STARKES STUDIUM.
PRIMA ZUKUNFT.

HOCHSCHULE HEILBRONN

TECHNIK WIRTSCHAFT INFORMATIK

Sicherheitstechnik, 3. Vorlesung (Safety Technology)

Campus Heilbronn

Campus Künzelsau
Reinhold-Würth-Hochschule

Campus Schwäbisch Hall

Fred Härtelt, Heilbronn

Beispiel (2012): Zulassung des ICE 3 (Velaro-D)

- Problematik: Verzögerung des Bremsvorgangs um bis zu 1,6 Sekunden durch das Zusammenkoppeln zweier Züge

Eisenbahn-Bundesamt

Neue ICE-Modelle: Eine Sekunde bis zum Stopp

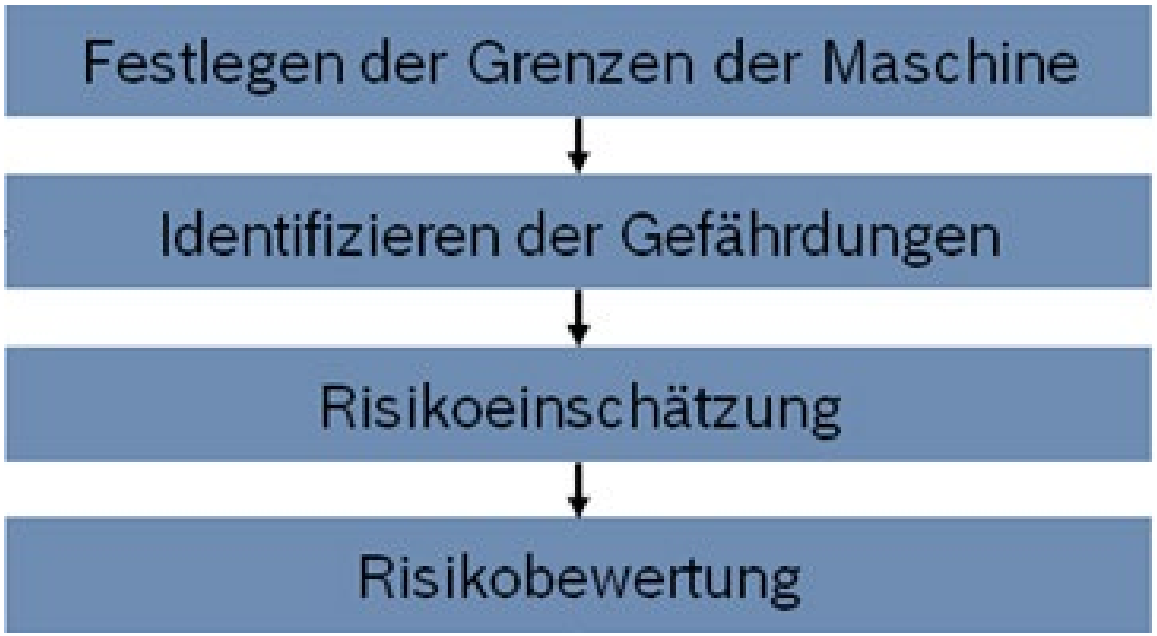
Ein digitales Detail stellt die Deutsche Bahn und den Siemens-Konzern vor große Probleme: Das Kommando zum Anhalten eines ICE-3-Zugs irrt etwa eine Sekunde lang durch den Rechner, bis es ausgeführt wird. Nach SPIEGEL-Informationen verweigerte das Eisenbahn-Bundesamt deshalb die Zulassung.

