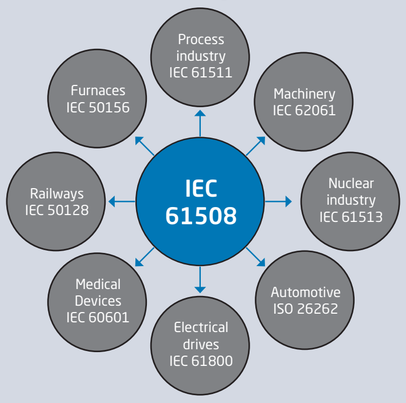
Process Industry Guide to SIL & Functional Safety

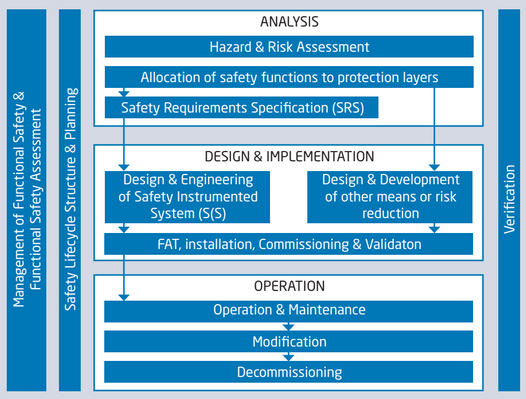
Functional Safety Fundamentals

Functional Safety Standards



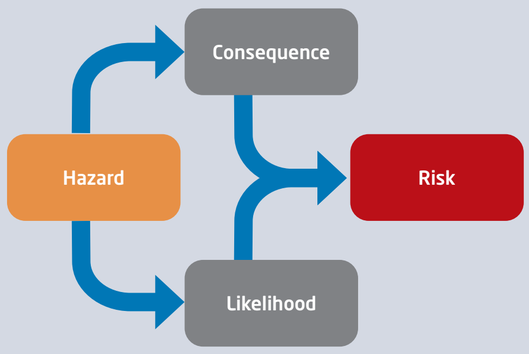
IEC 61508 is the umbrella Functional Safety standard and is the basis for industry specific functional safety standards.
For example **IEC 61511** is the standard specifically for use in the process industry.

IEC 61511 Safety Lifecycle



A **safety lifecycle** is used as the basis of safety. The **safety lifecycle** shown is based on IEC 61511 and is used by the process industry to demonstrate functional safety management from concept to decommissioning.

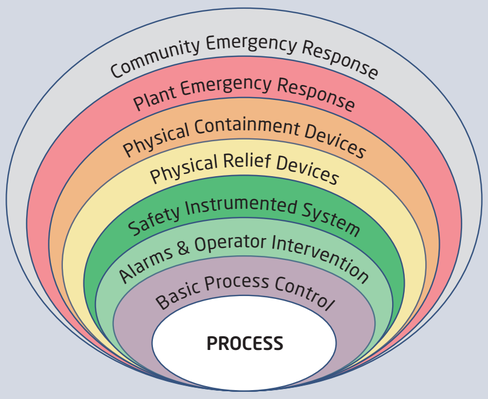
Hazard & Risk Assessment



A **hazard assessment** is carried out to identify potential hazards, and to understand the likelihood and consequences of specific associated events.
The **residual risk** is then compared against **tolerable risk**.

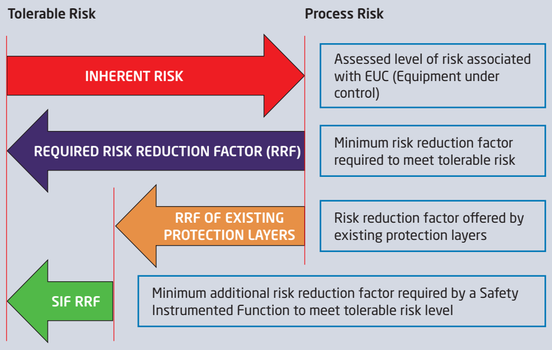
Target SIL Selection

Layer of Protection Analysis (LOPA)



Risk must be **quantified** to ensure existing risk reduction measures or layers of protection offer a risk reduction factor **(RRF)** large enough to reduce risk to a tolerable level.
A **LOPA** or layer of protection analysis is one method of doing this.

Target Risk Reduction Factor (RRF)



A **Safety Instrumented Function (SIF)** is required when the level of risk reduction offered by existing protection layers does not achieve a tolerable residual risk. A **Safety Integrity Level (SIL)** will be assigned depending on the additional risk reduction required.

Target SIL Assignment

Risk Reduction Factor (RRF)	Target SIL
> 10,000 to ≤ 100,000	**SIL 4**
> 1000 to ≤ 10,000	**SIL 3**
> 100 to ≤ 1,000	**SIL 2**
> 10 to ≤ 100	**SIL 1**

Risk Reduction Factor (RRF) vs Safety Integrity Level (SIL)

The minimum Risk Reduction Factor (RRF) required of the Safety Instrumented Function (SIF) determines its **Target SIL level.**
The above table shows the correlation between RRF and SIL, e.g. RRF of 200 = **SIL2** Safety Instrumented Function.

