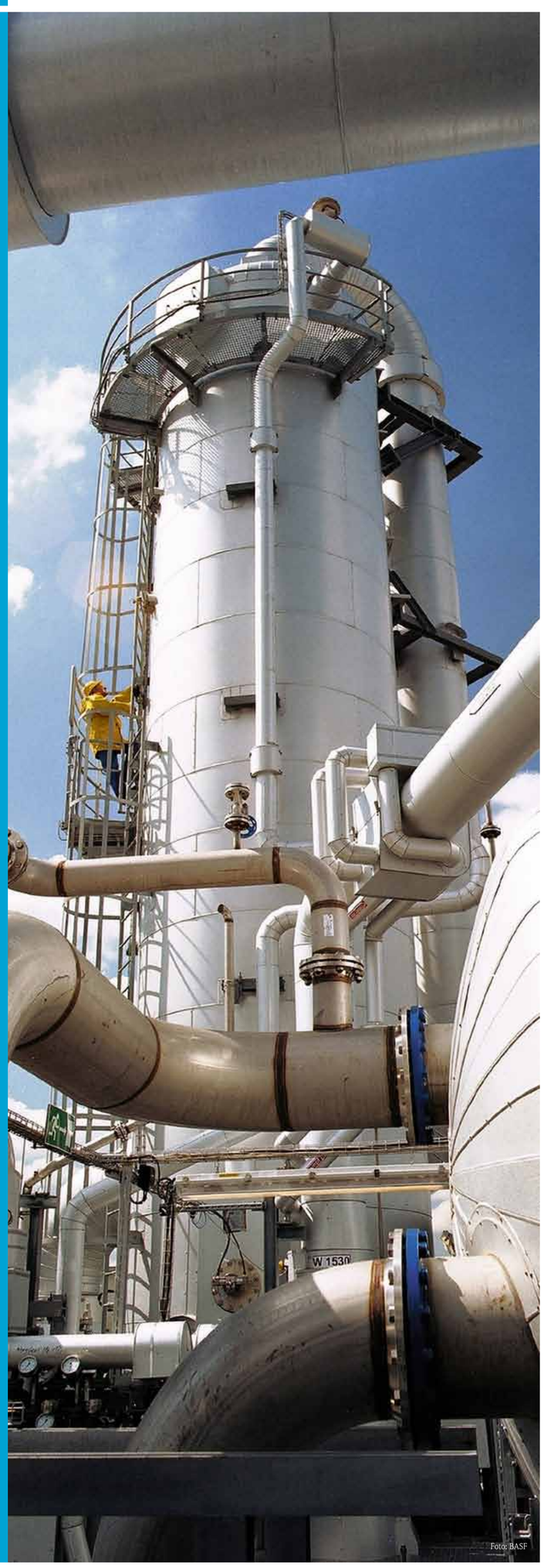
Functional Safety

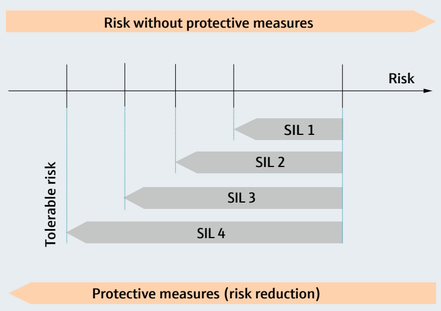
SIL (Safety Integrity Level)

