Safety@Festo

Evaluation and assessment of safety measures
in accordance with EN ISO 13849-1/IEC 61508/IEC 61511/IEC 62061

Risk assessment

Risk analysis → **Risk evaluation** → **Risk reduction**
- → Design measures
- → Technical measures
- → User information

10 safety functions

Pressurising; Maintaining pressure; Reducing pressure and force; Exhausting; Tamper-proof, prevention of unexpected starting-up
Two-hand control; Reducing speed; Free of forces; Reversing a movement; Stopping, holding and blocking a movement

Trigger event	Input	Logic	Output	Drive
What triggers the safety measure?	Device that recognises the trigger situation	Device that safely processes the signal	Device that controls the dangerous movement	
For example: • Approaching a hazardous area • Opening a safety door	• Light curtain • Safety door • Pressure mat • Emergency Stop • Failure • Laser scanner • Camera	• Hard-wiring • Safety relay • Safety PLC • Pneumatic control system	• Pneumatic • Elektrical • Hydraulic Energy	

FESTO

www.festo.com

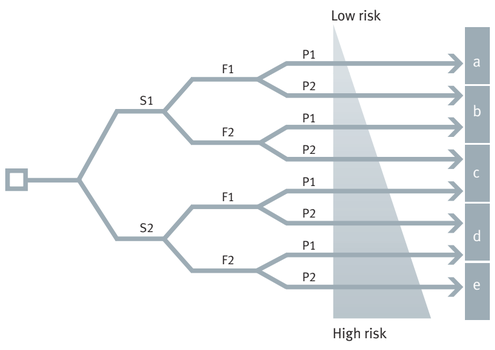
6 steps for evaluating whether safety measures are sufficient

EN ISO 13849-1 Applicable to safety-related parts of control systems and for all types of machines, regardless of the technology and power used – electric, pneumatic, hydraulic, mechanic.

IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems
IEC 61511 Functional safety – safety instrumented systems for the process industry sector.
IEC 62061 Safety of machinery – functional safety of safety-related electrical, electronic and programmable electronic control systems.

Evaluation of the application

1 Risk assessment Determining the required **Performance Level (PL_r)**



S Severity of injury
- S1 Slight (normally reversible injury)
- S2 Serious (normally irreversible injury, or death)

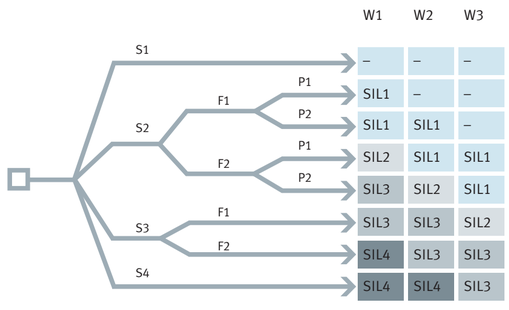
F Frequency and/or exposure to hazard
- F1 Seldom to less often and/or exposed time is short
- F2 Frequent to continuous and/or exposed time is long

P Possibility of avoiding the hazard
- P1 Possible under specific conditions
- P2 Scarcely possible

a – e Performance Level (PL_r)

Source: DIN EN ISO 13849-1 Appendix 1.2.3

Determining the required **Safety Integrity Level (SIL_r)**



- **SIL (Safety Integrity Level)**
  Four discrete steps (SIL1 to SIL4). The higher the SIL of a safety-related system, the lower the probability of the system not being able to execute the necessary safety functions.

S Consequence
- S1 Minor injuries to a person
- S2 Severe injury to multiple persons up to death of a person
- S3 Multiple deaths
- S4 Catastrophic effects with many deaths

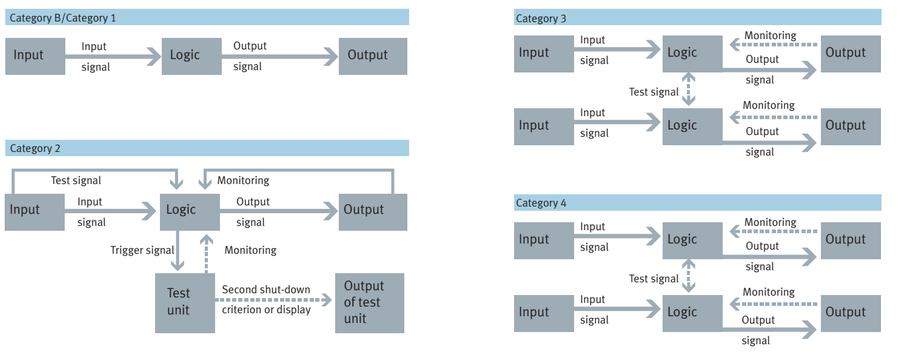
F Frequency
- F1 Seldom to reasonably frequent
- F2 Frequent to continuous

