.1 What is a barrier?

According to the principles for barrier management in the Petroleum industry by the Petroleum Safety Authority PSA (2017), now Ocean Industry Authority (HAVTIL), a barrier can be defined as:

> **Barrier:** A measure that can detect conditions that may lead to failure, hazard, and accident situations, prevent an actual sequence of events from occurring or developing, influence a sequence of events in a controlled way, or limit damage and/or loss.

Barriers can be technical, organizational, or operational. PSA adopts the following definitions:

- Technical barrier: Equipment and systems involved in the realization of a barrier function.
- Operational barrier: The actions or activities that personnel must perform to realize a barrier function.
- Organizational barriers: Personnel with the competence to serve defined roles or functions related to operational and technical barriers.

SIS is an example of a technical barrier, even if some human interaction is involved. Examples of other (non-SIS) technical safety barriers include a physical firewall, a drainage system to collect spills, and mechanically self-operated pressure-relief valves. Operational barriers relate to tasks, supported by procedures, for alarm handling, emergency response, and evacuation. Organizational barriers involve having necessary roles with defined responsibilities and competencies, as well as procedures and practices to manage various abnormal situations.

A barrier performs one or more barrier functions. Transferring to a SIS means that the SIS performs one or more SIFs.

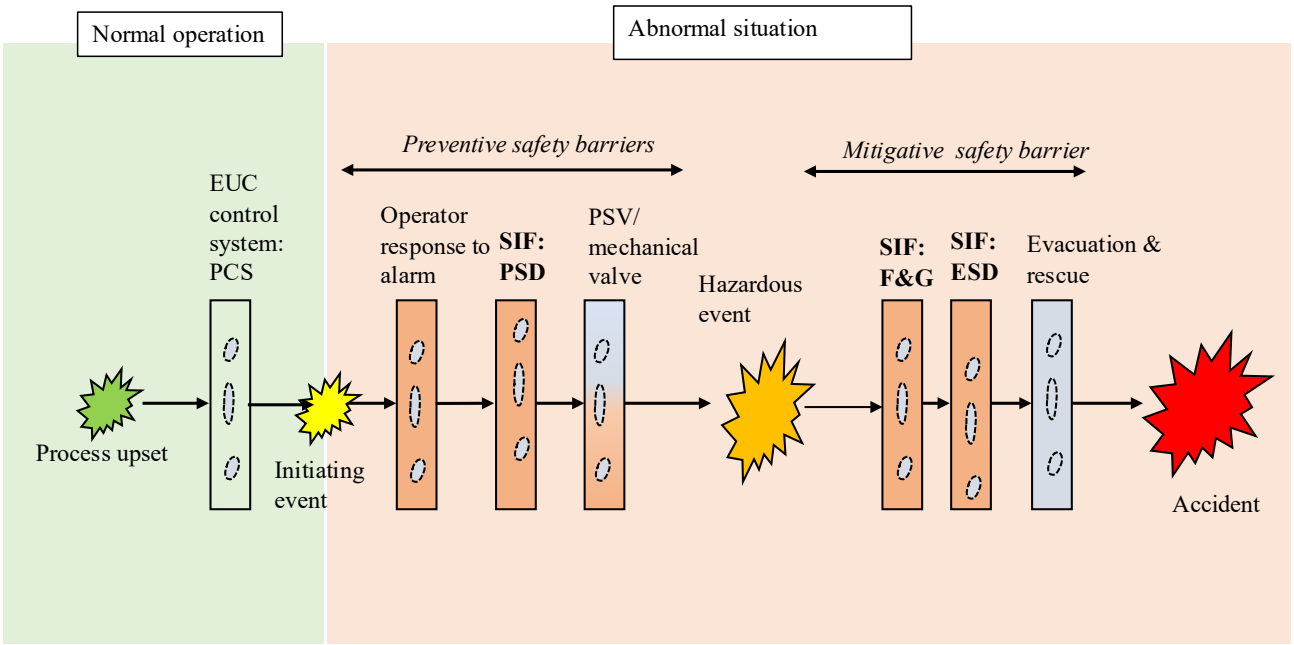


Fig. 11. Role of barriers

We may explain the concept of barriers by walls, as shown in Fig. 11: The goal of a process plant is to operate within the boundaries of regular operation. The facility's design, the capabilities of the PCS system, and tasks within operating procedures are contributing factors here. Yet something unexpected occurs when the normal operating envelope is exceeded; we may refer to these as hazards (conditions) and triggering/initiating events. The hazard is a potential uncontrolled flow, and the triggering event is an unexpected valve closure that increases pressure. If the triggering event is *not* handled, it may develop into a hazardous event.

> **Hazardous event:** The first significant occurrence that, if not addressed, could develop into an accident.

For example, a gas leak following over-pressurization of a pipe or tank could be considered a hazardous event. Barriers that are in place to respond to triggering and hazardous events are referred to as safety barriers.

If the hazardous event develops further, it may ultimately escalate into an accident. An accident with high severity, often referred to as a major accident, may have multiple fatalities or irreversible impacts on the environment. The successful performance of the barriers may result in no or negligible consequences. Consequently, we can classify barriers as either:

- **Preventive barriers** that will prevent a hazardous event from occurring.
- **Consequence-reducing or mitigative barriers** will reduce the consequences of the hazardous event so that the severity of its impacts is reduced.

The barriers are in place to interact with and, if possible, entirely prevent the event from propagating from a process upset to an accident. However, the barriers are never perfect, as illustrated by the holes inside each barrier in Fig. 11. The addition of holes is sometimes referred to as the Swiss cheese model, originally introduced by R. Reason to visualize human and organizational barriers.

6.6.2 Bow-tie model

Fig. 11 can be extended to what is called the bow-tie model in Fig. 12.

> **A bowtie diagram:** A graphical illustration of the relationship between the spectrum of causes and consequences relative to a specific hazardous event positioned at the center.

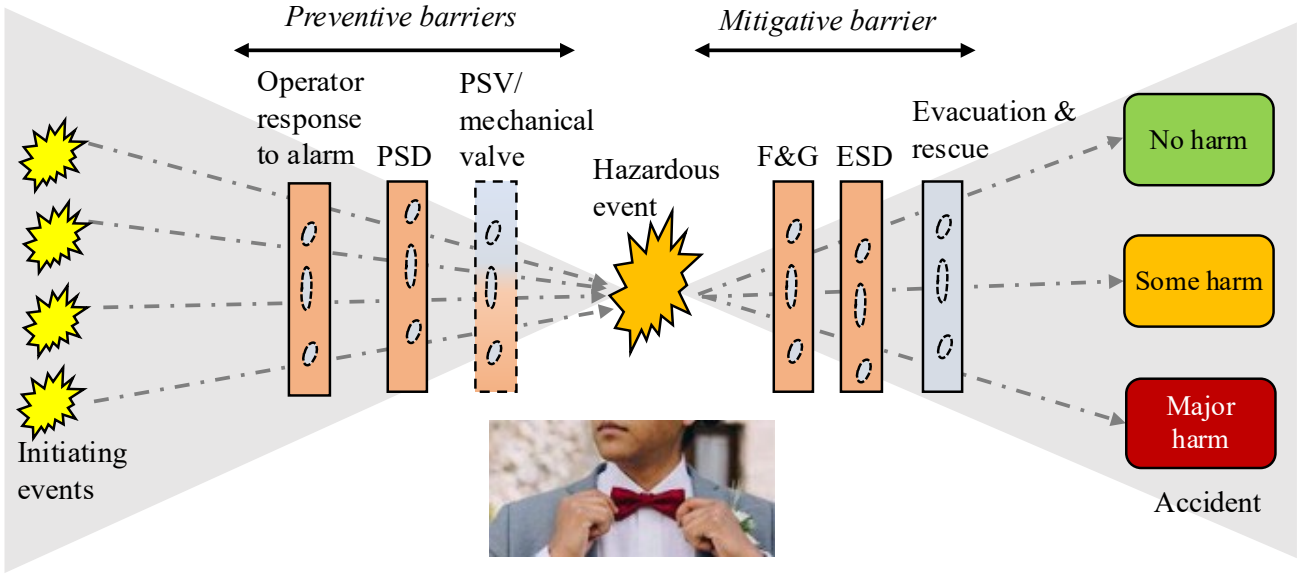


Fig. 12. Bow -tie model

The name has been chosen for its similarity to a bow tie worn by some people in official and party settings. The bowtie illustrates intuitively how different initiating events can combine to create a hazardous event if preventive barriers are ineffective. Similarly, the consequences of hazardous events depend on the effectiveness

of the mitigative barriers. The list of outcomes, ranging from no harm to significant harm, constitutes the consequence spectrum.

Bow-tie analyses are often used to identify and visualize barriers to specific operations or facilities. The results of the analysis can be used to create a barrier panel (or display) that combines all barriers with the relevant key performance indicators (KPIs) pertinent to each barrier's status.

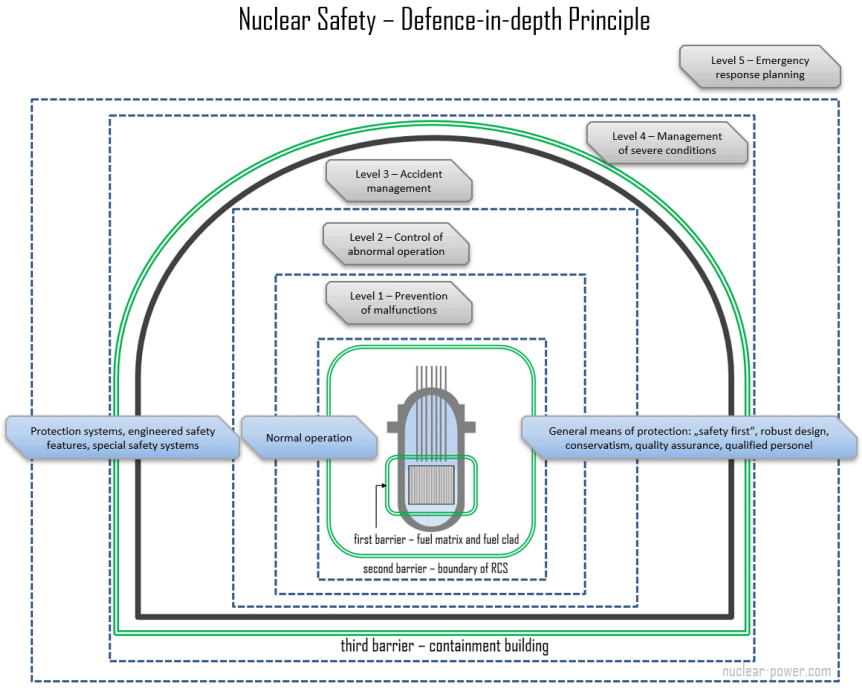


Fig. 13. **Defense in depth principle (from nuclear-power.com)**

6.6.3 Defense in depth

Defense in Depth is a strategy that involves establishing barriers, first introduced in the nuclear industry.

> The US Nuclear Regulatory Commission defines defense in depth as an approach to designing and operating nuclear facilities that prevents and mitigates accidents that release radiation or hazardous materials, where the key is creating multiple independent and redundant layers of defense to compensate for potential human and mechanical failures so that no single layer, no matter how robust, is exclusively relied upon.

Several types of defenses are mentioned, including access controls, physical barriers, redundant and diverse key safety functions, and emergency response measures. Fig. 13 illustrates the five primary defenses associated with a nuclear power plant.

6.6.4 Layers of protection

The process industry has adopted the layers-of-protection model as its preferred way to illustrate defense-in-depth for process facilities.

> **Layers of protection:** A defense-in-depth approach to risk reduction, often illustrated in an onion-like structure, with the inner layers being inherently safe design measures and process control, and the subsequent layers being preventive and mitigative barriers.

The onion-like structure is illustrated in Fig. 14, with a variant in Fig. 15, inspired by Goel et al. (2017),. It shows how a process upset may progress into more serious pressure buildups if some of the layers are not functioning as intended:

- With adequate process design, the pressure may decrease again; however, if not, the process control system will attempt to maintain the same level.
- Failing to reduce the pressure may trigger an alarm, allowing operators sufficient time to intervene, for example, by manually initiating tasks through the process control system or by manually operating valves in the field. The intervention often relies on information from and interaction with the process control system, meaning that the two layers are not fully independent.
- If the effort is insufficient, the SIS or PSD system is triggered at a given set point. If the response is not adequate or too late, the mechanical relief valves (PSVs) will open.
- When PSVs open, gas is routed to the flare system, and the pressure inside the tank or pipe is reduced.
- If PSV fails, the pressure may exceed what the process equipment can tolerate, leading to a leakage of gas that may be ignited. The F&G system detects the leakage while the ESD system will remove energy sources and shut down the complete facility. In the two illustrations, ESD & F&G are identified as separate sequential layers and separate but potentially acting at the same time in the sequence, because it is their totality of functions that can stop the continued escalation.
- Passive protection measures include systems that collect spills or isolate hot surfaces.
- Firefighting can mitigate further development and give more time for evacuation.
- In the event of environmental spills and casualties, an emergency response team must be mobilized.

