

# Armaturen in der Anlagensicherheit

## „Funktionale Sicherheit Safety Integrity Level – SIL – „

Karl Heinz Gutmann  
mail: karlheinz.gutmann@de.endress.com

---

Karl Heinz Gutmann

1

### ► „Funktionale Sicherheit – SIL –“

Anlagensicherheit

---

- Funktionale Sicherheit -  
ein „aktuelles“ Thema  
und ein wichtiger Beitrag zur Anlagensicherheit
- Anlagen mit einem hohen Gefährdungspotential müssen  
„sicher“ betrieben werden.
- Ein hohes Gefährdungspotential ist ein Risiko für  
Menschen und Umwelt oder können große Sachschäden  
verursachen

---

Karl Heinz Gutmann

2

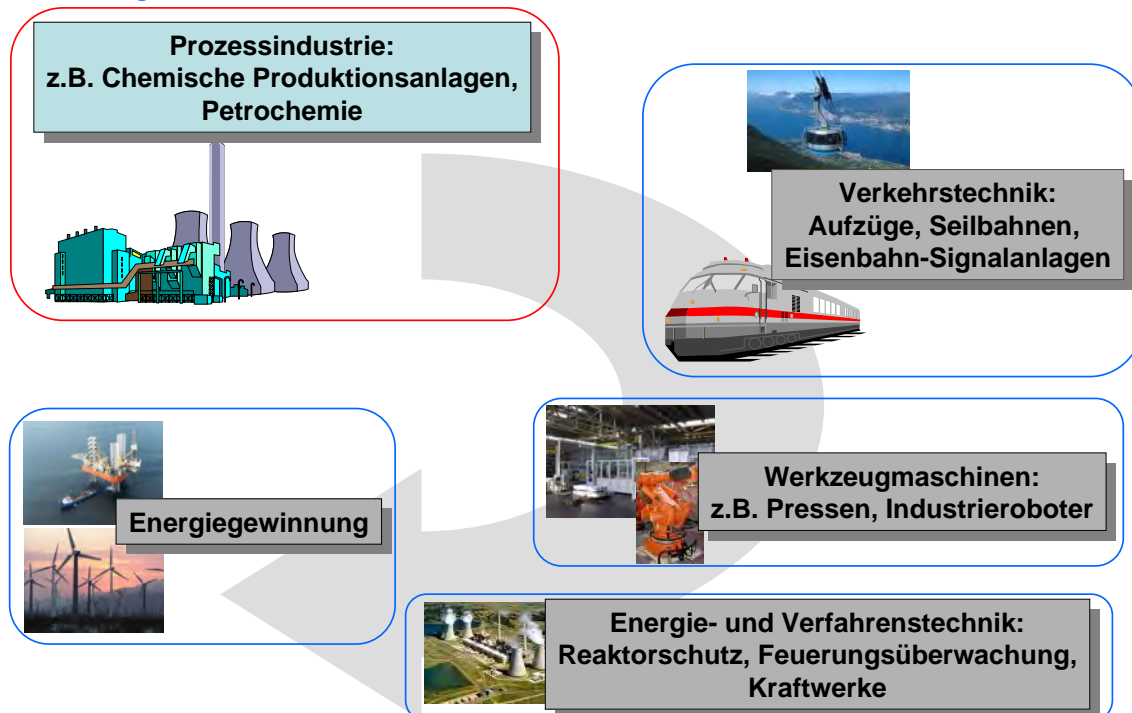
- **Stichworte sind:**
  - Gerichtsfester Nachweis
  - Normengerechte Umsetzung

- **Funktionale Sicherheit –  
nach**




**EN 61508, EN 61511, VDI/VDE 2180**

Informationen wie Sie die Realisierung der praxisgerechten Umsetzung von Sicherheitsanforderungen auf Ihre Anlage vornehmen können

**Anwendungsbereich der Normen**



Anwendungsbereich

E/E/PE-Systeme = Elektrische / Elektronische / Programmierbare Elektronische Sicherheits-Systeme			
Verfahrenstechnik Prozessindustrie (Elektronik)  DIN EN 61508 DIN EN 61511 VDI/VDE 2180 SIL 1 - 4  Low demand mode 1 Anforderung pro Jahr  <b>PFD-Werte</b>  Wer rastet, der rostet	Maschinensicherheit (Elektronik Mechanik)  DIN EN 62061 DIN EN 13849 SIL 1 - 3 PL a – e  Hight demand mode 1 Anforderung pro Stunde  <b>PFH-Werte</b>  Wer viel arbeitet, ermüdet	Feuerungstechnik  DIN EN 50156 VDE 0116 EN 746   Wer Fehler vermeidet, macht keine Fehler	Sonstige Arbeitsbereiche  Aufzüge  Bahntechnik  Signalanlagen  Kerntechnik  ... ...

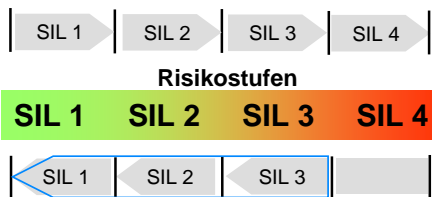
SIL = Safety Integrity Level  
 PL = Performance Level

PFD = Probability of dangerous on demand  
 PFH = Probability of dangerous Failure per Hour

Risikoreduzierung durch SIL



Risikoeinstufung der Anlage



Auswahl der Gerätekomponenten nach der Risikoeinstufung der Anlage



Risikoeinstufung der Anlage:

Dies wird durch den Anlagenbetreiber festgelegt. Durch eine Risikobetrachtung, wird eine Risikoeinstufung vorgenommen. Dieses kann z.B. durch den Risikographen nach verschiedenen Regelwerken vorgenommen werden.

