Chapter 1.
Introduction

Mary Ann Lundteigen   Marvin Rausand

RAMS Group
Department of Mechanical and Industrial Engineering
NTNU

(Version 0.1. May 2018)

NTNU – Trondheim
Norwegian University of
Science and Technology

Learning Objectives

The main learning objectives associated with these slides are to:

- Become familiar with what we mean by a safety-critical system
- Become familiar with the main building blocks and technologies of such sysetms
- Be able to recognize some of the application areas
- Become aware of some key design and operational considerations
- Become aware of standards that are important in the framing of safety-critical systems

The slides build on Chapter 1 in **Reliability of Safety-Critical Systems: Theory and Applications**. DOI:10.1002/9781118776353.

Outline of Presentation

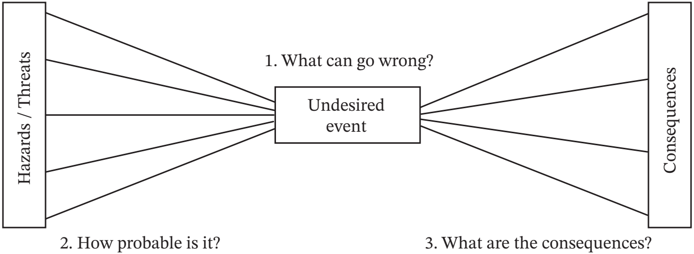
1. Introduction
2. Safety Barriers and Risk Reduction
3. Safety-Critical System and SIS
4. Examples of SIS Application Areas
5. SIS Technologies and Design Principles
6. SIS Interaction with Protected System
7. Functional Safety and Functional Safety Standards

Risk and Bow-Tie Model

Risk may be defined by asking the following three questions:

1. What can go wrong?
2. How probable is it?
3. What are the consequences?

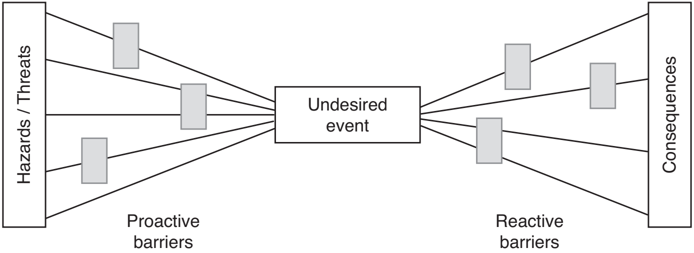
This definition can easily be related to the *bow-tie diagram* shown below, where the first question is answered by defining an undesired event, question two is answered by analysis of the leftside and question three by analysis on the right side.



Safety Barriers and Risk Reduction

Safety barriers (or just barriers) is a common termfor technical, human, or organizational measures introduced to reduce risk. Safety barriers may be introduced to reduce the probability of undesired events (as proactive barriers), or mitigate their consequences (as reactive barriers).

The role of safety barriers as means to reduce risk can be easily illustrated in the bow-tie model.



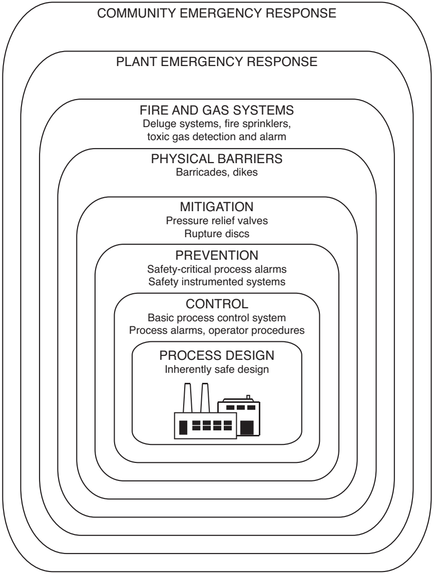
Classification of Safety Barriers

Safety barriers can be classified as either:

- Proactive or reactive (as illustrated in the bow-tie in previous slide)
- Technical, human, or organizational
- Passive (always available) or active (applied “on demand” when needed)

Layers of Protection

- A common model for safety barriers in the process industry is the "onion model'', or layers of protection.
- The model illustrates that safety is not managed by one barrier alone, but many. The model also identifies barriers that are not primarily for safety (e.g. control).
- The model recognizes different types of barriers, also those that are not primarily for safety. An important premise is that each layer (or barrier) is independent from the others.


