Safety@Festo

Evaluating and assessing safety measures in accordance with EN ISO 13849-1/EN 61508/EN 61511/EN 62061

FESTO

Risk assessment

Risk analysis > Risk evaluation > Risk reduction

- > Design measures
- > Technical measures
- > User information

More information → www.festo.com/safety-guideline

Safety sub-functions of pneumatic drive technology

- **STO** Safe torque off
- **PUS** Prevention of unexpected start-up
- **SSC** Safe stopping and closing
- **SDI** Safe direction
- **SSB** Safe stopping and blocking
- **SLS** Safely limited speed
- **SLT** Safely limited torque (force)

Safety sub-functions of electric drive technology

- **STO** Safe torque off
- **SS1** Safe stop 1
- **SS2** Safe stop 2
- **SDI** Safe direction
- **SSB** Safe stopping and blocking
- **SLS** Safely limited speed
- **SLT** Safely limited torque

Safety-related block diagram

Trigger event	Input	Logic	Output → Drive
What triggers the safety request?	A device that recognises the trigger situation	A device that safely processes the signal	A device that safely controls the dangerous movement
For example: - Approaching a hazardous area - Opening a safety door - Process exceeds specified limit value	- Light barrier - Safety door - Pressure mats - Emergency stop - Fault - Laser scanner - Camera - Temperature sensor - Pressure sensor - Flow sensor	- Wiring - Safety relay - Safety PLC - Pneumatic control system	- Pneumatic energy - Electrical energy - Hydraulic energy - Potential (position) energy

Six steps to evaluate the safety functions

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 or mechanical.

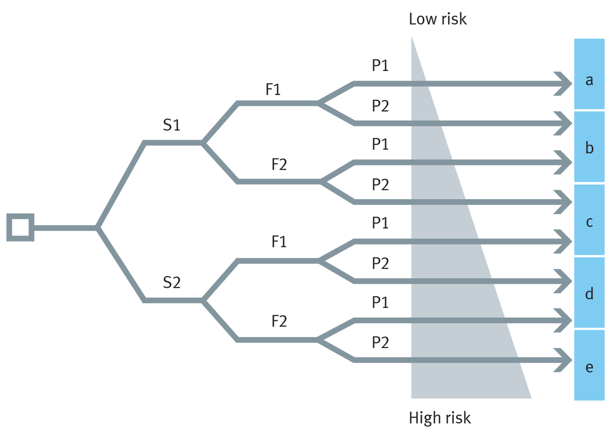
EN 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems.

EN 61511 Functional safety of safety-related systems for the process industry sector.

EN 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 Minor (normally reversible injury)
- S2 Serious (normally irreversible injury, including death)

F Frequency and/or duration of exposure to the hazard
- F1 Seldom to less often and/or briefly
- F2 Frequent to continuous and/or long

P Possibility of avoiding the hazard
- P1 Possible under certain conditions
- P2 Rarely possible

a – e Performance Level (PL)

Source: EN ISO 13849-1

Risk assessment – Determining the required Safety Integrity Level (SIL_r)

Path	W1	W2	W3
S1	–	–	–
S2 F1 P1	SIL1	–	–
S2 F1 P2	SIL1	SIL1	–
S2 F2 P1	SIL2	SIL1	SIL1
S2 F2 P2	SIL3	SIL2	SIL1
S3 F1	SIL3	SIL3	SIL2
S3 F2	SIL4	SIL3	SIL3
S4	SIL4	SIL4	SIL3

S Severity of damage
- S1 Minor injury to a person
- S2 Severe injury to multiple people up to the 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 Avoiding/mitigating the danger
- P1 Possible under certain conditions
- P2 Rarely possible