Der Safety-Integritätslevel SIL 4 ist die höchste Stufe der Sicherheitsintegrität und der Safety-Integritätslevel SIL 1 die niedrigste.

Je **höher** der Safety Integrity Level der sicherheitsbezogenen Systeme ist, um so **geringer** ist die Wahrscheinlichkeit, dass sie die geforderten Sicherheitsfunktionen nicht ausführen.

Auswahl der Gerätekomponenten:

Abhängig von der Anlageneinstufung ist die sicherheitstechnische Geräteauswahl bzw. sicherheitstechnische Installation dieser Komponenten vorzunehmen.

Einige Begriffe

**SIL** (Safety Integrity Level)  
Maß der Risikoreduzierung

**SFF** (Safe Failure Fraction)  
Anteil der ungefährlichen Ausfälle bezogen auf die Summe aller Ausfälle in Prozent

**PFD<sub>avg</sub>** (Probability of dangerous on demand)  
mittlere Wahrscheinlichkeit eines gefährlichen Ausfalls der Sicherheitsfunktion bei Anforderung zugrunde gelegt ist ein Anforderungsintervall von einem Jahr  
Anwendung bei „low demand“

**PFH** (Probability of dangerous Failure per Hour)  
mittlere Wahrscheinlichkeit eines gefährlichen Ausfalls der Sicherheitsfunktion pro Stunde  
Anwendung bei „hight demand“ bzw. „continuos mode“

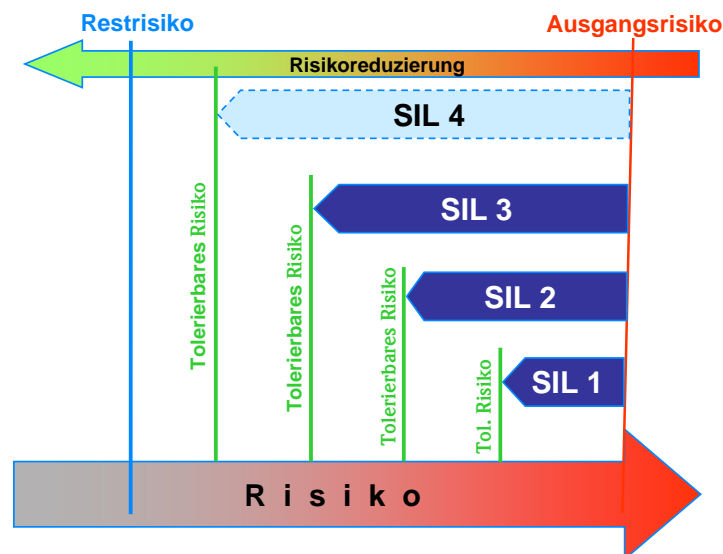
**HFT** (Hardware Fault Tolerance)  
Hardware Fehlertoleranz: N+1 Fehler führen zum Verlust der Sicherheitsfunktion

**Ti** (Prüfintervall)

...

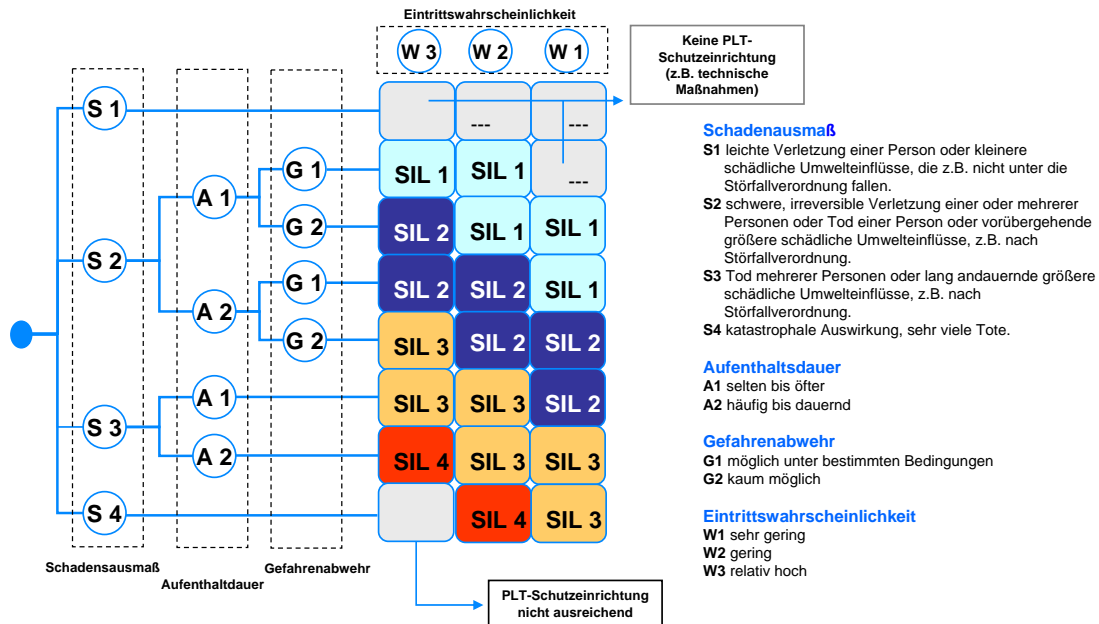
Risikoreduzierung durch SIL

Anlagensicherheit / Maschinensicherheit /Feuerungstechnik / usw.