COMMUNITY EMERGENCY RESPONSE
PLANT EMERGENCY RESPONSE
FIRE AND GAS SYSTEMS
Deluge systems, fire sprinklers, toxic gas detection and alarm
PHYSICAL BARRIERS
Barricades, dikes
MITIGATION
Pressure relief valves
Rupture discs
PREVENTION
Safety-critical process alarms
Safety instrumented systems
CONTROL
Basic process control system
Process alarms, operator procedures
PROCESS DESIGN
Inherently safe design

Safety-Critical System

☞ Safety-critical system: A system whose failure may lead to harm to people, large economic losses, and/or environmental damage.

Safety-critical systems overlap with the concept of *technical* safety barriers, and be classified as either:

- **Active systems** interacting with the system to be protected:
  - Digital technologies, such as electrical, electronic, or programmable electronic (E/E/PE) technologies (our focus)
  - Instrumentation, based on mechanical, pneumatic, or hydraulic technologies
- **Passive systems** that provide continuous protection, such as firewalls, dikes, and containment systems

Our focus in these slides is on the active safety-critical systems that employ E/E/PE technologies.

Safety-Related System

The term safety-*related* system is sometimes used instead of safety-critical. Here, we suggest the following distinction between the two:

- Safety-critical systems: A safety system where the main purpose is **to ensure safety** (e.g. airbag system in a car), and where the consequence can create hazardous events, whereas
- Safety-related system: A safety system where the main purpose is **not to ensure safety**, but where the consequence of failure can create hazardous events (e.g. systems for driver assistance like cruise/automatic speed control)

Thus, safety-related covers a broader scope of systems than safety-critical by this distinction. In practise, we will focus on both type of systems, as our concern is to reduce the risk of accidents caused system failures.

E/E/PE Safety-Critical Systems

Many of the *active* safety-critical systems are“digitalized”, i.e. using logic solvers, sensors and actuating devices. The most central technologies involved are electical, electronic, and programmable electronic (E/E/PE) technologies. For these systems, we introduce:

☞ E/E/PE safety-critical (related) system: A system whose failure may lead to harm to people, economical loss, and/or environmental damages and which is realized by (at least some) electrical, electronic, or programmable electronic (E/E/PE) technologies.

Safety-Instrumented System (SIS)

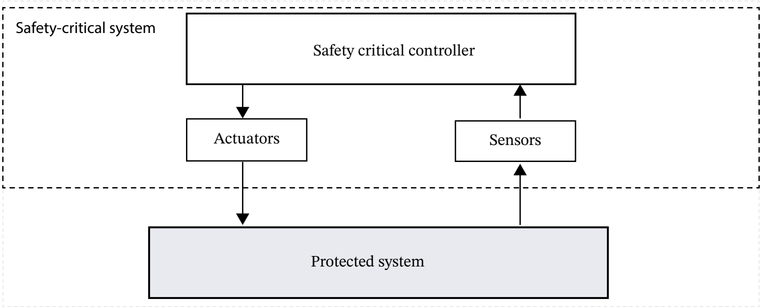
The process industry has adapted the term **safety-instrumented system (SIS)** rather than E/E/PE safety-critical (related) systems:

☞ Safety-instrumented system (SIS): A system used to implement one or more safety instrumented functions (SIFs), using E/E/PE in combination with other active (e.g. mechanical) technologies.

We adapt the term “SIS ” even if outside the application of process industry, due to its simplicity. It is important to note that different industries use different names depending on application and tradition.

Protected System or EUC

The system which is protected by the SIS is called protected system or equipment under control (EUC).



The SIS is sometimes installed within the protected system, and the separation is not always so distinct as illustrated above.