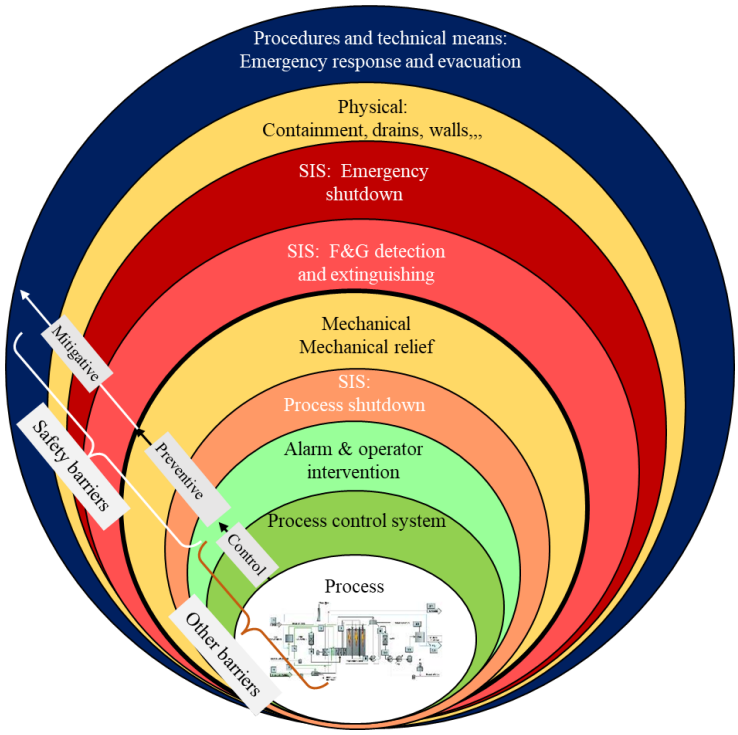
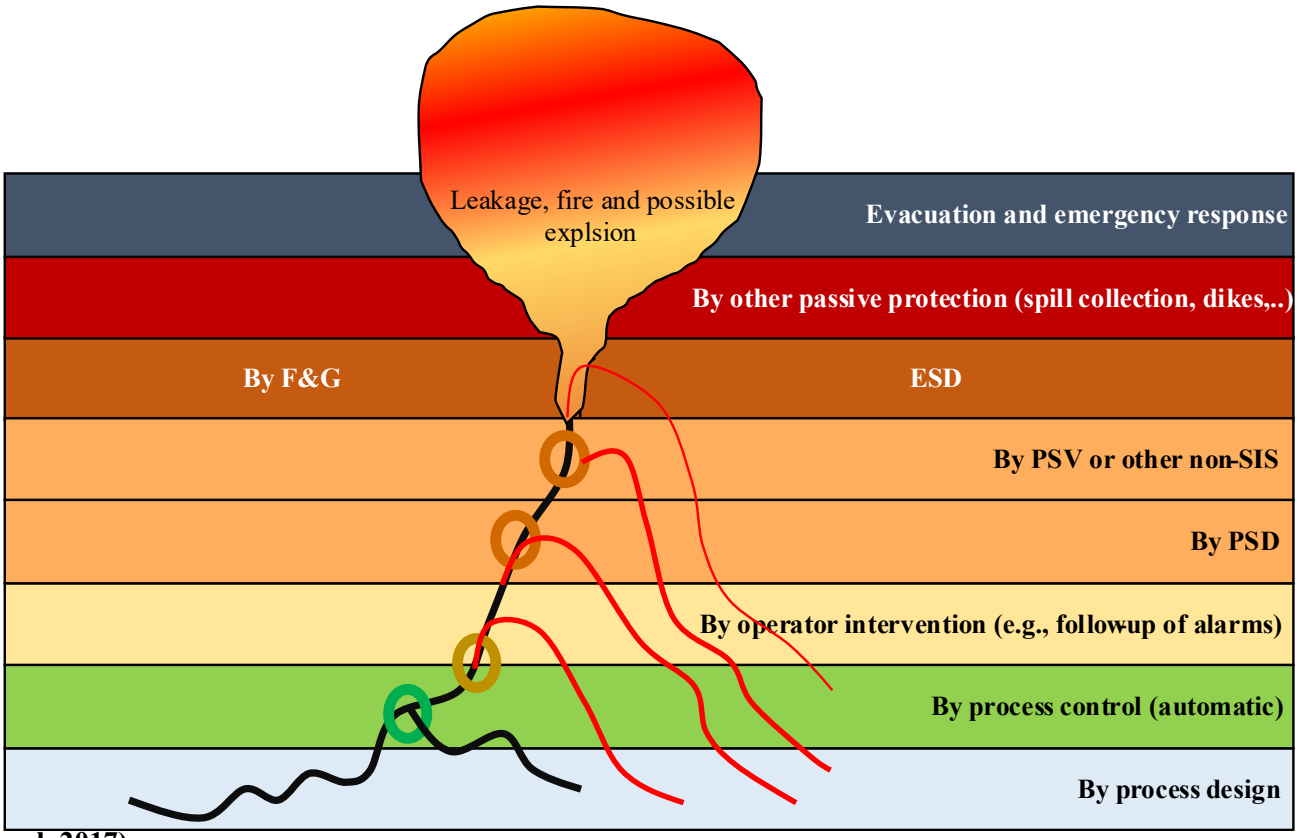


Fig. 14. Layers of protection

	A PSV performs a safety function but is not SIF as no E/E/PE technologies are involved in its activation. How does a PSV work? Watch this short video on YouTube for spring-operated (loaded) and this webpage for pilot-operated (loaded).

The process industry has developed a structured method for determining the reliability requirements for each layer, known as the layers-of-protection analysis (LOPA) method. LOPA is performed after the hazards and risk assessments, for example, after having completed a hazards and operability study (HAZOP), and the results of the hazards and risk analysis become input to the LOPA analysis.



al, 2017)

6.7 Examples of regulatory requirements

SIS systems are subject to legal and regulatory requirements due to their role in preventing harm to people, the environment, and critical societal assets. The content and focus of regulations and standards are dependent on the industrial application area. The Norwegian Petroleum Safety Authority (PSA), renamed Havindustritilsynet as of January 1, 2024, oversees regulations for the petroleum sector and CO2 capture, storage, and injection, covering both offshore and onshore facilities associated with the oil and gas industry. Other land-based industries are regulated by the Norwegian Directorate for Civil Protection (DSB). While HAVTIL has its own set of regulations, DSB refers to lovdata.no, where the user must identify themselves to determine which ones are applicable.

We are using the Ocean Industry Authority (HAVTIL) regulations to illustrate how regulations applicable to petroleum and CO2 are formulated. For example, HAVTIL refers to IEC 61508 and IEC 61511 as applicable for implementing authority requirements related to SIS. In contrast, the Norwegian Directorate for Civil Protection (DSB) (regulating onshore industries) does not, meaning that other land-based industries can make their own choice on the use of these standards.

HAVTIL also makes reference to safety-relevant national standards, for example, on technical safety with NORSOK S-001 (2021), automation systems with NORSOK I-002 (2021) and the Norwegian Offshore guideline Offshore Norway GL 070 (2026) on the application of IEC 61508 and IEC 61511.

Other SIS related standards are IEC 62061 (2021) and ISO 13849 (2023), two standards applicable for machine builders to be compliant with the EU Machinery Directive (Directive 2006/42/EC, 2006). Railway signaling systems in Europe follow the three European Norms (which also have their IEC variants); EN 50126 (2017), EN 50128 (2017), and EN 50129 (2018). The automotive industry uses ISO 26262, not because of any regulation, but because of the usefulness of having common standardized approaches and requirements to functional safety. ISO 26262 consists of 10 parts, including ISO 26262-1 (2018) and ISO 26262-2 (2018).

Chapter 9 on functional safety will introduce some of the requirements for SIS design, with a focus on IEC 61508 and IEC 61511. The remainder of this chapter (6) will focus on concepts and properties relevant to this context.

6.7.1 HAVTIL requirements for barriers

Clause 5 of the Management Regulations outlines the general requirements for barriers, which apply to technical, operational, and organizational barriers.

Management Regulations § 5 Barriers

Barriers shall be established that at all times can
a. identify conditions that can lead to failures, hazard, and accident situations,
b. reduce the possibility of failures, hazard and accident situations occurring and developing,
c. limit possible harm and inconveniences.

Where more than one barrier is necessary, there shall be sufficient independence between barriers.
The operator or the party responsible for operation of an offshore or onshore facility, shall stipulate the strategies and principles that form the basis for design, use and maintenance of barriers, so that the barriers' function is safeguarded throughout the offshore or onshore facility's life.
Personnel shall be aware of what barriers have been established and which function they are intended to fulfil, as well as what performance requirements have been defined in respect of the concrete technical, operational, or organisational barrier elements necessary for the individual barrier to be effective.

Personnel shall be aware of which barriers and barrier elements are not functioning or have been impaired.
Necessary measures shall be implemented to remedy or compensate for missing or impaired barriers.

The regulatory text outlines some key principles or requirements for safety barriers:

- The safety barriers shall have the capability to detect and interact.
- Safety barriers shall be independent of each other to a sufficient level, meaning that it must be unlikely that the failure of one barrier has an impact on the others.
- People, such as operators, maintenance technicians, and support engineers, shall be aware of which barriers are in place, their status, performance requirements, and if they are temporarily put out of service.
- If safety barriers are out of service, there must be compensating measures.

6.7.2 HAVTIL requirements to safety functions

Requirements for technical safety systems are found in clause 8 of the Facilities Regulations. These requirements apply to all safety functions, including active safety functions, such as SIFs, and align well with the structure of a typical SIF (detect, decide, and act) and SIFs being placed in different SISs (prevent vs mitigate).

Facility Regulations §8 Safety functions

Facilities shall be equipped with necessary safety functions that can at all times
a. detect abnormal conditions,
b. prevent abnormal conditions from developing into hazard and accident situations,
c. limit the damage caused by accidents.

Requirements shall be stipulated for the performance of safety functions.
The status of active safety functions shall be available in the central control room.

6.7.3 HAVTIL requirements relevant to PSD systems

Requirements for processing safety systems are outlined in Clause 34 of the Facilities Regulations. For this system, two independent layers are required, and the guideline suggests that they should rely on diverse technologies. The most common approach is to combine an instrumented SIS system, known as a process shutdown system (PSD), with a mechanical (self-opening) pressure safety valve (PSV).

Facility Regulations §34 Process safety system

Facilities outfitted with or attached to process facilities, shall have a process safety system. The system shall be able to perform the intended functions independently of other systems. The process safety system shall be designed such that it enters or maintains a safe condition if a fault occurs that can prevent the system from functioning. The process safety system shall be designed with two independent levels of safety to protect equipment.

There are scenarios when PSVs cannot be installed, and the second level of protection must be SIS. To maintain two independent levels of protection, a second SSI, often referred to as High Integrity Pressure Protection System (HIPPS) may be introduced. To avoid vulnerability to common-cause failures (CCFs), some diversity is necessary in addition to having separate sensors, controllers, and actuated devices. For example, the use of different types of sensors in PSD and HIPPS, if applicable, or different types of controllers, such as solid-state or hardwired logic for the HIPPS system and a programmable safety controller for the PSD system.

6.7.4 HAVTIL requirements for F&G systems

Requirements for processing safety systems are outlined in Clause 32 of the Facilities Regulations.

Facility regulations §32 Fire and gas detection system

Facilities shall have a fire and gas detection system that ensures quick and reliable detection of near-fires, fires, and gas leaks. The system shall be able to perform the intended functions independently of other systems. In the event of fire or gas detection, automatic actions shall limit the consequences of the fire or gas leak. The placement of detectors shall be based on relevant scenarios and simulations or tests.

The regulations emphasize that the correct placement of detectors is crucial for reliable detection. This also requires experimental analyses and simulations to investigate how wind direction, air currents, and equipment placement in the area affect the flow of gas and smoke. A smoke development or gas cloud may move differently depending on whether the area is naturally ventilated, wholly or partially enclosed, and the presence of obstacles, such as other equipment, in the area.

6.7.5 HAVTIL requirements for ESD system

Requirements for processing safety systems are outlined in Clause 33 of the Facilities Regulations.

Facility regulations §33 Fire and gas detection system

Facilities shall have an emergency shutdown system that can prevent the development of hazard and accident situations and limit the consequences of accidents, cf. Section 7. The system shall be able to perform the intended functions independently of other systems.
The emergency shutdown system shall be designed so that it enters or maintains safe conditions if a fault occurs that can prevent the system from functioning. The emergency shutdown system shall have a simple and clear command structure. The system shall be capable of being activated manually from trigger stations that are in strategic locations on the facility. It shall be possible to manually activate functions from the

manned control centre that bring the facility to a safe condition independently of the parts of the system that can be programmed.
Emergency shutdown valves shall be installed that can stop streams of hydrocarbons and chemicals to and from the facility and to and from wells, and which isolate and/or partition the fire areas on the facility.

By reading the regulatory text, we find that:

- Unlike the PSD system, the ESD system must be manually activated. Push buttons must be placed in strategic locations at the plant. On an offshore oil and gas platform, this will occur on different decks and areas of the process, including the control room, the vicinity of the lifeboats, and the helicopter deck. For onshore facilities, push buttons are in the control room and various areas of the processing facility.
- The ESD system must have a manual activation option that is independent of the programmable systems. This requirement has been met by introducing a critical action panel (CAP) in the control room, where signals are routed one by one from the I/O cards and into the CAP panel buttons and lamps.
- Simplicity and clarity are advocated so that the system is easy to understand and, thereby, possible to monitor its status.

6.7.6 HAVTIL Requirements for ignition source control

Ignition source controls are functions that remove ignition sources capable of igniting flammable gas mixtures. The requirements address (i) how the electrical devices are designed to avoid the generation of sparks or the spreading of sparks to the environment, (ii) disconnecting the power supply to consumers that can be ignition sources, and (iii) measures that keep the temperature below the ignition temperature of gas mixtures. Some of the ignition control functions (i.e., ii) are implemented in the ESD system.

Facility regulation §10b Ignition source control

In order to prevent and protect against ignition of combustible liquids and explosive gases, a systematic mapping of potential electric and non-electric ignition sources shall be performed. In addition, the necessary technical, operational, and organisational measures shall be implemented so as to reduce the risk of ignition as far as possible.
Equipment and safety systems in classified areas shall fulfil requirements for use in explosive areas. For permanently placed facilities, equipment and safety systems in all areas where explosive atmospheres can be formed, shall be selected on the basis of the categories stipulated in Regulations relating to equipment and protective systems intended for use in potentially explosive areas (in Norwegian only), Annex I.
Equipment and safety systems that are meant to be operational in abnormal situations, where an explosive atmosphere can exist outside classified areas, shall fulfil requirements to zone 2, minimum, or be placed in protective rooms. Other non-critical equipment that represents an ignition source, shall deactivate automatically on gas detection, but manual deactivation shall also be possible when it is practical to do so from a central or strategic location, in accordance with the facility specific strategy for fire and explosion safety.