Quellen: www.spiegel.de, www.zeit.de , http://www.eba.bund.de

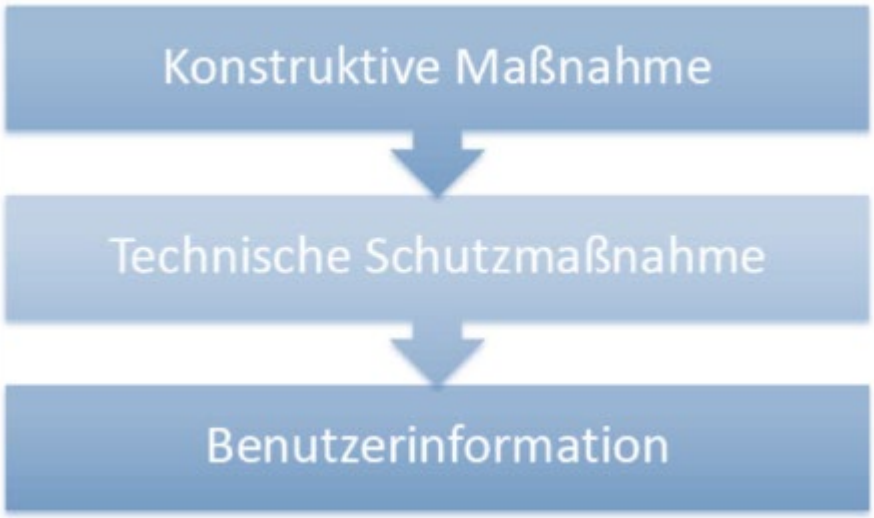
Sicherheitstechnik: zeitlicher Überblick

- 1. V: Definition Sicherheit, Normen und Vorschriften (14.03.2022)
- 2. V: Festlegung von Grenzen und Gefährdungen (21.03.2022)
- **3. V: Risikobeurteilung, -minimierung, Risikograph (28.03.2022)**
- 4. V: Verteilungsfunktion, Ausfallraten, Fehlerbeherrschung (04.04.2022)
- 5. V: Fehlervermeidung, Fehlerentdeckung, FMEA (11.04.2022)
- Keine Vorlesung am 18.04.2022 (Ostermontag)
- Keine Vorlesung am 25.04.2022
- 6. V: Redundanz, Strukturierungsmaßnahmen, FTA (02.05.2022)
- 7. V: Berechnung von Ausfallraten, FMEDA, Aufgabenstellung Belegarbeit, **Einteilung der Gruppen** (09.05.2022)
- 8. V: Prozess vs. Technik, Besonderheiten HW/SW, Zuverlässigkeit SW Entwicklungsprozess, Bsp. Belegarbeit, **Beginn der Gruppenarbeit** (16.05.2022)
- Rückfragen bezüglich Gruppenarbeit am 23.05., 30.05. und 13.06.2022 (WebEx)
- Abgabetermin der Gruppenarbeiten: **20.06.2022** (vor Beginn der Präsentationen)
- Präsentationstermine der Gruppen: **20.06.2022** (vorläufiger Stand)

Sicherheitstechnik: Wiederholung



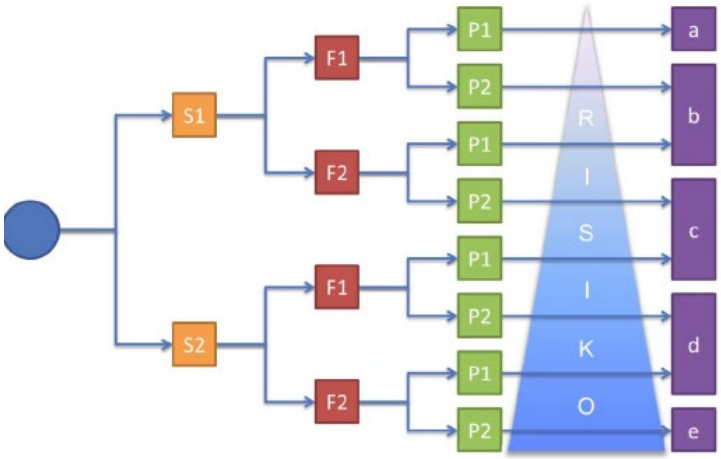
Sicherheitstechnik: Wiederholung



Sicherheitstechnik: Wiederholung

- Berechnung des Performance Level (PL) mit einem Risikograph

S	**Schwere der Verletzung**
S1 – leicht (üblicherweise reversible Verletzung)	S2 – ernst (üblicherweise irreversible Verletzungen einschließlich Tod)
F	**Häufigkeit und Dauer der Gefahrdungsexposition**
F1 – selten bis weniger häufig und/oder die Dauer der Gefahrdungsexposition ist kurz (nicht häufiger als 2-Mal am Tag und insgesamt nicht langer als 15 min.)	F2 – häufig bis dauernd und/oder die Dauer der Gefahrdungsexposition ist lang
P	**Vermeidung der Gefährdung**
P1 – möglich unter bestimmten Bedingungen	P2 – kaum möglich