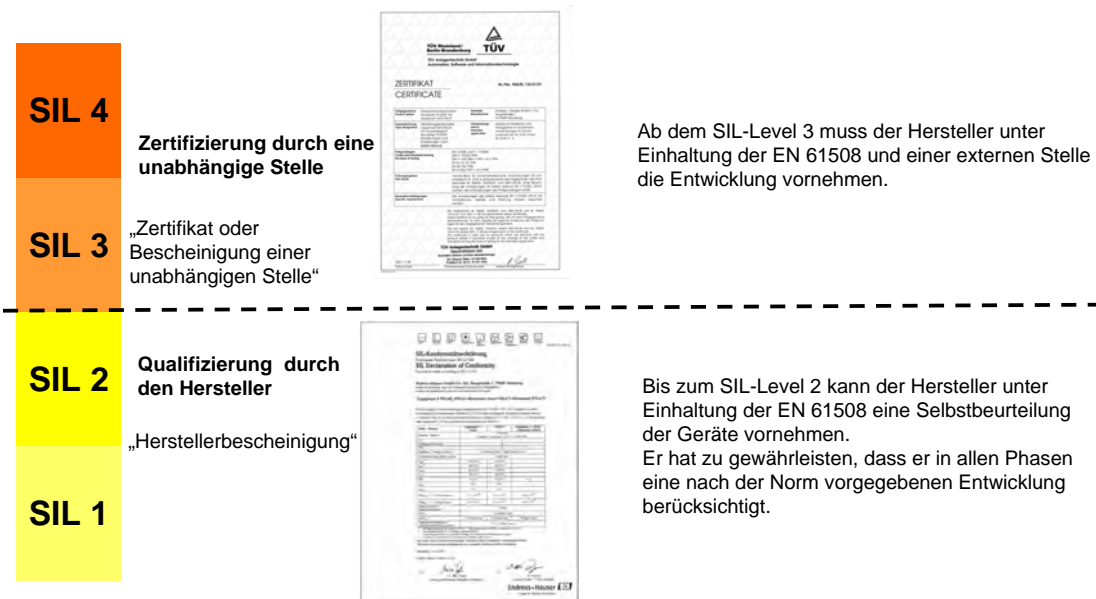
„SIL“ ist ein Maß für die Risikoreduzierung

Erforderlicher Safety Integrity Level (SIL) durch Risikograph

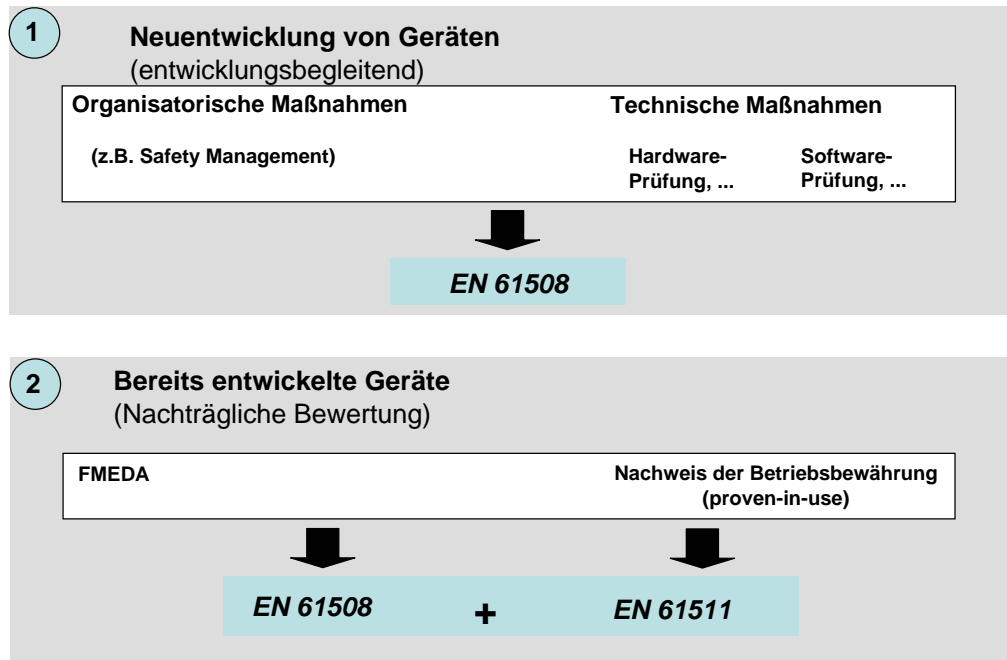


Risikoreduzierung durch SIL

Vier Levels: SIL 1 bis SIL 4



SIL-Bewertung für neue Geräte oder bereits entwickelte Geräte



Was muss der Hersteller berücksichtigen?

Angepasste Entwicklungs- und Fertigungsprozesse



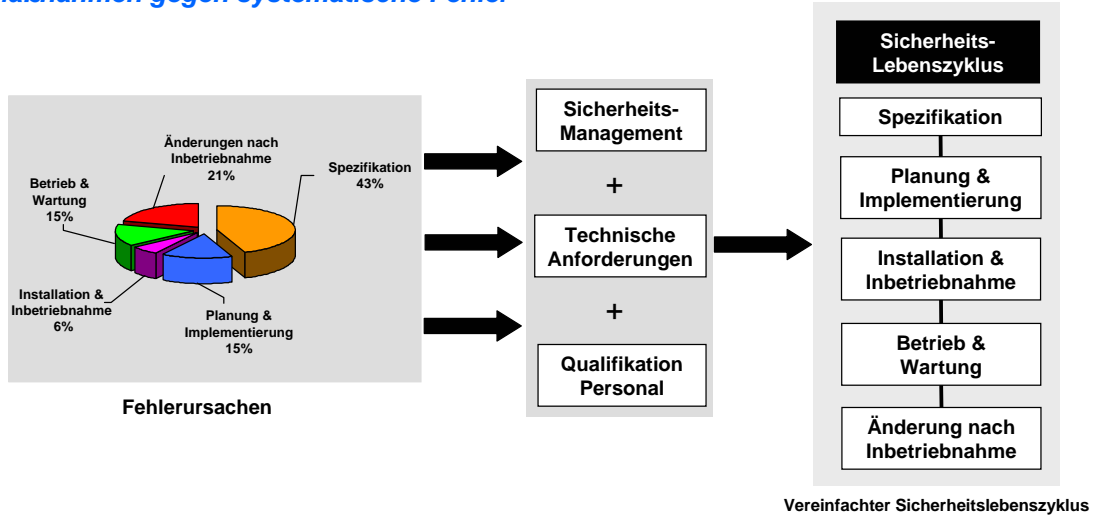
- ⇒ Konzept
- ⇒ Entwicklung
- ⇒ Fertigung
- ⇒ Betrieb und Wartung