Definition of EUC

☞ Equipment under control (EUC): Equipment, machinery, apparatus, or plant used for manufacturing, process, transportation, medical, or other activities. This is what we also call “the protected system”.

An important task is to define the boundaries of the EUC, i.e. what is included as part of EUC:

- The boundaries can be set based on physical or operational considerations
- Hazards identification techniques are used to identify hazards and hazardous events associated with the EUC
- Allocation methods are used to decide what types of systems, including safety-critical systems, that are needed

EUC Examples

Examples

Industry	Examples of EUC		
Process industry:	Production separator	Fire area	Pipeline section
Railway:	Block/rail section	Station	Tunnel
Hospital:	Patient	Critical medicine dosing apparatus	
Cutting machine:	Machine itself	Humans (operators or maintenance personnel)	Room where machine is located

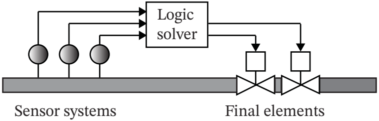
Safety-Instrumented Function (SIF)

A SIS may carry out one or more SIFs.

☞ Safety-instrumented function (SIF): A safety function that is performed by a SIS.

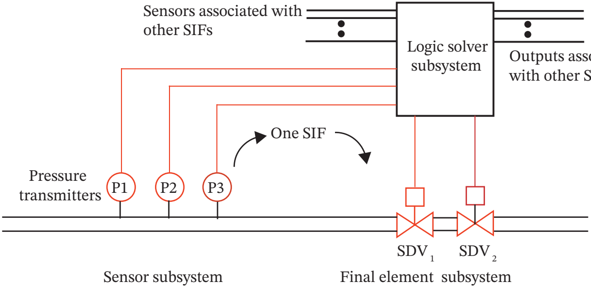
A SIF is often split into three subsystems:

1. Sensor (S) subsystem: Monitors some process parameter or presence of a command.
2. Logic solver (LS) subsystem: Decides if it is necessary to act upon the monitored signals.
3. Final element (FE) or actuating elements subsystem: Carries out the necessary tasks, if decided to act.



SIS versus SIF

A SIF is only a subset of SIS functions, which can be illustrated as below:



From the illustration we note that:

- A SIS can carry out more than one SIF
- Some SIS elements may be shared by several SIFs, such as the logic solver

Often more than one SIS

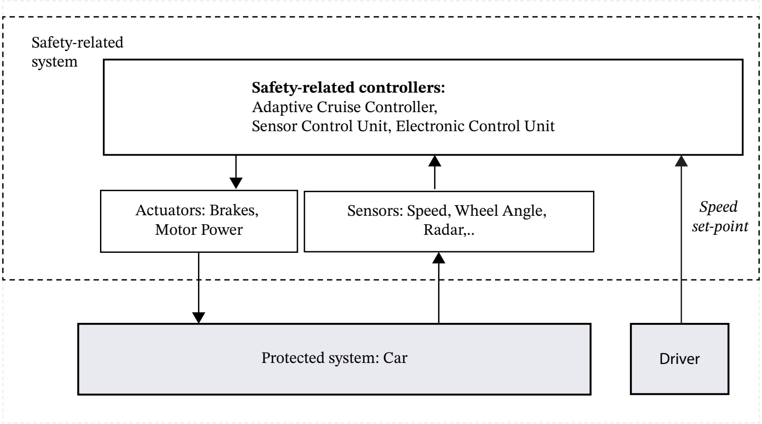
Large plants and systems will often use more **than one** SIS to implement all necessary SIFs. Recall the “onion model”.

