

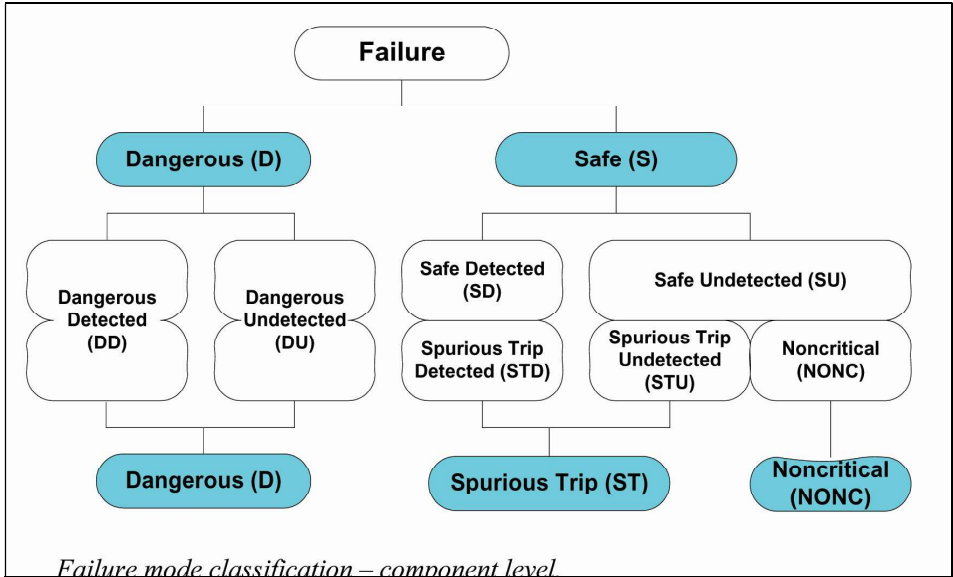
-Figure 7 Failure probability distribution

The fraction of failure probabilities that produce a safe condition is now called SFF (Safe Failure Fraction) and is therefore:

$$SFF = \sum \lambda \text{ safe} / (\sum \lambda \text{ safe} + \sum \lambda \text{ dangerous})$$

The λ_s is also called in English STR (Spurious Trip Rate). STR is a measure of availability according to operability

The failure probability classification with the usual English terms according to IEC61508 looks like this:



-Figure 8 Failure probability distribution

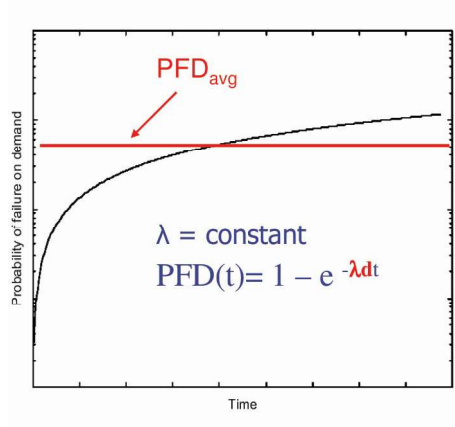
λ is difficult to obtain from manufacturers. Often companies build a (reliability) database with their own data.

The term MTBF is also used, i.e. Mean Time Between Failure

$$MTBF = 1 / \lambda - \lambda = 1 / \lambda$$

Possible Failure on Demand (PFD)

The term PFD (Possible Failure on Demand) is often used, which is the probability that a system designed to prevent an accident will fail at the very moment when the preventive function is called upon. PFD is therefore a measure of safety availability. The relationship between λ and PFD is as follows:



-Figure 9 PFD distribution

Failure frequency λ_{du} is used here and is assumed to be constant (which is often not the case).

The chance of failure therefore increases exponentially over time.