Bei der **Hardware- und Software-Entwicklung** sind vom Hersteller Organisatorische Vorgaben zu erfüllen:

SIL-Level	Beurteilung durch:
<b>SIL 4</b>	Unabhängige Organisation
<b>SIL 3</b>	Unabhängige Organisation
<b>SIL 2</b>	Unabhängige Abteilung
<b>SIL 1</b>	Unabhängige Person

Der Hersteller muss die Abläufe gemäß EN 61508 organisieren.

Maßnahmen gegen systematische Fehler



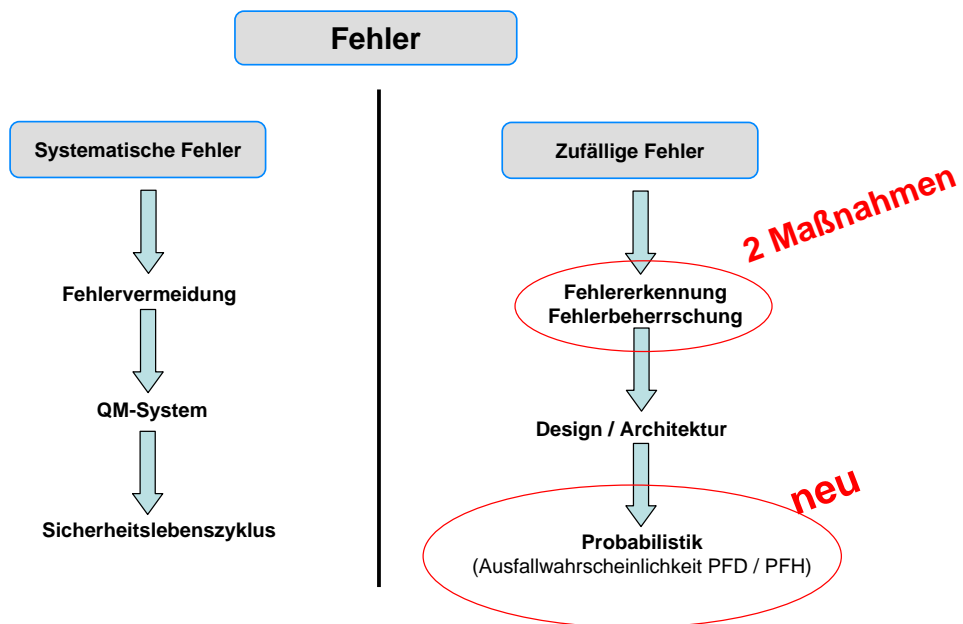
**Hersteller**

Entwicklung nach EN 61508  
 FMEDA  
 QS-Statistik  
 Betriebsbewährung

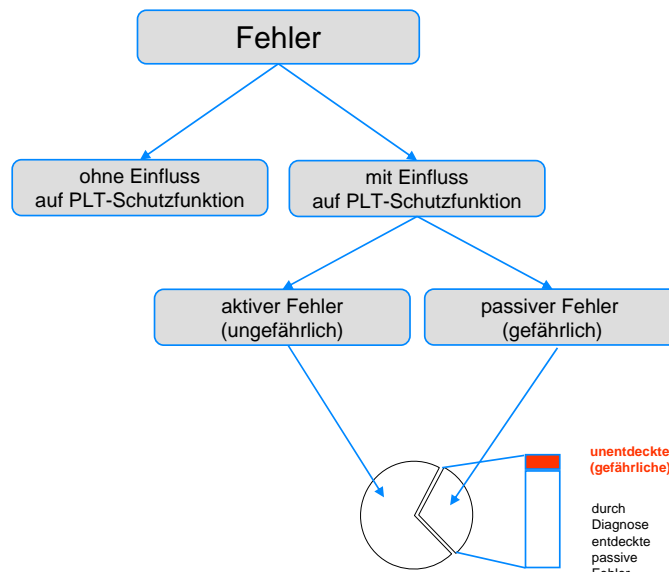
**Anwender**

Genaue Spezifikation  
 Messstellenblatt gemäß Blatt 5 VDI/VDE 2180  
 Betriebsbewährung  
 Fortlaufende Beobachtung im Einsatz

Systematische und zufällige Fehler (Maßnahmen)



Fehler in PLT-Schutzeinrichtungen

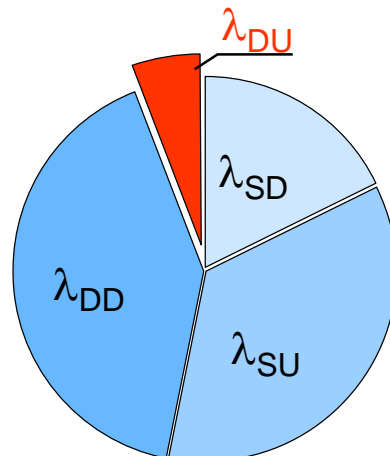


**Aktiver Fehler**  
Fehler, der Schutzfunktionen auslöst, ohne dass die aufgabengemäß festgelegten Bedingungen erfüllt sind.