For example, at a process plant, we may identify the following SISs:

- PSD: Process shutdown system: Stop of process and processing equipment
- ESD: Emergency shutdown system: Isolation of general power supply and start of emergency power
- HIPPS: High integrity pressure protection system
- Fire and gas detection (F&G) system

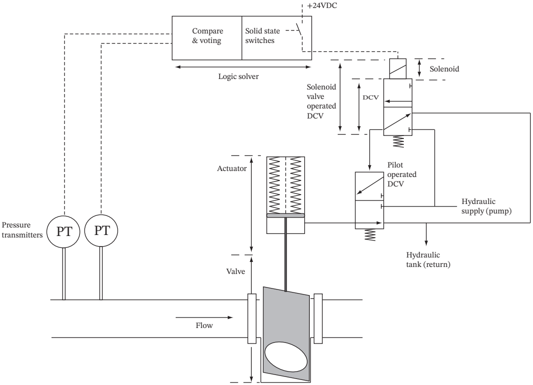
Cars: Automatic/Adaptive Speed Control

A car has many safety-related as well as safety-critical systems. The simplified illlustration below is for the the adaptive cruise control (a safety-related system).


Safety-related system
Safety-related controllers:
Adaptive Cruise Controller,
Sensor Control Unit, Electronic Control Unit
Actuators: Brakes, Motor Power
Sensors: Speed, Wheel Angle, Radar,..
Speed set-point
Protected system: Car
Driver

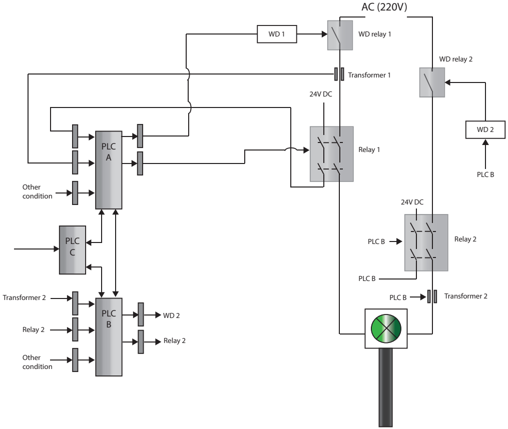
Process Industry: Over-Pressure Protection

High-integrity pressure protection system (HIPPS) is one eaxample of a safety-critical system used to protect pipelines and vessels that are not designed to withstand highest possible pressure. A simplified illustration of the main SIS components involved are shown below.



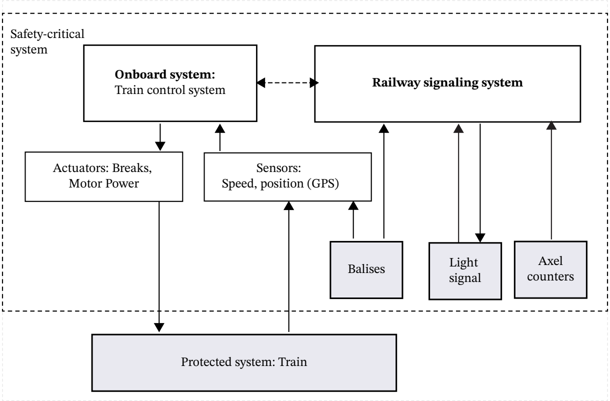
Railway: Railway Signaling System

Railway signaling system is a safety-critical system that detects train position and sets light signals for either drive or stop. A simplified example of how the green (drive) signal can be controlled is shown below.



Railway: Railway Signaling System

Modern railway signaling, like the European railway traffic management system (ERTMS), places more safety-critical functions onbard the train. The onboard train systems interact with sensors along the trackside. A simplified illustration of this system is shown below.



Sensors

Purpose: A sensor measures a physical state within the protected system and sends the information to the logic solver.

Example of states to measure:

- Processing plant: Temperature, pressure, level, flow, status of pushbuttons, etc
- Railway signaling: Relay position, position of rail switch, train speed and position, electrical current (in cable to light signal)

Sensors

Need for conversion of measurement: The logic solver can only receive digital/analogue information, and sensors must convert the measurements.

Examples of converted signals

- Analog wired signal (e.g., 4-20 mA)
- Voltage wired signal (0 V/12V, or 0 V/24 V)
- Digital “packages” (For wired or wireless communication)

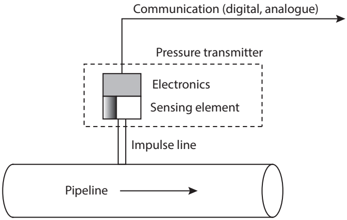
Example

A pressure sensor has to convert a pressure reading 10-20 bar to digital signal or an analogue value in the range of 4 mA and 20 bar into 20 mA. If signal is lost, or outside the range, it is recognized as a fault.