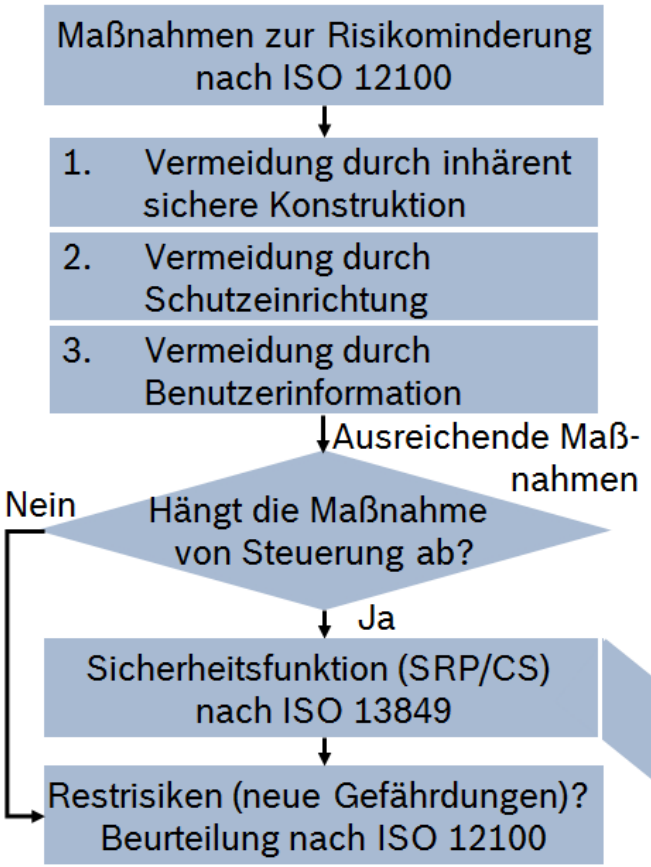


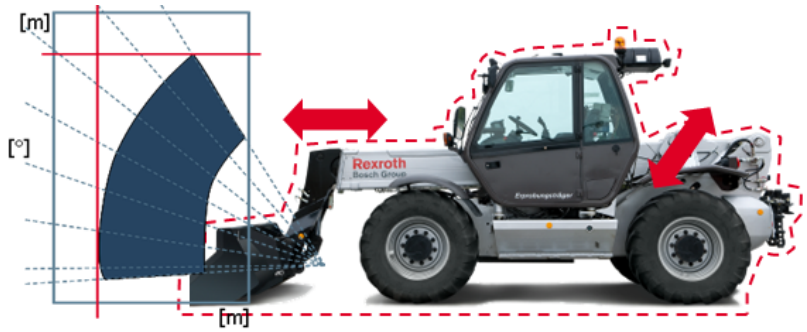
Beispiel

1. Risikobeurteilung und –minderung
2. Identifikation der Sicherheitsfunktionen
3. **Bestimmen des PL_r**
4. Auswahl der Systemarchitektur
5. Modellieren des Systems als Blockdiagramm
6. Fehler und Diagnose
7. Bestimmen des PL
8. Bewerten der Robustheit der Steuerung - Fehlervermeidung
9. Software-Anforderungen
10. Verifizieren und Validieren

Quelle: Nach [4]

