Wissenswertes zur Funktionalen Sicherheit

PILZ
THE SPIRIT OF SAFETY

AUTOMATION
ON TOUR
with Pilz

Agenda

01 Einführung in die funktionale Sicherheit

02 Grundlagen der Norm EN ISO 13849-1

03 Verifikation des Performance Levels

01

- Einführung in die funktionale Sicherheit

Einführung in die funktionale Sicherheit

Bedeutung

- **Funktionale Sicherheit** (abgekürzt auch **FuSi**) bezeichnet die zuverlässige Erbringung von Sicherheitsfunktionen eines Systems.

  Sie soll mögliche Risiken deutlich begrenzen, indem systematische Fehler vermieden, zufällige Fehler erkannt und auf erkannte Fehler reagiert wird.

- Nicht zur funktionalen Sicherheit gehören u. a. elektrische Sicherheit, Brandschutz oder Strahlenschutz.

Einführung in die funktionale Sicherheit

Bedeutung

Inhalte der EN 61508 Reihe

Sicherheits-Lebenszyklus

Im ersten Teil der Norm wird der komplette **Sicherheits-Lebenszyklus** mit detaillierten Anforderungen an Vorgehen und Inhalt der einzelnen Schritte betrachtet. Dieser Teil ist sowohl für Maschinenbauer wie auch für Hersteller von Sicherheitskomponenten von zentraler Bedeutung.

Entwurf von elektrischen Systemen

Ein weiterer Fokus der Norm liegt auf dem **Entwurf von elektrischen Systemen und der zugehörigen Software**. Den größten Nutzen aus der Norm haben voraussichtlich **Hersteller von Sicherheitskomponenten**.

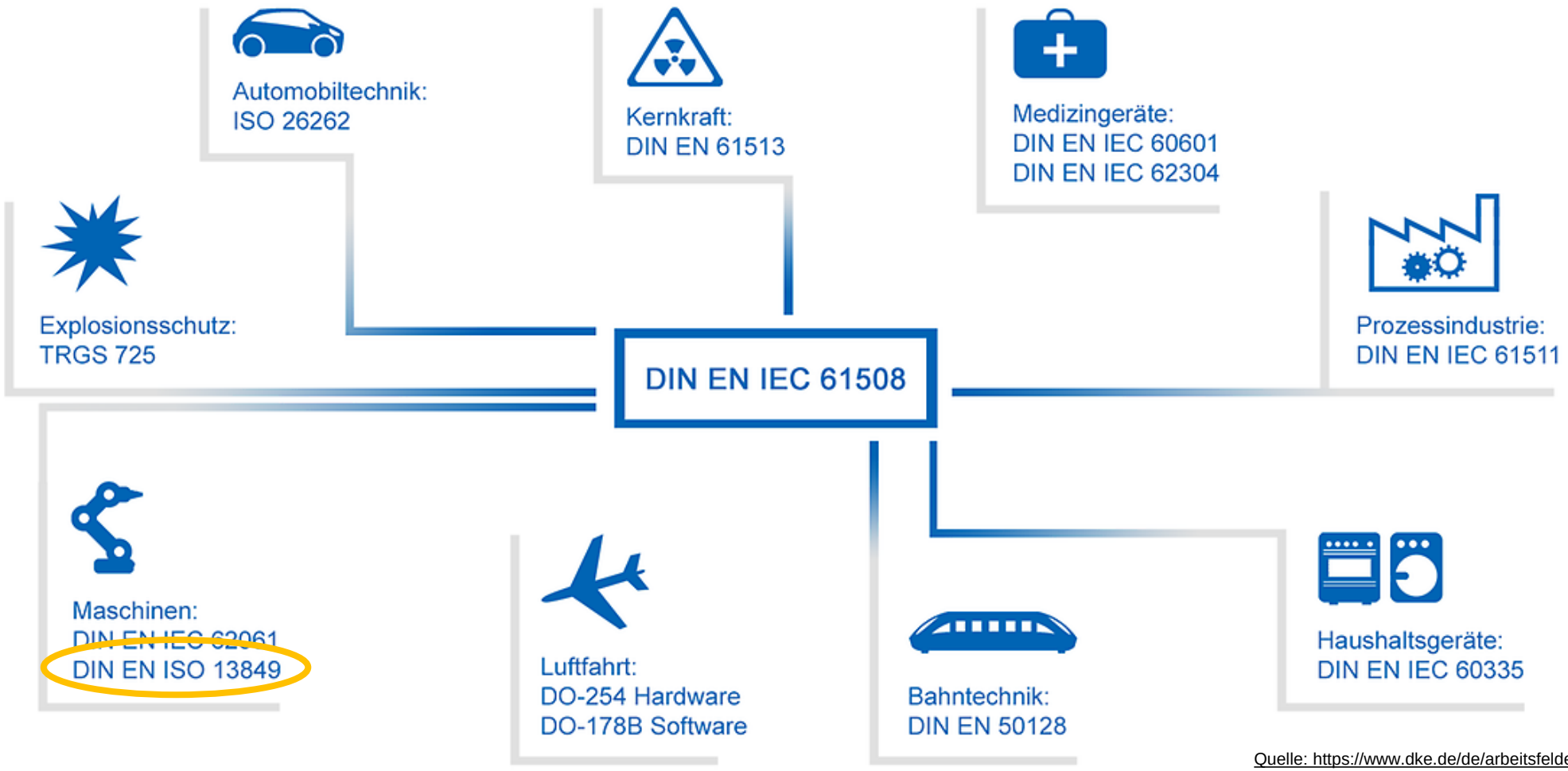
Normung der EN 61508 Reihe

Die Norm EN 61508 Reihe "Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme" besteht aus folgenden Teilen:

Teil 1: Einführung in Konzept der Funktionalen Sicherheit,
Überblick über die Normen der Reihe IEC 61508
Teil 2: Anforderungen an sicherheitsbezogene
elektrische/elektronische/programmierbare elektronische Systeme
Teil 3: Anforderungen an Software
Teil 4: Begriffe und Abkürzungen
Teil 5: Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität
Teil 6: Anwendungsrichtlinie für Teil 2 und Teil 3
Teil 7: Anwendungshinweise über Verfahren und Maßnahmen

Einführung in die funktionale Sicherheit

Zusammenhänge



Quelle: https://www.dke.de/de/arbeitsfelder/core-safety/funktionale-sicherheit

Einführung in die funktionale Sicherheit

Maschinenbau

Mutter (Basis-)norm

EN 61508 - Funktionale Sicherheit von Steuerungssystemen

- Sicherheits-Lebenszyklus
- Entwurf von elektrischen Systemen + Software
- SIL 1-4
- 7 Teile

Tochternorm

EN ISO 13849 – Performance Level (PL a-e)

