Safety@Festo

Bewertung und Beurteilung von Sicherheitsfunktionen nach EN ISO 13849-1/EN 61508/EN 61511/EN 62061

FESTO

Risikobeurteilung

Risikoanalyse > Risikobewertung > Risikominderung

- **> Konstruktive Maßnahmen**
- **> Technische Maßnahmen**
- **> Benutzerinformation**

Mehr Informationen → **www.festo.com/leitfaden-st**

Sicherheits-Teilfunktionen der pneumatischen Antriebstechnik

- **STO** Sicher abgeschaltetes Moment
- **PUS** Vermeidung von unerwartetem Wiederanlauf
- **SSC** Sicheres Anhalten und Absperren
- **SDI** Sichere Bewegungsrichtung
- **SSB** Sicheres Anhalten und Blockieren
- **SLS** Sicher begrenzte Geschwindigkeit
- **SLT** Sicher begrenztes Moment (Kraft)

Sicherheits-Teilfunktionen der elektrischen Antriebstechnik

- **STO** Sicher abgeschaltetes Moment
- **SS1** Sicherer Stopp 1
- **SS2** Sicherer Stopp 2
- **SDI** Sichere Bewegungsrichtung
- **SSB** Sicheres Anhalten und Blockieren
- **SLS** Sicher begrenzte Geschwindigkeit
- **SLT** Sicher begrenztes Moment (Safely-limited Torque)

Sicherheitsbezogenes Blockdiagramm

Auslöseereignis	Eingang	Logik	Ausgang → Antrieb
Was löst die Sicherheitsanforderung aus? Zum Beispiel: - Annäherung an eine Gefahrenstelle - Öffnen einer Schutztür - Prozess überschreitet einen definierten Grenzwert	Ein Gerät, das die Auslösesituation erkennt - Lichtschranke - Schutztür - Trittmatten - Not-Halt - Fehler - Laserscanner - Kamera - Temperatursensor - Drucksensor - Durchflusssensor	Ein Gerät, das das Signal sicher verarbeitet - Verdrahtung - Sicherheitsrelais - Sicherheits-SPS - Pneumatische Steuerung	Ein Gerät, das die gefahrbringende Bewegung sicher ansteuert - Pneumatische Energie - Elektrische Energie - Hydraulische Energie - Potentielle (Lage) Energie

Sechs Schritte zur Bewertung von Sicherheitsfunktionen

EN ISO 13849-1 Anwendbar bei sicherheitsbezogenen Teilen von Steuerungen und allen Arten von Maschinen, ungeachtet der verwendeten Technologie und Energie – elektrisch, pneumatisch, hydraulisch oder mechanisch.

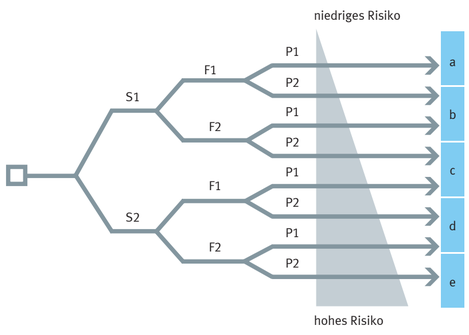
EN 61508 Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme.

EN 61511 Funktionale Sicherheit sicherheitstechnischer Systeme für die Prozessindustrie.

EN 62061 Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Steuerungssysteme.

Bewertung der Anwendung

1 Risikoeinschätzung – Bestimmung des erforderlichen Performance Level (PL_r)



S Schwere der Verletzung
- S1 leicht (üblicherweise reversible Verletzung)
- S2 ernst (üblicherweise irreversible Verletzung, einschließlich Tod)

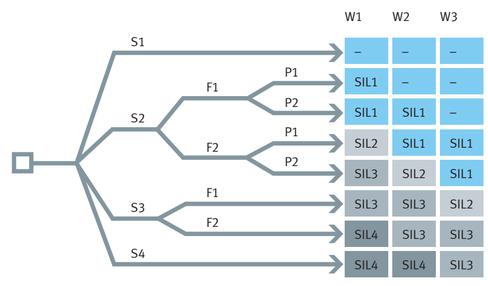
F Häufigkeit und/oder Dauer der Gefährdungsexposition
- F1 selten bis weniger häufig und/oder kurz
- F2 häufig bis dauernd und/oder lang

P Möglichkeit der Vermeidung von Gefährdung
- P1 möglich unter bestimmten Bedingungen
- P2 kaum möglich

a – e Performance Level (PL_r)

Quelle: EN ISO 13849-1

Risikoeinschätzung – Bestimmung des erforderlichen Safety Integrity Level (SIL_r)



SIL (Safety Integrity Level)
Vier diskrete Stufen (SIL1 bis SIL4). Je höher der SIL-Wert einer Sicherheitsschaltung ist, desto besser können die umgesetzten Sicherheitsfunktionen einen Schaden verhindern oder zumindest reduzieren.