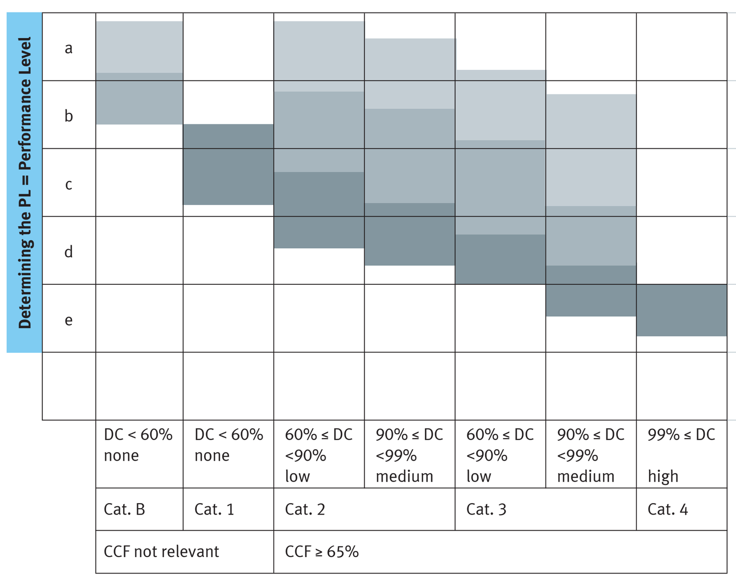
W Probability of occurrence
- W1 Relatively high
- W2 Low
- W3 Very low

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.

Evaluation of the safety function

2 Determining the necessary reliability parameters from PL_r and SIL_r

Determining $MTTF_D$ = mean time to failure (dangerous)



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: EN ISO 13849-1

Determining the necessary reliability parameters from PL_r and SIL_r

SIL level

SIL level	High demand mode	Max. acceptable failure of the safety system	Type A SFF < 60%	Type A 60…90%	Type A 90…99%	Type A >99%	Type B SFF < 60%	Type B 60…90%	Type B 90…99%	Type B >99%	Low demand mode	Max. acceptable failure of the safety system
	$10^{-5} \le PFH < 10^{-4}$	One risk of failure every 10,000 hours										
1	$3 \cdot 10^{-6} \le PFH < 10^{-5}$	One risk of failure every 1,250 days	HFT 0				HFT 1	HFT 0			$10^{-2} \le PFH < 10^{-1}$	Once every 10 years
1	$10^{-6} \le PFH < 3 \cdot 10^{-6}$	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		$10^{-3} \le PFH < 10^{-2}$	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	$10^{-4} \le PFH < 10^{-3}$	Once every 1,000 years
4	$10^{-9} \le PFH < 10^{-8}$	One risk of failure every 11,157.41 years		HFT 2	HFT 1 / HFT 2	HFT 1 / HFT 2			HFT 2	HFT 1 / HFT 2	$10^{-5} \le PFH < 10^{-4}$	Once every 10,000 years

[per hour]

Device type A
Device for which the failure behaviour of all components and the failure characteristics are adequately determined.

Device type B
Device for which the failure behaviour of at least one component and the failure characteristics are not sufficiently determined.

3 Control structure – Defining the category

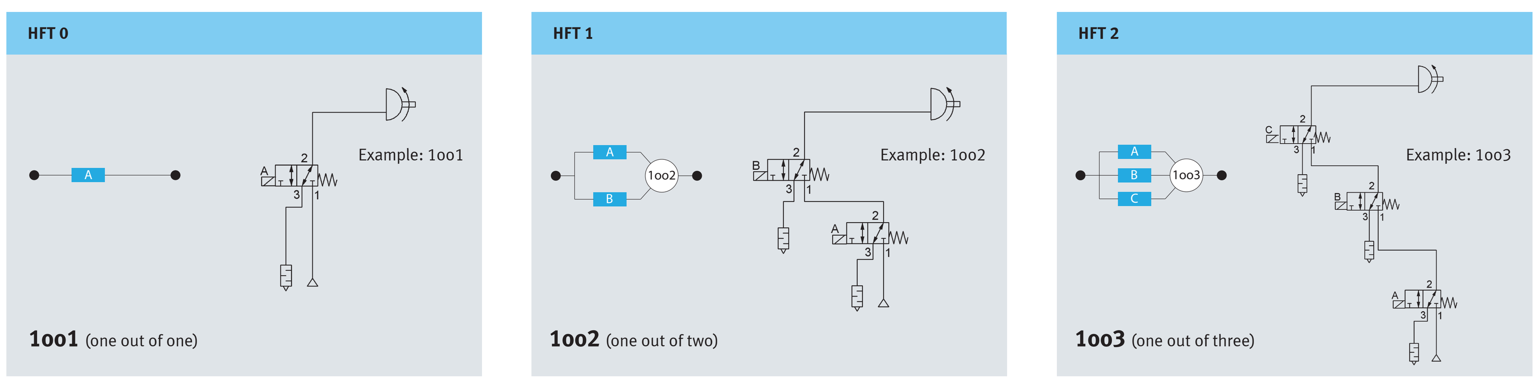
Category B/Category 1
Input → Input signal → Logic → Output signal → Output