Beispiel



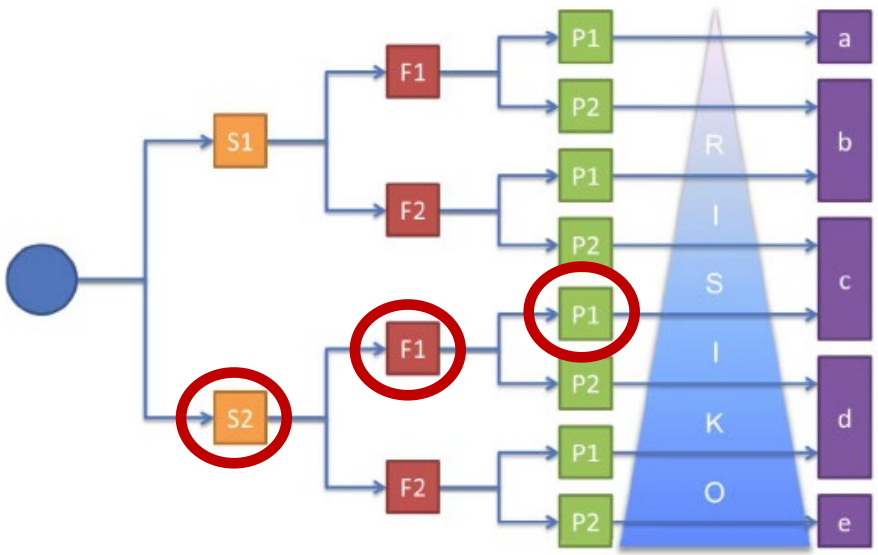


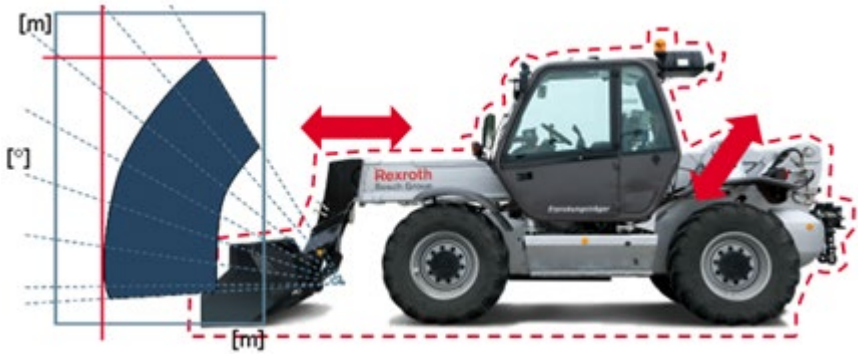
Procedure	Machine	Joystick	Controller	Valve
Identify the hazard	Unexpected telescopic movement	-	-	-
Define the trigger event	User commands stop	Joystick in neutral position	-	-
Define the safe state	Telescopic movement stopped	-	-	Valve in neutral position
Specify the reaction	Stop movement	Send stop signal to controller	Process stop signal, shut off valve	Stop oil flow
Safety (related) function	**Prevent unexpected start-up of the telescopic movement**	Provide neutral position to controller	Process stop signal	Shut off oil flow
	Safety function	Safety related function		

Quelle: Nach [4]

Beispiel

Prevent unexpected start-up of the telescopic movement





Measure	SIL	PL_r
e.g. safety function (SF)	3	e
e.g. safety function (SF)	2	d
e.g. safety function (SF)	1	c
Other measure or SF	-	b
Other measure or SF	-	a

Quelle: Nach [4]

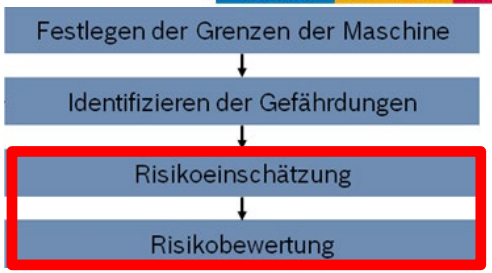
Beispiel

Risk index R = S * K			Class K = F + W + P									
			3	4	5	7	8	10	11	13	14	15
S	Death or permanent injury	4	12	16	20	28	32	40	44	52	56	60
	Permanent injury	3	9	12	15	21	24	30	33	39	42	45
	Reversibel injury	2	6	8	10	14	16	20	22	26	28	30
	Reversibel injury	1	3	4	5	7	8	10	11	13	14	15

Risk evaluation according to severity S and class K	Measure	SIL	PL_r
	e.g. safety function (SF)	3	e
	e.g. safety function (SF)	2	d
	e.g. safety function (SF)	1	c
	Other measure or SF	-	b
	Other measure or SF	-	a

Quelle: Nach [4]

Sicherheitstechnik: Übung 3



Schadensausmaß (severity)

S1 leichte Verletzungen (reversibel)

S2 schwere Verletzungen (irreversibel)

Möglichkeit zum Erkennen und Ausweichen der Gefahr (avoidance)

A1 möglich unter bestimmten Umständen

A2 kaum möglich

Aufenthaltsdauer im Gefahrenbereich (frequency)

F1 selten bis öfter

F2 häufig bis dauernd

Wahrscheinlichkeit des Eintretens des Ereignisses (occurrence probability)

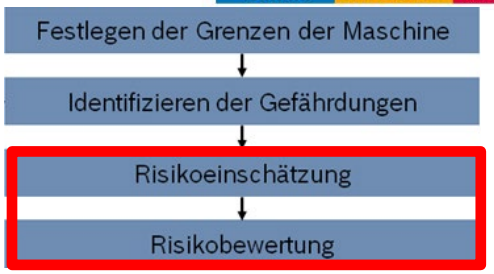
O1 klein (unwahrscheinlich)