Sensors

All sensors have different sub-elements. A pressure sensor system constitutes the following sub-elements:

- Impulse line, which connects the sensing element to the process pressure
- Sensing element, with diaphragm and a reference pressure (atmospheric or vacuum)
- Electronics, with electrical signal generation from diaphragm deflection, diagnostics features and (if included) digital communication interface



Logic Solver

Purpose: A logic solver makes decisions on what to do, based on sensor readings. The decision-rules are often implemented by software or by digital/electronic components.

Examples of tasks carried out by the logic solver as part of decision-making:

- Compare sensor signals with pre-set targets or ranges (set-points)
- Give commands to actuators

It is critical that the ltiming and sequence of commands are adequate to be efficient. Timers may be used to delay commands.

Logic Solver: Different Realizations

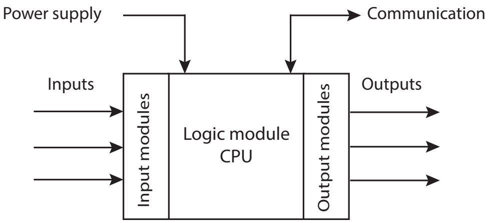
A logic solver can be realized by different technologies:

- Hardwired, meaning that all control/decisions is carried out by the use of relays and contactors.
- Solid state, meaning that the control/decisions is carried out by a fixed arranged and programmed set of electronic components.
- Programmable, meaning that the control/decisions is carried out by an application program (software).

- Modern logic controllers are of programmable type and well suited for large SISs. These are often called Programmable Electronic Controller (PLC).
- Solid state logic solvers are very robust and suitable for a SIS that has only one or very few SIFs.

Programmable Logic Solver: Main Elements

The main elements of a programmable logic solver are illustrated below:



Communication includes interaction with operator stations/screens and exchange of information and signals with other safety and non-safety systems.

Final Elements

Final element: A final element (also called actuating device) is a device that is able to interact directly or indirectly with the protected system. The final element converts the signal from the logic solver into a physical movement.

Examples:

- Actuators in combination with valves: Mechanical or electro/mechanical devices used to restrict, increase, or re-direct flow. E.g. shutdown valves and solenoid operated valves.
- Switches, relays and circuit breakers: Electrical/electronic components that can isolate or provide power to circuits and electrical equipment.
- Rotating equipment that is started or stopped. E.g. start of emergency power generator or start of fire pump.
- Brakes, that are applied to stop or reduce rotation. E.g. brakes applied when driving.

Examples are provided later in the slides.

Safe Design Principles

A SIS (and its elements) can be designed as either:

- Energize-to-trip: Activation by provision of energy
- de-energize-to-trip: Activation by removal of energy

What principle to choice, depends on the application. Relevant questions to ask are:

- Is it always safe to activate if energy is accidentally removed? (if yes, then de-energize-to-trip may be more suitable)
- Can it be unsafe to activate if energy is accidentally removed? (if yes, then energize-to-trip may be more suitable)

Safe Design Principles

Other safe design principles include:

- Provision of redundancy: Having more than one item to carry out the same function
- Ensuring adequate hardware fault tolerance (HFT): Considering the number of faults tolerated (in a subsystem) before the function is lost.

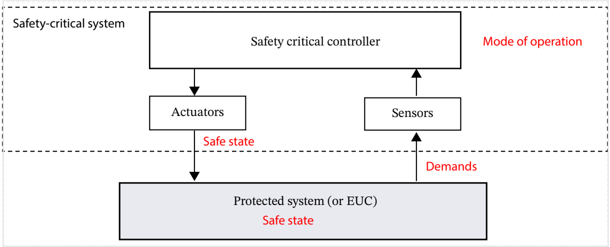
Redundancy and HFT are related concepts, but not the same. HFT is given by the voting, and HFT > 1 means that a subsystem has implemented redundancy voted $k$oo$n$ with $k < n$.