**Passiver Fehler**  
Fehler, der Schutzfunktionen blockiert, obwohl alle aufgabengemäß festgelegten Bedingungen erfüllt sind.

SSF (Safe Failure Fraction)

$\lambda$  = Ausfallrate / Fehlerverteilung



Ausfallrate

$\lambda_{SD}$  = sicher erkannt

$\lambda_{SU}$  = sicher unerkannt

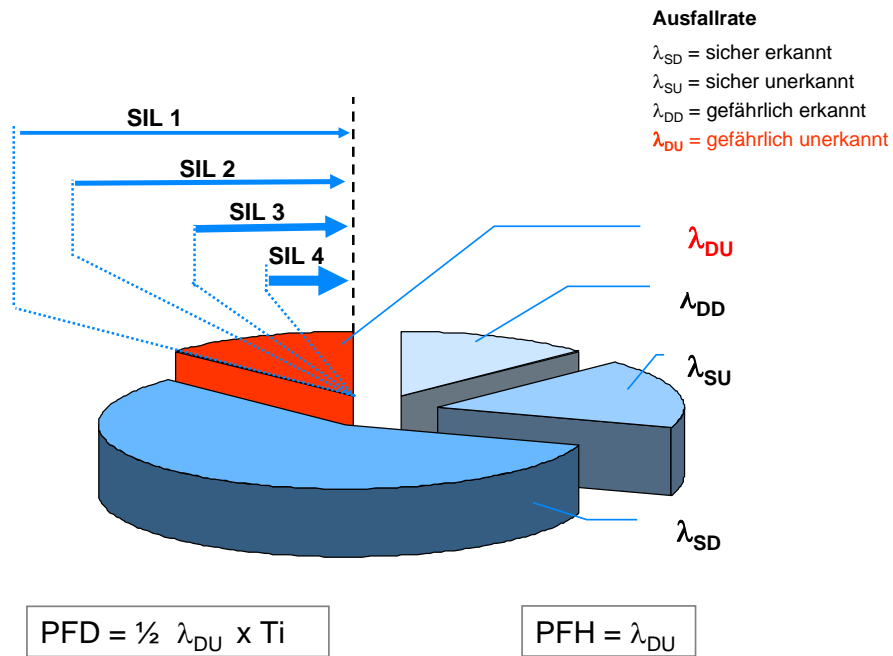
$\lambda_{DD}$  = gefährlich erkannt

$\lambda_{DU}$  = gefährlich unerkannt

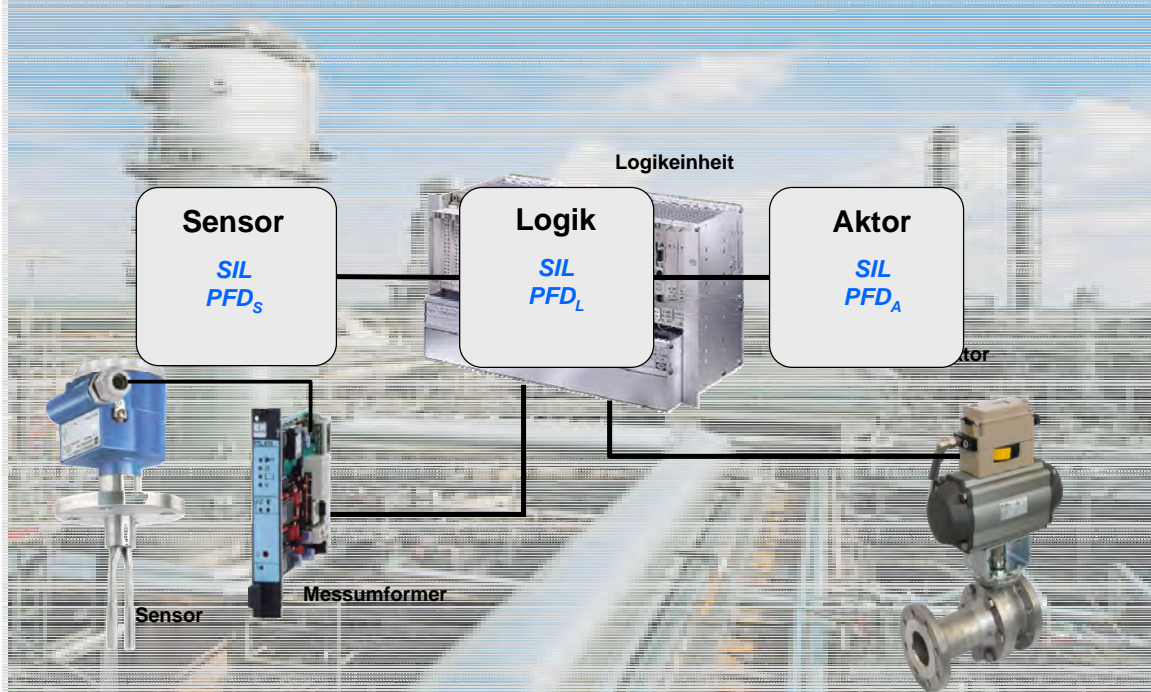
$$SSF = \frac{\lambda_{SD} + \lambda_{SU} + \lambda_{DD}}{\lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}}$$