O2 mittel (wird wahrscheinlich einige Male eintreten)

O3 groß (wird häufig eintreten)

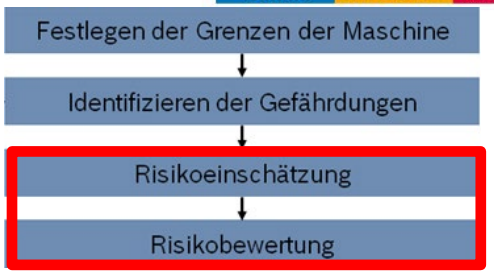
		Risk index calculation					
		O1		O2		O3	
		A1	A2	A1	A2	A1	A2
S1	F1	1				2	
	F2						
S2	F1	2			3		4
	F2	3	4		5		6

Sicherheitstechnik: Lösung Übung 3



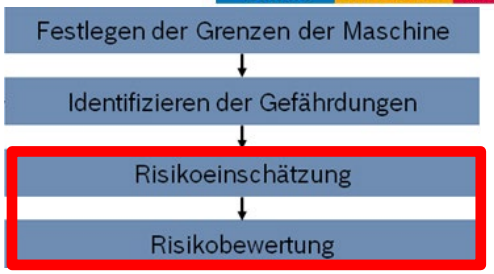
	Lebens-phasen	Gefährdung	Risiko-einschätzung 1	Maßnahmen zur Risikominderung	Risiko-einschätzung 2
1	Transport	Gefährdungen durch unsachgemäßen Transport der Maschine	S = S2, F = F1, O = O1, A = A1, **RI = 2**	1. Gesamtgewicht in der Betriebsanleitung angeben. 2. Korrekte Transportmöglichkeiten in der Betriebsanleitung beschreiben.	S = S1, F = F1, O = O1, A = A1, **RI = 1**

Sicherheitstechnik: Lösung Übung 3



2	Betrieb	Herunterfallen von Holzstücken auf die Beine/Füße der Bedienperson, wenn diese gespalten werden.	S = S2, F = F1, O = O3, A = A1, **RI = 3**	Halteeinrichtung für das Holzstück anbauen. Halteeinrichtung so gestalten, dass das Holzstück vor - während oder nach dem Spalten nicht auf die Füße der Bedienperson fällt, wenn diese in Arbeitsposition ist.	S = S1, F = F1, O = O1, A = A1, **RI = 1**

Sicherheitstechnik: Lösung Übung 3



3	Betrieb	Verletzungen der Hände bei unsachgemäßer Handhabung der Maschine, wenn sich Holzklötze verklemmt haben.	S = S2, F = F1, O = O2, A = A1, **RI = 2**	1. Hinweis in der Betriebsanleitung, wie bei verklemmten Holzklötzen vorzugehen ist. 2. Hinweis in der Betriebsanleitung, dass der Arbeitsbereich frei von Holzresten und Hindernissen gehalten	S = S1, F = F1, O = O1, A = A1, **RI = 1**

Sicherheitstechnik: Lösung Übung 3

4	Betrieb	Schneiden bzw. Abschneiden von Händen oder Fingern am Spaltkeil beim Auflegen oder Halten von Spaltmaterial und gleichzeitigem Auslösen des Spaltvorgangs.	S = S2, F = F1, O = O3, A = A1, **RI = 3**	1. Zweihandschaltung einbauen. Das Auslösen des Spaltvorgangs darf nur unter Verwendung beider Hände erfolgen können. Zweihandschaltung nach EN 574 gestalten. Die Zwei-handsteuerung muss mindestens Kategorie 1 (DIN EN 954-1) erfüllen. (Forderung aus DIN EN 609-1). 2. Sicherheitshinweise auf der Spaltmaschine: „Vorsicht! Bewegte Maschinenteile!“, „Nur für Betrieb durch 1 Person!“ 3. Hinweis in der Betriebsanleitung: „Warnung! Die Schutzeinrichtung der Spaltmaschine ist nur dann wirksam, wenn die Bedienung durch eine einzelne Person erfolgt. Bedienung niemals durch mehrere Personen!“ 4. Hinweis in der Betriebsanleitung, dass die Schutzeinrichtung regelmäßig auf korrekte Funktion geprüft werden muss.	S = S1, F = F1, O = O1, A = A1, **RI = 1**