In practice, the average PFD is used. The simplest formula for the average PFD (PFD_{avg}) is defined as follows (for 1oo1 switching)

$$PFD_{avg} = \lambda^{DU} \times \frac{TI}{2}$$

-- $\gamma_{OU} = 1/MTTF_{YOU}$

λ_{du} = undetected unsafe failure rate
 TI = time interval between two manual tests.
 MTTF = Mean Time To Failure

In the literature the term β is also often used. β is the common cause failure factor and is a measure of the degree of mutual interference between components, that is, the occurrence of errors and failures with a common cause. This factor is used in the PFD calculation but is omitted here. This can be optimized by avoiding mutual influence or limiting its consequences, through: separation of system components (e.g. different transmission paths), diversity of components (e.g. different measuring principles or brands, different programming languages) and sufficient training

The relationship between the SIL level and the average PFD now looks like this:

PFD	SIL
$10^{-2} < \text{PFD} \leq 10^{-1}$	1
$10^{-3} < \text{PFD} \leq 10^{-2}$	2
$10^{-4} < \text{PFD} \leq 10^{-3}$	3
$10^{-5} < \text{PFD} \leq 10^{-4}$	4

-Figure 10 SIL as a function of PFD

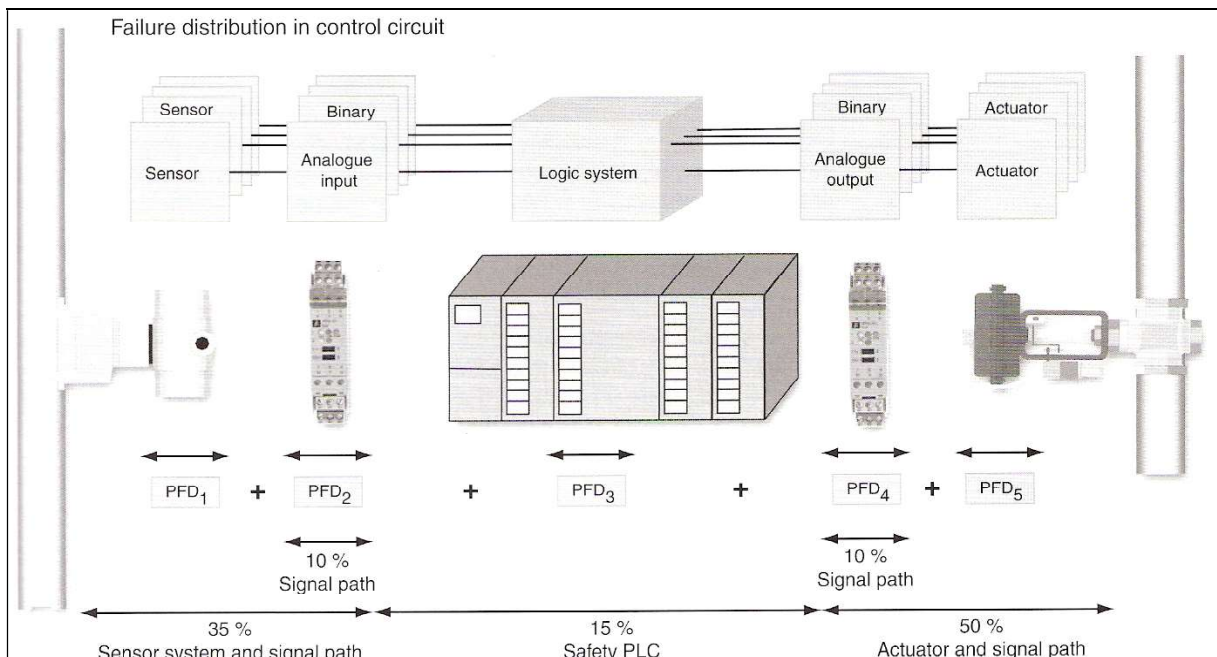
The term $\text{RRF} = 1 / \text{PFD avg}$ is also often used; i.e. the Risk Reduction Factor.