S Schadensausmaß
- S1 leichte Verletzung einer Person
- S2 schwere Verletzung mehrerer Personen bis hin zum Tod einer Person
- S3 Tod mehrerer Personen
- S4 katastrophale Auswirkungen mit vielen Toten

F Aufenthaltswahrscheinlichkeit
- F1 selten bis etwas öfter
- F2 häufig bis andauernd

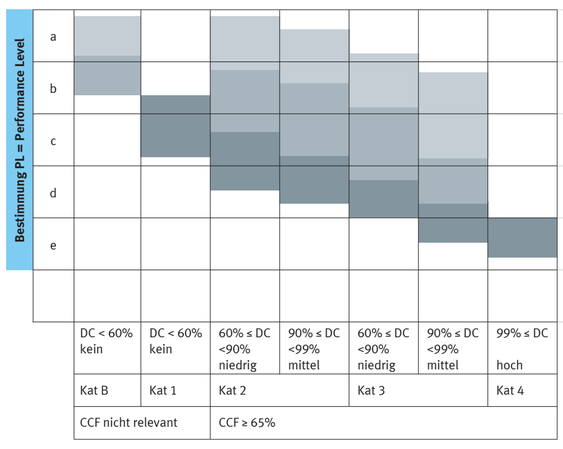
P Gefahrenabwehr/Vermeidung
- P1 möglich unter bestimmten Bedingungen
- P2 kaum möglich

W Eintrittswahrscheinlichkeit
- W1 relativ hoch
- W2 gering
- W3 sehr gering

Bewertung der Sicherheitsfunktion

2 Ermittlung der erforderlichen Zuverlässigkeitsparameter aus PL_r und SIL_r

Bestimmung $MTTF_D$ = Mean Time To Failure (dangerous)



Bewertung	$MTTF_D$
Niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
Mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
Hoch	30 Jahre ≤ $MTTF_D$ < 100 Jahre

Quelle: EN ISO 13849-1

Ermittlung der erforderlichen Zuverlässigkeitsparameter aus PL_r und SIL_r

SIL-Level	High Demand Mode	Max. akzeptabler Ausfall des Sicherheitssystems	Gerätetyp A – Safe Failure Fraction (SFF) < 60%	Gerätetyp A 60...90%	Gerätetyp A 90...99%	Gerätetyp A >99%	Gerätetyp B – Safe Failure Fraction (SFF) < 60%	Gerätetyp B 60...90%	Gerätetyp B 90...99%	Gerätetyp B >99%	Low Demand Mode	Maximal akzeptabler Ausfall des Sicherheitssystems
	$10^{-5} \le PFH < 10^{-4}$	ein Risikoausfall alle 10.000 Stunden										
1	$3 \cdot 10^{-6} \le PFH < 10^{-5}$	ein Risikoausfall alle 1.250 Tage	HFT 0				HFT 1	HFT 0			$10^{-2} \le PFH < 10^{-1}$	einmal in 10 Jahren
1	$10^{-6} \le PFH < 3 \cdot 10^{-6}$	ein Risikoausfall alle 115,74 Jahre	HFT 0				HFT 1	HFT 0				
2	$10^{-7} \le PFH < 10^{-6}$	ein Risikoausfall alle 115,74 Jahre	HFT 1	HFT 0			HFT 2	HFT 1	HFT 0		$10^{-3} \le PFH < 10^{-2}$	einmal in 100 Jahren
3	$10^{-8} \le PFH < 10^{-7}$	ein Risikoausfall alle 1.157,41 Jahre	HFT 2	HFT 1	HFT 0	HFT 0		HFT 2	HFT 1	HFT 0	$10^{-4} \le PFH < 10^{-3}$	einmal in 1.000 Jahren
4	$10^{-9} \le PFH < 10^{-8}$	ein Risikoausfall alle 11.157,41 Jahre		HFT 2	HFT 1 HFT 2	HFT 1 HFT 2			HFT 2	HFT 1 HFT 2	$10^{-5} \le PFH < 10^{-4}$	einmal in 10.000 Jahren