P Possibility of avoidance
- P1 Possible under certain conditions
- P2 Scarcely possible

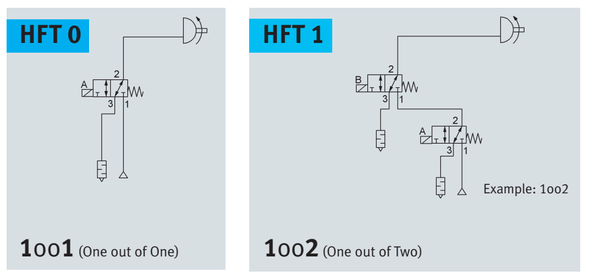
W Probability of occurrence
- W1 Relatively high
- W2 Low
- W3 Very low

Evaluation of safety measures

2 Designated architectures Specifications of **categories**



HFT Defining the **Hardware Failure Tolerance**



A single failure can lead to a loss of safety

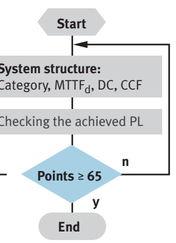
At least 2 failures must occur simultaneously to cause a loss of safety

At least 3 failures must occur simultaneously to cause a loss of safety

- **HFT (Hardware Failure Tolerance)**
  Ability of a required function to still perform in case of failures and deviations

3 CCF Common Cause Failure/DC Determining Diagnostics Coverage

Measures against CCF	Points
Separation/Segregation	15
Diversity	20
Design/application	20
Assessment/analysis	5
Competence/training	5
Environmental	35



Component
- What failures could occur?
- Are the failures dangerous?
- Can the dangerous failures be detected?

$$DC_1 = \frac{\Sigma\,(\text{Detected dangerous failures})}{\Sigma\,(\text{Total dangerous failures})}$$

Entire system
$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d1}} + \frac{DC_2}{MTTF_{d2}} + \ldots + \frac{DC_n}{MTTF_{dn}}}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + \ldots + \frac{1}{MTTF_{dn}}}$$

$$SFF = \frac{\lambda_{DD} + \lambda_S}{\lambda_D + \lambda_S}$$
$DC \le SFF \le 1$
for $\lambda_S = 0 \dashrightarrow SFF = DC$
for $\lambda_D = 0 \dashrightarrow SFF = 1$

SFF Defining the **Safe Failure Fraction**

High Demand Mode

FME(D)A		
Type of failure	**Detected**	**Undetected**
safe λ_S	**safe detected** λ_{SD}	**safe undetected** λ_{SU}
dangerous λ_D	**dangerous detected** λ_{DD}	**dangerous undetected** λ_{DU}

$$SFF = \frac{\Sigma\,\lambda_{SD} + \Sigma\,\lambda_{SU} + \Sigma\,\lambda_{DD}}{\Sigma\,\lambda_{Total}} \qquad DC = \frac{\Sigma\,\lambda_{DD}}{\Sigma\,\lambda_D}$$

Low Demand Mode

FME(D)A		
Type of failure	**Detected**	**Undetected**
safe λ_S	**safe detected** λ_{SD}	**safe undetected** λ_{SU}
dangerous λ_D	**dangerous detected** λ_{DD}	**dangerous undetected** λ_{DU}

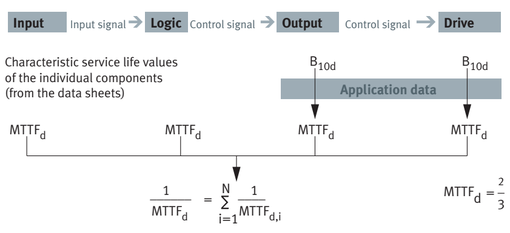
$$SFF = \frac{\Sigma\,\lambda_{SD} + \Sigma\,\lambda_{SU} + \Sigma\,\lambda_{DD}}{\Sigma\,\lambda_{Total}} \qquad DC = \frac{\Sigma\,\lambda_{DD}}{\Sigma\,\lambda_D}$$