6.7.7 HAVTIL CO2 regulations

HAVTIL has published separate regulations for CO2 facilities, specifically addressing onshore CO2 storage, transport, and injection. Among these, clause §15 concerns safety functions and safety systems. The text includes selected principles from petroleum regulations, but the wording suggests greater flexibility, given that the risks are lower than in hydrocarbon systems.

6.7.8 Example where independence is partially implemented

The requirement that ESD, PSD, and F&G systems be independent of other systems would ideally imply the use of diverse technologies, such as systems from different manufacturers.

However, practical considerations often determine what constitutes a sufficient level of independence, considering system complexity, the feasibility of installing additional equipment, available space, and other factors. For example, in areas where there are several valves available to stop the flow, it is sometimes accepted that some of these valves are shared between PSD and ESD, as shown in Fig. 16. Here, Offshore Norway GL 070 (2026) explains the conditions as follows:

- ESD and PSD activate the shutdown valve via separate solenoid valves
- The arrangement of ESD and PSD solenoid valves is such that the ESD system maintains its ability to close the shutdown valve when the PSD solenoid valve fails.
- The valve position is reported back to the PCS system and is not part of the safety function.

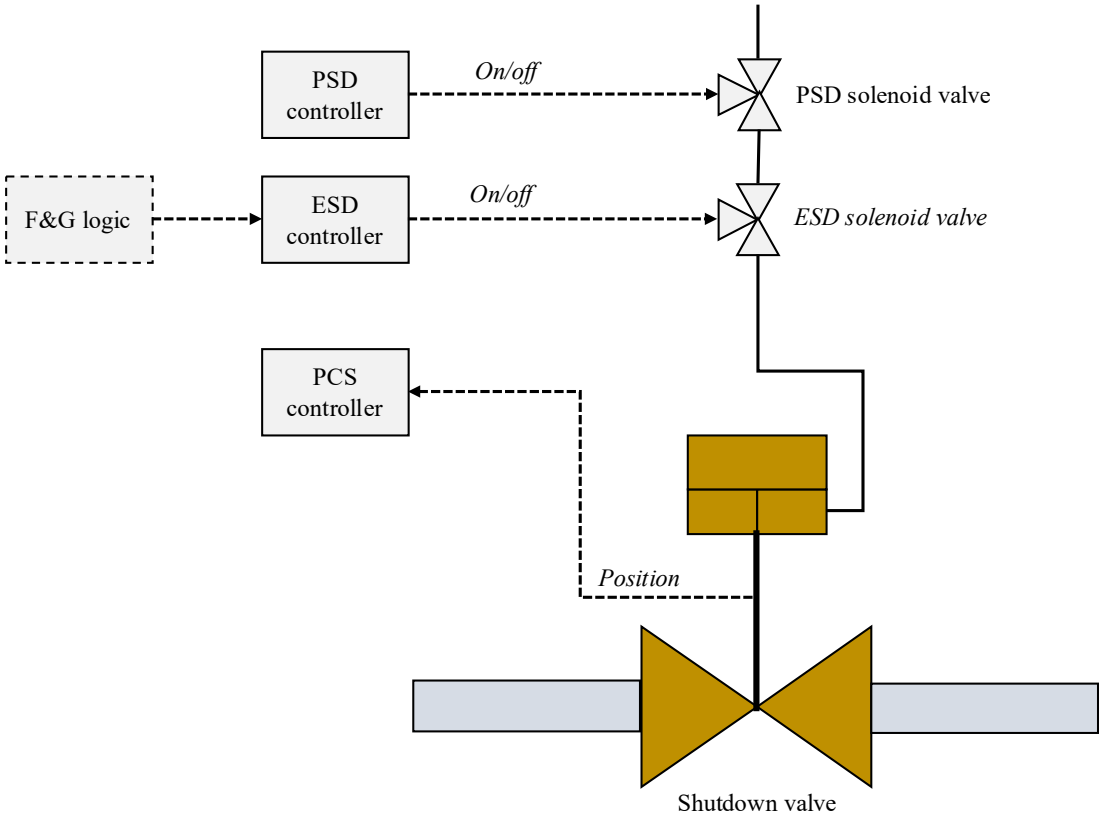


Fig. 16. ESD and PSD system sharing the same valve (GL 070)

Using the same types of devices across systems, such as the same solenoid valve for PSD and ESD activation, requires a focus on avoiding systematic failures. Systematic failures arise from errors in design (for example, selecting a level transmitter with insufficient range), installation (for example, mounting in conflict with the manufacturer's recommendations), and maintenance (for example, applying the calibration procedure incorrectly). Systematic failures are likely to occur if errors are not identified and corrected. Regular and adequate training, audits, and supervision are therefore measures to achieve independence.

6.8 SIS design principles

The standards on functional safety, like IEC 61508 (2010) and IEC 61511-1 (2016) have several requirements that determine the details of the SIS design, such as device selection, redundancy, and fail-safe implementation, among others. IEC 61508 and IEC 61511 employ a risk-based approach, meaning that the SIS design is

influenced by the reliability requirements of the associated functions (SIFs). Here, we introduce some general design concepts relevant to SIS.

6.8.1 Redundancy

Using redundancy to enhance the ability to perform safety functions is a commonly employed design principle in SIS systems. In contrast, in control systems, it is less common unless redundancy is needed to improve availability during operation.

> **Redundancy:** More than one physical device (hardware), network/communication link, or programmed function (software) that can perform the same function.

The ideal redundancy is implemented with diverse technologies. In this way, it is highly unlikely that the same type of fault, event/exposure will affect redundant systems or devices. However, diversity is not always practical or possible, and a more common alternative is to use identical devices. For example, use two identical controllers to execute the same functions in parallel. The use of identical devices requires extra attention to training, awareness, and the adequacy and correctness of operation and maintenance procedures, as well as analysis of reported failures to prevent their recurrence.

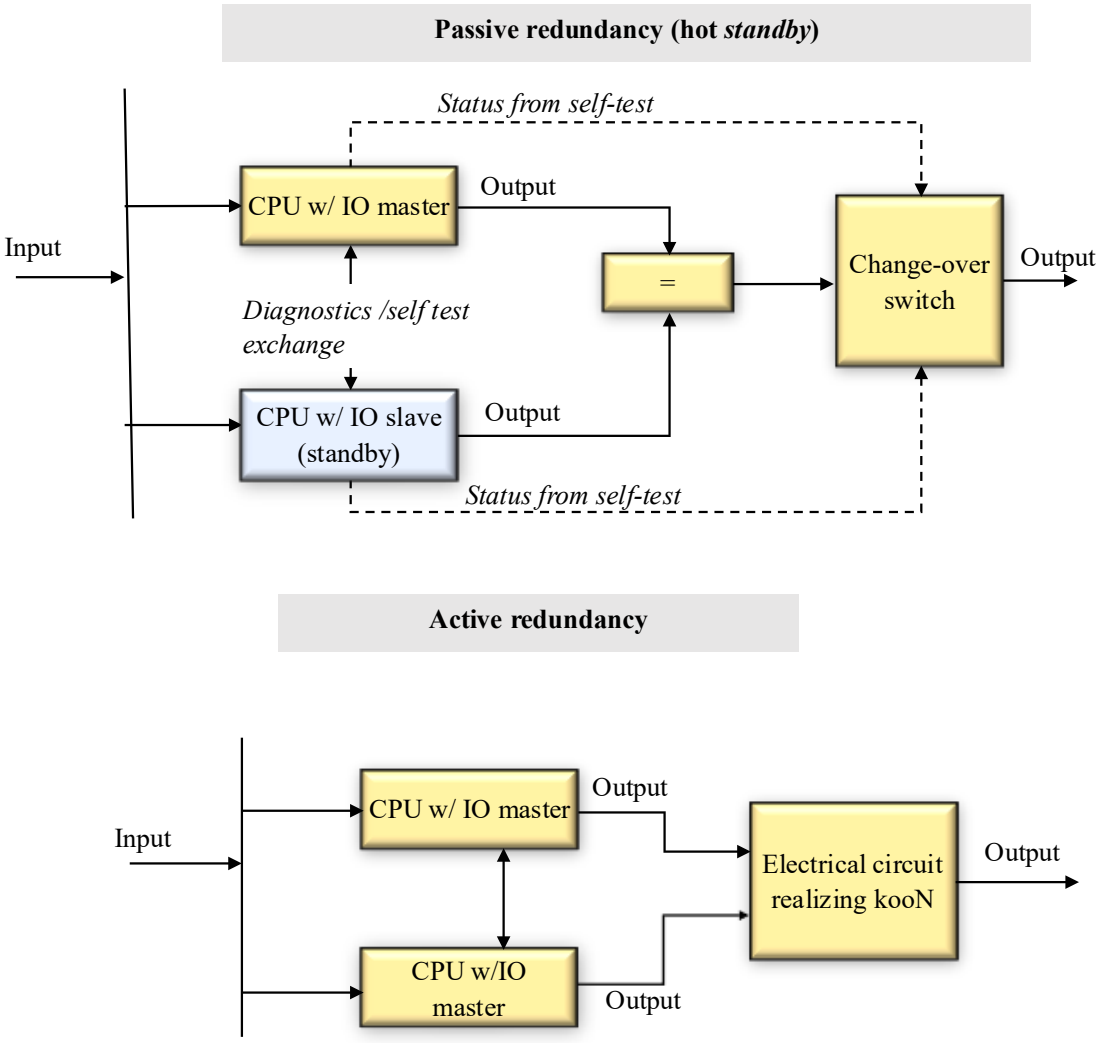


Fig. 17. Passive vs active (hot) redundancy (of controllers)

Redundancy may be implemented as either passive or active. Active means that the redundant components are always performing their functions, and the voting or mounting of the components determines how the results

are treated. Passive redundancy occurs when some redundant components do not participate in decision-making unless required to take over when the active components fail. Active redundancy is the most common strategy for field devices, while controllers can apply both strategies, as shown in Fig. 17.

Passive redundancy for controllers, here with a focus on the central processing units (CPUs), is characterized by:

- Two or more CPUs are running in parallel, but only one of them participates in executing commands
- Shifts in each cycle between being master and slave
- Checking themselves and each other.
- Only the healthy controller is allowed to place a command.

Passive redundancy involves a self-test on the active, running CPU. Upon detecting a fault, the redundant unit (slave) CPU is instructed to start up and assume the master function. The changeover can be repeated if the faulty CPU has been upgraded or replaced. Self-checking includes:

- Own health check (both CPUs)
- Exchange of health checks
- Comparison of outputs

The implications of choosing passive redundancy are that:

- One must trust that the internal self-check has a high diagnostic coverage (DC)
- This type of redundancy is primarily to improve system uptime and not for safety. The configuration remains as a 1-out-of-1 (1oo1) ("single") configuration from a safety standpoint.

With active redundancy, shown in Fig. 17, both CPUs are executing their functions as masters, and a voting arrangement is necessary to determine the resulting action. Voting for two active redundancy CPUs can be implemented in two ways: both controllers must agree to act, resulting in 2oo2 voting, or it is sufficient for one controller to issue an activation command, resulting in 1oo2 voting. For safety, 1oo2 is generally better than 2oo2, as a single CPU can continue operating if the other fails.

6.8.2 Voting

The decision taken by the logic solver on how to act on the input signals (or sensor values) is determined by how the input values are voted.

- Being voted means that a certain number of inputs (K) of all inputs (N) will trigger an action, and this is referred to as K-out-of-N voting.

The action can focus on safety or on keeping the process running. In this course, we always relate voting to safety.

Voting is, strictly speaking, not limited to what action the logic solver takes. It can also be the result of how the final elements activated by the logic solver are physically installed. For example, two shutdown valves installed one after the other in the same pipeline are always voted 1oo2, meaning that the flow stops if either valve closes, regardless of how the inputs are voted.

To sum up, and related to SIS systems, voting is typically applied for:

- Of logic solvers
- Of individual systems within the logic solver, such as:
  - CPUs
  - Input and output cards
- Sensors, such as transmitters, detectors, and pushbuttons (often implemented in the application program of the logic solver)
- Actuated devices, such as solenoid-controlled valves, on/off valves, and switches, are based on how the devices are physically installed.

6.8.3 Fault tolerance

If we know the "K" and "N" values for a redundant system, we can also express its fault tolerance. A kooN system will tolerate N-K faults but will fail if the number of faults exceed N-K+1.

Each subsystem may have its own voting, even if sensor voting is implemented by the application program, since the comparison of measurements is performed there. Fault tolerance is therefore a property of a subsystem determined by the chosen voting. While individual devices can have fault tolerance built into their software, we use it more often in hardware architecture.

> **Hardware fault tolerance:** The maximum number of failed devices (hardware) tolerated by a subsystem without losing the ability to perform its function, in our case, the SIF function.

The fault tolerance can be calculated as N-K for a KooN-voted subsystem. For example, the fault tolerance of a 1oo3-voted system is 2, meaning that the subsystem can still perform its function in the presence of two faults. A 1oo1-voted system tolerates no failures and has a fault tolerance of 0.

6.8.4 Built-in self-test

Self-testing, also referred to as diagnostics, is used to detect internal faults in the application program, its execution, and the hardware. Some of the self-test concepts are explained in IEC 61131-6 (2012), appendix B.

> **Self-test:** Various functions are implemented to enable the device to detect faults, notify users via alarms, and (in some cases) perform corrective actions or transition to a safe state.

Examples of what a self-test can focus on are:

- All instructions, flags, addresses, and registers are correct (CPU).
- That all parts of the program in the CPU are run through.
- Execution time within min/max time.
- In case of built-in redundancy: Comparing inputs and/or output values.
- Pulse test of the output, with read-back to check if the output changes and gets the intended effect.
- Link the known value on the input instead of the process value.