[pro Stunde]

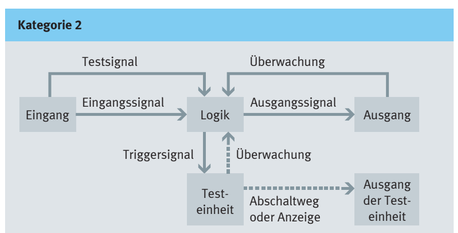
Gerätetyp A
Gerät, bei dem das Ausfallverhalten aller eingesetzen Bauteile und das Fehlerverhalten ausreichend bestimmt ist.

Gerätetyp B
Gerät, bei dem das Ausfallverhalten min. eines eingesetzten Bauteils und das Verhalten im Fehlerfall nicht ausreichend genug bestimmt ist.

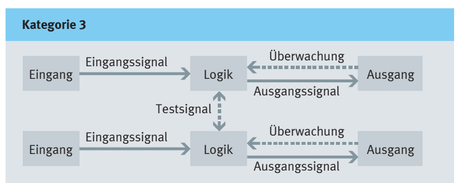
3 Steuerstruktur – Festlegung der Kategorie

Kategorie B/Kategorie 1

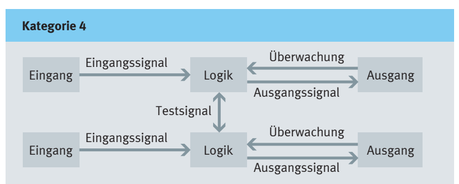
Kategorie 2



Kategorie 3

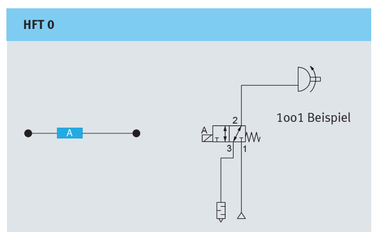


Kategorie 4



HFT – Festlegung der Hardware-Fehlertoleranz

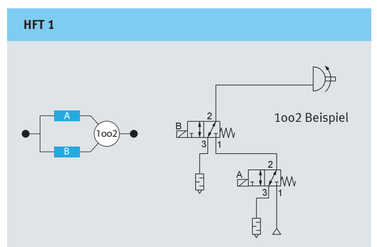
HFT 0



1oo1 (One out of One)

Ein einzelner Fehler kann zum Sicherheitsverlust führen.

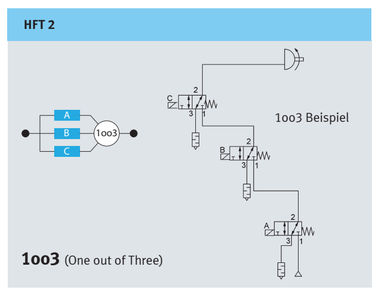
HFT 1



1oo2 (One out of Two)

Mindestens 2 Fehler müssen gleichzeitig auftreten, um einen Sicherheitsverlust zu verursachen.

HFT 2



1oo3 (One out of Three)

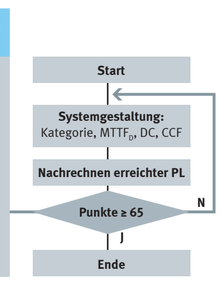
Mindestens 3 Fehler müssen gleichzeitig auftreten, um einen Sicherheitsverlust zu verursachen.

HFT (Hardware Failure Tolerance)
Fähigkeit eine geforderte Funktion bei Fehlern und Abweichungen weiter auszuführen

4 Maßnahmen zur Fehlerbeherrschung und Fehlererkennung

Maßnahmen gegen Ausfälle gemeinsamer Ursache (CCF)

Maßnahmen	Punkte
Trennung/Abtrennung	15
Diversität	20
Entwurf/Anwendung	20
Beurteilung/Analyse	5
Kompetenz/Ausbildung	5
Umgebung/Einflüsse	35



Diagnosedeckungsgrad (DC)

Komponente

- **Welche Fehler können auftreten?**
- **Sind die Fehler gefährlich?**
- **Können die gefährlichen Fehler erkannt werden**

$$DC_1 = \frac{\Sigma \text{ (erkannter gefährlicher Fehler)}}{\Sigma \text{ (gesamter gefährlicher Fehler)}}$$