Sicherheitstechnik: PL bestimmen

Angewandtes Diagramm nach DIN EN ISO13849-1 zur Bestimmung des erforderlichen Performance-Level (PL):

Schwere der Verletzung (severity)

S1: leichte Verletzung

S2: Tod oder schwere Verletzung

Häufigkeit und Aufenthaltsdauer (frequency)

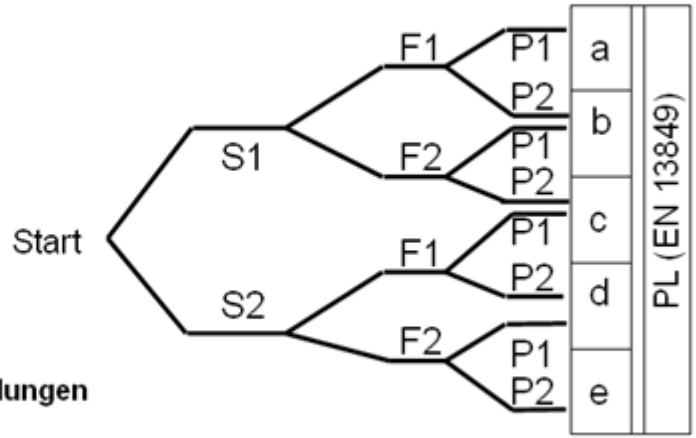
F1: selten bis öfter

F2: häufig bis dauernd

Möglichkeit zur Vermeidung von Gefährdungen (possibility of avoidance)