- Für den klassischen Maschinenbau
- Elektrik, Pneumatik, Hydraulik

EN ISO 13849 – 1 Allgemeine Gestaltungsleitsätze	EN ISO 13849 – 2 Validierung

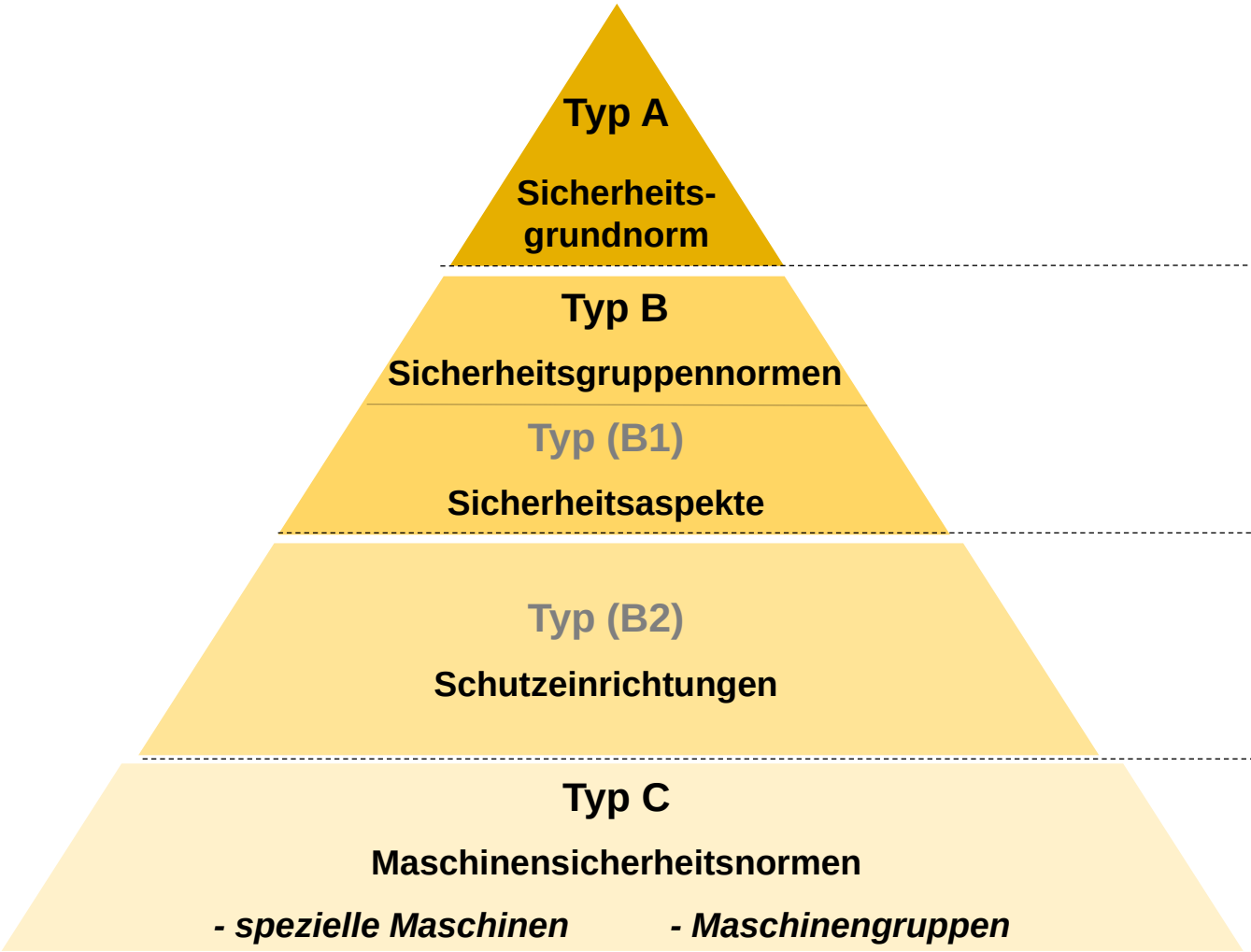
Tochternorm

EN IEC 62061 – SIL (1-3)

- für rein elektronische Systeme
- bei Anwendung von komplexen, rein elektrischen Steuerungssystemen

Einführung in die funktionale Sicherheit

Sicherheitsnormen



- **DIN EN ISO 12100:2010**
  Sicherheit von Maschinen –
  Allgemeine Gestaltungsleitsätze –
  Risikobeurteilung und Risikominderung

- **EN ISO 13849-1/-2**
  Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze – Teil 2: Validierung

- **EN ISO 14119**
  Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen

- **EN ISO 10218-1 und -2**
  Industrieroboter – Sicherheitsanforderungen –
  Teil 1: Roboter - Teil 2: Robotersysteme und Integration

02

- Grundlagen der Norm EN ISO 13849-1

Funktionale Sicherheit - EN ISO 13849

Einführung EN ISO 13849

Steuerungen für die automatische Aktivierung, bevor Personen den Gefahrenbereich erreichen können, müssen gemäß den folgenden Normen konstruiert und implementiert werden:

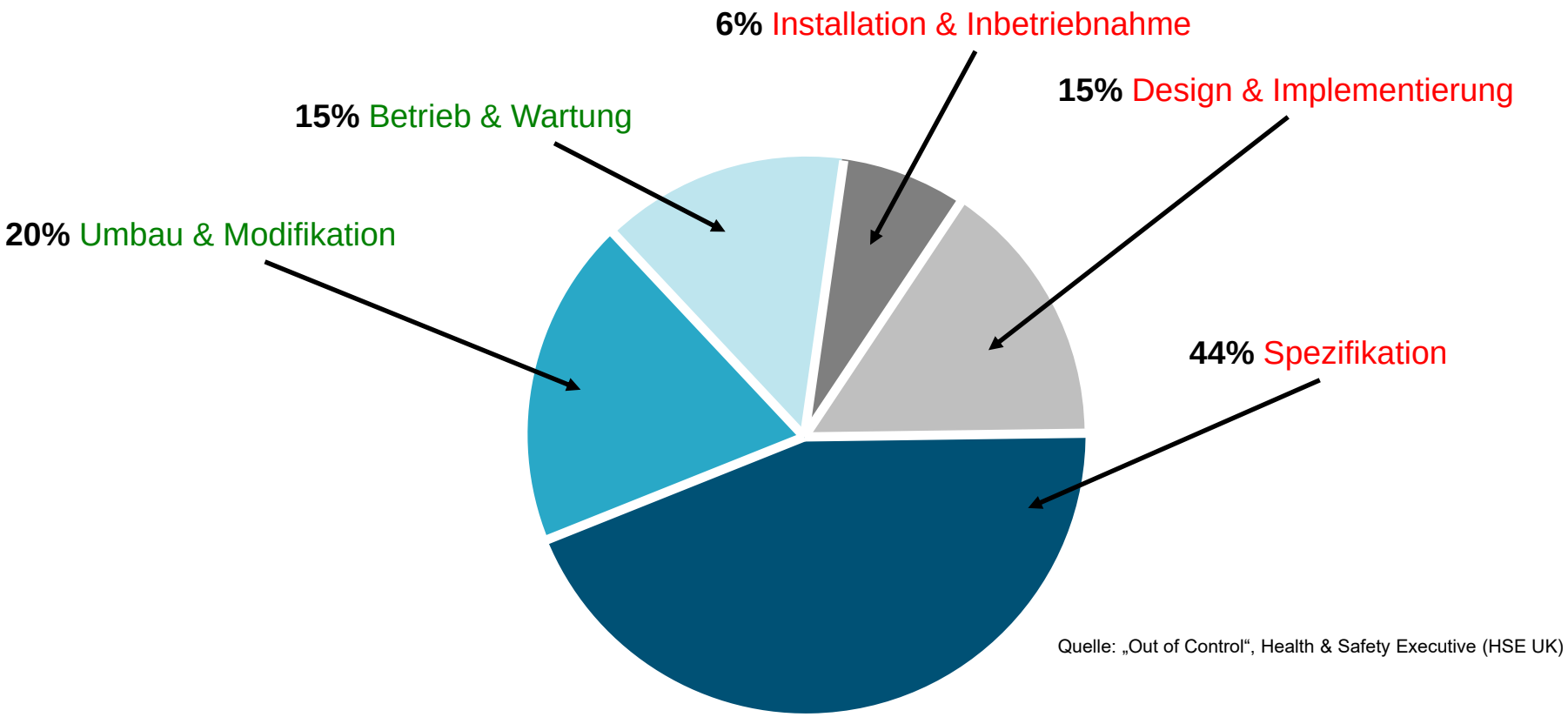
- **EN ISO 13849-1** Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze
- **EN ISO 13849-2** Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 2: Validierung

Die folgenden Gesichtspunkte müssen berücksichtigt werden:

- **muss** den beabsichtigten Betriebsbeanspruchungen und externen Einflüssen **widerstehen**
- **Hard-/Softwarefehler** an/in der Steuerungslogik **führen nicht zu gefährlichen Situationen**
- **vernünftigerweise vorhersehbare Bedienungsfehler** führen **nicht** zu Gefährdungssituationen

Funktionale Sicherheit - EN ISO 13849

Versagensursachen



Quelle: „Out of Control“, Health & Safety Executive (HSE UK)

1/3 Betrieb

2/3 Konstruktion & Design

Funktionale Sicherheit - EN ISO 13849

Versagensursachen

Zufällige Hardwarefehler

Fehler zu einem beliebigem Moment, auf Grund einer oder mehrerer zufälliger Ausfälle in der Hardware.