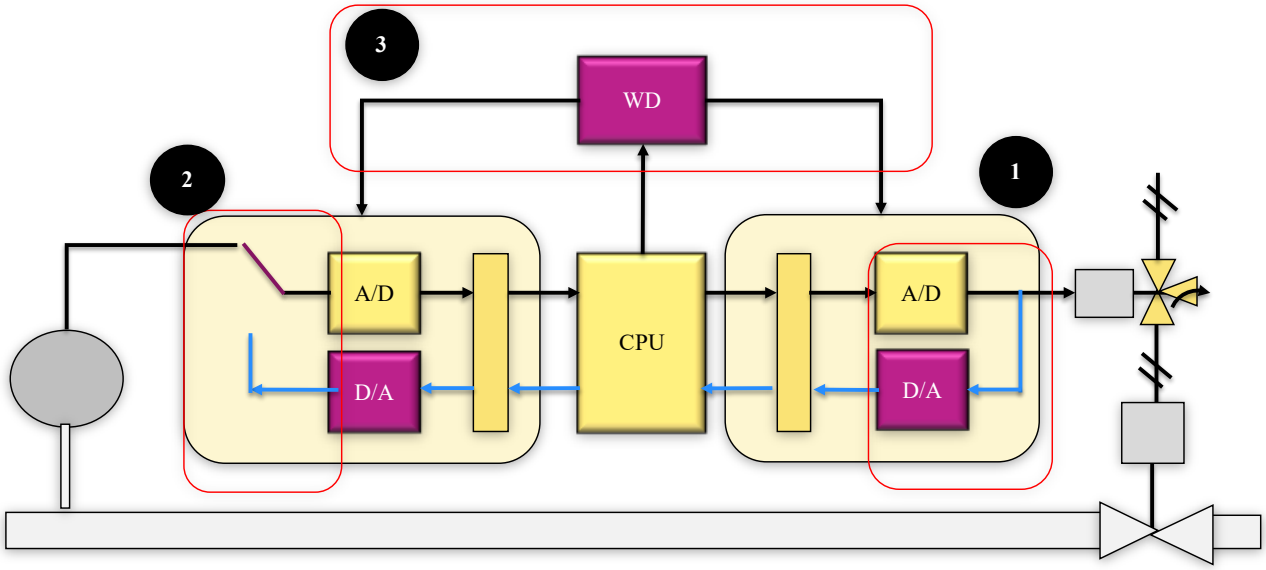


Fig. 18. Self-tests examples for logic solver

Fig. 18 illustrates three different types of self-tests that may be implemented with a logic solver:

1. Compare with known value (input). Verify that the input card is functioning correctly by reading back the value.
2. Pulse test: Rapid polarity changes on output card (in milliseconds) – long enough to read back and check that the output has changed.
3. Use of a separate component (often called a watchdog) to detect if exceeding a certain response time and/or loss of pulsed clock signal.

The proportion of faults that can lead to the loss of a safety function but are detected by online diagnostics is defined as the diagnostic coverage (DC). More precisely, we define DC as:

$$DC = \frac{\lambda_{DD}}{\lambda_D}$$

Here, λ_{DD} is the dangerous detected (DD) failure rate, and λ_D is the total rate of dangerous failures. A dangerous failure prevents the safety function from being performed. The DC value of an SIS controller is often 80-99%, while SIS sensors are 70-90%. Shutdown valves have limited diagnostics, and the DC is often 0. The inability to achieve a high DC value is compensated for by a high probability of entering the safe state upon failure, resulting in a high degree of fail-safe performance.

Additionally, field devices, such as transmitters and valves, may have built-in diagnostics and are then referred to as smart or intelligent devices.

6.8.5 Fail-safe design

A fail-safe device has already been introduced. In some cases, it is useful to introduce a complementary term: fail-safe *design*.

Fail-safe design: A Collection of measures that can be implemented to achieve fail-safe capability.

Fail-safe design refers to a set of measures, rather than a single measure, with the aim of achieving a fail-safe device or fail-safe system of devices. For example, a fail-safe device implements physical or programmed measures to ensure fail-safe operation, such as a spring return for a valve or switch, or the combination of a normally energized control signal (NE) with a normally open (NO) contact.

The list of possible measures to apply is quite long, and a fail-safe design is characterized by having chosen several of them:

- Redundancy
- Selecting high-reliability components (long service life)
- Design principles where foreseeable faults result in the transition to the safe state (e.g., spring return for valves, loss of signal from the transmitter(s) automatically provides activation of the safety function)
- Applying safety margins for temperature, noise, vibration, etc.
- Alarms and notifications of detected faults
- Built-in self-test/diagnostics (manual or automatic initiated)
- The possibility of automatic or manual compensation for detected faults. For example, change from 2oo3 to 1oo2 voting if one fault is detected since a 1oo2 is more reliable than 2oo2.
- Built-in tolerance to human error (layout control center, interlocking against errors in device operation)
- The design work process, i.e., activities directed to avoid introducing errors and detecting errors so that they are corrected before the device is installed. General measures for quality assurance and traceability in requirements, documentation, analyses, and tests are relevant here.
- Regular functional testing and inspections
- Applying systems for condition monitoring (where relevant)
- Replacement of the device before it reaches the end of its service life or checking whether the device can be expected to have a longer service life than initially assumed.

A fail-safe design does not guarantee 100% fail-safe operation, but implementing a combination of them increases the likelihood of achieving this important property.

6.9 SIS in railway industry

The railway industry does not use the term SIS but implements safety systems that rely on the same types of technologies, i.e., electrical, electronic, and programmable technologies developed specifically for use in safety applications. The most important of these is the railway signaling system, and, although not the correct term, we will refer to it as the railway version of SIS.

Railway signaling systems control the movement of trains, rail switches, and rail crossings. Each of these operations is safety-critical, as a wrong decision may lead to train collisions, derailments, and collisions at level crossings. Since operations are always required, we can define railway signaling systems as Safety Instrumented Systems (SISs) operating in a high-demand mode.

Some of the material explained here is based on Bane Nor's technical requirements. Signaling systems (outside train stations) are configured for either double-track types, in which each track allows trains to move in only one direction, or for single-track systems, in which trains can move in both directions. Here, we focus primarily on the single-track systems found in most areas with railway transportation in Norway.

6.9.1 Distributed control and track sections

The railway signaling system is a form of distributed control. The rail track between two defined sites, for example, two train stations, is split into rail block sections (In Norwegian: blokk or seksjon) that are controlled separately. Each section will have its own entrance and exit light signal masts, as illustrated in Fig. 19.

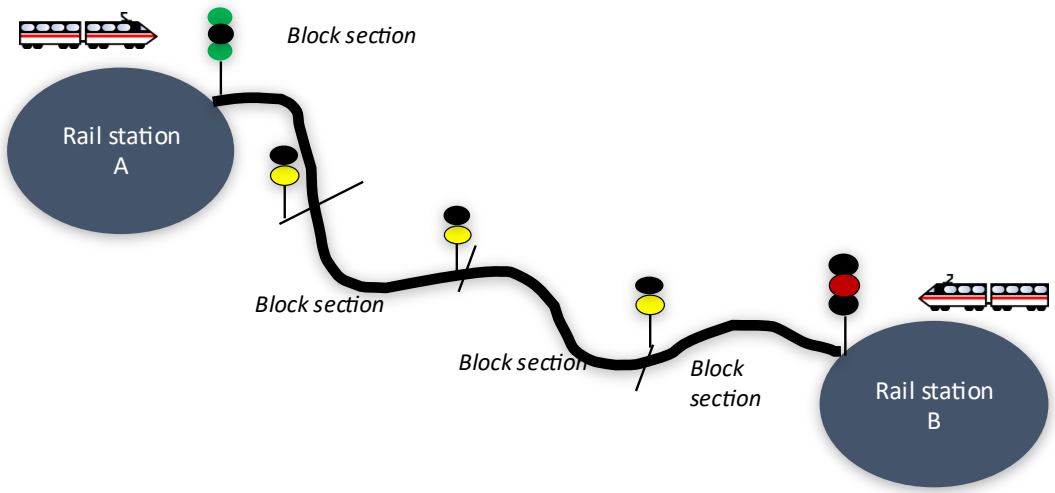


Fig. 19. Rail tracks and sections

The signal can indicate either “drive” (green), “stop” (red), or a combination of yellow (blinking or non-blinking) as a pre-warning. The signal can be of different types:

- Main signal: The mast-mounted signal lights how the signal for either allowance to enter (alternatively, exit) the block section
- Pre-signal: The mast-mounted signal light (often as a beacon, i.e., flashing light) shows what signal to expect when entering the next block section using prewarning signals

Most light signals are provided by two or three bulbs. The tree bulb type is used near the station, as an extra bulb is needed to inform the train driver if the train is moving straight into the station or using a deviating track (parallel). The red signal is always provided by one bulb, while the green light can be provided by one or two bulbs, depending on the specified conditions for how the train enters the station. For more details about railway signals, refer to Bane Nor's technical regulation for light signals.

Traditionally, light signals have been physically mounted on masts near the tracks. In the new European railway signaling systems being introduced to Norway, which are discussed in more detail later, the masts are removed from the tracks and the light signals are only displayed only on the train's operator panel or at the location where the train is operated from (if unmanned).

6.9.2 Railway signaling subsystems

The traditional railway signaling system consists of subsystems shown in Fig. 20, with some pictures of field devices in Fig. 21. The yellow-colored subsystems are safety-critical, meaning they must comply with safety standards and be assessed and approved by an independent body or organization. In contrast, the train operation center has the authority only to request, not to overrule, the railway signaling system.

The Bane Nor technical regulations do place requirements on individual SIF, meaning safety functions end-to-end, for each subsystem. These are referred to as "Sikkerhetskritisk funksjon" (SKF), and they are numbered as shown in Fig. 20.

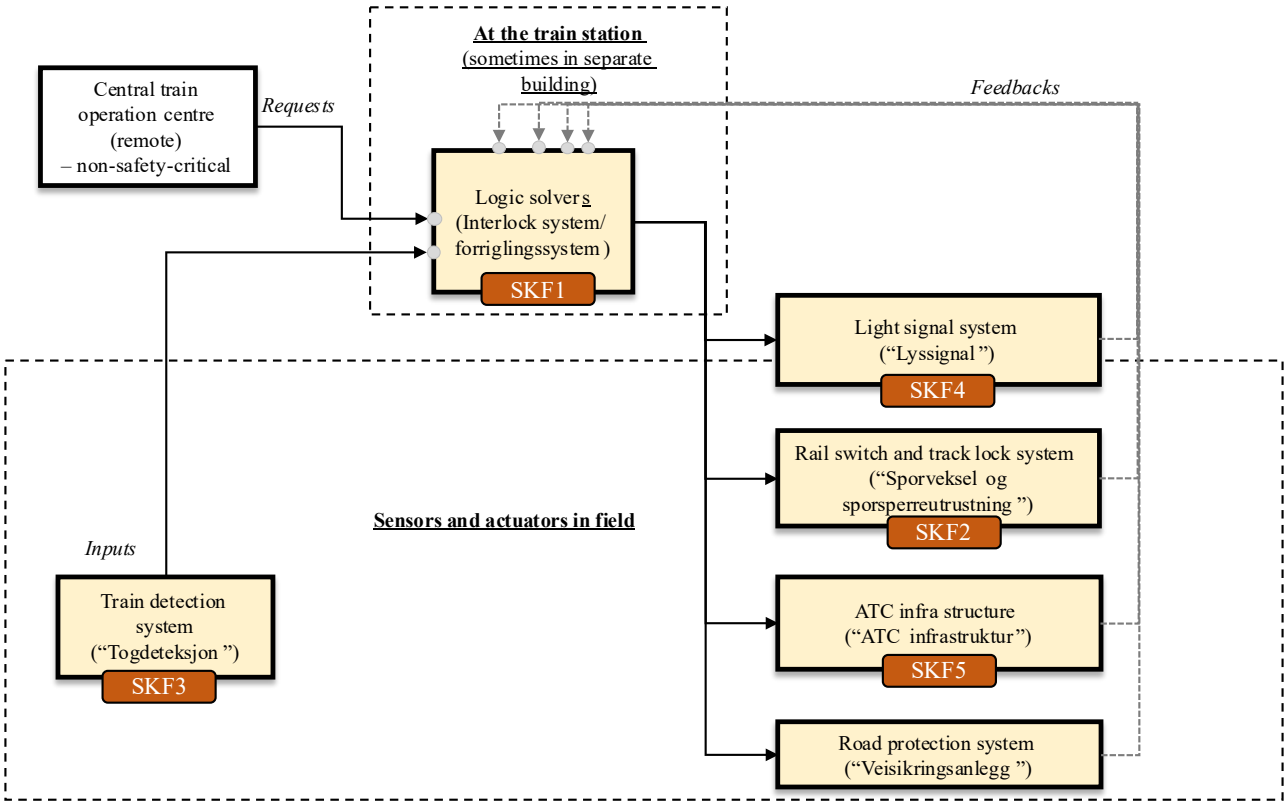


Fig. 20. Railway signaling subsystems (traditional)

Each of the SKFs may be explained as follows:

- Logic solvers, also called interlocking systems, (i) receive requests for train movement according to a schedule from the central train operation center, (ii) receive information about train position (from the train detection system), and (iii) send commands to the various systems needed to manage the safety of the train movement.
- Train detection system, sending information about the position of all trains.
    - Older train detection systems use short-circuit detection when a train is present in the block. The block may be split into several sub-blocks (in Norwegian, "sportfelt") with an electrical circuit that will short-circuit when a train is inside.

  - Newer train detection systems use a combination of axle counters that count the number of train wheels entering and exiting a block and in/aside-track balises that detect if a train is passing above.
- Rail switch and track lock system, which operates the rail switches and secures the rail block sections as needed for a particular movement of trains.
  - The position of a rail switch is changed by a motor mounted nearby.
  - Securing a block section involves verifying that the necessary conditions are met before allowing a train to enter. Conditions relate to the position of trains at, approaching, or exiting the block section, as well as the status of rail switches and the protection of level crossings.
- Light signal system, which provides the signals mentioned earlier for go/run, stop, and pre-warning.
- Automatic train control (ATC), consisting of balises and an onboard emergency stop system.
  - Balises are devices mounted on the ground in the middle of the rail tracks to perform in-track transfer of position to the train as it passes above. It also receives the state of light signals in the vicinity.
  - The emergency-stop system reads the information provided by the balises as the train passes by and activates the emergency stop if the train moves while the signal is red or if the train has not started to slow down according to the upcoming light signals.
- Road protection system for the operation of level crossings.