Gesamtsystem

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

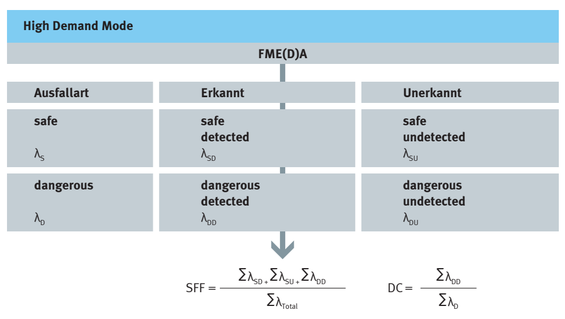
Safe Failure Fraction (SFF) – Ermittlung des Fehleranteils

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

$DC \le SFF \le 1$

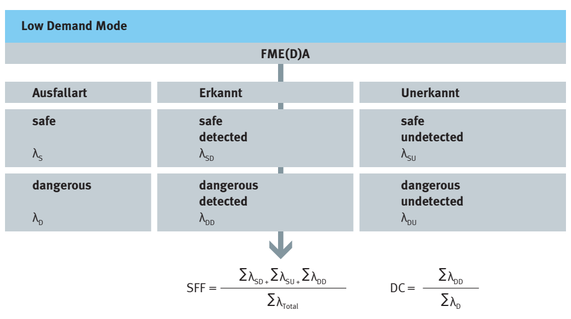
für $\lambda_S = \rightarrow SFF = DC$
für $\lambda_D = \rightarrow SFF = 1$

High Demand Mode



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

Low Demand Mode



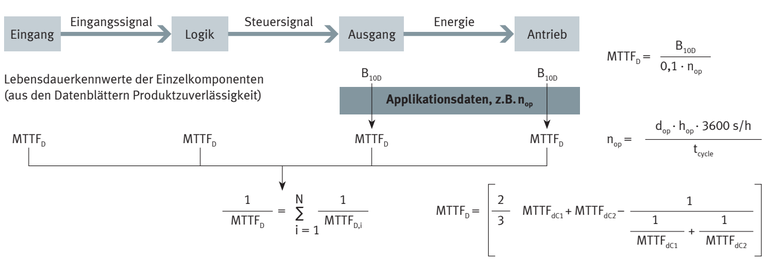
$$SFF = \frac{\Sigma\lambda_{SD} + \Sigma\lambda_{SU} + \Sigma\lambda_{DD}}{\Sigma\lambda_{Total}} \qquad DC = \frac{\Sigma\lambda_{DD}}{\Sigma\lambda_D}$$

λ (Ausfallraten)
- λ_S: Gesamtausfallrate für sichere Ausfälle
- λ_D: Gesamtausfallrate für gefährliche Ausfälle
- λ_{SD}: Gesamtausfallrate für sichere, erkannte Ausfälle
- λ_{SU}: Gesamtausfallrate für sichere, unerkannte Ausfälle
- λ_{DD}: Gesamtausfallrate für gefährliche, erkannte Ausfälle
- λ_{SU}: Gesamtausfallrate für gefährliche, unerkannte Ausfälle

FME(D)A (Failure Modes, Effects and Diagnostics Analysis)
Analysemethode zur quantitativen Ermittlung von Ausfallarten und Ausfallraten

SFF (Safe Failure Fraction)
Anteil sicherer Fehler an der Gesamtfehleranzahl

5 $MTTF_D$ – Bestimmung des Mean Time To Failure



$$MTTF_D = \frac{B_{10D}}{0{,}1 \cdot n_{op}}$$

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

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

$$MTTF_D = \left[\frac{2}{3}\ MTTF_{dC1} + MTTF_{dC2} - \frac{1}{\frac{1}{MTTF_{dC1}} + \frac{1}{MTTF_{dC2}}}\right]$$

Formel zur Ermittlung des $MTTF_D$-Wertes für ein mechanisches Element in einem Kanal