SIS Interaction with Protected System

The interaction between the SIS and the protected system is important to define, to ensure a suitable design of the SIS.

Key parameters that defines the interaction are:

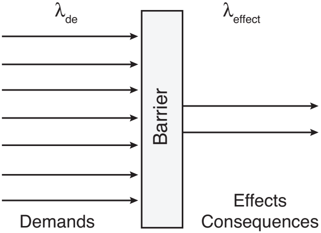
- Demands, their rate, and duration
- Mode of operation
- What is the safe state of the protected system or EUC



Demands and Demand Rates

☞ Demand: An event or a condition that requires a SIF to be activated (i) to prevent an undesired event from occurring, or (ii) to mitigate the consequences of an undesired event.

The frequency of occurrences of demands, the *demand rate* is often modeled as a homogeneous Poisson process with demand rate λ_{de}.



$$\text{Risk reduction factor} = \frac{\lambda_{\text{de}}}{\lambda_{\text{effect}}}$$

Demands and demand rate

Demands are often treated as random events with no duration ("shock events") and modelled by the **homogeneous Poisson process** (HPP) with rate λ_{de}.

An estimate for the demand rate is then:

$$\lambda_{\text{de}} = \frac{N_{\text{de}}(t)}{t}$$

where $N_{\text{de}}(t)$ is the number of demands expected or experienced during a time period of length t.

Modes of Operation

A SIF can be classified according to **how often** the functions are demanded. This is referred as mode of operation.

It is common to distinguish between three modes of operation:

- Low-demand mode: The safety function operates in the low-demand mode if demanded less often than once every year
- High-demand mode: A safety-critical function operates in the high-demand mode if demanded once a year or more often
- Continuous mode: This is a special case of a high-demand mode where the safety-critical function operates continuously (always at demand)

High-demand and continuous demand are sometimes merged into one mode.

Mode of Operation

Examples

System	Low-demand	High-demand	Continuous
Air bag release system (automotives)	X		
Emergency shutdown system (process industry)	X		
Presence-sensing safeguarding devices around robots (manufacturing)		X	
Anti-lock breaking system (ABS) for cars (automotive)		X	
Fly-by-wire systems (aviation)			X
Dynamic positioning system (marine/ship systems)			X
Signaling systems (Railway)			X[a]

[a] Depends on how frequent trains pass at the tracks controlled by the system

Demand duration

In some cases, it may not be realistic to assume zero/no duration of the demand.

Some examples:

- **Fire extinguishing system:** Start of fire extinguishing system is in itself not enough to stop fire. It is also important that fire water is provided over some time.
- **Railway signaling system:** Rail tracks are split into section, where each section must be locked from other trains to enter if a train is already present. The locking of the rail section must be maintained until the train leaves the section.

The effect of demand duration can be studied using Markov models.

Hazardous events

A hazardous event can call for a response by the SIS or occur as a consequence of SIS failure.

☞ Hazardous event: An event in a sequence that, if not controlled, will lead to an undesired consequences to some assets.

An hazardous event may occur if:

- The SIS is unable to *start responding* to the demand, or
- The SIS fails *while responding* to the demand

Example: An hazardous event occurs if the fire pump fails to start upon detected fire, or fails while running.

Hazardous event frequency (HEF)

Hazardous event *frequency* (HEF) is influenced by two factors: (i) how often a barrier is demanded and (ii) how likely it is that the barrier fails to respond to the demand.

This means that:

$$\mathrm{HEF} = \mathrm{PFD}_{\mathrm{avg}} \cdot \lambda_{\mathrm{de}}$$

where λ_{de} is the demand rate, and $\mathrm{PFD}_{\mathrm{avg}}$ is the average probability that the SIF is unavailable at the time when demanded.