Bane Nor suggests quantitative requirements for all SKFs, and they have been translated into SIL requirements. The SKFs with the highest SIL requirement (SIL 4) are:

- SKF1: The logic solvers shall set correct outputs, given that the inputs are correct, for example, setting a green light signal when not supposed to or operating the rail switch when not supposed to)
- SKF2: The rail switch shall lock the switch and provide correct information to the logic solver about position and lock status.
- SKF3: The train detection system shall detect and report correct information about the availability of a specific rail block section.

The primary standards that frame the realization of the railway signaling system are EN 50126 (2017), EN 50128 (2017), and EN 50129 (2018). More details about these safety functions and others can be found in Bane NOR Technical Requirements. Pictures of some of the devices involved are shown in Fig. 21.

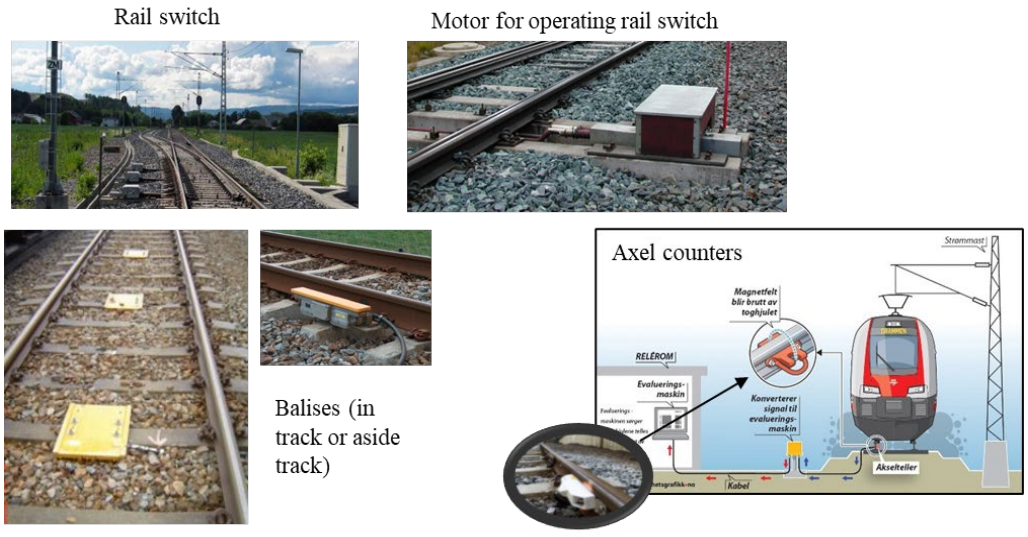


Fig. 21. Examples of in-field mounted systems

6.9.3 Example of logic solver configuration

The SIL 4 requirement implies exceptionally reliable logic solvers in a redundant configuration with fault tolerance of at least 1. Previously, it was an explicit requirement that independent teams develop diverse software applications, sharing only the same specification. A more common way now is to run the same software program, but with all outputs inverted on one controller.

The system architecture, with the logic controllers interacting with the field devices, varies depending on the control system supplier and the signaling system generation. The NSB-94 railway signaling system was among the first to use logic controllers and is still in use in Norway, awaiting replacement by the new European train control systems (ETC), which are widely used there. The "94" refers to the year the system type was first installed.

Fig. 22 is a simplified illustration of the NSB-94 system architecture for controlling green light.

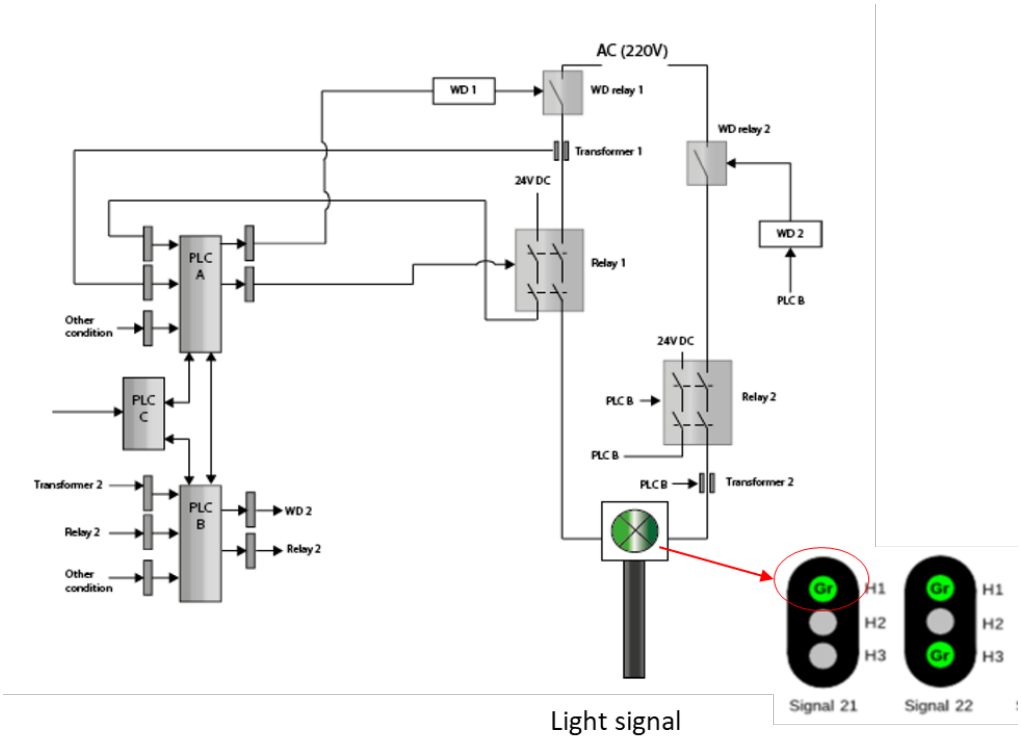


Fig. 22. Example of logic solver configuration

The conditions for approving and setting a green light is as follows:

- The request from the central operation center is received by a non-safety-critical controller, here named PLC C. The PLC submits a request to the two redundant safety logic solvers, here referred to as PLC A and PLC B.
- PLC A and PLC B must actively send a power signal high to a relay set that controls the current flowing through the light bulb.
- There is one relay set for PLC A and one for PLC B. The relays have double-contact sets, meaning two sets of switches are operated. Additionally, the relays have a primary contact set and a secondary contact set, with the secondary set replicating the operation of the primary set. PLC A and PLC B read the status of the secondary contact set as confirmation that the positions of the contact set correspond to the command given.
- If one of the PLCs (A or B) detects that conditions for setting the green light are not met, it will remove the signal to the relay, causing the contacts to open so that power is removed from the circuit feeding the light signal. The voting to remove the green light signal is therefore 1oo2, while it is 2oo2 for setting

the green light. This aligns well with using the most restrictive (fault-tolerant) solution for the most critical operation.

- The two PLCs also read the measured current in the primary circuit for the light signals. Finally, a watchdog, one for PLC A and one for PLC B, monitors the condition of the PLCs. In cases where a fault is detected, the watchdog will remove power from the circuit feeding the light signal.

6.9.4 ERTMS

Railway signaling systems have, until recently, not been harmonized across nations, for example, in Norway. If you study, for example, the look of light signals along the tracks in Sweden, you may notice that they differ from those in Norway. Europe has therefore developed the ERTMS system, the new European railway traffic management system. The goal is to establish a standardized signal system across Europe, thereby eliminating technical barriers to cross-border railway traffic.

The ERTMS system consists of the following sub-systems:

- European train control system (ETCS), which would be the new name for a railway signaling system
- GSM-R, the global system for mobile communication made for railways. It is worth noting that this system is also utilized in conjunction with existing railway signaling systems for messaging (SMS, phone) and data services. With ERTMS, GSM-R is used more actively to execute safety-critical functions.
- Common traffic management rules.

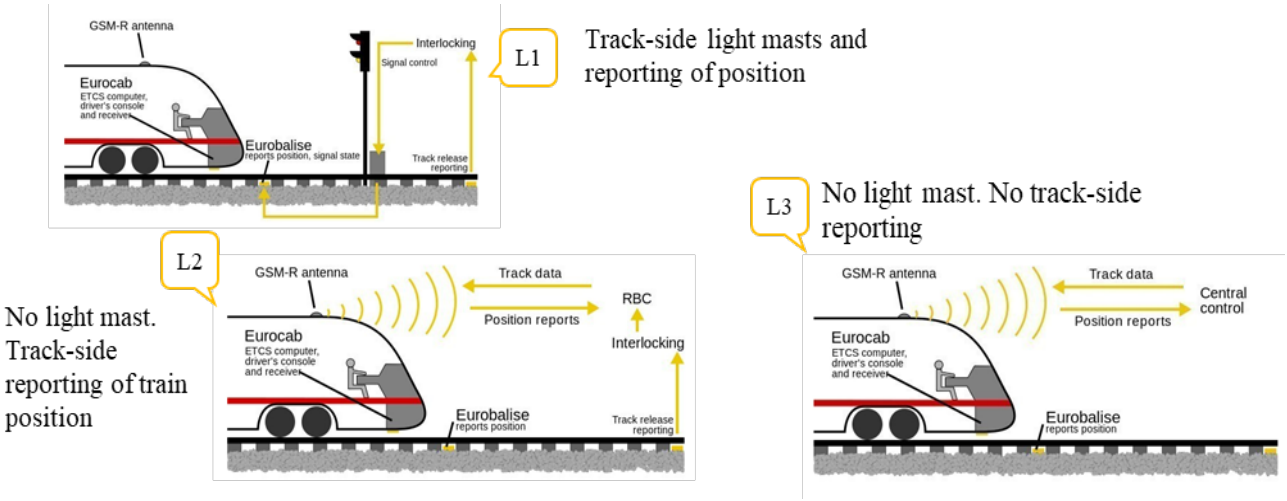


Fig. 23. ERTMS (or ETCS) levels 1,2, and 3

ETCS can be implemented at one of three levels: Level 1 (L1), Level 2 (L2), or Level 3 (L3).

- L1 is a partial implementation of ERTMS that combines ERTMS-compatible systems (on-board the train and at balises) with conventional signaling systems.
- L2 goes a step further by not using light masts. Instead, the light signals are displayed to the train driver via onboard displays. The position of the train is detected by axle counters and reported by Euro balises via the track-side railway signaling system and GSM-R communication.
- L3 is the most extensive implementation, also allowing the axle counter to be removed. The train detects its position using Euro balises and GSM tracking. L3 also implements dynamic section blocks, allowing the blocks to follow the train with a safety margin in front and at the back, calculated based on speed and braking curves.

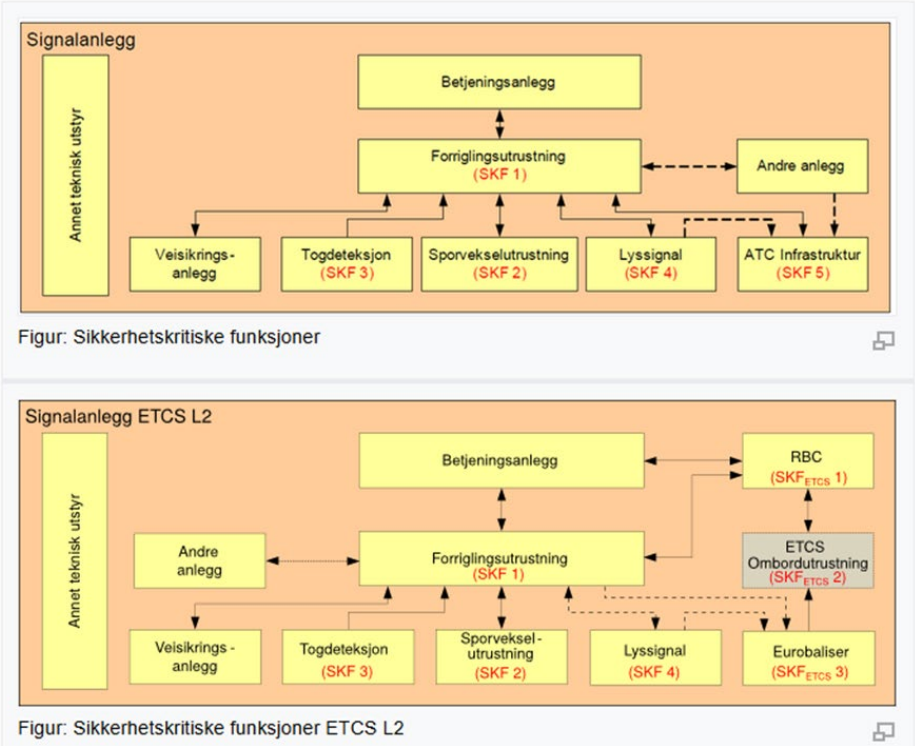


Fig. 24. Comparison of SKFs in traditional and new European (ETCS level 2) signaling systems

Norway is introducing ETCS L2, according to Bane Nor's webpages. Bane Nor has begun providing requirements for the ERTMS signaling system, ETCS, which can be found at https://trv.banenor.no/wiki/Signal/Prosjektering/ETCS. It is worth noting that some new SKFs have been introduced to accommodate the signaling system's new architecture, as illustrated in Fig. 24.

6.10 SIS for carbon capture and storage (CCS)

Carbon capture and storage (CCS) is a fast-emerging industry sector. The first CCS value chain in Norway has been Longship and covers:

- Ship transport of CO2 (as liquids) from the Heidelberg process plant in Brevik and the waste facility Celsio Hafslund in Oslo to the CO2 terminal in Øygarden (west coast of Norway)
- CO2 receiving terminal with ship port, buffer storage tanks, pumps, and heaters
- Pipeline to the offshore Johansen Formation south of the Troll field.
- CO2 injection well with control and instrumentation for the injection of CO2 into the subsurface reservoir (approximately 2600 meters below the sea floor).

