SIL
(Safety Instrument Level)

Safety function
(Sensor + logic solver + actuator)

Function that is intended to achieve or maintain a safe state for equipment under control (EUC), with respect to a specific hazardous event.

Failure types of safety functions and subsystems

Failure type	Detected	Undetected
Safe	Safe detected SD	Safe undetected SU
Dangerous	Dangerous detected DD	Dangerous undetected DU

= SFF (Safe Failure Fraction) in %

Determination of safety-related parameters

FMEDA

Failure rates λ_{SD} , λ_{SU} , λ_{DD} , λ_{DU}

SFF, PFD_{av}, HFT, MTBF

Low demand mode of operation

Frequency of demands on a safety-related system is not 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 is greater than one per year or greater than twice the proof-test frequency.

PFD$_{av}$ (Average probability of dangerous failure on demand)

Average probability of failure of a safety function working in the low demand mode of operation.

Dangerous Failure Rate [1 / h]

Probability of failure of a safety function working in high demand or continuous mode of operation.

Device type A (simple subsystem)

Device in which the failure modes of all seential components are well defined.

Device type A (complex subsystem)

Device in which the failure modes of at least one essential component is not well defined (e.g. µC, ASIC).

SFF (Safe Failure Fraction)

Percentage of safe failures and dangerous detected failures of a safety function sub-system related to all failures.

HFT (Hardware Fault Tolerance)

HFT = n means that n+1 faults could cause a loss of the safety function.

Proven-in-use

Demonstration according to IEC 61511 that a device (safety function subsystem) has worked without failure within a defined number of operating hours and applications.

SIL
(Safety Instrument Level)

FMEDA (Failure Modes, Effects and Diagnostics 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.

MTBF (Mean Time between Failures)

Mean time between two failures.

SIL (Safety Integrity Level)

Four discrete level (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 function.

	Safety Integrity Level (SIL)	**SIL 1**		
Safety function	**PFD**	**$10^{-2} \le … < 10^{-1}$**		
	Safety - related availability	> 90 %		
	Risk reduction factor	> 10		
	Dangerous Failure Rate [1/h]	**$\ge 10^{-6} … < 10^{-5}$**		
Safety function subsystem	**HFT**	**0**	**1**	**2**
	Type A: SFF[1]	< 60 %	<60 %	<60 %
	Type B: SFF[1]	60 <...<90 %	<60 %	<60 %
	Type B proven-in-use[2] : SFF[3]	60 <...<90 %	<60 %	<60 %

	Safety Integrity Level (SIL)	**SIL 2**		
Safety function	**PFD**	**$10^{-3} \le … < 10^{-2}$**		
	Safety - related availability	> 99 %		
	Risk reduction factor	> 100		
	Dangerous Failure Rate [1/h]	**$\ge 10^{-7} … < 10^{-6}$**		
Safety function subsystem	**HFT**	**0**	**1**	**2**
	Type A: SFF[1]	60 <...< 90 %	<60 %	<60 %
	Type B: SFF[1]	90 <...<99 %	60 <...<90 %	<60 %
	Type B proven-in-use[2] : SFF[3]	60 <...<90 %	60 <...<90 %	<60 %

SIL
(Safety Instrument Level)

	Safety Integrity Level (SIL)	SIL 3		
Safety function	**PFD**	**$10^{-4} \leq … < 10^{-3}$**		
	Safety - related availability	> 99,9 %		
	Risk reduction factor	> 1.000		
	Dangerous Failure Rate [1/h]	**$\geq 10^{-8} … < 10^{-7}$**		
Safety function subsystem	**HFT**	**0**	**1**	**2**
	Type A: SFF[1]	≥ 90 %	60 <…<90 %	<60 %
	Type B: SFF[1]	≥ 99 %	90 <…<99 %	60 <…<90 %
	Type B proven-in-use[2] : SFF[3]	≥ 99 %	60 <…<90 %	60 <…<90 %

	Safety Integrity Level (SIL)	SIL 4		
Safety function	**PFD**	**$10^{-5} \leq … < 10^{-4}$**		
	Safety - related availability	> 99,99 %		
	Risk reduction factor	> 10.000		
	Dangerous Failure Rate [1/h]	**$\geq 10^{-9} … < 10^{-8}$**		
Safety function subsystem	**HFT**	**0**	**1**	**2**
	Type A: SFF[1]	-	≥ 90 %	≥ 60 %
	Type B: SFF[1]	-	≥ 99 %	≥ 90 %
	Type B proven-in-use[2] : SFF[3]	-	-	-

[1] acc. to IEC 61508

[2] for sensors, actuators and non-progarmmable logic solvers

[3] acc. To IEC 61511