SIL (Safety Integrity Level)

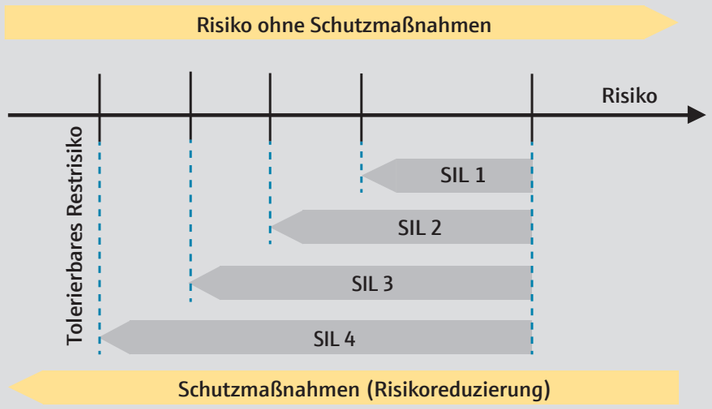
Funktionale Sicherheit

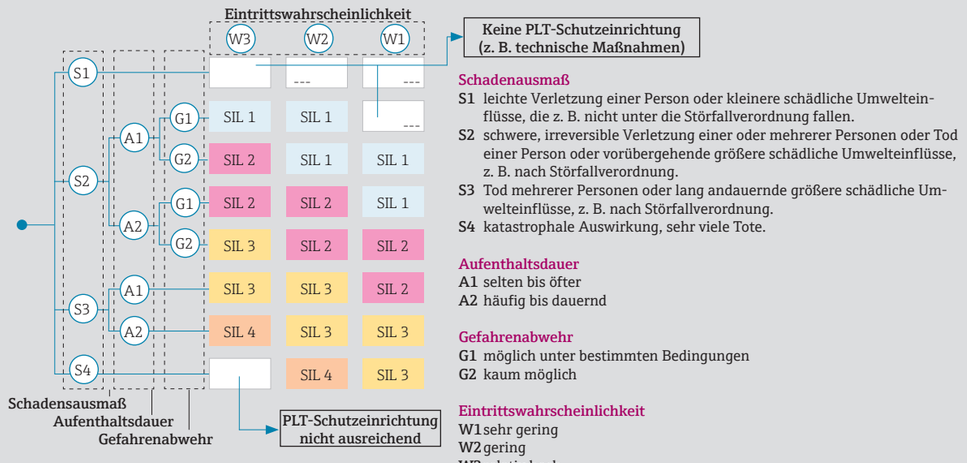
Anlagenrisiko

Verfahrenstechnische Anlage, Maschine

Risiken für Personen, Umwelt und Sachwerte

Risikoreduzierung durch SIL





Schadenausmaß
- **S1** leichte Verletzung einer Person oder kleinere schädliche Umwelteinflüsse, die z. B. nicht unter die Störfallverordnung fallen.
- **S2** schwere, irreversible Verletzung einer oder mehrerer Personen oder Tod einer Person oder vorübergehende größere schädliche Umwelteinflüsse, z. B. nach Störfallverordnung.
- **S3** Tod mehrerer Personen oder lang andauernde größere schädliche Umwelteinflüsse, z. B. nach Störfallverordnung.
- **S4** katastrophale Auswirkung, sehr viele Tote.

Aufenthaltsdauer
- **A1** selten bis öfter
- **A2** häufig bis dauernd

Gefahrenabwehr
- **G1** möglich unter bestimmten Bedingungen
- **G2** kaum möglich

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

Technische Anforderungen

Ermittlung der sicherheitstechnischen Kenngrößen
FMEDA

Technische Anforderungen		
Ausfallarten von Sicherheitsfunktionen		
Ausfallart	erkannt (detected)	unerkannt (undetected)
sicher	safe detected **λSD**	safe undetected **λSU**
gefährlich	dangerous detected **λDD**	dangerous undetected **λDU**