Northern Lights, a partnership between Equinor, Shell, and TotalEnergies, is responsible for transporting CO2 from capture locations to the onshore receiving terminal, then to permanent offshore storage. The planned completion of the first phase of Northern Light's scope is 2024/25. This section builds on presentation material shared by Northern Light for external use.

Some details of the systems involved are shown in Fig. 25. The terminals have several storage tanks, each with control and pressure-protection systems, as well as pumps to transport CO2 into pipelines at a sufficient pressure to reach the offshore reservoir. The terminals have no flare system; in the event of an overpressure situation, which is rare, pressure relief valves will open to release the gases into the environment.

The onshore CO2 receiving terminal will be remotely operated and controlled from the Sture terminal located approximately 7 km away, while the offshore CO2 injection is remotely operated from one of the nearby

offshore facilities. The CO2 receiving terminal is powered from the local/community electrical distribution network.

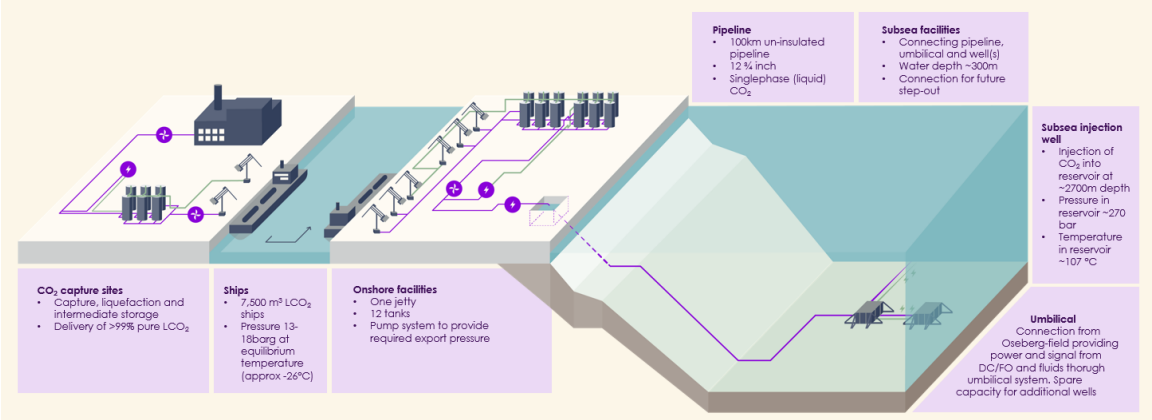


Fig. 25 Systems involved (Northern Lights)

6.10.1 Regulations and standards

The Longship system is subject to regulations from two Norwegian authorities:

- Directorate for Civil Protection ("DSB") that covers the onshore facility parts. DSB provides regulations aligned with EU directives on the Handling of flammable, reactive, and pressurized substances, as well as the equipment and facilities used in their handling. Through this regulation, the need to:
  - Perform a hazard and risk analysis
  - Apply IEC 61511, the sector-specific implementation of IEC 61508, in the design, implementation, and operation/maintenance of SIS
- The Ocean industry authority (In Norwegian: HAVTIL) has published a new CO2 safety regulation for the offshore part and the onshore receiving terminal sections related to pipeline operations.

6.10.2 Identified hazards and hazardous events

The need for SIS systems is identified in hazards and risk assessment. For example, the temporary storage and the export system within the stippled area in Fig. 26 may be split into several process related and areas specific EUCs.

Examples of hazards that may be identified include:

- Collects at low points: Potential for suffocation, even if not defined as toxic: CO2 is a heavy gas that may collect in low points (like ditches). Since the gas has no odor, it's difficult to detect its presence.
- Can reach low temperatures (< -78°C) if released from liquid form: Exposed equipment can freeze or degrade, and people may experience cryogenic burns.
- Boiling liquid expanding vapor explosion (BLEVE): This may occur if there is a leakage of CO2 stored or transported under high pressure. It may cause suffocation, flying debris, and pressure waves, potentially harming people and damaging equipment.
- Dry ice formation: This may occur if pressure is released into the environment, in the event of a leakage, or when the pressure relief valves open. It may harm people if inhaled and clog equipment, leading to malfunction.
- Material challenges:
  - CO2 has solvent properties that increase with temperature and pressure, leading to the potential degradation of gaskets. Gaskets are needed to keep flanges and connections on valves, tanks, and pipes tight, preventing CO2 from leaking.

  - Corrosiveness: CO2 in contact with free water becomes corrosive and may cause corrosion of affected equipment.
- Static electricity: CO2 flow, especially dry ice particles, may cause static electricity that can be an ignition source if it is close to other process facilities that involve flammable substances. A key learning point from the CO2 test center at the Mongstad refinery was that the proximity of CO2 systems to hydrocarbon systems necessitated costly measures to mitigate ignition risks.

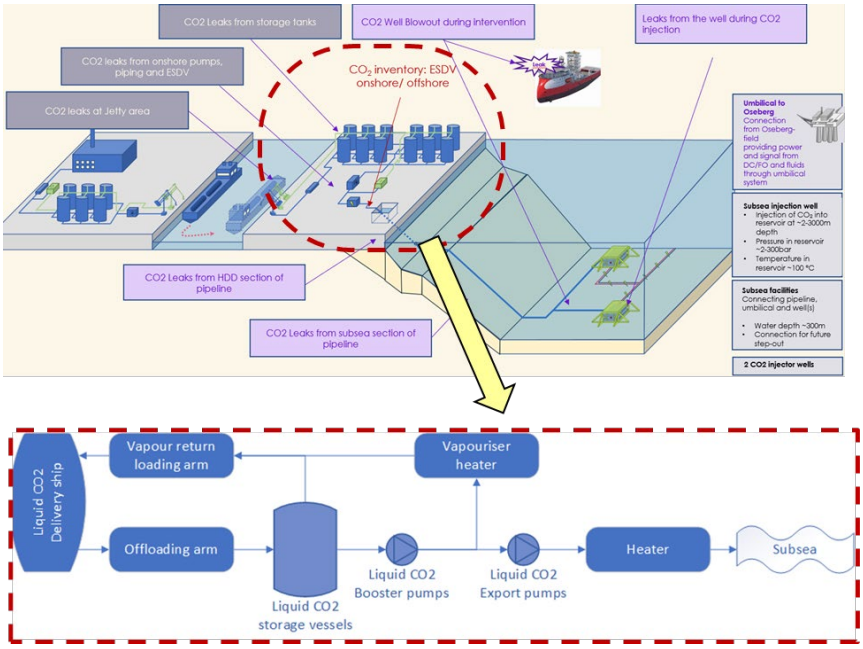


Fig. 26. Onshore facility for handling CO2 before injection (Northern Light)

The hazard and risk assessment may identify a number of risk-reducing measures, such as:

- Facility design/Layout: CO2 installation should be sited to minimize the risk to personnel, local population, and property.
- Process control system for monitoring and controlling the level and pressure in tanks and pipes.
- Measures to prevent hydrate formation (clogging of CO2 as ice).
- Dimension for accidental loads like natural events (wind, snow, earthquake) and low temperatures from CO2 accidental leakages.
- Introduce pressure protection systems, involving SIFs and pressure safety (relief) valves (PSVs). It is important to note that PSVs release directly to the environment, which is safer than doing so via a flare system. The PSVs are designed so that the valve exit side has a very wide opening, reducing pressure rapidly.
- Ensure natural ventilation when possible and, otherwise, the use of HVAC, for example, in administrative buildings.
- Design for ignition source control, with the possibility for isolation of power to electrical devices if CO2 leakages are detected, explosion-proof protection of electrical devices (Chapter 12), and encapsulation of potentially hot surfaces.
- Ensure the possibility of segmenting the process volumes, for example, with ESD valves in the incoming and outgoing CO2 piping from/to ships and the outgoing CO2 pipeline (to offshore injection).
- Add necessary escape, evacuation, and rescue facilities.
- Prevention and mitigation for BLEVE scenarios (that could result in explosions).
- Protection of muster areas and critical rooms by a safe distance or dimensioning to withstand accidental loads. The facility does not have a control room as it is remotely operated.

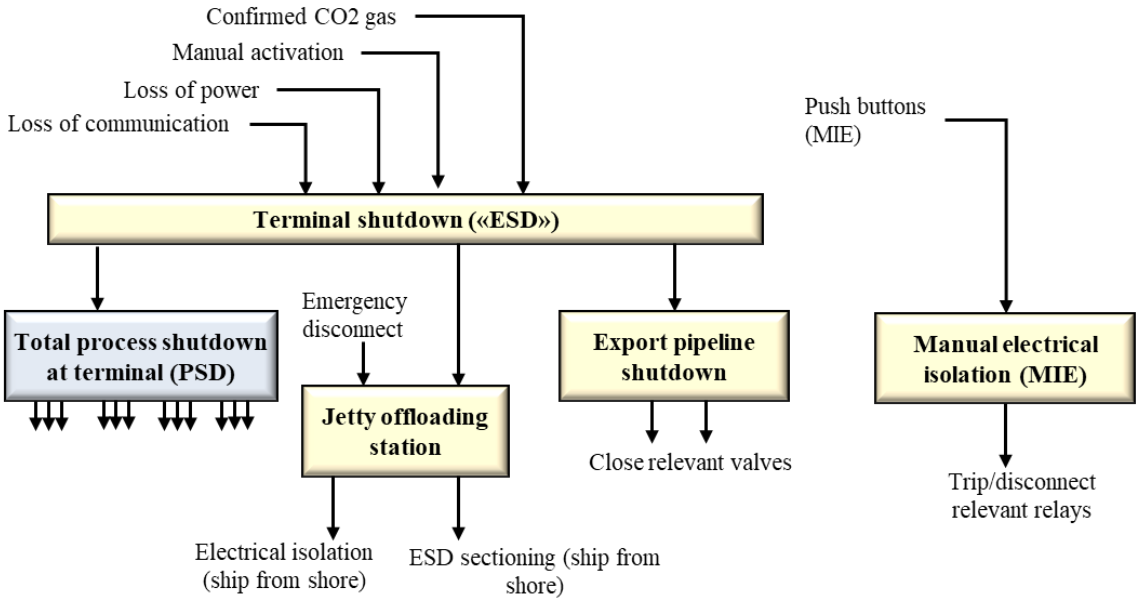


Fig. 27. Examples of SIFs for onshore facility CCS facility

6.10.3 Examples of SIS systems and SIFs

An example of possible safety functions related to F&G detection, ESD, and PSD is shown in Fig. 27, which identify:

- A complete terminal (onshore) shutdown is initiated if there is a loss of communication with the remote-control center, upon loss of power (external), manual activation (by pushbuttons in the remote-control room or locally at the terminal), or confirmed CO2 gas leakage.
- The terminal shutdown activates the PSD system (with functions listed later), secures the Jetty offload station (by closing ESD valves to/from ships and removing ignition sources), and closes valves in the export pipeline.
- The Jetty offloading station can also be manually initiated from the ships as an "emergency disconnect."
- The power supply can be disconnected manually by pushbuttons (remote or local), with the result that the circuit breakers (trip incomers) are opened.

Examples of safety functions implemented for the PSD system for the onshore facility are shown in Tab. 2. Here, only the initiators are identified, and the corresponding actuated devices would be identified in a cause-and-effect (C&E) matrix.

Tab. 2. Examples of SIFs for the CO2 onshore facility

CO2 storage tanks	PAHH storage tank pressure
	PALL storage tank pressure
	LAHH storage tank level
	LALL storage tank level
	PALL liquid CO2 drain
Booster pump	PAHH booster pump discharge
(Export pipeline) heater	PAHH Liquid CO2 export heater
	TAHH Liquid CO2 export heater
	TALL Liquid CO2 export heater

6.11 SIS for nuclear industry

Nuclear power plants have received increased attention, also in Norway, to solve future energy demands. It is often claimed that Norway lacks the competence to explore this issue, but that is not true. For example, the Institute for Energy Research (IFE) in Norway has researched nuclear power technologies and safe control strategies, including control room design, dating back to as early as 1948.

Fig. 28. The Halden project participants (IFE)

IFE used to have two nuclear reactors for research purposes, one at Kjeller (closed in 2019) and one in Halden (closed in 2021/22). A key flagship of Norwegian nuclear research activity has been the Halden project, an international initiative led by IFE since 1958, in which new research topics are identified every three years. Today, the program encompasses research institutes, agencies, companies, and associations from 19 countries worldwide, under the auspices of the Organization for Economic Co-operation and Development (OECD) and its associated Nuclear Energy Agency (NEA). Fig. 28 shows the countries and their involved partners. Among the Norwegian partners are, in addition to IFE, Equinor, NTNU, Høgskolen i Østfold, and the Norwegian Nuclear Decommissioning Directorate (NND).

The content of this section is based on a presentation by IFE held externally, and the author was permitted to use the material for educational purposes.

6.11.1 Why introduce nuclear power plants?

Nuclear power plants have been assessed as posing a high risk to the environment due to the radioactive materials involved and the handling of radioactive waste generated during the nuclear process. However, some of the advantages being advocated are:

- Carbon-free, meaning that no CO2 is generated
- Low footprint: A nuclear facility needs fewer natural resources compared to, e.g., the large areas affected by, e.g., onshore wind farms and solar farms. The amount of uranium required in modern nuclear plants is low compared to the past, which may allow for mixtures with other elements, such as thorium. Several solutions for thorium-based reactors have been proposed, and some are in operation, but in combination with uranium fuel. However, the footprint is debated as waste needs to be securely managed over thousands of years.
- Stable energy source: The process is not dependent on the amount of wind, sun, or other resources.

Nuclear power plants can be a stable producer of electricity in the larger energy mix of power distribution systems. Smaller modular reactors (SMR) are considered safer than conventional plants and may be integrated as modules in larger nuclear facilities.

6.11.2 How does a nuclear power plant work?

A nuclear power plant is sometimes referred to as a hot water kettle. Nuclear power plants generate electricity in three main steps: First, the nuclear reactor process creates heat. This heat raises the water temperature, allowing steam to be generated. The steam rotates a turbine connected to a generator, which in turn produces electricity.