+

systematische Fehler

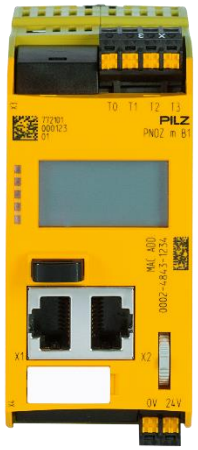
oftmals menschl. Versagen während :

- der Formulierung der Spezifikation
- der Formulierung der Dokumentation
- der Design-Umsetzung
- der Hardwareinstallation
- des Software-Integration und -Design

EN ISO 13849-1	Performance Level	- PL (a,b,c,d,e)
EN IEC 62061	Safety Integrity Level	- SIL (1,2,3)

Funktionale Sicherheit - EN ISO 13849

Simple Darstellung einer Sicherheitsfunktion



Eingang (Input)	→	Logik (Logic)	→	Ausgang (Output)

Funktionale Sicherheit - EN ISO 13849

Ausfallswahrscheinlichkeit eines Systems (Performance)

Zufällige Hardwareausfälle

Fehler gem. Ursache
(CCF, ß*)

PFHd

Probability of Failure
per Hour (dangerous)

Architektur
(Kat. B - 4)

Diagnosefähigkeit
(DC, SFF*)

Komponentenverfügbarkeit
(MTTFd, B10d, T10d…)

Test Interval*
(Lifetime T1
Diagnose Test Interval T2)

*EN 62061 Begriffe

Funktionale Sicherheit - EN ISO 13849

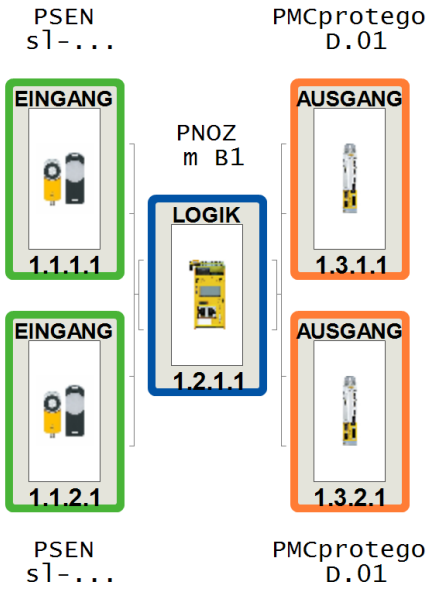
PFHd – Gefährlicher Ausfall pro Stunde

PFHd **probability of failure per hour (dangerous)**

„durchschnittliche (mittlere) Wahrscheinlichkeit eines Ausfalls je Stunde“

Gefährliche Ausfallswahrscheinlichkeit der Sicherheitsfunktion
z.B. **2,65x10^{-7}** = 0,000000265 Wahrscheinlichkeit / Ausfall pro Stunde