$$SSF = 1 - \frac{\lambda_{DU}}{\lambda}$$

Risikoreduzierung



Der Sicherheitskreis



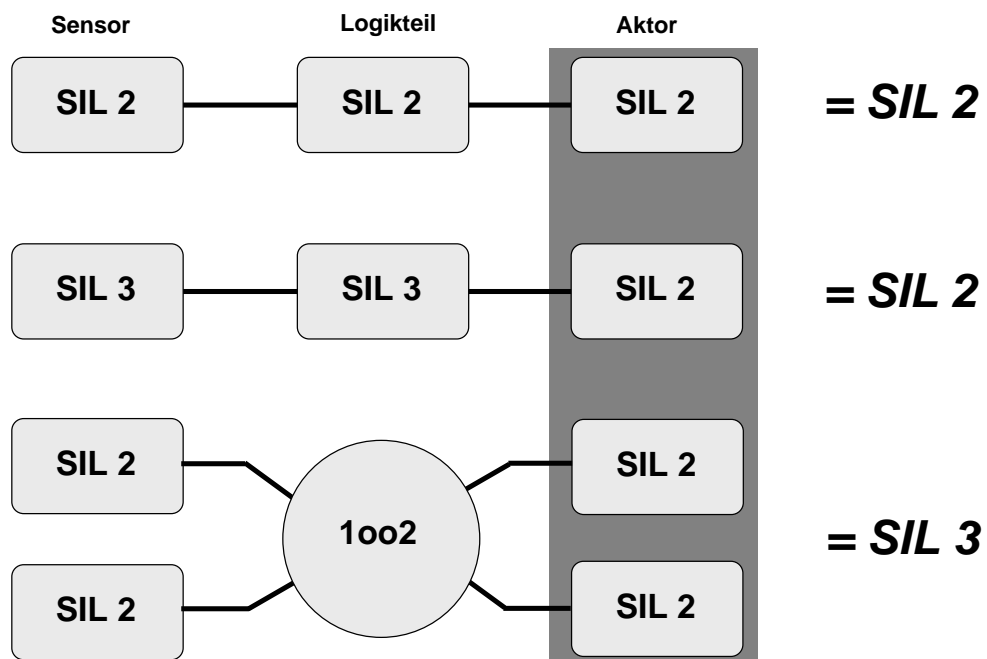
## Der Sicherheitskreis: Das Absperrorgan

Tabelle 6 EN 61511-1

SIL	HFT (Architektur) (Absch. 11.4.3 und 11.4.4)
1	0
2	1
3	2
4	Spezial requirements (EN 61508)

**HFT 0**  
 Ein Sicherheitskreis mit nur einem Ventil erreicht maximal **SIL 2**,  
 und das auch nur wenn eine Betriebsbewährung für das Ventil vorliegt