- **λ (failure rates)**
  λ_S: Failure rate for safe failures
  λ_D: Failure rate for dangerous failures
  λ_{SD}: Failure rate for safe, detected failures
  λ_{SU}: Failure rate for safe, undetected failures
  λ_{DD}: Failure rate for dangerous, detected failures
  λ_{DU}: Failure rate for dangerous, undetected failures

- **FME(D)A (Failure Modes, Effects and Diagnostics Analysis)**
  Methods of analysis for quantitative determination of types of failure and failure rates

- **SFF (Safe Failure Fraction)**
  Proportion of all safe and detected failures based on the total amount of failures

4 $MTTF_d$ Definition of the **Mean Time To Failure**



$$MTTF_d = \frac{B_{10d}}{0{,}1 \cdot n_{op}}$$
Formula for determining the $MTTF_d$ value for a mechanical element in a channel

$$n_{op} = \frac{d_{op} \cdot h_{op} \cdot 3600\ s/h}{t_{cycle}}$$
Mean number of annual actuations n_{op} for the mechanical element

$$\frac{1}{MTTF_d} = \sum_{i=1}^{N} \frac{1}{MTTF_{d,i}}$$

$$MTTF_d = \frac{2}{3}\left[MTTF_{dC1} + MTTF_{dC2} - \frac{1}{\frac{1}{MTTF_{dC1}} + \frac{1}{MTTF_{dC2}}}\right]$$
Calculation of total $MTTF_d$ for two different channels

- $MTTF_d$ (Mean Time to Failure)
  Mean time until a dangerous failure
- MTTR (Mean Time to Restoration)
  Mean repair time

Evaluation	$MTTF_d$
Low	3 years ≤ $MTTF_d$ < 10 years
Medium	10 years ≤ $MTTF_d$ < 30 years
High	30 years ≤ $MTTF_d$ < 100 years

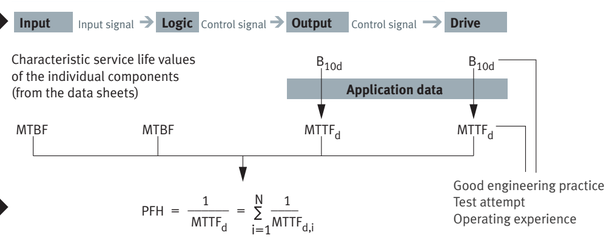
Source: DIN EN ISO 13849-1, Chapter 4.5.2

$$MTBF = MTTF + MTTR$$
for $MTTF \gg MTTR$
$\dashrightarrow MTBF = MTTF$

$$PFH = \frac{1}{MTTF_d}$$

PFH/PFD Determination of the **probability of failure**

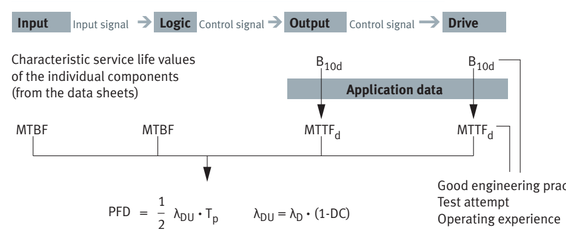
High Demand Mode



$$PFH = \frac{1}{MTTF_d} = \sum_{i=1}^{N} \frac{1}{MTTF_{d,i}}$$

- **PFH (Probability of failure per hour)**
  Probability of failure of a safety function under continuous use
- **MTBF (Mean Time between Failure)**
  Mean time between two successive failures

Low Demand Mode

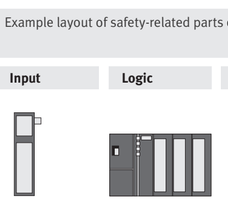


$$PFD = \frac{1}{2}\,\lambda_{DU} \cdot T_p \qquad \lambda_{DU} = \lambda_D \cdot (1\text{-}DC)$$

- **PFD (Probability of Failure on Demand)**
  Probability that a safety function will not be executed on demand at a low requirement rate
- **T_p (Proof test interval)**
  Regularly complete examination of the function

5 Entire system – Target: $PL \ge PL_r$

Example layout of safety-related parts of a control system



Input	Logic	Output	Drive
		Component 1 / Component 2	
$B10_d$		$B10_d$ / $B10_d$	
		$MTTF_d$ / $MTTF_d$	
$MTTF_d$		$MTTF_d$ per channel	
Cat		Cat	
DC		DC	
CCF		CCF	
PL	PL	PL	