	You can find simple animations of the process with explanations at the webpage by the US National Regulatory Commission at https://www.nrc.gov/reading-rm/basic-ref/students/what-is-nuclear-energy.html. The Massachusetts Institute of Technology (MIT) also provides useful descriptions of nuclear plants with a basis in their own MIT research reactor at https://nrl.mit.edu/

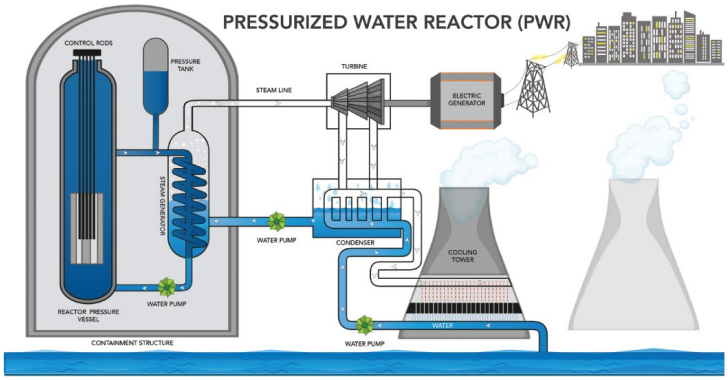


Fig. 29. Pressurized water reactor (PWR) (US Department of Energy)

The nuclear reactor process relies on fission. During this process, neutrons collide with the uranium isotope U235, resulting in a split into lighter uranium isotopes and more neutrons that can collide again. As part of this process, large amounts of energy are generated.

There are several types of nuclear reactor designs. One is the pressurized water reactor (PWR), as presented by the Department of Energy in Fig. 29. Complemented with explanations in the glossary from the U.S National Regulator Commission, the PWR reactor consists of:

- Reactor vessel where the fission reaction is taking place. The reactor consists of fuel (in this case, uranium), a moderator (in this case, water), a reflector (to conserve escaping neutrons), an interface for the coolant to remove heat, and a set of control rods. A rod consists of material such as Hafnium, Boron, or others that can absorb neutrons from the process. The rate of the fission process can be controlled by lowering or lifting the rods in the water.
- Steam generator, which generates steam for power generation.
- Containment structure, which is designed to prevent hazardous and radioactive material from escaping. This containment is dimensioned to withstand various accidental loads, including earthquakes, flooding, tsunamis, airplane crashes, and other potential hazards.

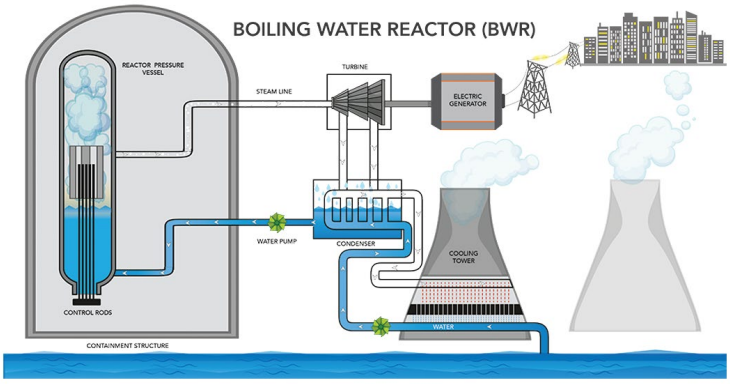


Fig. 30. Boiling water reactor (BWR) (US Department of Energy)

Systems interacting with the reactor are:

- Turbines and generators
- Condenser that cools down the steam so that water reenters the reactor at the temperature that is optimal for the steam generation
- External water supply, which is essential for the steam generation process and as a cooling medium for the reactor in an emergency and in a period after the reactor has been shut down (where rest energies remain for up to weeks and months).

A key characteristic of the PWR reactor is that it separates the systems for heating (the reactor vessel) from the closed-loop systems for steam and cooling water. An alternative to the PWR reactor is the boiling water reactor (BWR), which integrates these two systems. This means that water is added directly to the reactor, allowing the steam to become reactive. PWR and BWR are often referred to as light water reactors.

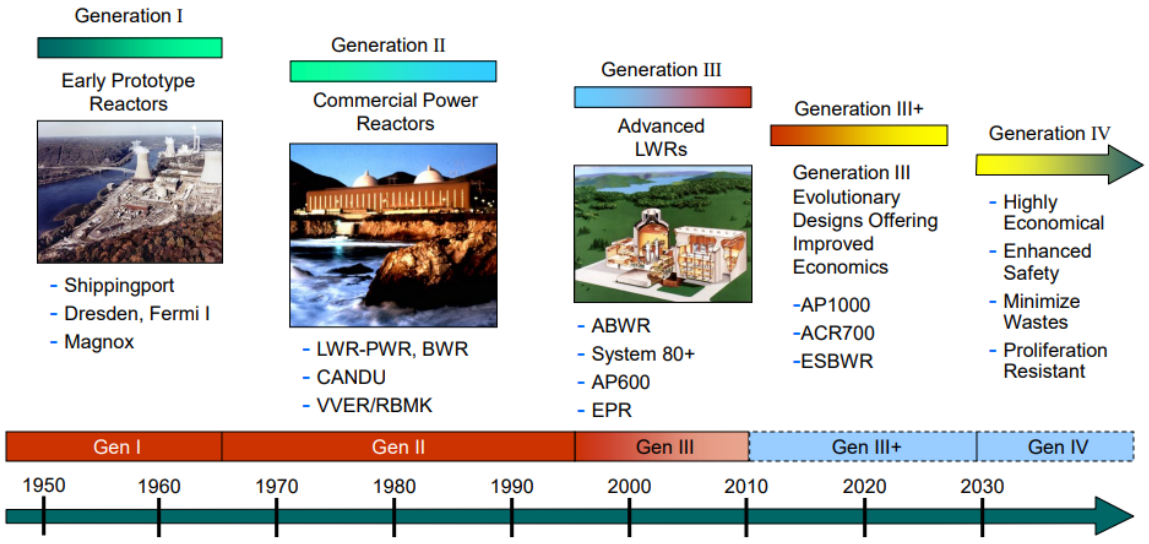


Fig. 31. Nuclear history at glance (U.S. DoE)

Examples of other reactor types are explained in documents published by the World Nuclear Association. The US Department of Energy made a timeline for when the different reactor types were introduced, organized into four generations, as shown in Fig. 31. We notice that PWR and PWR belong to Generation II. An internet search can explain the meaning of abbreviations for the various reactor types mentioned.

For generation III and above, the abbreviations mean:

- ARC – affordable, robust, compact
- AP – Advanced passive (for a pressurized water reactor)
- ESBWR – Economic simplified boiling water reactor
- EPR - European pressurized reactor

6.11.3 Small reactor modules (SMR)

Recent trends point to small reactor modules (SMRs), a concept applicable to generation III+ and above. According to the International Atomic Energy Agency (IAEA) and OECD's Nuclear Energy Agency (NEA), SMRs are reactors with power capacities from 10 to 300 MW per unit. They are characterized as:

- Small, meaning that they physically are a fraction of the size of conventional nuclear power reactors.
- Modular, meaning that systems and components can be factory-assembled and transported as *one* unit to a location for installation.
- Today, Generation III is often referred to as light water reactors (LWR). Future developments that are not yet built will be based on Generation IV technologies.
- Reactors – harnessing nuclear fission to generate heat to produce energy.

Fig. 32. Illustrations of SMR reactors (KAIST, neuronbytes)

Factors that make SMR an attractive solution, according to IAEA, are:

- Lower footprint compared to conventional nuclear plants
- Lower capital investments for site construction, as more assembly can be done in a factory, like a "commercial on the shelf" product.
- Scalable, meaning that more capacity can be added or removed by adding or removing modules
- Simpler design: In general, reduced complexity may lead to fewer maintenance needs, less manual intervention, and improved safety.
- Improved safety: More use of passive systems and inherent safety characteristics, such as low power and operating pressure, less reliance on human intervention, more reliance on natural circulation, convection, gravity, and self-pressurization, and less dependency on instrumented systems.
- Reduced fuel refilling needs (every 3-7 years and up to even 30 years) compared to conventional plants (every 1-2 years).
- Higher efficiency and modularity enable the scaling of energy supply to, for example, hydrogen production and as supplements to wind and solar energy sources.

SMRs may be "just around the corner," at least in some countries. More than 80 commercial designs have been developed worldwide, according to the IAEA.

	The OPEN100 project is a US academic development framework for a small SMR that is intended to be placed in a populated area. On their webpage, they share descriptions of equipment, technical documentation, and operational concepts. The chosen concept is the pressurized water reactor. You can find the information at https://www.open-100.com/ Also, the OECD's NEA has made a webpage acting as a dashboard for SMR status reports

6.11.4 Safety design principles

The governing principle for ensuring safe design and operation:

- Defense-in-depth, defined in the Nuclear Regulatory Commission (NRC) glossary as an approach to designing and operating nuclear facilities that prevents and mitigates accidents that release radiation or hazardous materials. The key is to create multiple independent and redundant layers of defense to compensate for potential human and mechanical failures, so that no single layer, no matter how robust, is relied upon exclusively. Defense in depth includes the use of access controls, physical barriers, redundant and diverse key safety functions, and emergency response measures.
- Risk-informed safety, meaning that the design of the nuclear facility relies on a combination of:
    - Deterministic rules (given in technical specifications for the nuclear industry)
    - Probabilistic safety assessments, often based on fault tree and event tree analysis

The nuclear industry has developed templates for fault tree analysis and event tree analysis that identify which scenarios to include. Three types of dimensioning accident loads (types of events that could lead to the most severe accidents) are considered:

- Avoid core damage
- Avoid radioactive release (given core damage)
- Avoid public deaths (given radioactive release)

6.11.5 Nuclear reactor hazards and safety functions

There are three main categories of hazards related to nuclear power plants, and for each of these, the corresponding safety functions are listed:

Hazard	**Safety functions**
Control reactivity and heat generation	SCRAM (rapid emergency shutdown) Control of rods
Control heat removal	Core cooling Decay heat removal
Confinement of radioactive material	Containment (Safety fans for ventilation for selected rooms and areas)

Decay heat refers to the heat generated after the reactor has been shut down. The reactor requires prolonged cooling, often lasting a week or more, due to residual activity from the fission process. Active water pumps are typically required for this purpose, powered by an external electricity grid or emergency diesel generator(s).

In the design of safety functions, emphasis is placed on the following principles:

- Using inherently safe systems (instrumented, mechanical, other), focusing on:
    - Fail-safe design (various measures and margins built into the system to make it as safe as possible, also in the presence of foreseeable failures).
    - Using natural phenomena, e.g., gravity and natural circulation, to prevent or mitigate the consequences of hazards and hazardous events.
- Utilization of passive systems that are available when needed, including access to large amounts of water sufficient to submerge the core in water basins for cooling.

The nuclear industry is generally considered more conservative than other industries. This means, for example, that many plants maintain an analog/hardwired control and safety system in addition to digitalized, more modern PLC/DCS-based systems.

6.11.6 Requirements for SIS systems

The standard for functional safety in the nuclear industry is IEC 61513 (2011). Instead of the term SIS, the standard uses the term instrumentation and control (I&C), which is important for safety and covers both active

(control) and passive (on-demand) systems. This standard does not apply to safety integrity level (SIL). Instead, IEC 61513 is saying that the nuclear industry applies a deterministic method to determine the safety significance of I&C functions classified as type A, type B, or type C according to criteria in IEC 61226 (2020). A simplified explanation of these is:

- Category A: Function that is a primary role for achieving or maintaining nuclear power plant safety.
- Category B: Function that is complementary to the achievement or maintenance of nuclear power plant safety.
- Category C: Function that has an auxiliary or indirect role in the achievement or maintenance of nuclear power plant safety.

The criteria that determine the categorization is more complex than described here. IEC 61513 (2011) links category with classes 1, 2, and 3 in this manner (also a bit simplified)

- Type A functions must meet the requirements for class 1
- Type B functions must meet the requirements of class 2
- Type C functions must meet the requirements of class 3

Examples of how commonly used nuclear power plant I&C systems align with the classes are shown below.

System type	**Class 1**	**Class 2**	**Class 3**	**Not classified**
Plant automation and control systems		x	x	x
Human-machine interface (HMI) systems	x*	x	x	x
Protection system and safety actuation system	x			
Emergency power actuation system	x			
*Class 1 HMI may be restricted to a few critical indicators and push buttons				

The detailed requirements relating to work processes and tools are provided in IEC 61513. For software aspects related to application program development, the standard references:

- IEC 60880 (2006) Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions.
- IEC 62138 (2018) Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category B or C functions.

Common cause failures (CCFs) receive significant focus, and many methods for modeling CCFs in reliability calculations originate in the nuclear industry.

	Want to learn more? Watch the presentations and discussions about managing the safety of nuclear facilities organized by IFE, the Norwegian Institute for Energy, at Arendalsuka 2024 – available on YouTube. https://youtu.be/SqaIMZsO7k0. IFE has experience with operating nuclear facilities in Norway (Halden and Kjeller reactors) and research in the design and operation of nuclear plants. IFE has also been leading international research programs, collaborating with other countries that operate nuclear facilities.
	If you want to learn about the measures taken to build competence within the nuclear industry in Norway, you can visit the "Norsk Nukleært senter" at https://www.nnrc.uio.no/. The Norwegian government has also appointed an expert committee to investigate all aspects, including regulations and the integration of nuclear energy plants into the overall energy mix. Their final report is scheduled for April 1st, 2026.

6.12 SIS for subsea production processes

Fig. 33 identifies examples of SIS systems protecting subsea systems and receiving facilities:

- Topside ESD is performing a well isolation, meaning that all valves related to the well closes, by removing the power supply to subsea systems.
- Topside PSD is performing well for isolation on some selected well valves.
- High integrity pressure protection system (HIPPS) shall prevent damage to the pipeline when the whole pipeline cannot withstand the maximum well pressure.