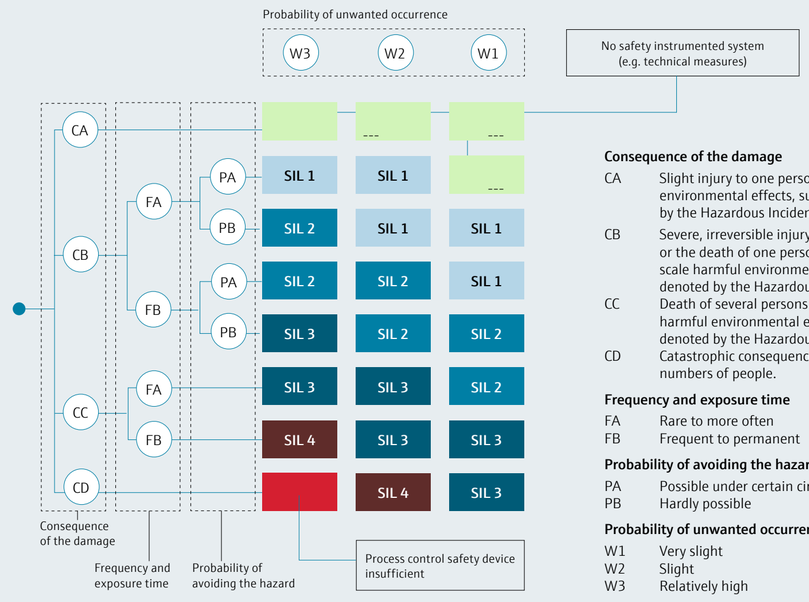


Process risk

Process plant, machine
Risks for people, environment and assets

Risk reduction by implementation of SIL





Consequence of the damage
- CA Slight injury to one person or minor harmful environmental effects, such as those not covered by the Hazardous Incidence Ordinance.
- CB Severe, irreversible injury to one or more persons or the death of one person or temporary, large-scale harmful environmental effects such as those denoted by the Hazardous Incidence Ordinance.
- CC Death of several persons or persistent, large-scale harmful environmental effects, such as those denoted by the Hazardous Incidence Ordinance.
- CD Catastrophic consequences, death of large numbers of people.

Frequency and exposure time
- FA Rare to more often
- FB Frequent to permanent

Probability of avoiding the hazard
- PA Possible under certain circumstances
- PB Hardly possible

Probability of unwanted occurrence
- W1 Very slight
- W2 Slight
- W3 Relatively high

Technical requirements

Determination of safety parameters
FMEDA

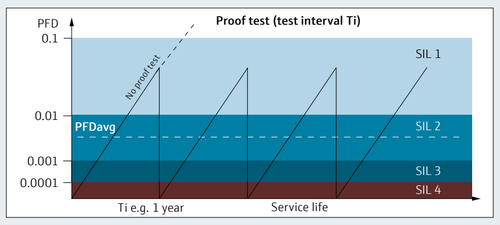
Technical requirements		
Failure types of safety functions and subsystems		
Failure type	Detected	Undetected
Safe	Safe detected λSD	Safe undetected λSU
Dangerous	Dangerous detected λDD	Dangerous undetected λDU

SIL – PFDavg – PFH – modes of operation		
Safety Integrity Level (SIL)	Average probability of failure to perform a safety function on demand – PFD (Average failure probability of the safety function with low demand) (less then 1/year)	Probability of a dangerous failure per hour – PFH (High demand or continuous mode of operation)
SIL 4	$\geq 10^{-5}$ to $<10^{-4}$	$\geq 10^{-9}$ to $<10^{-8}$
SIL 3	$\geq 10^{-4}$ to $<10^{-3}$	$\geq 10^{-8}$ to $<10^{-7}$
SIL 2	$\geq 10^{-3}$ to $<10^{-2}$	$\geq 10^{-7}$ to $<10^{-6}$
SIL 1	$\geq 10^{-2}$ to $<10^{-1}$	$\geq 10^{-6}$ to $<10^{-5}$

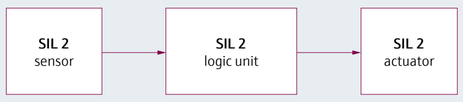
SFF – HFT – SIL – type A, type B

Safe failure fraction (SFF)	Hardware fault tolerance (Type A – simple equipment)			Hardware fault tolerance (Type B – complex equipment)		
	0	1	2	0	1 (0*)	2 (1*)
<60 %	SIL 1	SIL 2	SIL 3	Not permitted	SIL 1	SIL 2
60 % to <90 %	SIL 2	SIL 3	SIL 4	SIL 1	SIL 2	SIL 3
90 % to <99 %	SIL 3	SIL 4	SIL 4	SIL 2	SIL 3	SIL 4
≥99 %	SIL 3	SIL 4	SIL 4	SIL 3	SIL 4	SIL 4

* With proven-in-use demonstration acc. to IEC 61511 (for SIL ≤3 only)