$$PFH_{d\,Ges} = \sum PFH_d$$



Funktionale Sicherheit - EN ISO 13849

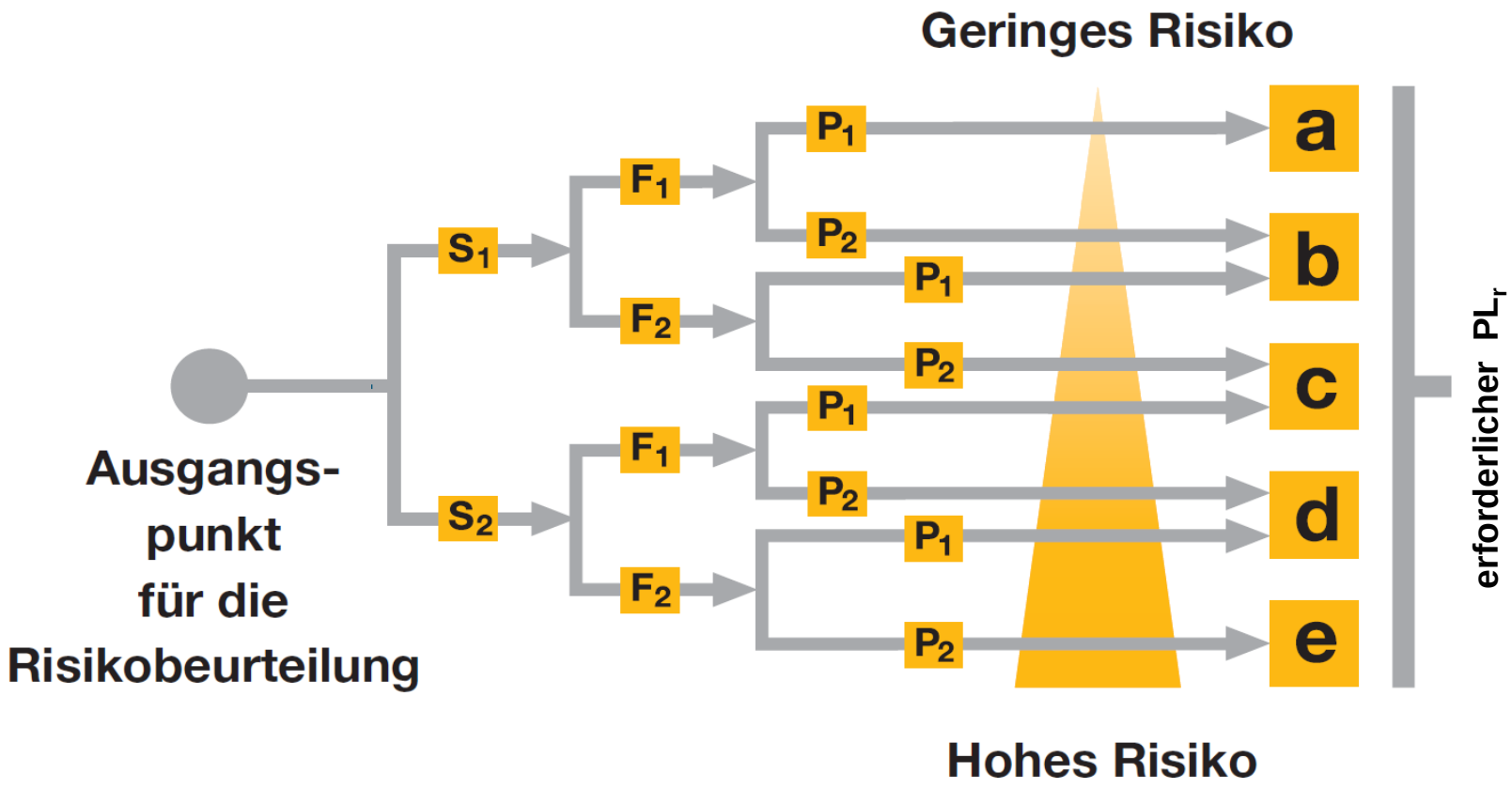
Umschlüsselung PFHd in PL

	Durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde (1/h) und der zugehörige Performance Level (PL)															
$MTTF_d$ für jeden Kanal Jahre	Kat. B DC_{avg} = kein	PL	Kat. 1 DC_{avg} = kein	PL	Kat. 2 DC_{avg} = niedrig	PL	Kat. 2 DC_{avg} = mittel	PL	Kat. 3 DC_{avg} = niedrig	PL	Kat. 3 DC_{avg} = mittel	PL	Kat. 4 DC_{avg} = hoch	PL
3	$3{,}80 \times 10^{-5}$	a			$2{,}58 \times 10^{-5}$	a	$1{,}99 \times 10^{-5}$	a	$1{,}26 \times 10^{-5}$	a	$6{,}09 \times 10^{-6}$	b		
3,3	$3{,}46 \times 10^{-5}$	a			$2{,}33 \times 10^{-5}$	a	$1{,}79 \times 10^{-5}$	a	$1{,}13 \times 10^{-5}$	a	$5{,}41 \times 10^{-6}$	b		
3,6	$3{,}17 \times 10^{-5}$	a			$2{,}13 \times 10^{-5}$	a	$1{,}62 \times 10^{-5}$	a	$1{,}03 \times 10^{-5}$	a	$4{,}86 \times 10^{-6}$	b		
3,9	$2{,}93 \times 10^{-5}$	a			$1{,}95 \times 10^{-5}$	a	$1{,}48 \times 10^{-5}$	a	$9{,}37 \times 10^{-6}$	b	$4{,}40 \times 10^{-6}$	b		
4,3	$2{,}65 \times 10^{-5}$	a			$1{,}76 \times 10^{-5}$	a	$1{,}33 \times 10^{-5}$	a	$8{,}39 \times 10^{-6}$	b	$3{,}89 \times 10^{-6}$	b		
4,7	$2{,}43 \times 10^{-5}$	a			$1{,}60 \times 10^{-5}$	a	$1{,}20 \times 10^{-5}$	a	$7{,}58 \times 10^{-6}$	b	$3{,}48 \times 10^{-6}$	b		
5,1	$2{,}24 \times 10^{-5}$	a			$1{,}47 \times 10^{-5}$	a	$1{,}10 \times 10^{-5}$	a	$6{,}91 \times 10^{-6}$	b	$3{,}15 \times 10^{-6}$	b		
5,6	$2{,}04 \times 10^{-5}$	a			$1{,}33 \times 10^{-5}$	a	$9{,}87 \times 10^{-6}$	b	$6{,}21 \times 10^{-6}$	b	$2{,}80 \times 10^{-6}$	c		
6,2	$1{,}84 \times 10^{-5}$	a			$1{,}19 \times 10^{-5}$	a	$8{,}80 \times 10^{-6}$	b	$5{,}53 \times 10^{-6}$	b	$2{,}47 \times 10^{-6}$	c		
6,8	$1{,}68 \times 10^{-5}$	a			$1{,}08 \times 10^{-5}$	a	$7{,}93 \times 10^{-6}$	b	$4{,}98 \times 10^{-6}$	b	$2{,}20 \times 10^{-6}$	c		
7,5	$1{,}52 \times 10^{-5}$	a			$9{,}75 \times 10^{-6}$	b	$7{,}10 \times 10^{-6}$	b	$4{,}45 \times 10^{-6}$	b	$1{,}95 \times 10^{-6}$	c		
8,2	$1{,}39 \times 10^{-5}$	a			$8{,}87 \times 10^{-6}$	b	$6{,}43 \times 10^{-6}$	b	$4{,}02 \times 10^{-6}$	b	$1{,}74 \times 10^{-6}$	c		
9,1	$1{,}25 \times 10^{-5}$	a			$7{,}94 \times 10^{-6}$	b	$5{,}71 \times 10^{-6}$	b	$3{,}57 \times 10^{-6}$	b	$1{,}53 \times 10^{-6}$	c		
10	$1{,}14 \times 10^{-5}$	a			$7{,}18 \times 10^{-6}$	b	$5{,}14 \times 10^{-6}$	b	$3{,}21 \times 10^{-6}$	b	$1{,}36 \times 10^{-6}$	c		
11	$1{,}04 \times 10^{-5}$	a			$6{,}44 \times 10^{-6}$	b	$4{,}53 \times 10^{-6}$	b	$2{,}81 \times 10^{-6}$	c	$1{,}18 \times 10^{-6}$	c		
12	$9{,}51 \times 10^{-6}$	b			$5{,}84 \times 10^{-6}$	b	$4{,}04 \times 10^{-6}$	b	$2{,}49 \times 10^{-6}$	c	$1{,}04 \times 10^{-6}$	c		
13	$8{,}78 \times 10^{-6}$	b			$5{,}33 \times 10^{-6}$	b	$3{,}64 \times 10^{-6}$	b	$2{,}23 \times 10^{-6}$	c	$9{,}21 \times 10^{-7}$	d		
15	$7{,}61 \times 10^{-6}$	b			$4{,}53 \times 10^{-6}$	b	$3{,}01 \times 10^{-6}$	b	$1{,}82 \times 10^{-6}$	c	$7{,}44 \times 10^{-7}$	d		
16	$7{,}13 \times 10^{-6}$	b			$4{,}21 \times 10^{-6}$	b	$2{,}77 \times 10^{-6}$	c	$1{,}67 \times 10^{-6}$	c	$6{,}76 \times 10^{-7}$	d		
18	$6{,}34 \times 10^{-6}$	b			$3{,}68 \times 10^{-6}$	b	$2{,}37 \times 10^{-6}$	c	$1{,}41 \times 10^{-6}$	c	$5{,}67 \times 10^{-7}$	d		
20	$5{,}71 \times 10^{-6}$	b			$3{,}26 \times 10^{-6}$	b	$2{,}06 \times 10^{-6}$	c	$1{,}22 \times 10^{-6}$	c	$4{,}85 \times 10^{-7}$	d		
22	$5{,}19 \times 10^{-6}$	b			$2{,}93 \times 10^{-6}$	c	$1{,}82 \times 10^{-6}$	c	$1{,}07 \times 10^{-6}$	c	$4{,}21 \times 10^{-7}$	d		
24	$4{,}76 \times 10^{-6}$	b			$2{,}65 \times 10^{-6}$	c	$1{,}62 \times 10^{-6}$	c	$9{,}47 \times 10^{-7}$	d	$3{,}70 \times 10^{-7}$	d		
27	$4{,}23 \times 10^{-6}$	b			$2{,}32 \times 10^{-6}$	c	$1{,}39 \times 10^{-6}$	c	$8{,}04 \times 10^{-7}$	d	$3{,}10 \times 10^{-7}$	d		
30			$3{,}80 \times 10^{-6}$	b	$2{,}06 \times 10^{-6}$	c	$1{,}21 \times 10^{-6}$	c	$6{,}94 \times 10^{-7}$	d	$2{,}65 \times 10^{-7}$	d	$9{,}54 \times 10^{-8}$	e
33			$3{,}46 \times 10^{-6}$	b	$1{,}85 \times 10^{-6}$	c	$1{,}06 \times 10^{-6}$	c	$5{,}94 \times 10^{-7}$	d	$2{,}30 \times 10^{-7}$	d	$8{,}57 \times 10^{-8}$	e
36			$3{,}17 \times 10^{-6}$	b	$1{,}67 \times 10^{-6}$	c	$9{,}39 \times 10^{-7}$	d	$5{,}16 \times 10^{-7}$	d	$2{,}01 \times 10^{-7}$	d	$7{,}77 \times 10^{-8}$	e
39			$2{,}93 \times 10^{-6}$	c	$1{,}53 \times 10^{-6}$	c	$8{,}40 \times 10^{-7}$	d	$4{,}53 \times 10^{-7}$	d	$1{,}78 \times 10^{-7}$	d	$7{,}11 \times 10^{-8}$	e
43			$2{,}65 \times 10^{-6}$	c	$1{,}37 \times 10^{-6}$	c	$7{,}34 \times 10^{-7}$	d	$3{,}87 \times 10^{-7}$	d	$1{,}54 \times 10^{-7}$	d	$6{,}37 \times 10^{-8}$	e
47			$2{,}43 \times 10^{-6}$	c	$1{,}24 \times 10^{-6}$	c	$6{,}49 \times 10^{-7}$	d	$3{,}35 \times 10^{-7}$	d	$1{,}34 \times 10^{-7}$	d	$5{,}76 \times 10^{-8}$	e
51			$2{,}24 \times 10^{-6}$	c	$1{,}13 \times 10^{-6}$	c	$5{,}80 \times 10^{-7}$	d	$2{,}93 \times 10^{-7}$	d	$1{,}19 \times 10^{-7}$	d	$5{,}26 \times 10^{-8}$	e
56			$2{,}04 \times 10^{-6}$	c	$1{,}02 \times 10^{-6}$	c	$5{,}10 \times 10^{-7}$	d	$2{,}52 \times 10^{-7}$	d	$1{,}03 \times 10^{-7}$	d	$4{,}73 \times 10^{-8}$	e
62			$1{,}84 \times 10^{-6}$	c	$9{,}06 \times 10^{-7}$	d	$4{,}43 \times 10^{-7}$	d	$2{,}13 \times 10^{-7}$	d	$8{,}84 \times 10^{-8}$	e	$4{,}22 \times 10^{-8}$	e
68			$1{,}68 \times 10^{-6}$	c	$8{,}17 \times 10^{-7}$	d	$3{,}90 \times 10^{-7}$	d	$1{,}84 \times 10^{-7}$	d	$7{,}68 \times 10^{-8}$	e	$3{,}80 \times 10^{-8}$	e
75			$1{,}52 \times 10^{-6}$	c	$7{,}31 \times 10^{-7}$	d	$3{,}40 \times 10^{-7}$	d	$1{,}57 \times 10^{-7}$	d	$6{,}62 \times 10^{-8}$	e	$3{,}41 \times 10^{-8}$	e
82			$1{,}39 \times 10^{-6}$	c	$6{,}61 \times 10^{-7}$	d	$3{,}01 \times 10^{-7}$	d	$1{,}35 \times 10^{-7}$	d	$5{,}79 \times 10^{-8}$	e	$3{,}08 \times 10^{-8}$	e
91			$1{,}25 \times 10^{-6}$	c	$5{,}88 \times 10^{-7}$	d	$2{,}61 \times 10^{-7}$	d	$1{,}14 \times 10^{-7}$	d	$4{,}94 \times 10^{-8}$	e	$2{,}74 \times 10^{-8}$	e
100			$1{,}14 \times 10^{-6}$	c	$5{,}28 \times 10^{-7}$	d	$2{,}29 \times 10^{-7}$	d	$1{,}01 \times 10^{-7}$	d	$4{,}29 \times 10^{-8}$	e	$2{,}47 \times 10^{-8}$	e