The HIPPS system in Fig. 33 protects a subsea pipeline and the receiving topside facility against overpressures that exceed the pipeline's design limits. Designing a pipeline to withstand the full shut-in pressure (i.e., the maximum pressure generated by the well when flow has been stopped) is not always possible. For example, the wall thickness required by the shut-in pressure may result in a pipeline that is too stiff, leading to higher steel costs. For marginal fields, the pipelines may become too expensive, and excessively high pressures may be required for a shorter period of reservoir production.

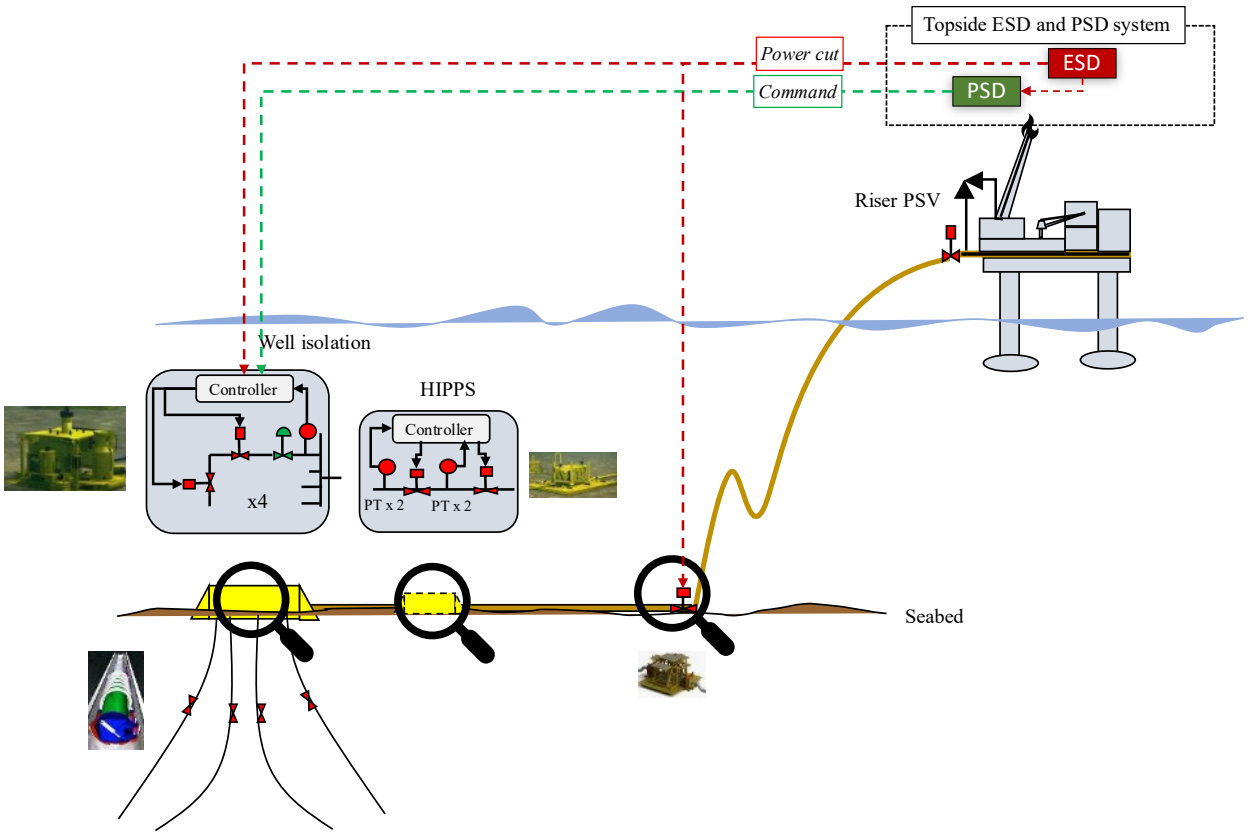


Fig. 33. Subsea safety systems with HIPPS

The general motivation for introducing a HIPPS system is to compensate for the lack of inherently safe process design or to replace the function of a mechanical pressure relief valve. The design limitations can stem from cost considerations or from changes in operating conditions, such as higher volumes or treating fluids at pressures exceeding those specified in the original design. Examples of systems protected by HIPPS are flare systems, vessels, and pipelines. When a HIPPS system is introduced, it must be entirely independent of all other systems, including other SIS systems, and dedicated to performing one single SIF, for example, to detect high pressure and close specific valves in a pipeline, as shown in Fig. 33. Since a HIPPS system is a replacement for

an inherently safe process design, it often must meet SIL 3 requirements, leading to redundancy and fault-tolerance requirements for pressure sensors, controllers, and valves.

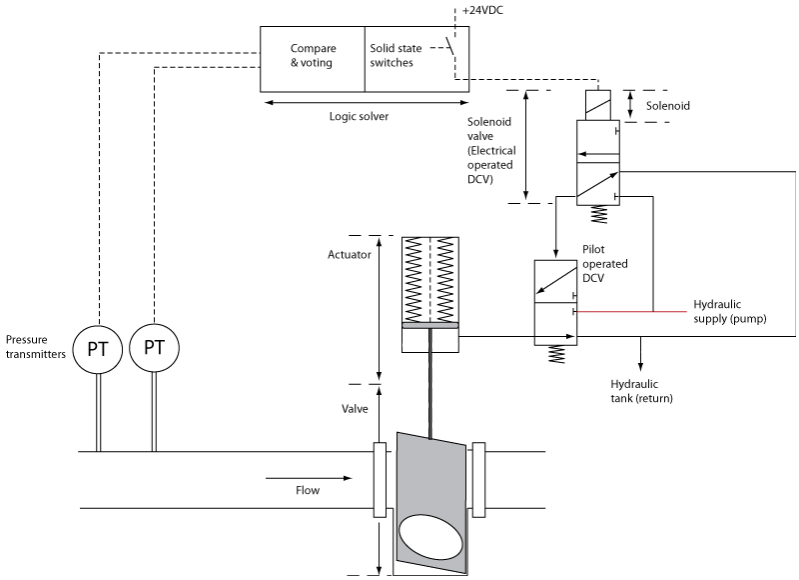


Fig. 34. An example of a principal arrangement HIPPS system

Fig. 34 shows how a HIPPS system may be designed. For simplicity, only two pressure transmitters and one shutdown valve have been included.

- The pressure transmitters convert pipeline pressure to an analog (current) signal in the range of 4-20 mA.
- The logic solver reads the electrical signals, performs a comparison against the threshold (or setpoint), and acts (based on the selected voting) by sending a signal to the solenoid valve. In this context, acting means opening or closing relays that control the power supply to the solenoid valve. If the pressure transmitter readings exceed a certain threshold outside the measurement range, indicating a faulty detector or miscalibration, the logic solver raises an alarm.
- The solenoid valve controls the signal to the secondary pilot-operated valve. When the solenoid loses power, the position of the solenoid valve switches so that the pilot signal to the secondary valve is removed.
- The secondary valve is a pilot-operated DCV, where the pilot signal may be hydraulic or pneumatic pressure. Upon loss of the pilot signal, the valve switches to depressurize the line to the connected shutdown valve.
- The HIPPS valves are designed to fail safely – usually towards the closed position, which means that the valve will close in the event of foreseeable fault situations, such as power loss. Each HIPPS valve comprises the valve body and the valve actuator. The valve actuator opens the valve when fluid enters and is trapped within it, and closes it when the fluid exits. Some valves may rely on ambient (subsea) pressure to ensure fail-safe operation when handling fluids under extremely high pressure. In this case, the spring provides only marginal additional assistance during valve closure. The required closure time for fast-acting HIPPS valves may range from 2 to 5 seconds. However, some pipeline conditions allow for a longer closure time.

With a SIL 3 requirement, the HIPPS system generally needs two HIPPS in the pipeline rather than one.

6.13 SIS protecting flare system at a process plant

Process plants that involve flammable and explosive gases require a dedicated pipe system that routes the gases to a safe location, meaning a safe distance away from the plant, the control room, and areas where people may be present.

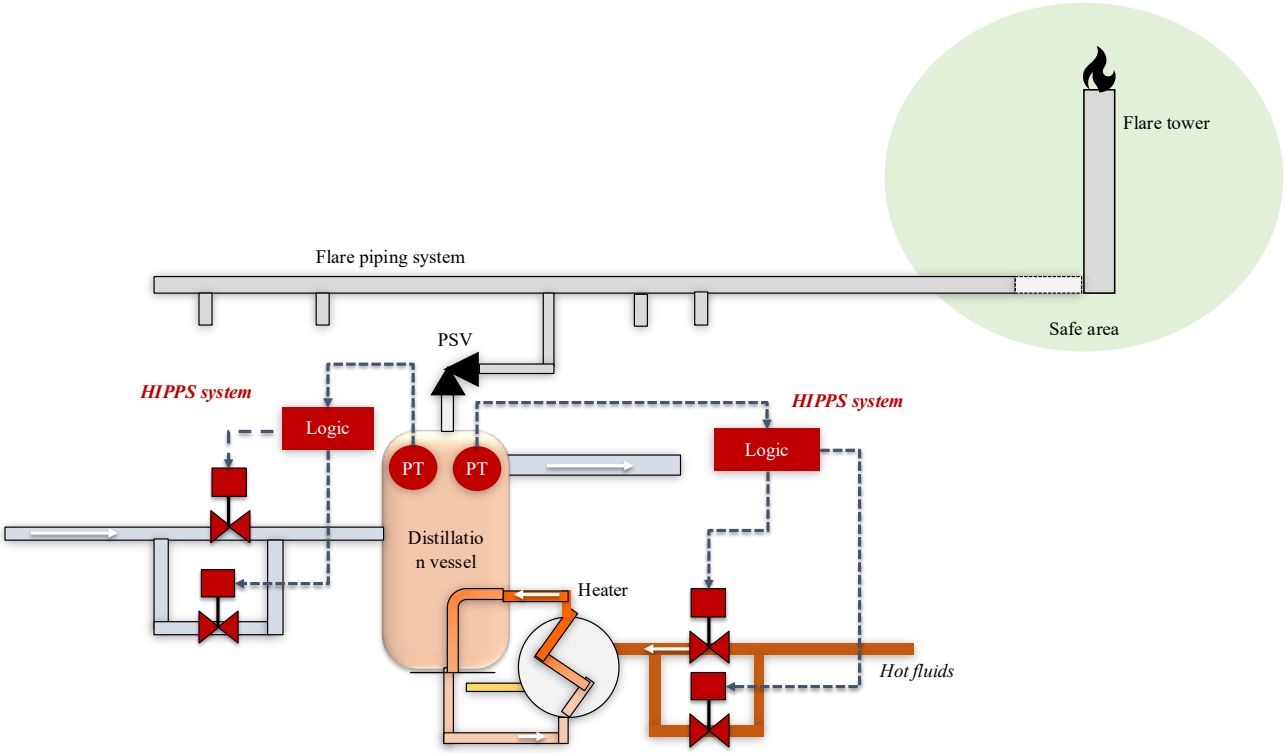


Fig. 35. HIPPS system installed to reduce demand on the flare system

This specialized system is commonly called a flare system because all pipes lead to a flare stack, where gases are released and, if needed, ignited to produce less hazardous gases. An example of such a process is shown in Fig. 35.

The need to route gases away from the plant can arise from pressure buildup in one or more systems within the plant, triggered by a process upset, an SIS failure, or a fire that generates heat around process equipment. For example, a vessel must be equipped with pressure-relief valves (PSVs) that activate when a specified pressure limit is reached. The PSVs connect the process systems to the flare system, and when opened, gases flow from the process side (e.g., a vessel) into the flare system.

We assume the flare system was initially designed to accommodate the expected gas routing capacities. However, over time, the plant may be rebuilt and expanded, and the flare system may not have sufficient capacity to handle all new pressure-buildup scenarios. A high-integrity pressure protection system (HIPPS) is sometimes introduced to reduce pressure buildup and minimize the number of vessels releasing gases into the flare system simultaneously. The HIPPS detects early pressure buildup and prevents escalation by stopping flow into the pressurized tank and into the heated medium used for assistance, such as in distillation processes. When such HIPPS systems operate simultaneously, pressure buildup is prevented, and fewer PSV valves need to be opened across the facility.

6.14 Bibliography

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

EN 50126. (2017). *Railway Applications The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS). Part 1: Generic RAMS Process*. European Committee for Electrotechnical Standardization (CENELEC).

EN 50128. (2017). *Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems*. European Committee for Electrotechnical Standardization (CENELEC).

EN 50129. (2018). *Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling*. European Committee for Electrotechnical Standardization (CENELEC).

Goel, P., Datta, A., & Mannan, M. S. (2017). Industrial alarm systems: Challenges and opportunities. *Journal of Loss Prevention in the Process Industries*, *50*, 23–36. https://doi.org/https://doi.org/10.1016/j.jlp.2017.09.001

IEC 60880. (2006). *Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions*. International Electrotechncal Commision.

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

IEC 61226. (2020). *Instrumentation, control and electrical power systems important to safety*

Categorization of functions and classification of systems. International Electrotechnical Commission.

IEC 61508. (2010). *Functional safety of electrical/electronic/programmable electronic safety-related systems (Seven parts)*. 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 61513. (2011). *Nuclear power plants - Instrumentation and control important to safety - General requirements for systems*. International Electrotechnical Commission.

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

IEC 62138. (2018). *Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category B or C functions*. International Electrotechncal Commision.

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

ISO 26262-1. (2018). *Road vehicles — Functional safety — Part 1: Vocabulary*. International Organization for Standardization.

ISO 26262-2. (2018). *Road vehicles — Functional safety — Part 2: Management of functional safety*. IInternational Organization for Standardization.

NORSOK I-002. (2021). *Industrial automation and control systems*. Standard Norge.

NORSOK S-001. (2021). *Technical safety*. Standard Norge.

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/

PSA. (2017). *Principles for barrier management in the petroleum industry. Barrier memorandum 2017*. Petroleum Safety Authority Norway.

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