Mittlere Anzahl jährlicher Betätigungen n_{op} für das mechanische Element

Berechnung gesamt $MTTF_D$ bei mehreren parallelen Kanälen

$MTBF = MTTF + MTTR$

für MTTF ›› MTTR gilt MTBF = MTTF

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

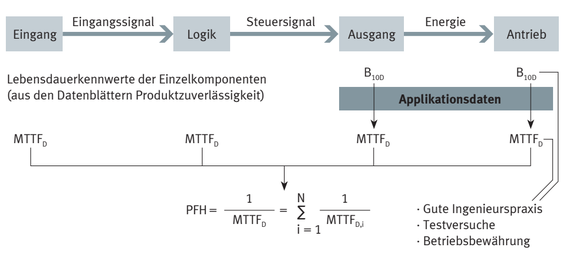
$MTTF_D$ (Mean Time to Failure)
Mittlere Zeit bis zu einem gefahrbringenden Fehler

MTTR (Mean Time to Restoration)
Mittlere Reparaturzeit

Bewertung $MTTF_D$
Niedrig: 3 Jahre ≤ $MTTF_D$ < 10 Jahre
Mittel: 10 Jahre ≤ $MTTF_D$ < 30 Jahre
Hoch: 30 Jahre ≤ $MTTF_D$ < 100 Jahre
(Quelle: EN ISO 13849-1)

PFH/PFD – Ermittlung der Versagenswahrscheinlichkeit

High Demand Mode



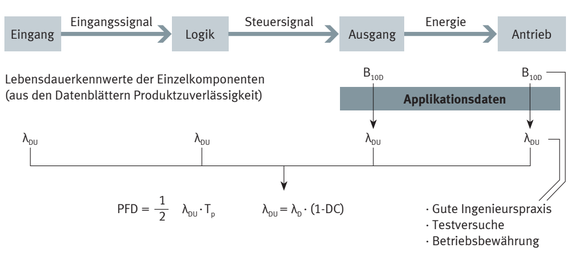
$$PFH = \frac{1}{MTTF_D} = \sum_{i=1}^{N} \frac{1}{MTTF_{D,i}}$$

- Gute Ingenieurspraxis
- Testversuche
- Betriebsbewährung

PFH (Probability of failure per hour)
Versagenswahrscheinlichkeit einer Sicherheitsfunktion

MTBF (Mean Time between Failure)
Mittlere Zeit zwischen zwei aufeinanderfolgenden Fehlern

Low Demand Mode



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

- Gute Ingenieurspraxis
- Testversuche
- Betriebsbewährung

PFD (Probability of Failure on Demand)
Versagenswahrscheinlichkeit einer Sicherheitsfunktion

T_p (Proof test interval)
Prüfintervall

6 Gesamtsystem – Ziel: $PL \ge PL_r$

Beispiellayout einer Sicherheitsschaltung

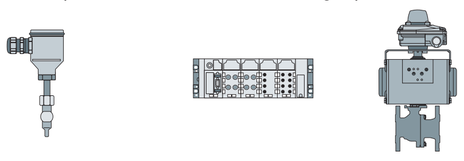
Eingang	Logik	Ausgang	Antrieb
$B10_D$		$B10_D$	
		$MTTF_D$	
$MTTF_D$		$MTTF_D$ pro Kanal	
Kat		Kat	
DC		DC	
CCF		CCF	
PL	PL	PL	

- anwendungsabhängig zu ermitteln
- vom Hersteller bekannt gegeben (Informationen zur Bestimmung des $B10_D$-Wertes sollten vom Hersteller bereitgestellt werden)

$PL \ge PL_r$

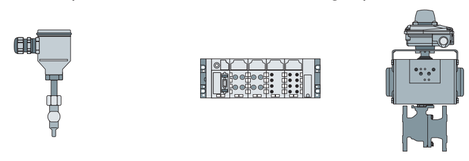
Ziel: $SIL \ge SIL_r$

Übliche Verteilung des PFH auf die Teilsysteme einer Sicherheitsfunktion bei einkanaligen Systemen



Sensor ≥ 35%		Logik ≥ 15%		Aktor ≥ 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}
$SIL_{erforderlich}$ (SIL_r)					
PFH_{gesamt}					

Übliche Verteilung des PFD auf die Teilsysteme einer Sicherheitsfunktion bei einkanaligen Systemen



Sensor ≥ 35%		Logik ≥ 15%		Aktor ≥ 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}
$SIL_{erforderlich}$ (SIL_r)					
PFD_{gesamt}					

$SIL \ge SIL_r$

Beim Konvertieren von PL nach SIL oder umgekehrt sind die zusätzlichen Anforderungen aus den angewendeten Normen (EN ISO 13849-1, EN 61508, EN 61511, EN 62061) zu berücksichtigen.

136099 de 2021/02 – Änderungen und Irrtümer vorbehalten