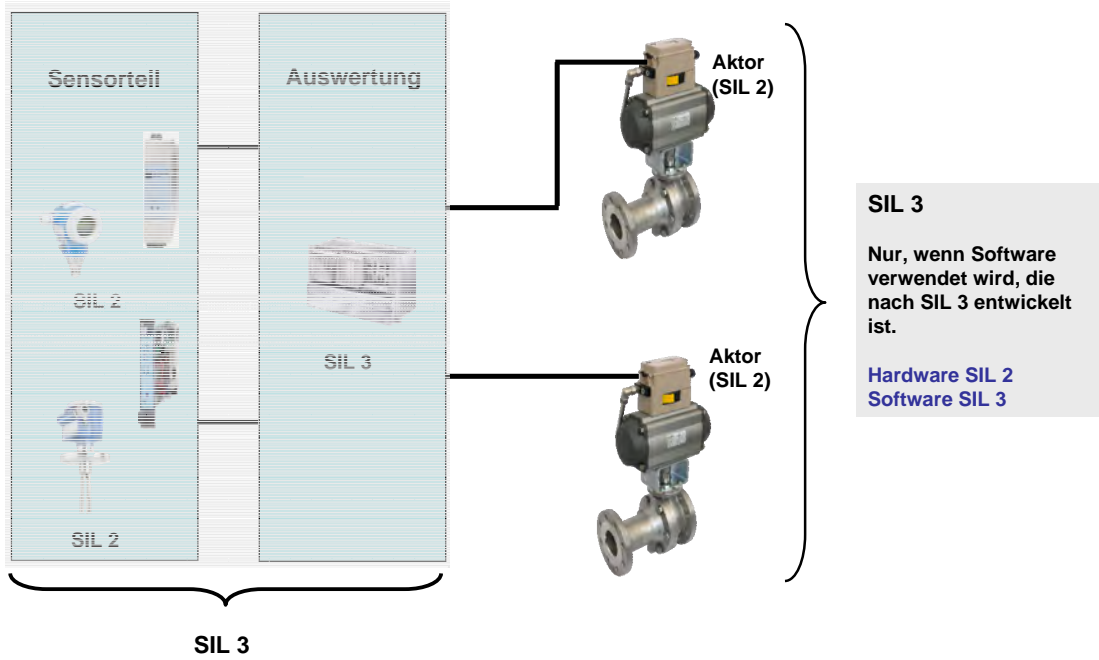
### Faustformel



**Der jeweils kleinere SIL ist maßgebend!**

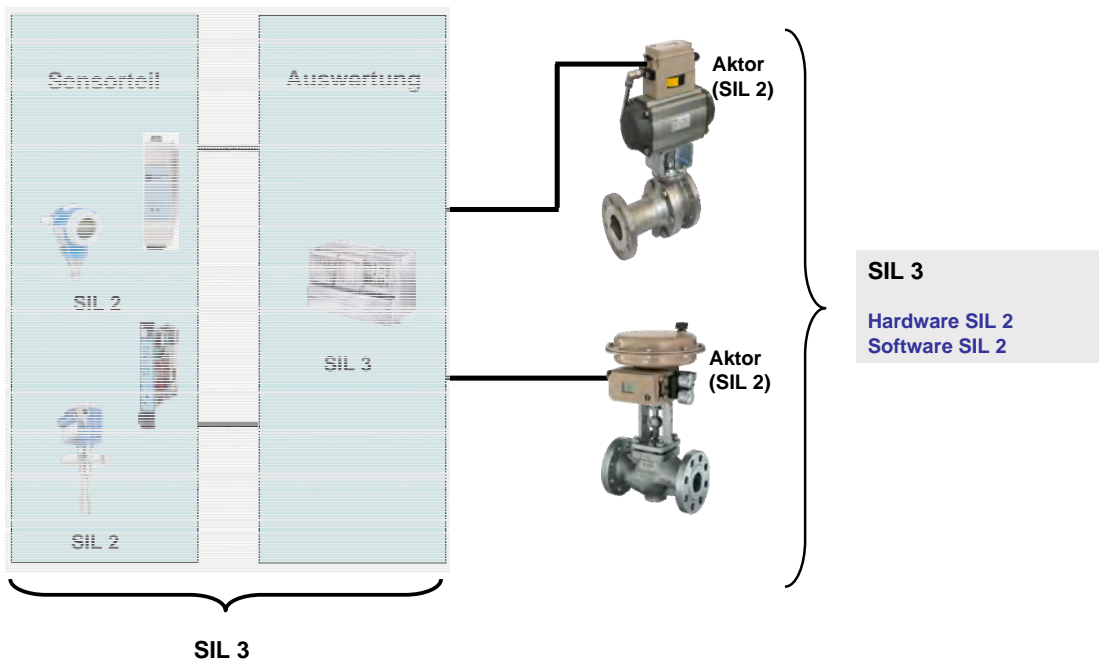
► „Funktionale Sicherheit – SIL –“

Zweikanalige Architektur (homogene Redundanz)




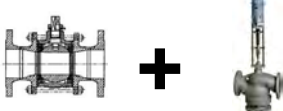


► „Funktionale Sicherheit – SIL –“

Zweikanalige Architektur (diversitäre Redundanz)

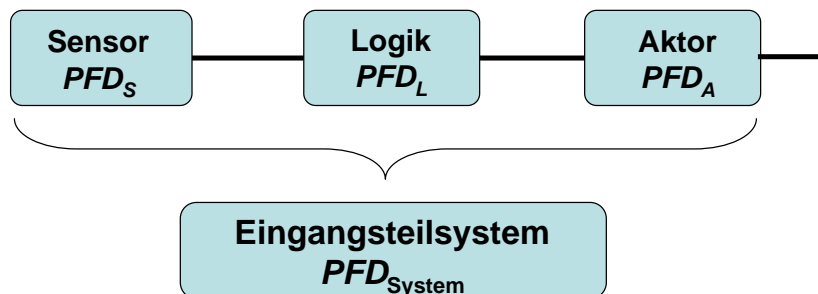


Architektur (einkanalig / redundant)

<p><b>Aufbau einkanalig</b> Ein einzelnes Gerät</p>	
<p><b>Aufbau homogen redundant</b> Zwei gleiche Geräte</p>	
<p><b>Aufbau diversitär redundant</b> Zwei unterschiedliche Geräte  (Maßnahme, dass ein systematischer Fehler nicht gleichzeitig auftreten kann)</p>	
<p><b>Aufbau diversitär redundant</b> Zwei unterschiedliche Technologien  (verschiedene Prinzipien)</p>	

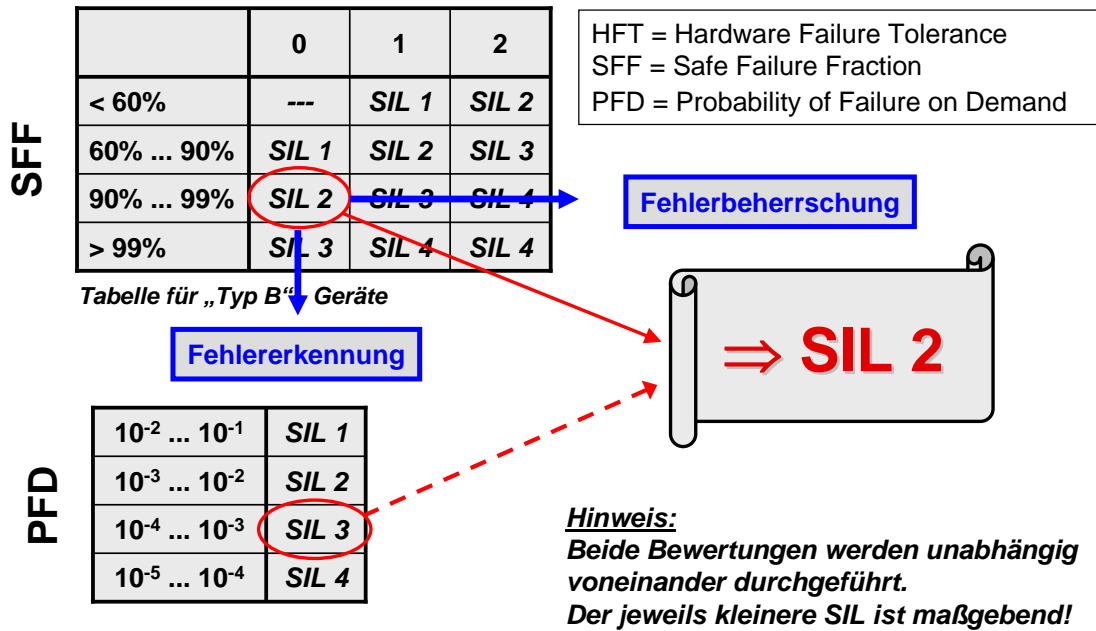
- ➡ Für den Anwender ist es wichtig für seine Anlage die richtige Instrumentierung auswählen zu können
- ➡ Für bestehende Anlagen brauchen die Anwender verlässliche Zahlen der Betriebsbewährung