For all SIFs in a SIS the (average) PFD looks like this (see also fig.11):

$$\text{PFD sis} = \sum \text{PFD 1} + \sum \text{PFD 2} + \sum \text{PFD 3} + \sum \text{PFD 4} + \sum \text{PFD 5}$$

PFD 1 = PFD sensor (of a specific SIF) PFD 2 = PFD input card (of a specific SIF) PFD 3 = PFD logic system (of a specific SIF) PFD 4 = PFD output card (of a specific SIF) PFD 5 = PFD actuator (of a specific SIF)

Graphically this looks like this:



-Figure 11 PFD distribution of a SIS

Once the total PFD is known, the SIL classification can be determined using Fig. 10.

Hardware fault tolerance (HFT):

A SIS or part of a SIS is said to be fault-tolerant if it continues to perform its safety function despite the presence of one or more failed components.

The SFF is used to determine the (hardware) fault tolerance of a subsystem. There are two types of subsystems: type A (for example transmitters) for this the possible failure probabilities can be determined for all elements; for type B (for example logic solvers in PLCs) the possible failure probabilities can be determined for all elements not all possible failure probabilities are determined. The HFT itself also has three classes, namely 0, 1 and 2. The following tables now apply:

Safe failure fraction (SFF)	Hardware fault tolerance (HFT)		
	0	1	2
< 60 %	SIL1	SIL2	SIL3
60 % ... 90 %	SIL2	SIL3	SIL4
90 % ... 99 %	SIL3	SIL4	SIL4
> 99 %	SIL3	SIL4	SIL4

-Figure 12 HFT type A

Safe failure fraction (SFF)	Hardware fault tolerance (HFT)		
	0	1	2
< 60 %	not allowed	SIL1	SIL2
60 % ... 90 %	SIL1	SIL2	SIL3
90 % ... 99 %	SIL2	SIL3	SIL4
> 99 %	SIL3	SIL4	SIL4

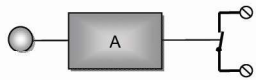
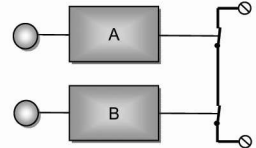
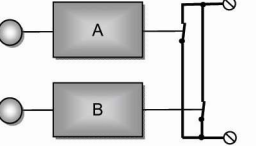
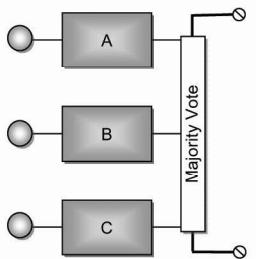
-Figure 13 HFT type B

Reliability and availability :

The reliability of a system can be defined as the probability (chance) that it performs its function successfully for a given period of time. For a SIF this means that the availability of a system (or function) can be defined as the probability (chance) that it performs its function successfully during the test interval. If no repair takes place during the test interval then: reliability = availability.

Hardware architecture:

Sensors and PLCs can be constructed according to different systems - also called architectures. Depending on the construction, the λ_d and λ_s can increase or decrease. Depending on whether one wants a system with higher safety and/or higher redundancy, one can choose from different configurations. The system in a SIF that reads the inputs, executes an algorithm and can send the output(s) to a safe state is called a logic solver. See the following description of safety PLCs for this. The architecture for sensors is called logic voting. The following architectures are discussed: 1oo1, 1oo2, 2oo2 and 2oo3. In fig. 14, A and B are transmitters and/or switches. The middle column shows the architecture, the right column shows the PFD avg.

1oo1		$PFD_{avg} = \lambda_{DU} \times \frac{TI}{2}$
1oo2		$PFD_{avg} = ((\lambda_{DU})^2 \times TI^2) / 3$
2oo2		$PFD_{avg} = \lambda_{DU} \times TI$
2oo3		$PFD_{avg} = (\lambda_{DU})^2 \times TI^2$

-Figure 14 Voting systems