P1: möglich unter bestimmten Bedingungen

P2: kaum möglich



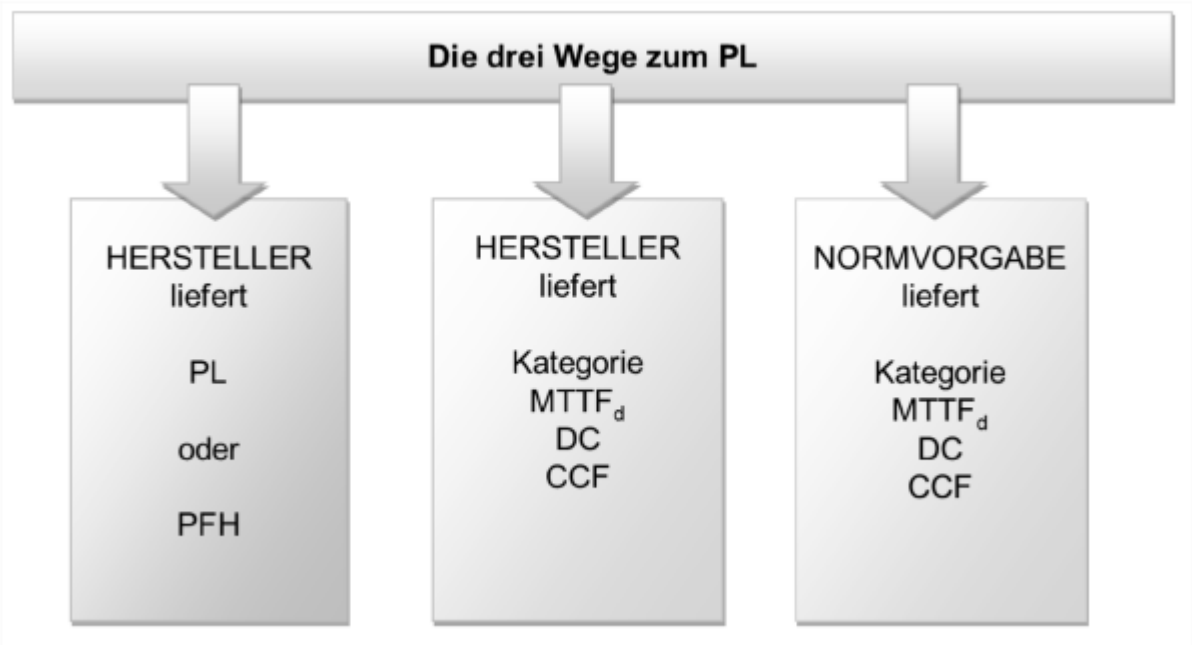
PL: Performance-Level

Gestalten der Sicherheitsfunktionen

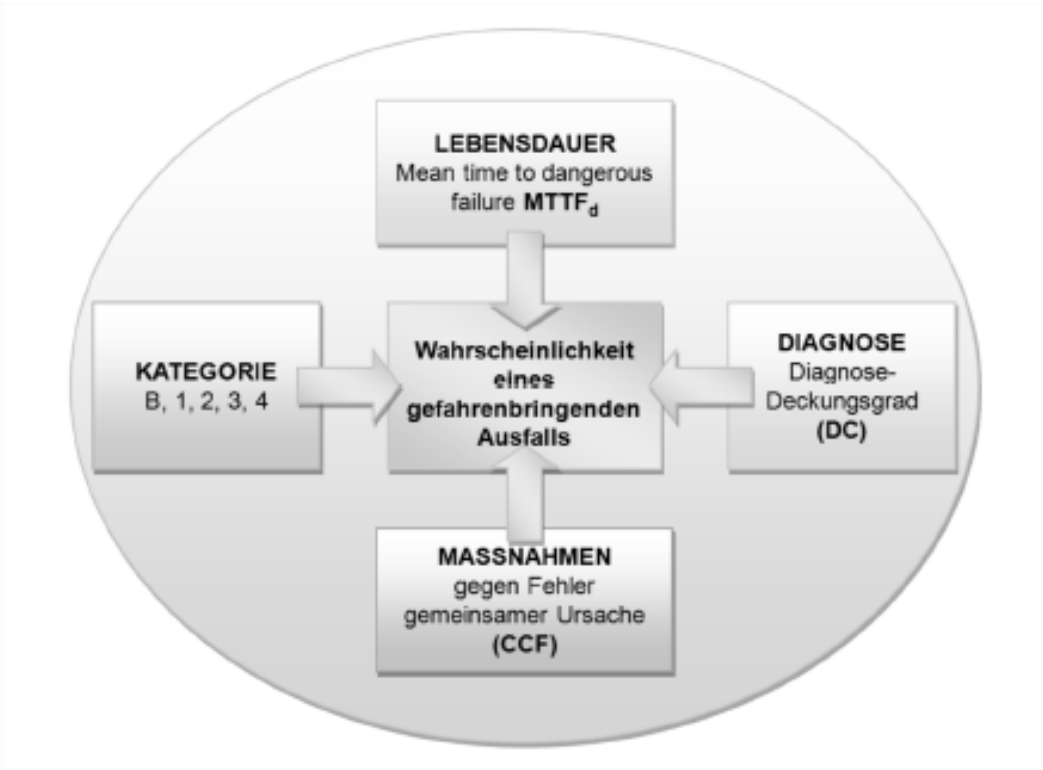
- E • Eingabe - Sensoren
- V • Verarbeitung - Auswerteeinheit
- A • Ausgabe - Aktoren

Gestaltung der Sicherheitsfunktionen
Identifizierung der sicherheitsbezogenen Teile

Ermittlung PL der sicherheitsbezogenen Teile



Ermittlung PL: Einflussfaktoren

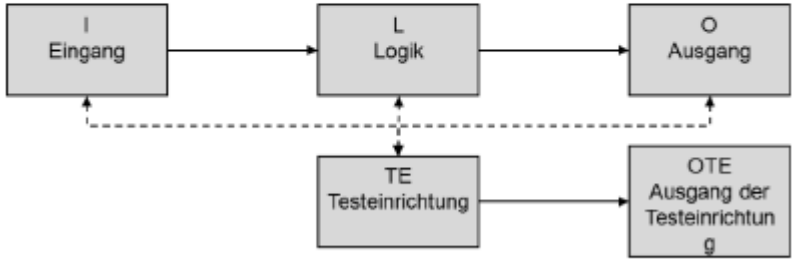


Ermittlung PL: Kategorien

Merkmal	Kategorie				
	B	1	2	3	4
Gestaltung gemäß zutreffender Normen, zu erwartenden Einflüssen standhalten	X	X	X	X	X
Grundlegende Sicherheitsprinzipien	X	X	X	X	X
Bewährte Sicherheitsprinzipien		X	X	X	X
Bewährte Bauteile		X			
Mean Time to Dangerous Failure - $MTTF_d$	niedrig bis mittel	hoch	niedrig bis hoch	niedrig bis hoch	hoch
Fehlererkennung (Tests)			X	X	X
Einfehlersicherheit				X	X
Berücksichtigung von Fehlerakkumulation					X
Diagnosedeckungsgrad - DC_{avg}	kein	kein	niedrig bis mittel	niedrig bis mittel	hoch
Maßnahmen gegen Fehler gemeinsamer Ursache (CCF)			(X) bedingt	X	X
Hauptsächlich charakterisiert durch	Bauteilauswahl		Struktur		