Tabelle K.1

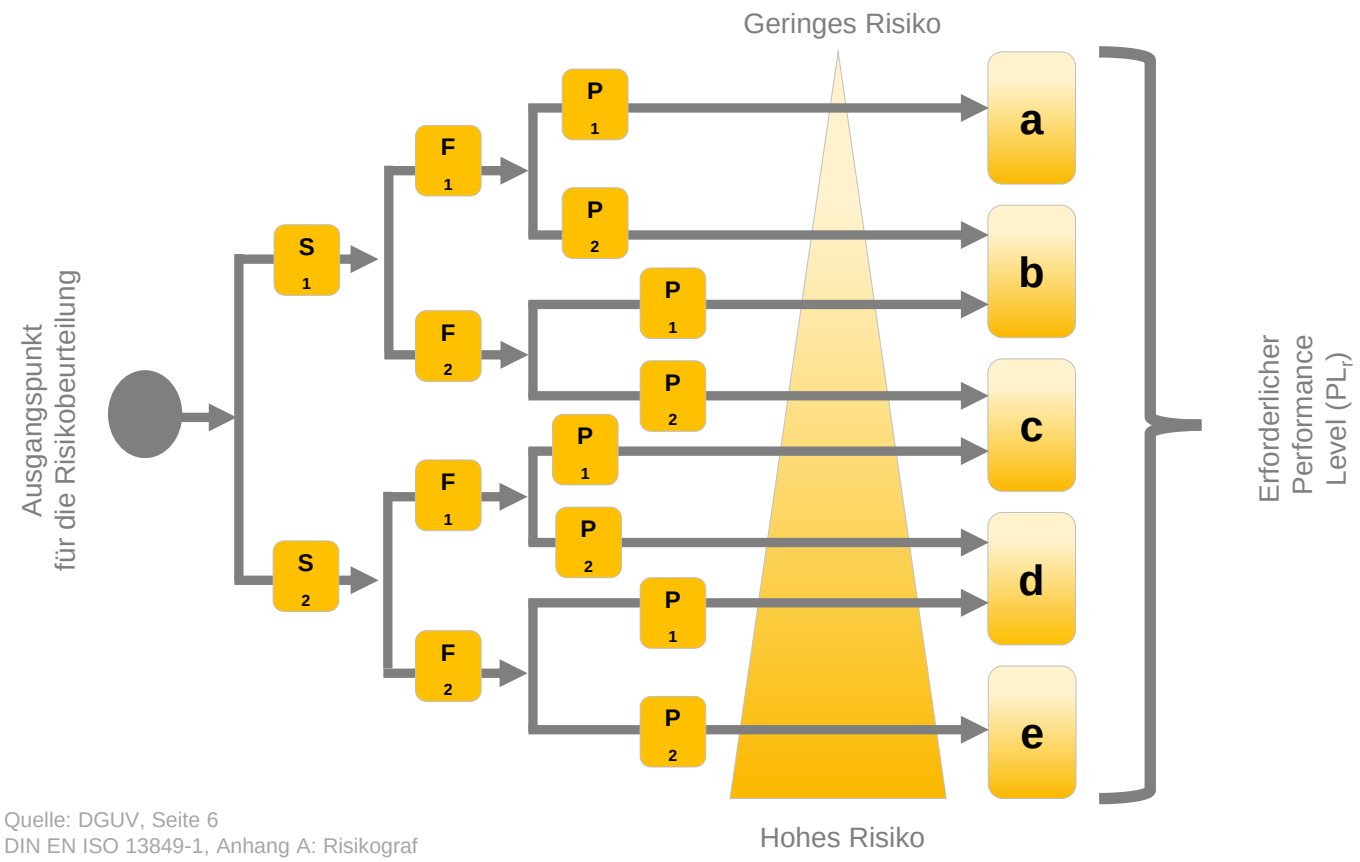
Funktionale Sicherheit - EN ISO 13849

Performance Level (PLr) Ermittlung



Funktionale Sicherheit - EN ISO 13849

Bedeutung des Performance Levels (PL)



PL	Maximal tolerierter Ausfallgrad PFHd
a	Ein gefährlicher Ausfall pro 10.000 Stunden
b	Ein gefährlicher Ausfall pro 100.000 Stunden
c	Ein gefährlicher Ausfall pro 300.000 Stunden
d	Ein gefährlicher Ausfall pro 1000.000 Stunden
e	Ein gefährlicher Ausfall pro 10.000.000 Stunden