The barrier may of course also fail while responding to the demand (fire pump fails after having started to pump fire water). We may extend the formula with this situation:

$$\mathrm{HEF} \approx \left(\mathrm{PFD}_{\mathrm{avg}} + \overline{\lambda}^{*}_{\mathrm{SF}} \cdot \mathrm{MDD}\right) \lambda_{\mathrm{de}}$$

where $\overline{\lambda}^{*}_{\mathrm{SF}}$ is the average dangerous failure rate of the SIF (barrier) and MDD is the mean duration of demand.

Safe State

☞ Safe state: A state of the EUC where safety is achieved. [IEC 61508]

The objective of a SIF is to bring the EUC to a safe state, or to keep the EUC in a safe state after a demand has occurred. The safe state should also be reached in case of failure of SIS.

Safe state is not always well defined

Is it always safe to...:

- Stop a process in a processing plant?
- Stop the train?
- Activate the air bag (in a car)?
- Turn engine off for the plane?
- Stop the lift between two floors?

Fail-safe design principles

Fail-safe design means to ensure that the safe state of the protected system is achieved in case SIS reports failure, or SIS looses vital supportive systems like power.

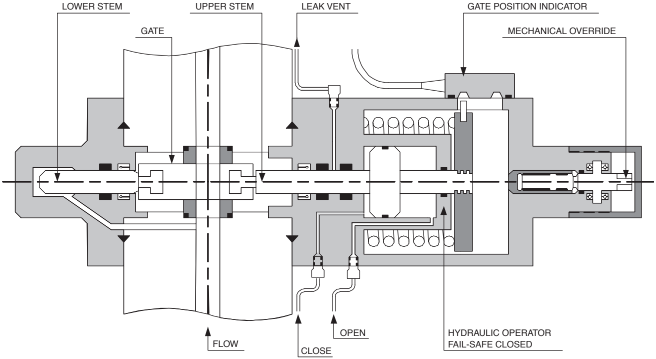
Typical fail-(to)-safe design principles in process industry are to:

- **Stop the protected system**: In this case, the de-energize to trip may be more
- **Do nothing**: In this case energize-to-trip may be suitable

Sometimes, the two above alternatives are not enough. In railway and aviation, it is sometimes distinguished between:

- **Fail-active**: SIS is able to change and maintain a new safe state, with provision of energy.
- **Fail-passive**: SIS is able to enter a safe state while energy is removed.
- **Fail-operational**: SIS is able to continue normal operation in presence of fault.

Example of Fail-Safe Design Principle of Valve



Functional Safety

☞ Functional safety: Part of the overall safety relating to the EUC and the EUC control system that depends on the correct functioning of the E/E/PE safety-related systems and other risk reduction measures. [IEC 61508]

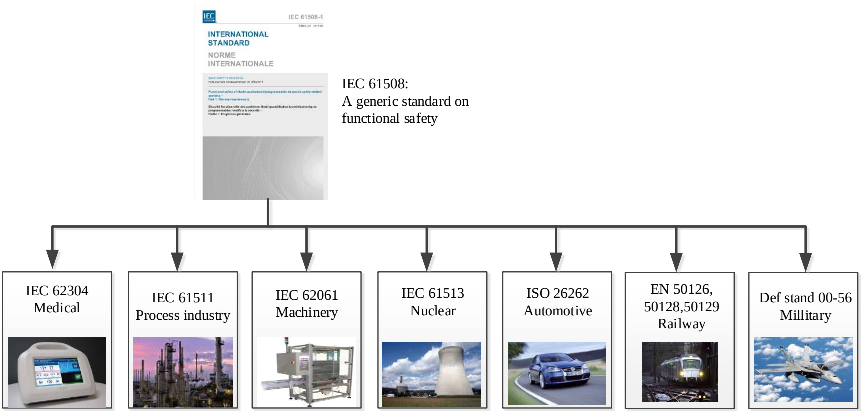
Functional safety is about the SIS's ability to:

- Interact with the EUC to prevent of mitigate the consequences of undesired events
- Ensure the safe state of the EUC in case of SIS failure

Functional Safety Standards

Functional safety standards have been introduced to ensure that the SIS is designed and operated so that the necessary risk reduction is achieved.