SIL – PFD – PFH - Betriebsarten		
Safety Integrity Level (SIL)	**Mittlere Wahrscheinlichkeit eines Ausfalls der Sicherheitsfunktion bei Anforderung – PFD (Betriebsart: Low demand mode) (weniger als 1 x/Jahr)**	**Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde – PFH (Betriebsart: High demand mode oder continius mode)**
SIL 4	$\geq 10^{-5}$ bis $< 10^{-4}$	$\geq 10^{-9}$ bis $< 10^{-8}$
SIL 3	$\geq 10^{-4}$ bis $< 10^{-3}$	$\geq 10^{-8}$ bis $< 10^{-7}$
SIL 2	$\geq 10^{-3}$ bis $< 10^{-2}$	$\geq 10^{-7}$ bis $< 10^{-6}$
SIL 1	$\geq 10^{-2}$ bis $< 10^{-1}$	$\geq 10^{-6}$ bis $< 10^{-5}$

Rechnerische SIL-Nachweis

Sensorsystem → Steuerung → Aktorsystem

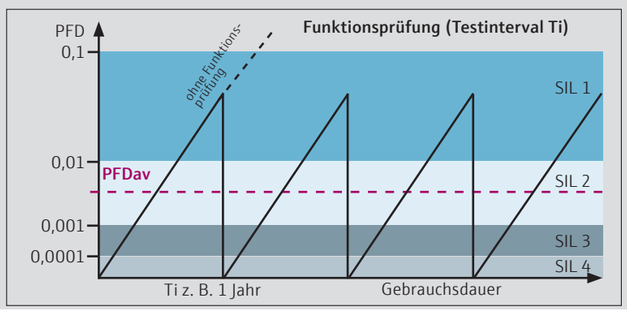
Einkanaliger Systemaufbau

Die PFD-/PFH-Werte aller Komponenten müssen addiert und entsprechend bewertet werden.

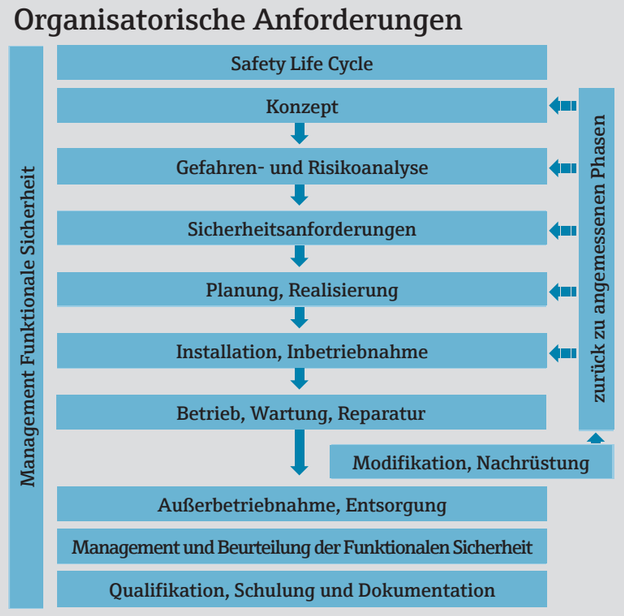
$PFD = ½ \lambda_{DU} \times Ti$ $PFH = \lambda_{DU}$

SFF – HFT – SIL – Typ A, Typ B						
Safe Failure Fraction (SFF)	**Hardware Fehlertoleranz (Typ A – einfaches Betriebsmittel)**			**Hardware Fehlertoleranz (Typ B – komplexes Betriebsmittel)**		
	0	1	2	0	1 (0*)	2 (1*)
< 60 %	SIL 1	SIL 2	SIL 3	nicht erlaubt	SIL 1	SIL 2
60 % bis < 90 %	SIL 2	SIL 3	SIL 4	SIL 1	SIL 2	SIL 3
90 % bis < 99 %	SIL 3	SIL 4	SIL 4	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4	SIL 3	SIL 4	SIL 4

* Mit Nachweis der Betriebsbewährung nach IEC/EN 61511 (nur für SIL ≤ 3)



Organisatorische Anforderungen



Begriffe

- **Funktionale Sicherheit:**
Teil der Gesamtanlagensicherheit, der von der korrekten Funktion sicherheitsbezogener Systeme zur Risikoreduzierung abhängt. Funktionale Sicherheit ist gegeben, wenn jede Sicherheitsfunktion wie spezifiziert ausgeführt wird.

- **Sicherheitsbezogenes System:**
System, das Sicherheitsfunktionen ausführt, um einen sicheren Zustand für ein überwachtes System zu erreichen oder aufrecht zu erhalten.