Quelle: DGUV, Seite 6
DIN EN ISO 13849-1, Anhang A: Risikograf

Funktionale Sicherheit - EN ISO 13849

Ermittlung des PLr aus den Parametern S, F und P

- **Schwere** der Verletzung, S1 und S2

S1	leichte (üblicherweise reversible) Verletzung, z.B. Quetschungen, Fleischwunden
S2	Ernste (üblicherweise irreversible) Verletzung, z.B. Amputation, Tod

Funktionale Sicherheit - EN ISO 13849

Ermittlung des PLr aus den Parametern S, F und P

- **Häufigkeit** und /oder **Expositionsdauer** der Gefährdung, F1 und F2

	Verhältnis der Expositionsdauer zur **gesamten** Betriebsdauer	
	< 1/20	**> 1/20**
Häufigkeit > 1x/15min	**F2**	**F2**
Häufigkeit < 1x/15min	**F1**	**F2**

EN ISO 13849-1:2006/FprA1:2015 (D)
F1 darf gewählt werden, wenn die **gesamte** Expositionsdauer 1/20 der **gesamten** Betriebsdauer nicht überschreitet **und** die Häufigkeit nicht höher als einmal alle 15 Minuten ist.

Funktionale Sicherheit - EN ISO 13849

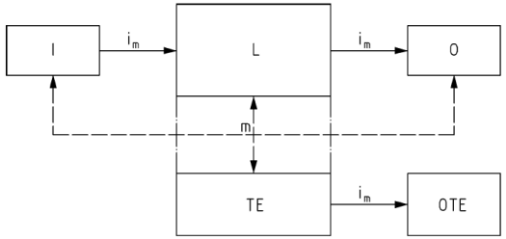
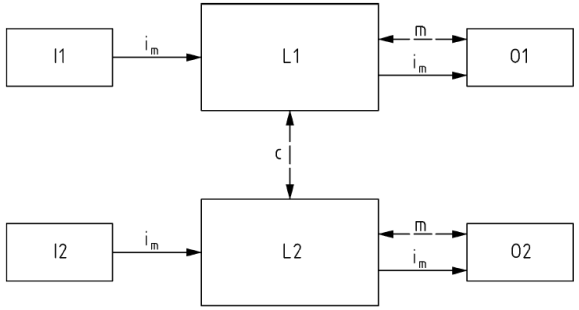
Ermittlung des PLr aus den Parametern S, F und P

- **Möglichkeiten** zur **Vermeidung** der Gefährdung, P1 und P2

P1	Möglich unter bestimmten Bedingungen, d.h. es besteht eine reelle Chance den Unfall zu vermeiden oder der Gefährdung auszuweichen.
P2	Kaum möglich, d.h. es besteht nahezu keine Chance der Gefährdung auszuweichen.

Funktionale Sicherheit - EN ISO 13849

Architektur und Anforderungsübersicht

Kategorie	Schema	Bedingungen
B, 1		<u>B:</u> Verwendung von **grundlegenden Sicherheitsprinzipien** <u>1:</u> Verwendung **bewährter Bauteile** und **bewährter Sicherheitsprinzipien**
2		**MTTFD des Testkanals beträgt mindestens 10 Jahre** Verwendung **bewährter oder betriebsbewährter Bauteile**, Verwendung **bewährter Sicherheitsprinzipien**. Bei Kategorie 2 gilt dies nach der Norm auch für den Testkanal. ausreichende Maßnahmen gegen CCF und für jedes Bauteil **DC min. „niedrig“**
3		Verwendung **bewährter oder betriebsbewährter Bauteile**, Verwendung **bewährter** Sicherheitsprinzipien. Ausreichende Maßnahmen gegen CCF und für jedes Bauteil **DC min. „niedrig“.**
4		Verwendung **bewährter oder betriebsbewährter Bauteile**, Verwendung **bewährter** Sicherheitsprinzipien. ausreichende Maßnahmen gegen **CCF** und für jedes Bauteil **DC „hoch“**

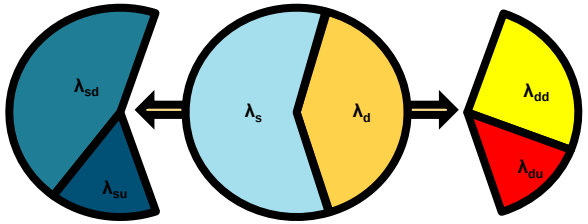
Funktionale Sicherheit - EN ISO 13849

DC - Diagnosedeckungsgrad

- **Bei mehrfacher Diagnose erfolgt eine Mittelung**:

$$DC_{avg} = \frac{\sum \lambda_{dd}}{\sum \lambda_{dd} + \sum \lambda_{du}}, \qquad DC_{avg} = \frac{\sum \frac{DC}{MTTF_d}}{\sum \frac{1}{MTTF_d}}$$

→ Ergebnis nach Bewertung:



Bewertung	Bereich des DC
ohne	DC < 60%
low	60% <= DC < 90%
medium	90% <= DC < 99%
high	99% <= DC

→ Fehlerausschlüsse gem. EN ISO 13849-2 beachten!
Müssen über ges. Einsatzzeit bestehen und sind zu dokumentieren!

Funktionale Sicherheit - EN ISO 13849

Fehler gemeinsamer Ursache – Common Cause Failure (CCF)

Quantifizierung von Fehlern gemeinsamer Ursache CCF

F.2 Abschätzung der Auswirkung des CCF

Dieser quantitative Prozess sollte für das gesamte System angewendet werden. Jedes Teil der sicherheitsbezogenen Teile der Steuerung sollte berücksichtigt werden.

Die Tabelle F.1 listet Maßnahmen und enthält zugehörige Werte, basierend auf einer ingenieurmäßigen Beurteilung, die den Beitrag jeder Maßnahme zur Reduzierung der Ausfälle infolge gemeinsamer Ursache repräsentieren.

Für jede der gelisteten Maßnahmen kann nur die volle Punktezahl oder nichts beansprucht werden. Wird eine Maßnahme nur teilweise erfüllt, ist die entsprechende Punktezahl null.

Tabelle F.1 — Verfahren zur Punktevergabe und Quantifizierung für Maßnahmen gegen CCF

Nr.	Maßnahme gegen CCF	Punkt-zahl
1	**Trennung/Abtrennung**	
	Physikalische Trennung zwischen den Signalpfaden, z. B.: — Trennung der Verdrahtung/Verrohrung; — Erkennen von Kurzschlüssen und Unterbrechungen in Kabeln durch dynamische Prüfung; — getrennte Abschirmung des Signalpfads jedes Kanals; — ausreichende Luft- und Kriechstrecken auf gedruckten Schaltungen.	15
2	**Diversität**	
	Unterschiedliche Technologien/Gestaltung oder physikalische Prinzipien werden verwendet, z. B.: — der erste Kanal elektronisch oder programmierbar elektronisch und der zweite Kanal elektromechanisch fest verdrahtet, — unterschiedliche Initiierung der Sicherheitsfunktion für jeden Kanal (z. B. Position, Druck, Temperatur), und/oder digitale und analoge Messung von Variablen (z. B. Abstand, Druck oder Temperatur) und/oder Bauteile von unterschiedlichen Herstellern.	20
3	**Gestaltung/Anwendung/Erfahrung**	
3.1	Schutz gegen Überspannung, Überdruck, Überstrom, Übertemperatur, usw.	15
3.2	Verwendung bewährter Bauteile.	5
4	**Beurteilung/Analyse**	
	Für jedes Teil von sicherheitsbezogenen Teilen eines Steuerungssystems wurde eine Ausfallarten- und Effekt-Analyse durchgeführt und deren Ergebnisse berücksichtigt, um Ausfälle infolge gemeinsamer Ursache bei der Gestaltung zu vermeiden.	5
5	**Kompetenz/Ausbildung**	
	Ausbildung der Konstrukteure, um die Gründe und Auswirkungen von Ausfällen infolge gemeinsamer Ursache zu verstehen.	5
6	**Umgebung**	
6.1	Für elektrische/elektronische Systeme, Verhindern von Verunreinigungen und elektromagnetischen Störungen (EMV) zum Schutz vor Ausfällen infolge gemeinsamer Ursache entsprechend den einschlägigen Normen (z. B. IEC 61326-3-1) Fluidische Systeme: Filtrierung des Druckmediums, Verhinderung von Schmutzeintrag, Entwässerung von Druckluft, z. B. in Übereinstimmung mit den Anforderungen des Herstellers für die Reinheit des Druckmediums ANMERKUNG Bei kombinierten fluidischen und elektrischen Systemen sollten beide Aspekte berücksichtigt werden.	25
6.2	Andere Einflüsse: Berücksichtigung der Anforderungen hinsichtlich Unempfindlichkeit gegenüber allen relevanten Umgebungsbedingungen wie Temperatur, Schock, Vibration, Feuchte (z. B. wie in den zutreffenden Normen festgelegt).	10
	Gesamt	**[max. erreich-bar 100]**

