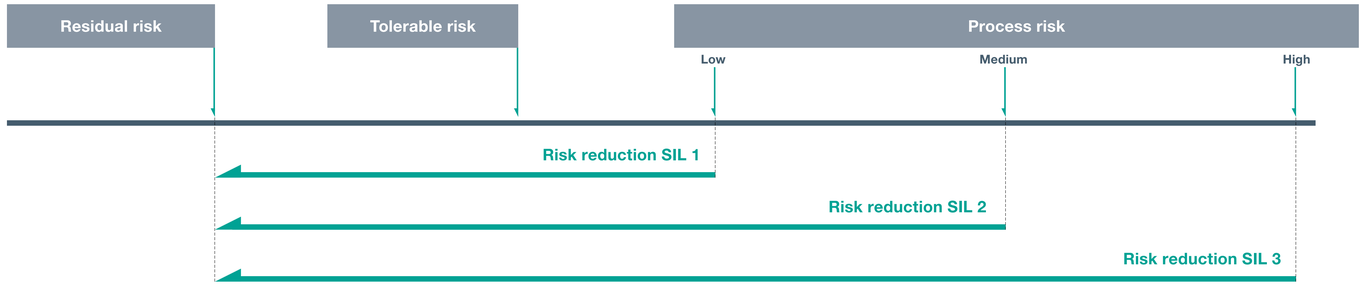
Functional Safety in the Process Industry

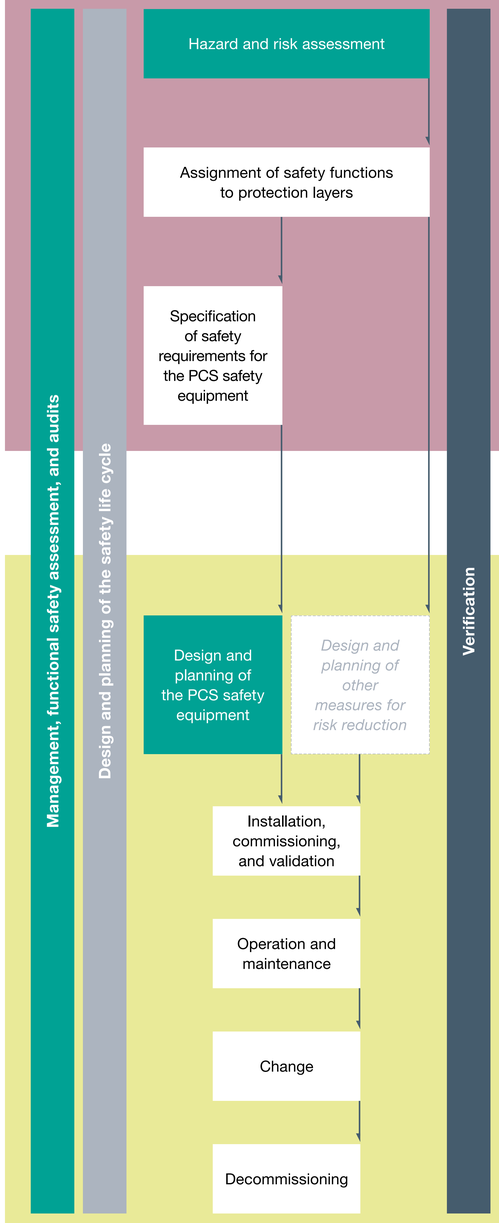
www.pepperl-fuchs.com/functional-safety

Risk-Based Approach



Possibilities of Device Qualification
Manufacturer declaration
Proven in use
Fault elimination
Type examination
Full diagnosis