Examples of Standards



IEC 61508:
A generic standard on functional safety

IEC 62304
Medical

IEC 61511
Process industry

IEC 62061
Machinery

IEC 61513
Nuclear

ISO 26262
Automotive

EN 50126, 50128,50129
Railway

Def stand 00-56
Millitary

IEC 61508

IEC 61508 is the generic standard on functional safety, and is used by in particular by manufacturers that develop E/E/PE equipment and systems for use in safety-related applications.

IEC 61508 is named *Functional safety of electrical/electronic/programmable electronoic safety-related systems* and comprises 7 parts, of which 4 are mandatory and 3 are informative. The 1st edition came in 1998, and the current edition (2nd edition) is from 2010.

The purposes of IEC 61508 are to:

- Serve as a guideline for development of sector-specific standards.
- Serve as a standard where sector-specific standards do not exist or have certain restrictions on application areas.

IEC 61508

IEC 61508 is the umbrella standard for a collection of functional safety standards that aim to:

- Frame the safe implementation of electrical/electronic/programmable-electronic technology in safety applications
- Ensure adaption of best practices in all stages of the safety life cycle, from concept definition and specification of requirements to construction, installation, operation, maintenance, modifications, and eventually, decommissioning

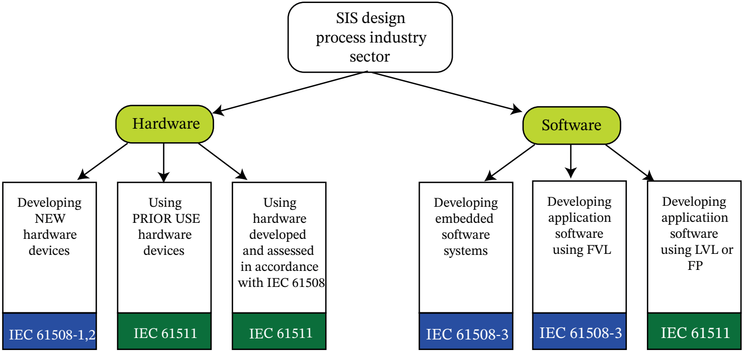
IEC 61508 in Parts

Part	Name	Comment	Status[1]
1	General requirements	Cover all life-cycle phases, from concept definition to decommissioning	N
2	Requirements for electrical/ electronic/ programmable electronic safety-related systems	Concerns hardware design and the integration hardware and software	N
3	Software requirements	Concerns requirements for software development, software development tools, and software architectures	N
4	Definitions and abbreviations	Given by the title.	N
5	Examples of methods for the determination of safety integrity levels	Explains methods like risk matrix, risk graph, and LOPA	I
6	Guidelines for the application of IEC 61508-2 and IEC 61508-3	Includes formulas for quantifying PFD and PFH and checklists for beta	I
7	Overview of techniques and measures	Elaborates on referenced topics	I

[1] N is normative, I is informative

IEC 61511 for the Process Industry

IEC 61511 is the sector standard for process industry when “proven” or certified safety devices are used to construct a SIS.


SIS design process industry sector
Hardware
Software
Developing NEW hardware devices
IEC 61508-1,2
Using PRIOR USE hardware devices
IEC 61511
Using hardware developed and assessed in accordance with IEC 61508
IEC 61511
Developing embedded software systems
IEC 61508-3
Developing application software using FVL
IEC 61508-3
Developing application software using LVL or FP
IEC 61511

IEC 61508: Manufacturers’ standard
IEC 61511: End users’ standard

FVL: Fixed variable language
LVL: Limited variable language

FP: Fixed programming

Brief about Other Standards

Standard	Mode of operation in focus
IEC 61508:	All modes of operation
IEC 61511:	Mainly low-demand
IEC 62061:	Mainly high/continuous-demand
EN 50126/,28,29[2]:	Mainly high/continuous-demand
ISO 26262:	Mainly high/continuous-demand

[2] Remark: IEC 62278, IEC 62425, and IEC 62279 are identical to EN 50126, EN 50129, and EN 50128, however, the EN version is more often referenced.