Gesamtpunktzahl	Maßnahmen, um CCF[a] zu vermeiden
65 oder besser	Anforderungen erreicht
Kleiner als 65	Verfahren gescheitert ⇒ Auswahl zusätzlicher Maßnahmen

[a] Wenn technische Maßnahmen nicht relevant sind, können die Punkte der rechten Spalte bei der ausführlichen Berechnung berücksichtigt werden.

03

- Verifikation des Performance Levels

Verifikation des Performance Levels

Risikominderung mit funktionaler Sicherheit

Erfassen (Eingang) → **Verarbeiten (Logik)** → **Ausführen (Ausgang)**

Einfehlersicherheit
Redundanz
Diversität
Selbstüberwachung
Funktionsprüfung
Überdimensionierung

Schütze
Ventile
Antriebe

Risikoeinschätzung
Risikobewertung

→

EN ISO 13849-1 (PL)
DIN EN IEC 62061 (SIL)

Verifikation des Performance Levels

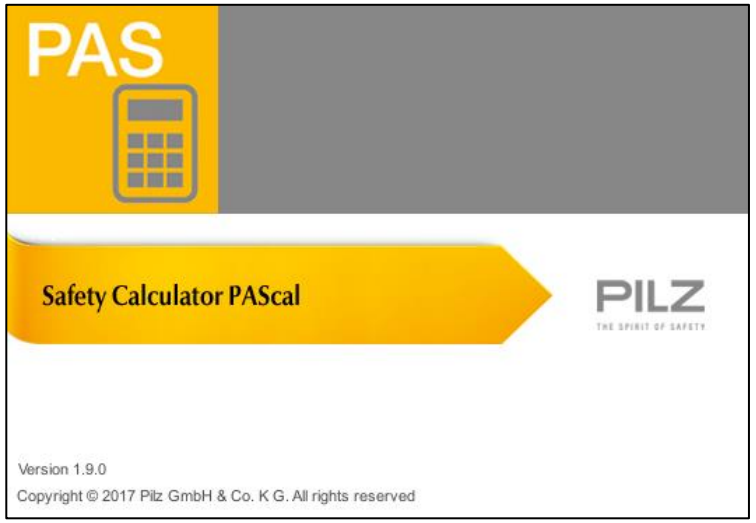
Safety Calculator PAScal

Definition Verifikation:

- Die Verifikation ist die rechnerische Beweisführung, dass die Sicherheitsfunktion den normativen Anforderungen nach DIN EN ISO 13849-1 bzw. EN 62061 entspricht.

- Auf Basis der Kenndaten aller eingesetzten Bauteile wird deren Ausfallwahrscheinlichkeit berechnet, wodurch eine Zuordnung in den Performance Level erfolgt.

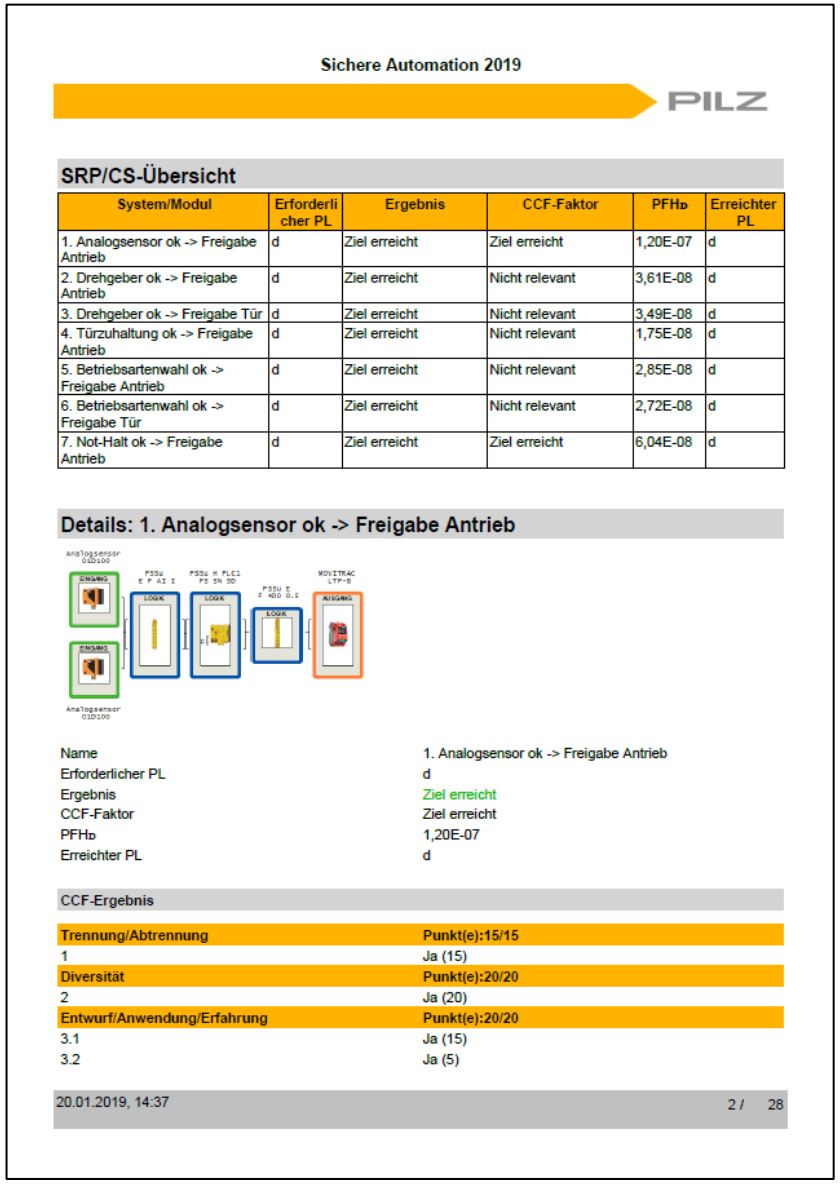
- **Praktisches Hilfsmittel → Safety Calculator PAScal**



Verifikation des Performance Levels

Safety Calculator PAScal

- Sicherheitsfunktionen einfach berechnen und verifizieren
- für Performance Level (EN 13849) und SIL (EN 62061)
- nutzerfreundliche, grafische und mehrsprachige Oberfläche
- Artikelverwaltung in VDMA-Bibliotheken
- automatische Generierung und Ausgabe des Ergebnisberichts im PDF-Format
- Unterstützung durch den Pilz TechSupport (Hotline)
- Tutorialvideo unter http://www.youtube.com/watch?v=xLH_G8XoVjE
- kostenfreier Download der Demo unter https://www.pilz.com/download/restricted/PAScal_1_9_1_3000679A21.zip