Category 2
Input → Input signal → Logic → Output signal → Output; Test signal; Monitoring; Trigger signal; Monitoring; Test unit; Shut-down feature or display; Output of test unit

Category 3
Input → Input signal → Logic → Output signal → Output; Monitoring; Test signal
Input → Input signal → Logic → Output signal → Output; Monitoring

Category 4
Input → Input signal → Logic → Output signal → Output; Monitoring; Test signal
Input → Input signal → Logic → Output signal → Output; Monitoring

HFT – Defining the hardware fault tolerance



- 1oo1: A single failure can lead to a loss of safety.
- 1oo2: At least 2 failures must occur simultaneously to cause a loss of safety.
- 1oo3: At least 3 failures must occur simultaneously to cause a loss of safety.

HFT (hardware fault tolerance)
Ability to continue to perform the required function in the event of faults and deviations

4 Measures to control and detect faults

Measures against common cause failures (CCF)

Measures	Points
Isolation/disconnection	15
Diversity	20
Design/application	20
Assessment/analysis	5
Competency/training	5
Environment/influences	35

Start → System design: Category, $MTTF_D$, DC, CCF → Checking the achieved PL → Points ≥ 65 (N / Y) → End

Diagnostic coverage (DC)

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

$$DC_i = \frac{\Sigma \text{ (Detected dangerous faults)}}{\Sigma \text{ (Total dangerous faults)}}$$

Entire system

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{D1}} + \frac{DC_2}{MTTF_{D2}} + \dots + \frac{DC_N}{MTTF_{DN}}}{\frac{1}{MTTF_{D1}} + \frac{1}{MTTF_{D2}} + \dots + \frac{1}{MTTF_{DN}}}$$

$$SFF = \frac{\lambda_{DD} \cdot \lambda_S}{\lambda_D \cdot \lambda_S}$$

$DC \le SFF \le 1$

for $\lambda_S = 0 \rightarrow SFF = DC$
for $\lambda_D = 0 \rightarrow SFF = 1$

Safe failure faction (SFF) – Determining the failure fraction

High demand mode

Type of failure	FME(D)A Detected	FME(D)A 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

Type of failure	FME(D)A Detected	FME(D)A 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: Total failure rate for safe failures
- λ_D: Total failure rate for dangerous failures
- λ_{SD}: Total failure rate for safe, detected failures
- λ_{SU}: Total failure rate for safe, undetected failures
- λ_{DD}: Total failure rate for dangerous, detected failures
- λ_{DU}: Total failure rate for dangerous, undetected failures

FME(D)A (failure modes, effects and diagnostics analysis)
Method of analysis for quantitative determination of types of failure and failure rates

SFF (safe failure fraction)
Proportion of safe failures based on the total number of failures

5 $MTTF_D$ – Determining the mean time to failure (dangerous)

Input → Input signal → Logic → Control signal → Output → Energy → Drive

Characteristic service life values of the individual components (from the product reliability data sheets)