Defined by manufacturer; To be determined by the system operator

Lowest PL PL_{low}	Number of lowest PL N_{low}	Entire system PL
a	>3	not allowed
	≤3	a
b	>2	a
	≤2	b
c	>3	b
	≤3	c
d	>3	c
	≤3	d
e	>3	d
	≤3	e

Target: $SIL \ge SIL_r$

Typical distribution of the PFH between the sub-systems of a safety function in single safety loops

Sensor ≤ 35%		Logic ≤ 15%		Actuator ≤ 50%	
PFH	λ_{SD}	PFH	λ_{SD}	PFH	λ_{SD}
SFF	λ_{SU}	SFF	λ_{SU}	SFF	λ_{SU}
HFT	λ_{DD}	HFT	λ_{DD}	HFT	λ_{DD}
MTBF	λ_{DU}	MTBF	λ_{DU}	MTBF	λ_{DU}
$SIL_{required}$ (SIL_r)					
PFH_{total}					

Defined by manufacturer; To be determined by the system operator

Typical distribution of the PFD between the sub-systems of a safety function in single safety loops

Sensor ≤ 35%		Logic ≤ 15%		Actuator ≤ 50%	
PFD	λ_{SD}	PFD	λ_{SD}	PFD	λ_{SD}
SFF	λ_{SU}	SFF	λ_{SU}	SFF	λ_{SU}
HFT	λ_{DD}	HFT	λ_{DD}	HFT	λ_{DD}
MTBF	λ_{DU}	MTBF	λ_{DU}	MTBF	λ_{DU}
$SIL_{required}$ (SIL_r)					
PFD_{total}					

Defined by manufacturer; To be determined by the system operator

6 Evaluation – Target: $PL \ge PL_r$

Definition of $MTTF_d$ = Mean Time To Failure (dangerous)

Definition of PL = Performance Level

	DC < 60% none	DC < 60% none	60% ≤ DC < 90% low	90% ≤ DC < 99% medium	60% ≤ DC < 90% low	90% ≤ DC < 99% medium	99% ≤ DC high
a							
b							
c							
d							
e							
	Kat B	Kat 1	Kat 2		Kat 3		Kat 4
	CCF not relevant		CCF ≥ 65 %				

Evaluation	$MTTF_d$
Low	3 years ≤ $MTTF_d$ < 10 years
Medium	10 years ≤ $MTTF_d$ < 30 Jahre
High	30 years ≤ $MTTF_d$ < 100 Jahre

→ $PL \ge PL_r$

Target: $SIL \ge SIL_r$

SIL-Level	High Demand Mode	Max. acceptable failure of the safety system	Device type A, Safe Failure Fraction (SFF) <60%	60...90%	90...99%	>99%	Device type B, Safe Failure Fraction (SFF) <60%	60...90%	90...99%	>99%	Low Demand Mode	
1	$10^{-5} \le PFH < 10^{-4}$	One risk of failure every 10,000 hours										
	$3 \cdot 10^{-6} \le PFH < 10^{-5}$	One risk of failure every 1,250 days	HFT 0				HFT 1	HFT 0			$10^{-2} \le PFD < 10^{-1}$	Once every 10 years
	$10^{-6} \le PFH < 3 \cdot 10^{-6}$	One risk of failure every 115.74 years										
2	$10^{-7} \le PFH < 10^{-6}$	One risk of failure every 115.74 years	HFT 1	HFT 0			HFT 2	HFT 1	HFT 0		$10^{-3} \le PFD < 10^{-2}$	Once every 100 years
3	$10^{-8} \le PFH < 10^{-7}$	One risk of failure every 1,157.41 years	HFT 2	HFT 1	HFT 0	HFT 0		HFT 2	HFT 1	HFT 0	$10^{-4} \le PFD < 10^{-3}$	Once every 1,000 years
4	$10^{-9} \le PFH < 10^{-8}$	One risk of failure every 11,574.1 yeras		HFT 2	HFT 1 HFT 2	HFT 1 HFT 2			HFT 2	HFT 1 HFT 2	$10^{-5} \le PFD < 10^{-4}$	Once every 10,000 years

[per hour]

- **Device type A**
  Device for which the failure behaviour of all components and the failure characteristics are sufficiently determined
- **Device type B**
  Device for which the failure behaviour of at least one component and the behaviour in case of a failure are not sufficiently determined.

→ $SIL \ge SIL_r$

54707 en 2010/05