SIL calculation

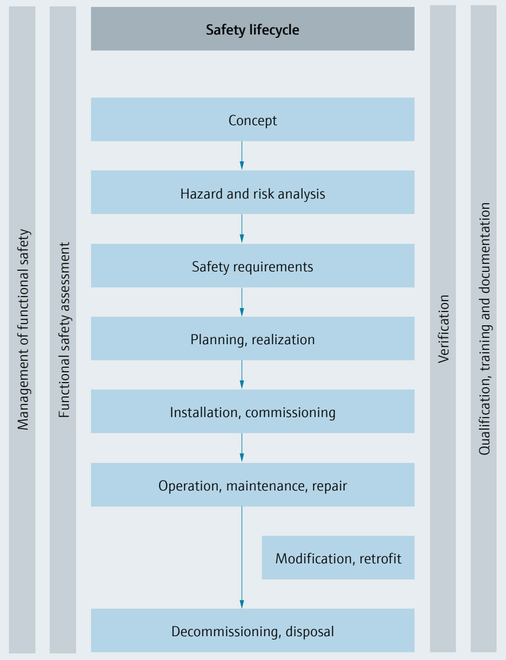


Single-channel architecture
The PFDavg/PFH values of all components have to be summed up and evaluated.

PFD = ½ λDU × Ti

PFH = λDU

Organizational requirements



Terminology

- **Functional safety:** Part of the overall safety which depends on the correct functioning of safety-related systems for risk reduction. Functional safety is achieved when every safety function is performed as specified.
- **Safety-related system:** System that implements the safety functions required to achieve or maintain a safe state for equipment under control (EUC).
- **Safety function:** Function which is intended to achieve or maintain a safe state for equipment under control (EUC), in respect of a specific hazardous event.
- **Safety lifecycle:** Describes all necessary activities involved in the implementation of safety-related systems, starting at the concept phase and ending at the decommissioning.
- **Management of functional safety:** Necessary management and technical activities and responsibilities during the safety lifecycle for achievement of functional safety.
- **Functional safety assessment:** Investigation, if functional safety was achieved by the safety-related systems.
- **Safety Integrity Level (SIL):** Four discrete levels (SIL 1 to SIL 4). The higher the SIL of a safety-related system, the lower the probability that it will not perform the required safety functions.
- **Average Probability of Failure on Demand (PFDavg):** Average probability of failure of a safety function working in low demand mode of operation.
- **Probability of Failure per Hour (PFH):** For high or continuous demand, the numerical measure of PFH is used, which specifies the probability of a failure of the safety function per hour (dangerous failure rate).
- **Safe Failure Fraction (SFF):** Percentage part of safe failures and dangerous detected failures of a safety function or a subsystem related to all failures.
- **Hardware Fault Tolerance (HFT):** HFT = n means, that n+1 faults could cause a loss of the safety function.
- **Low demand mode of operation:** Frequency of demands on a safety-related system no greater than one per year and no greater than twice the proof-test frequency.
- **High demand or continuous mode of operation:** Frequency of demands on a safety-related system greater than one per year or greater than twice the proof-test frequency.
- **Device type A (simple subsystem):** The failure modes of all constituent components are well defined and the behaviour under fault conditions can be completely determined.
- **Device type B (complex subsystem):** The failure mode of at least one constituent component is not well defined (e.g. µC, ASIC) and the behaviour under fault conditions cannot be completely determined.
- **FMEDA (Failure Modes, Effects and Diagnostic Analysis):** Systematic way to identify and evaluate the effects of different component failure modes, to determine what could eliminate or reduce the chance of failure, and to document a system in consideration.
- **Failure rates:**
  λSD: Total failure rate for safe detected failures
  λSU: Total failure rate for safe undetected failures
  λDD: Total failure rate for dangerous detected failures
  λDU: Total failure rate for dangerous undetected failures
- **Mean Time Between Failures (MTBF):** Statistical measure of failure rates to determine how reliable a component is.
- **Proof-test interval (T1):** Interval between periodic tests performed to detect failures in a safety-related system.

Standards

- **Basic standard:** IEC 61508
- **Application sector standards:**
  IEC 61511 (process industry
  IEC 61513 (nuclear power plants)
  IEC 62061 (machinery)
  IEC 61800-5-2 (power drive systems)

Safety Integrity Level SIL Endress+Hauser

Endress+Hauser

People for Process Automation