Safety Instrumented Function (SIF)

A Safety Instrumented Function (SIF) is made up of 3 subsystems, the sensor subsystem, logic solver and final element subsystem.

Sensor Subsystem
(e.g. sensors, I.S. interfaces)

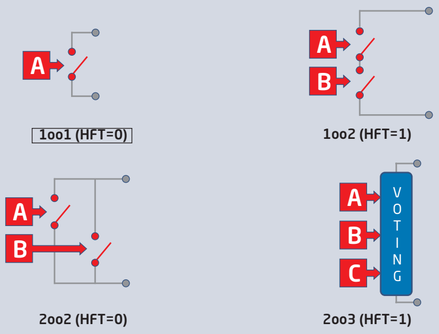
Logic Solver Subsystem
(e.g. safety PLC)

Final Element Subsystem
(e.g. valves, solenoids, I.S. interfaces)

To achieve a target SIL level, **IEC 61511** requires that the **Architectural Constraints, Hardware Integrity** and **Systematic Capability** of the SIF design are in accordance with the standard.
This is achieved through correct SIL **Component Selection**.

SIL Component Selection - Architectural Constraints

Example System Architectures



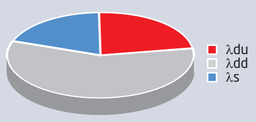
Various system architectures can be employed to meet the **Architectural Constraints or HFT** of the standard.
IEC 61511 Clause 11.4.3 states that **HFT** must comply with **IEC 61508 route 1H** or **IEC 61508 Route 2H / IEC 61511 clause 11.4.5 to 11.4.9**

Architectural Constraints - IEC 61508 Route 1_H

Safe Failure Fraction (SFF)		Hardware Fault Tolerance (HFT)		
Type A	**Type B**	**0**	**1**	**2**
	< 60%	N/A	SIL 1	SIL 2
< 60%	60% - < 90%	SIL 1	SIL 2	SIL 3
60% - < 90%	90% - < 99%	SIL 2	SIL 3	SIL 4
≥ 90%	≥ 99%	SIL 3	SIL 4	SIL 4

IEC 61508 Route 1_H HFT table

$$SFF = \frac{\lambda dd + \lambda s}{\lambda du + \lambda dd + \lambda s}$$



IEC 61508 Route 1_H defines hardware fault tolerance based on the Safe Failure Fraction SFF, and whether a Type A or B device.
Type A - Simple devices with well-defined failure modes.
Type B - Complex devices e.g. ASIC, microprocessor-based.

Architectural Constraints - IEC 61508 Route 2_H / IEC 61511

SIL	Demand Mode	Min. HFT
1	Any	0
2	Low Demand	0
2	High or Continuous	1
3	Any	1
4	Any	2

IEC 61508 Route 2_H / IEC 61511 HFT table

Route 2_H relies on field failure data to complement the FMEDA failure rates. Assuming a high confidence level is met in this data, then the reduced HFT can be applied. The **IEC 61511** route is based on prior use data and in accordance with **Clause 11.4.5 to 11.4.9**.

SIL Component Selection - Hardware Integrity

Probability of Failure

The mode of operation is used for classifying SIL.
Either **Low Demand** or **High / Continuous Demand** mode. Probability of failure is then determined via a **PDF_{avg}** of **PFH** calculation. The result must be within the target SIL range.

	Low Demand	High Demand
Target SIL	PFD_{avg} Range	PFH Range*
SIL 4	$\geq 10^{-5} < 10^{-4}$	$\geq 10^{-9} < 10^{-8}$
SIL 3	$\geq 10^{-4} < 10^{-3}$	$\geq 10^{-8} < 10^{-7}$
SIL 2	$\geq 10^{-3} < 10^{-2}$	$\geq 10^{-7} < 10^{-6}$
SIL 1	$\geq 10^{-2} < 10^{-1}$	$\geq 10^{-6} < 10^{-5}$

* IEC 61511, Clause 9.2.3 requirements

Low Demand mode safety functions require an average Probability of Failure on Demand - **PFD_{avg}** - calculation. This mode of operation is common in process industry applications.

PFD_{avg} Calculation

$$PFD_{avg} = \frac{\lambda du * TI}{2}$$

Simple 1oo1 **PFD_{avg}** calculation assuming 100% proof test effectiveness

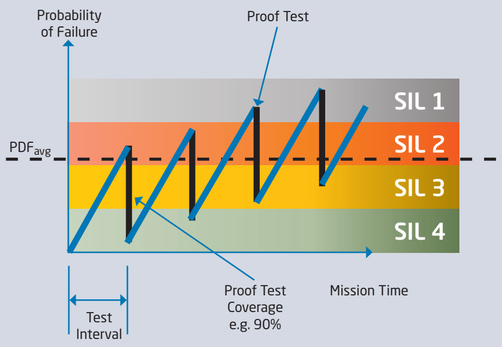
$$PFD_{avg} = \lambda dd * MTTR + \left[Cpt * \lambda du * \frac{TI}{2} \right] + \left[(1\text{-}Cpt) * \lambda du * \frac{MT}{2} \right]$$

More complex **1oo1 PFD_{avg}** calculation taking into account additional variables

- **λdd** Dangerous detected failures
- **λdu** Dangerous undetected failures
- **MTTR** Mean time to repair
- **Cpt** Proof test coverage
- **TI** Proof test interval
- **MT** Mission time

IEC 61508 Part 6 includes simplified equations for **PFD_{avg}** calculations.
For higher target SIL levels, adding additional variables to the calculation ensures a more accurate result.