Application data, e.g. n_{op}

B_{10D}, $MTTF_D$

$$\frac{1}{MTTF_D} = \sum_{i=1}^{N} \frac{1}{MTTF_{Di}}$$

$$MTTF_D = \frac{2}{3}\left[MTTF_{DC1} + MTTF_{DC2} - \frac{1}{\frac{1}{MTTF_{DC1}} + \frac{1}{MTTF_{DC2}}}\right]$$

$$MTTF_D = \frac{B_{10D}}{0.1 \cdot n_{op}}$$

Formula for determining the $MTTF_D$ value for a mechanical element in a channel

$$n_{op} = \frac{d_{op} \cdot h_{op} \cdot 3600 \text{ s/h}}{t_{cycle}}$$

Mean number of annual actuations n_{op} for the mechanical element

Calculation of total $MTTF_D$ for several parallel channels

$MTTF_D$ (Mean time to failure)
Mean time until a dangerous failure

MTTR (mean time to restore)
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: EN ISO 13849-1)

MTBF = MTTF + MTTR
for MTTF » MTTR
MTBF = MTTF

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

PFH/PFD – Determining the probability of failure

High demand mode

Input → Input signal → Logic → Control signal → Output → Energy → Drive

Characteristic service life values of the individual components (from the product reliability data sheets)

Application data

B_{10D}, $MTTF_D$

$$PFH = \frac{1}{MTTF_D} = \sum_{i=1}^{N} \frac{1}{MTTF_{Di}}$$

- Good engineering practice
- Test attempts
- Operational reliability

PFH (probability of failure per hour)
Probability of a safety function failing

MTBF (mean time between failure)
Mean time between two successive failures

Low demand mode

Input → Input signal → Logic → Control signal → Output → Energy → Drive

Characteristic service life values of the individual components (from the product reliability data sheets)

Application data

B_{10D}, λ_{DU}

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

- Good engineering practice
- Test attempts
- Operational reliability

PFD (probability of failure on demand)
Probability of a safety function failing

T_p (proof test interval)
Interval between proof tests

6 Entire system – Target: PL ≥ PL_r

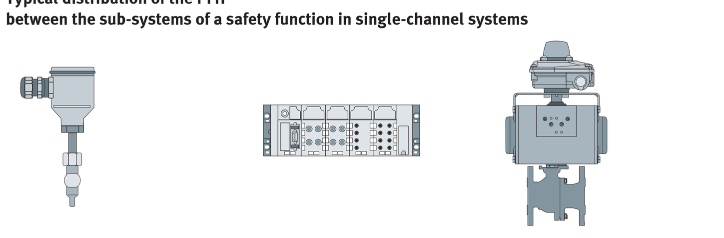
Sample layout of safety-related parts of a control system

Input	Logic	Output	Drive
$B10_D$		$B10_D$	
		$MTTF_D$	
$MTTF_D$		$MTTF_D$ per channel	
Cat.		Cat.	
DC		DC	
CCF		CCF	
PL	PL	PL	

- To be determined based on the application
- Communicated by the manufacturer (information for determining the $B10_D$ value should be provided by the manufacturer)

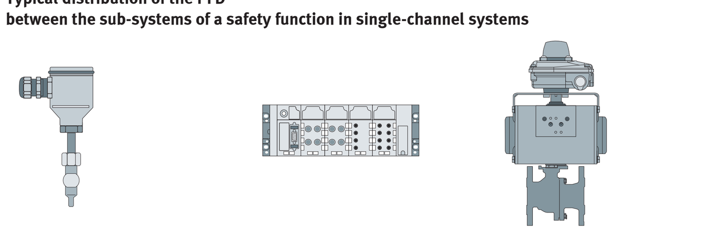
Target: SIL ≥ SIL_r

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



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}					

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



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}					

PL ≥ PL_r **SIL ≥ SIL_r**

When converting from PL to SIL or vice versa, the additional requirements contained in the applicable standards (EN ISO 13849-1, EN 61508, EN 61511, EN 62061) must be taken into account.

136100 en 2021/02 – Errors and omissions excepted