Verfahren zur Berechnung einkanaliger Systeme



$$PFD_{System} = PFD_S + PFD_L + PFD_A$$

Prinzip der SIL-Bewertung



Beispiele für Fehler im Aktorteilsystem und Möglichkeiten der Fehlererkennung (NE 106)

Die häufigsten Fehlerbilder an Aktorteilsystemen sind in nachfolgender Tabelle aufgeführt.  
Längere Prüfabstände stellen besonders die Aktorseite vor eine besondere Herausforderung.  
Hier ist eine automatische Diagnose wesentlich schwieriger zu realisieren als bei den Sensoren.  
Durch einen Ventilanlauf-Test (Partial Stroke Test) können viele Fehler bei laufendem Betrieb erkannt werden.

Fehlerbild	Mögliche Fehlerursache	Fehler erkennbar?		Fehlererkennung
		Ventilanlauf-Test	Vollhub-/Voll-drehungstest	
Magnetventil schaltet nicht	Ansteuerung zum Magnetventil defekt	erkennbar	erkennbar	Erkennung über Stellungsrückmeldung
Magnetventil schaltet nicht	Magnetventil defekt	erkennbar	erkennbar	Erkennung über Stellungsrückmeldung
Ventil reagiert zu langsam	Luftleitung zum Ventil gequetscht	erkennbar	erkennbar	Erkennung durch Überwachung der Zeit bis zur erfolgten Stellungsrückmeldung
Ventil reagiert zu langsam	Ventil schwergängig	erkennbar	erkennbar	Erkennung durch Überwachung der Zeit bis zur erfolgten Stellungsrückmeldung
Ventil schließt nicht oder nicht vollständig	Ventilsitz "vernarbt", Kegel "ausgewaschen"	nicht erkennbar	erkennbar	Erkennung über Ventilanlauf-Test nicht möglich
Ventil schließt nicht oder nicht vollständig	Ventilsitz enthält Ablagerungen	nicht erkennbar	erkennbar	Erkennung über Ventilanlauf-Test nicht möglich
Ventil schließt nicht	Ventilschaft blockiert	erkennbar	erkennbar	Erkennung über Stellungsrückmeldung

SIL-Herstellererklärung bzw. SIL-Konformitätsbescheinigung

<b>Hersteller</b>			
Hersteller			
Anschrift			
<b>Allgemein</b>			
Gerätebezeichnung und zulässige Ausführungen			
Sicherheitsbezogenes Ausgangssignal			
Fehlerstrom			
Bewertete Messgröße/ Funktion			
Sicherheitsfunktion(en)			
Gerätetyp gem. IEC 61508-2		<input type="checkbox"/> Typ A	<input type="checkbox"/> Typ B
Betriebsart		<input type="checkbox"/> Low Demand Mode	<input type="checkbox"/> High Demand oder Common Mode
Gültige Hardware-Version			
Gültige Software-Version			
Sicherheitshandbuch			
Art der Bewertung (nur eine Variante wählbar)		<input type="checkbox"/> Vollständige entwicklungsbegleitende HW/SW Bewertung inkl. FMEDA und Änderungsprozess nach IEC 61508-2, 3	
		<input type="checkbox"/> Bewertung über Nachweis der Betriebbewährung HW/SW inkl. FMEDA und Änderungsprozess nach IEC 61508-2, 3	
		<input type="checkbox"/> Auswertung von Feldtesten HW/SW zum Nachweis: Frühere Verwendung "Prior Use" gem. IEC 61511	
		<input type="checkbox"/> Bewertung durch FMEDA gem. IEC 61508-2 für Geräte ohne Software	
Bewertung durch (inkl. Berichtsnr. + FMEDA Datenquelle)			
Prüfunterlagen			
<b>SIL - Integrität</b>			
Systematische Sicherheitsintegrität		<input type="checkbox"/> SIL 2 fähig	<input type="checkbox"/> SIL 3 fähig
Hardware Sicherheitsintegrität		<input type="checkbox"/> Einmaliger Einsatz (HFT = 0)	<input type="checkbox"/> SIL 2 fähig
		<input type="checkbox"/> Mehrmaliger Einsatz (HFT >1)	<input type="checkbox"/> SIL 3 fähig
<b>FMEDA</b>			
Sicherheitsfunktion			
$A_{cu}^{(1)}$	FIT	FIT	
$A_{cu}^{(2)}$	FIT	FIT	
$A_{cu}^{(3)}$	FIT	FIT	
$A_{cu}^{(4)}$	FIT	FIT	
SFF - Safe Failure Fraction	%	%	
PTC <sup>(2)</sup>	%	%	
<b>Bemerkung</b>			
<b>Erklärung</b>			
<input type="checkbox"/> Unser firmeninternes Qualitätsmanagement stellt die Information von zukünftig bekannt gewordenen sicherheitsrelevanten systematischen Fehlern sicher.			

- Hersteller
- Typ A / B
- Hight- / Low-Demand
- FMEDA
- SIL
- HFT
- Fehlerraten (λ-Werte)
- SFF
- Testintervall (Ti)
- PFD-Wert
- SW-Version
- HW-Version

Dem Anwender sind zur Planung entsprechende Informationen zur Verfügung zu stellen.