Phases of the Safety Life Cycle



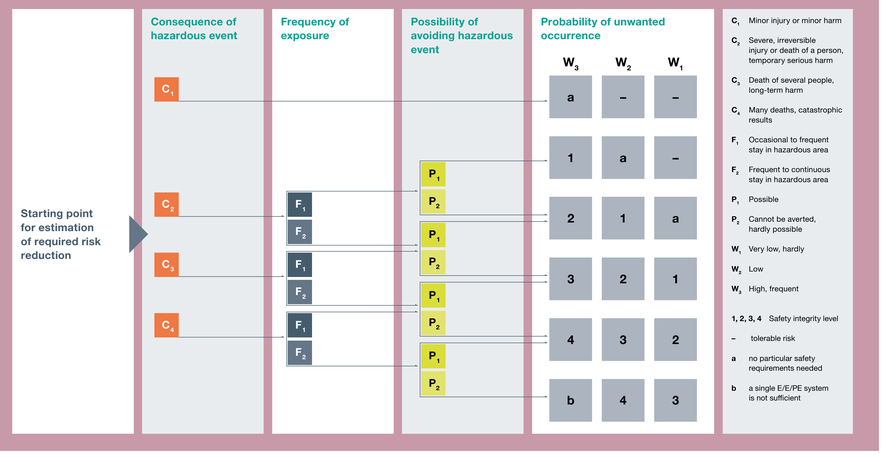
Identifying Sources of Danger

HAZOP/PAAG (IEC 61882)

Guide word	Meaning
No/not	Complete negation of the intended goal
More	Quantitative increase
Less	Quantitative decrease
Both/as well as	Qualitative change/increase
In part	Qualitative change/decrease
Reverse (of intent)	Logical opposite to the intended goal
Other than	Complete exchange/replacement

Early	Relative to the time of day
Late	Relative to the time of day
Before	Relative to the sequence or process
After	Relative to the sequence or process

Quantifying Required Risk Reduction



SIL IEC/EN 61508 → IEC/EN 61511 → VDI/VDE 2180

Design Requirements

Minimum hardware fault tolerance (HFT) depending on the SIL	
SIL	**HFT**
SIL 1—Every mode of operation	0
SIL 2—Mode of operation with low demand	0
SIL 2—Mode of operation with high/continuous demand	1
SIL 3—Every mode of operation	1
SIL 4—Every mode of operation	2

Note: Devices must be proven suitable for the application.

Probability of failure per hour at a high demand mode (> 1 demand per year)		
SIL	**PFH [1/h]**	**Max. accepted failure of the SIS**
SIL 1	≥ 10^{-6} to < 10^{-5}	Max. 1 dangerous failure per 100 000 hours
SIL 2	≥ 10^{-7} to < 10^{-6}	Max. 1 dangerous failure per 1 000 000 hours
SIL 3	≥ 10^{-8} to < 10^{-7}	Max. 1 dangerous failure per 10 000 000 hours
SIL 4	≥ 10^{-9} to < 10^{-8}	Max. 1 dangerous failure per 100 000 000 hours

Probability of failure at a low demand mode (≤ 1 demand per year)		
SIL	**PFD**	**Max. accepted failure of the SIS**
SIL 1	≥ 10^{-2} to < 10^{-1}	Max. 1 dangerous failure per 10 demands
SIL 2	≥ 10^{-3} to < 10^{-2}	Max. 1 dangerous failure per 100 demands
SIL 3	≥ 10^{-4} to < 10^{-3}	Max. 1 dangerous failure per 1000 demands
SIL 4	≥ 10^{-5} to < 10^{-4}	Max. 1 dangerous failure per 10 000 demands

Implementation

HFT	Reliability block diagram	Plant safety	Plant availability	PFD (according to VDI/VDE 2180)
0	A	o	o	$\lambda_{du} \cdot \frac{T_1}{2}$
0	A, B: 2oo2	-	+	$\lambda_{du} \cdot T_1$
1	A, B: 1oo2	+	-	$\frac{\lambda_{du}^2 \cdot T_1^2}{3} + \beta \cdot \lambda_{du} \cdot \frac{T_1}{2}$
1	A, B, C: 2oo3	+	+	$\lambda_{du}^2 \cdot T_1^2 + \beta \cdot \lambda_{du} \cdot \frac{T_1}{2}$
2	A, B, C: 1oo3	++	-	$\frac{\lambda_{du}^3 \cdot T_1^3}{4} + \beta \cdot \lambda_{du} \cdot \frac{T_1}{2}$