- **Sicherheitsfunktion:**
Aufgabe; Sicheren Zustand für ein überwachtes System erreichen oder aufrecht erhalten, wenn vorher festgelegte Bedingungen verletzt werden.

- **Safety Life Cycle:**
Beschreibt alle notwendigen Tätigkeiten bei der Realisierung sicherheitsbezogener Systeme von der Konzeptphase bis zur Außerbetriebnahme.

- **Management der Funktionalen Sicherheit:**
Erforderliche Managementtätigkeiten, technische Tätigkeiten und Verantwortlichkeiten während des Safety Life Cycle zur Erreichung der Funktionalen Sicherheit.

- **Beurteilung der Funktionalen Sicherheit:**
Untersuchung, ob die Funktionale Sicherheit durch die sicherheitsbezogenen Systeme erreicht wurde.

- **Safety Integrity Level (SIL):**
Vier diskrete Stufen (SIL 1 bis SIL 4). Je höher der SIL eines sicherheitsbezogenen Systems, umso geringer ist die Wahrscheinlichkeit, dass das System die geforderte Sicherheitsfunktion nicht ausführt.

- **Average Probability of Failure on Demand (PFD):**
Mittlere Versagenswahrscheinlichkeit einer Sicherheitseinrichtung bei niedriger Anforderungsrate.

- **Probability of Failure per Hour (PFH):**
Versagenswahrscheinlichkeit einer Sicherheitsfunktion bei hoher oder kontinuierlicher Anforderungsrate.

- **Safe Failure Fraction (SFF):**
Prozentualer Anteil sicherheitsgerichteter Ausfälle eines sicherheitsbezogenen Systems (Sicherheitsfunktion) bzw. Teilsystems.

- **Hardware Fehlertoleranz (HFT):**
HFT = n bedeutet, dass n + 1 Fehler zu einem Verlust der Sicherheitsfunktion führen kann.

- **Betriebsart: Low demand mode:**
Betriebsart mit niedriger Anforderungsrate. Anforderungsrate an sicherheitsbezogene Systemen mit nicht mehr als einmal pro Jahr und nicht größer als die doppelte Frequenz der Wiederholungsprüfung.

- **Betriebsart: High demand mode oder continuous mode:**
Betriebsart mit hoher oder kontinuierlicher Anforderung der Sicherheitsfunktion. Anforderungsrate an sicherheitsbezogenes System mehr als einmal pro Jahr oder größer als die doppelte Frequenz der Widerholungsprüfung.

- **Gerätetyp A (einfaches Betriebsmittel):**
Gerät, bei dem das Ausfallverhalten aller eingesetzten Bauteile und das Verhalten unter Fehlerbedingungen vollständig bekannt ist.

- **Gerätetyp B (komplexe Betriebsmittel):**
Gerät, bei dem das Ausverhalten der eingesetzten Bauteile und das Verhalten unter Fehlbedingungen nicht vollständig bekannt ist (z. B. µ-Prozessoren).

- **FMEDA (Failure Modes, Effects and Diagnostic Analysis):**
Analysemethode für elektronische Schaltungen und Mechanik zur quantitativen Ermittlung von Ausfallarten und Ausfallraten.

- **Ausfallraten:**
  - λ_{SD}: Gesamtausfallrate für sichere erkannte Ausfälle
  - λ_{SU}: Gesamtausfallrate für sichere unerkannte Ausfälle
  - λ_{DD}: Gesamtausfallrate für gefährliche erkannte Ausfälle
  - λ_{DU}: Gesamtausfallrate für gefährliche unerkannte Ausfälle

- **Mean Time Between Failures (MTBF):**
Mittlere Ausfallwahrscheinlichkeit

- **Mean Time to repair (MTTR):**
Mittlere Reparaturzeit

- **Intervall für Wiederholungsprüfungen (Ti):**
Zeitintervall zwischen wiederkehrenden Prüfungen einer Sicherheitsfunktion zur Aufdeckung gefährlicher, unerkannter Fehler

Normen

Basisstandard
IEC/EN 61508

Anwendungsspezifische Normen
IEC/EN 61511 (Prozessindustrie)
IEC/EN 61513 (Kernenergie)
IEC/EN 62061 (Maschinensicherheit)
VDI/VDE 2180

CP000132/11/DE/14.13 – 71008610

Endress+Hauser

People for Process Automation