Sichere Automation 2019

PILZ

SRP/CS-Übersicht

System/Modul	Erforderlicher PL	Ergebnis	CCF-Faktor	PFHD	Erreichter PL
1. Analogsensor ok -> Freigabe Antrieb	d	Ziel erreicht	Ziel erreicht	1,20E-07	d
2. Drehgeber ok -> Freigabe Antrieb	d	Ziel erreicht	Nicht relevant	3,61E-08	d
3. Drehgeber ok -> Freigabe Tür	d	Ziel erreicht	Nicht relevant	3,49E-08	d
4. Türzuhaltung ok -> Freigabe Antrieb	d	Ziel erreicht	Nicht relevant	1,75E-08	d
5. Betriebsartenwahl ok -> Freigabe Antrieb	d	Ziel erreicht	Nicht relevant	2,85E-08	d
6. Betriebsartenwahl ok -> Freigabe Tür	d	Ziel erreicht	Nicht relevant	2,72E-08	d
7. Not-Halt ok -> Freigabe Antrieb	d	Ziel erreicht	Ziel erreicht	6,04E-08	d

Details: 1. Analogsensor ok -> Freigabe Antrieb

Name	1. Analogsensor ok -> Freigabe Antrieb
Erforderlicher PL	d
Ergebnis	Ziel erreicht
CCF-Faktor	Ziel erreicht
PFHD	1,20E-07
Erreichter PL	d

CCF-Ergebnis

Trennung/Abtrennung	Punkt(e):15/15
1	Ja (15)
Diversität	Punkt(e):20/20
2	Ja (20)
Entwurf/Anwendung/Erfahrung	Punkt(e):20/20
3.1	Ja (15)
3.2	Ja (5)

20.01.2019, 14:37 2 / 28

Verifikation des Performance Levels

Herstellerliste Kennwert-Bibliotheken zum Einheitsblatt VDMA 66413

Kennwert-Bibliotheken im Format VDMA 66413

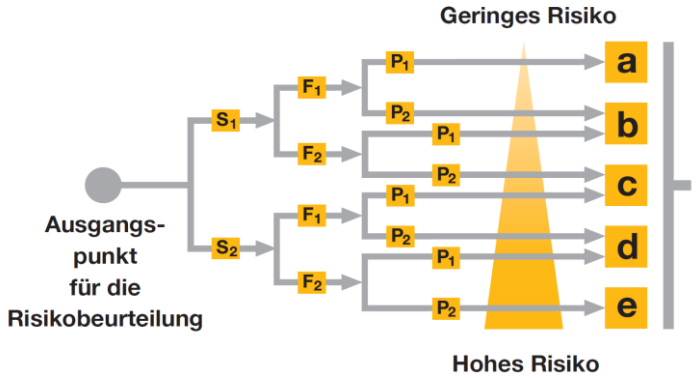
Herstellerliste Kennwert-Bibliotheken zum Einheitsblatt VDMA 66413 "Funktionale Sicherheit - Universelle Datenbasis"

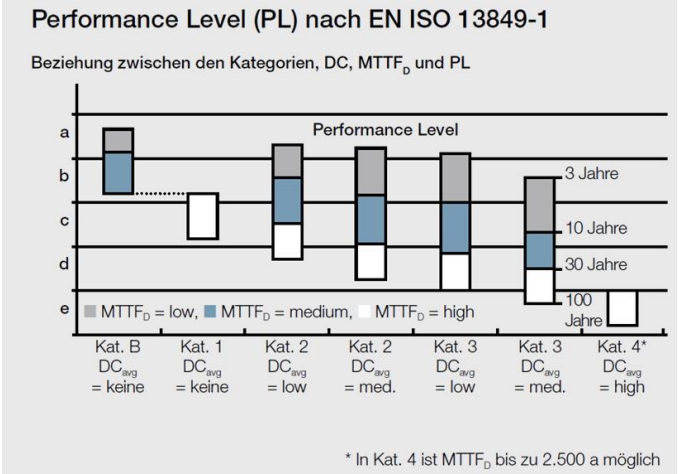
Kennwert-Bibliotheken	Einheitsblatt
ABB Automation Products GmbH ABB STOTZ-KONTAKT GmbH ABB Jokab Safety AB »Software	VDMA 66413:2012-10
Bihl+Wiedemann GmbH »Kennwert-Bibliotheken	VDMA 66413:2012-10
Bosch Rexroth AG NEU	VDMA 66413:2012-10
Eaton Industries GmbH »Software »Download Bibliothek für VDMA 66413	VDMA 66413:2012-10
Eckelmann AG	VDMA 66413:2012-10
elobau GmbH & Co. KG	VDMA 66413:2012-10
ENGEL Elektroantriebe GmbH NEU	VDMA 66413:2012-10
Pilz GmbH & Co. KG	VDMA 66413:2012-10

Quelle: https://www.vdma.org/v2viewer/-/v2article/render/15201678

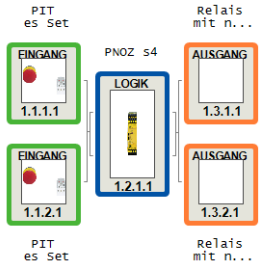
Funktionale Sicherheit - Zusammenfassung

Evaluierung





Verifikation (z.B. mit PAScal)

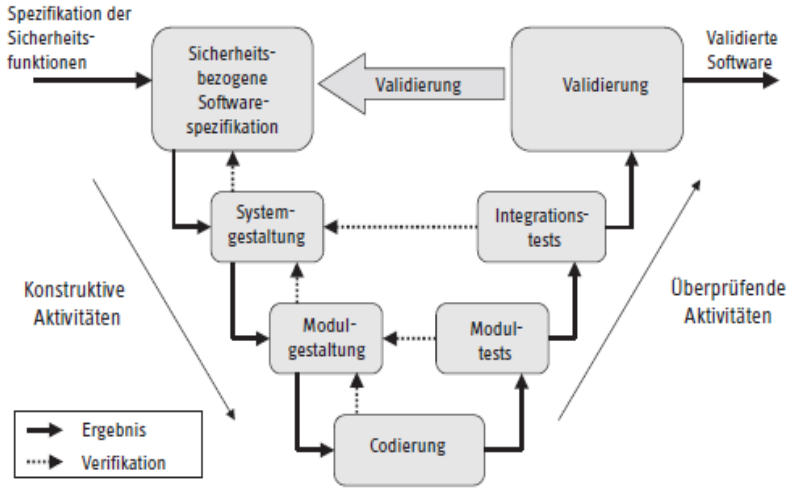


SRP/CS-Editor | CCF-Editor

Berechnungsgraph

Teilsystem/Kanal	Anteil am PL	PL	PFHD	Cat.	DCa...	MTTFD: be...	MTTFD: ...
Schulungsbeispiel 1: SF1.1		d	2,04E-07				
Not Halt: Eingang		d	1,01E-07	3	60,00%	100,00Jahre	100,00Ja...
1.1.1.1 - PIT es Set							
1.1.2.1 - PIT es Set							
1.2.1.1 - PNOZ s4		e	2,31E-09	4			
Relais: Ausgang		d	1,01E-07	3	60,00%	100,00Jahre	100,00Ja...
1.3.1.1 - Relais mit nominaler Last							
1.3.2.1 - Relais mit nominaler Last							

Validierung



Noch Fragen?

Schreiben Sie Ihre Fragen einfach an
automationontour@pilz.de