Glossary

BCPS—basic process control system	System which responds to input signals from the process, its associated equipment, other programmable systems and/or an operator and generates output signals causing the process and its associated equipment to operate in the desired manner.
CCF—Common Cause Failure (failure resulting from a common cause)	Failure resulting from one or more events that cause the failure of 2 or more separate channels in a multi-channel system and lead to a system failure.
EUC—equipment under control	Equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities.
Dangerous failure	Failure with the potential to place the safety instrumented system into a dangerous or inoperative condition.
Fault tolerance	The ability of a functional unit to continue carrying out a required function where there are faults or errors.
Functional safety	A part of overall safety, based on the process and the BPCS, and dependent on the intended function of the SIS and other levels of safety.
Lambda du (λ_{du})	The dangerous undetected failure rate (per hour) of a channel in a subsystem.
MooN system ("M out of N")	Safety instrumented system or part of it, consisting of "N" independent channels, which are connected in such a way that "M" channels are sufficient to fulfill the safety function in each case.
Necessary risk reduction	Risk mitigation to ensure that the acceptable risk (target risk) limit is not exceeded.
PCS safety equipment	Process control system which prevents an impermissible fault range from being reached either by an automatic intervention in the process or by means of a signal which alerts operating personnel.
PFD—Probability of Failure on Demand	Safety-related non-availability of an E/E/PE safety-related system to carry out a specified safety function when a demand comes from the EUC, the EUC management system, or the EUC control system.
PFH—Probability of Failure per Hour	Average frequency of a dangerous failure of an E/E/PE safety-related system to carry out the specified safety function for a defined time.
Protection Layer	Any independent mechanism that reduces risk by control, prevention or mitigation.
Process risk	Risk arising from process states caused by exceptional events (including malfunctions of the BPCS).
Proof test	Test for the detection of hidden faults in a safety instrumented system, so that, if necessary, the system can be brought back to the condition in which it fulfills its intended function.
Proven-in-use	A component is proven-in-use if an appropriately documented investigation has shown that evidence from prior applications is sufficient to prove that the component is suitable for use in a safety instrumented system.
Random failure	Failure that occurs at a random point in time and is caused by one or more possible hardware mechanisms that result in a deterioration of component properties.
Risk	Combination of probability of causing harm and the severity level of this harm.
Safe failure	Failure without the potential to place the safety instrumented system in a dangerous or inoperative condition.
Safety instrumented function for high/continuous demand mode	In cases where failure of the safety instrumented function may lead to a hazard, without further failure, if no action is taken to prevent this.
Safety instrumented function in demand modes	In cases where the specified action (e.g., closing a valve) is introduced as a response to process states or other demands. In the case of a dangerous failure of the safety instrumented function, a potential hazard only occurs where the process or BPCS fails.
Safety life cycle	The activities necessary for implementing safety instrumented functions during a period that begins with the conceptual phase of a project and ends when all safety instrumented functions are no longer available for use.
Safety manual	Manual that describes the safe use of a device, subsystem, or system.
SFF—Safe Failure Fraction	Proportion of overall failure rate for random failures of a device that result in either a safe failure or a dangerous detected failure.
SIF—Safety Instrumented Function	Function that is triggered by one or more protection layers. In the case of the occurrence of a defined harmful event SIF has the aim to achieve or maintain a safe state for the process.
SIL—Safety Integrity Level	One of 4 discrete steps for specifying the safety integrity requirements of the safety instrumented functions assigned to the safety instrumented system. Safety integrity level 4 is the highest level of safety integrity; safety integrity level 1 is the lowest.
SIS—Safety Instrumented System	Safety instrumented system for performing one or more safety instrumented functions. A SIS consists of one or more sensors, actuators, and a logic system.
Specification of the safety requirement	Specification containing all the requirements that apply to the safety instrumented functions to be carried out by the safety instrumented system.
Systematic failure	Systematic malfunction/failure for which a clear cause can be determined, and where this cause can only be eliminated by modifying the design or manufacturing process, the means of operation, instruction manual, or other influencing factors.
Tolerable risk	Risk that will be accepted in a given context based on applicable societal values.

Your automation, our passion.

PEPPERL+FUCHS