Proof Test

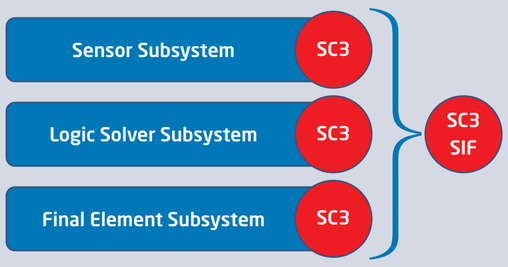


A **Proof Test** is carried out to identify hidden failures.
Proof Test Interval (TI), Proof Test Coverage (Cpt) and **Mission Time** are important variables in the SIL level **PFD_{avg}** calculation.

SIL Component Selection - Systematic Capability

Systematic Capability - SC1...SC4

Systematic Capability demonstrates the defence against systematic failures or errors in each subsystem. The **Systematic Capability** of a SIF is limited to the lowest **SC level** of the separate subsystem. **SC1 to SC4** relate to the Systematic Capability of each **SIL** level.



IEC 61511 Clause 11.5.2 guidelines state that devices selected for use in a SIF should be in accordance with **IEC 61508 Parts 2 & 3** and/or **IEC 61511 Clause 11.5.3** through 11.5.6 as appropriate.

IEC 61508 Certified - Route 1_S

IEC 61508 certified devices are independently assessed by an accredited certification body. They ensure that product hardware and software design is in accordance with the standard.

Parts 2 & 3 of **IEC 61508** detail strict guidelines for the design of both hardware and software to ensure systematic failures are reduced to a minimum:

IEC 61508-2:2010
Requirements for electrical/electronic/ programmable electronic safety-related systems
IEC 61508-3:2010
Software requirements


Certificate / Certificat
Zertifikat / 合格証
PREI 16031107 P002 C008
exida hereby confirms that the:
PR5435 / PR5437 / PR6437
Temperature Transmitters
Product Version V01.xx.xx
PR electronics A/S
Rønde - Denmark
Have been assessed per the relevant requirements of:
IEC 61508 : 2010 Parts 1-7
and meets requirements providing a level of integrity to:
Systematic Capability: SC 3 (SIL 3 Capable)
Random Capability: Type B Element
Evaluating Assessor
Certifying Assessor
Page 1 of 2

IEC 61508 certified devices will have a designated **SC level** from **SC1 to SC4** depending on the assessed SIL level. This will be clearly shown on the SIL certificate.

Prior Use - Route 2_S

IEC 61511 Clause 11.5.3 outlines selection of devices based on Prior Use. This route puts significant onus on the end user to provide the necessary reliability and usage data to meet the demands of the standard including:

- Demonstration of performance in same or similar operating environments
- Consideration of manufacturer's quality, management and configuration system
- Adequate identification and specification of devices
- H/W & S/W version control
- Volume of operating experience
- Full failure recording process
- Regularly reviewed failure modes

The main intent of the **Prior Use** evaluation is to gather credible, traceable and documented evidence that dangerous systematic faults have been reduced to a minimum.

Glossary

SIF	Safety Instrumented Function, typically consisting of a sensor subsystem, logic solver and final element subsystem
SIS	Safety Instrumented System consisting of one or more SIFs
SIL	Safety Integrity Level from SIL 1 to SIL 4
FIT	Failure in Time (1×10^9 / hour)
RRF	Risk Reduction Factor
Low Demand	Mode of operation with demand on safety function < 1 per year
High Demand	Mode of operation with demand on safety function > 1 per year
Continuous Demand	Mode of operation with continuous demand on safety function
HFT	Hardware Fault Tolerance
MTTR	Mean Time to Repair
PFD	Probability of Failure on Demand
PFH	Probability of Failure per Hour
DC	Diagnostic Coverage
SC	Systematic Capability
λdd	Dangerous detected failures (per hour)
λdu	Dangerous undetected failures (per hour)
λs	Safe failures (per hour)
Proof Test	Periodic test to identify hidden failures
Ti	Time Interval between Proof Tests
Cpt	Effectiveness of proof test expressed as a percentage
Useful Lifetime	Lifetime based on device bathtub curve
Mission Time	Proposed runtime prior to decommissioning
β factor	Multiplier based on common cause influences
D10	Multiplier based on cyclic devices, e.g. relays
1oo1	One out of one system architecture
1oo2	One out of two system architecture

www.prelectronics.com

1017UK (2307)