Kategorie B und Kategorie 1

Kategorie 2



Eigenschaften der Kategorien

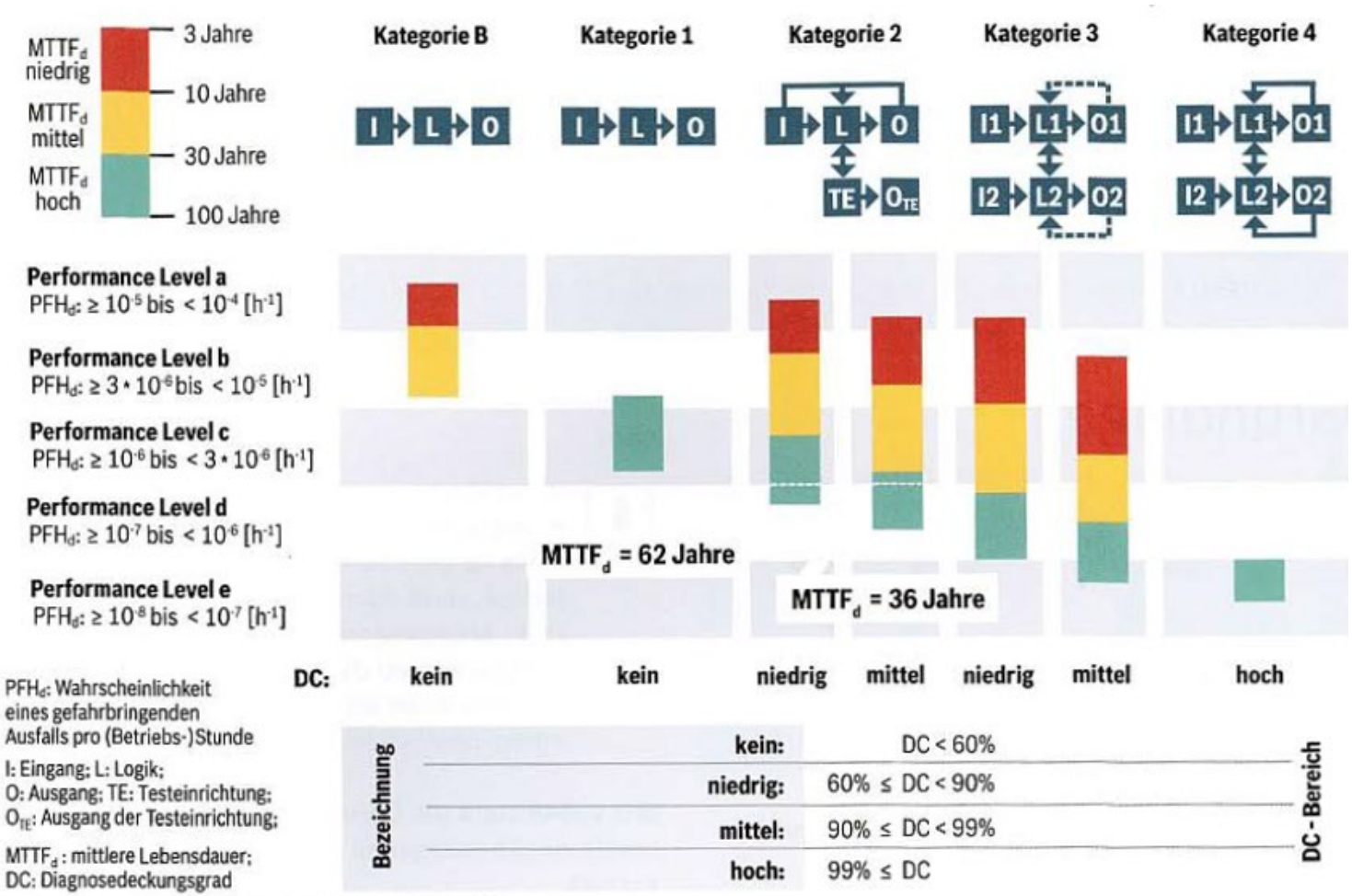


Abb. B-4.1: Beziehung zwischen Kategorien und PL

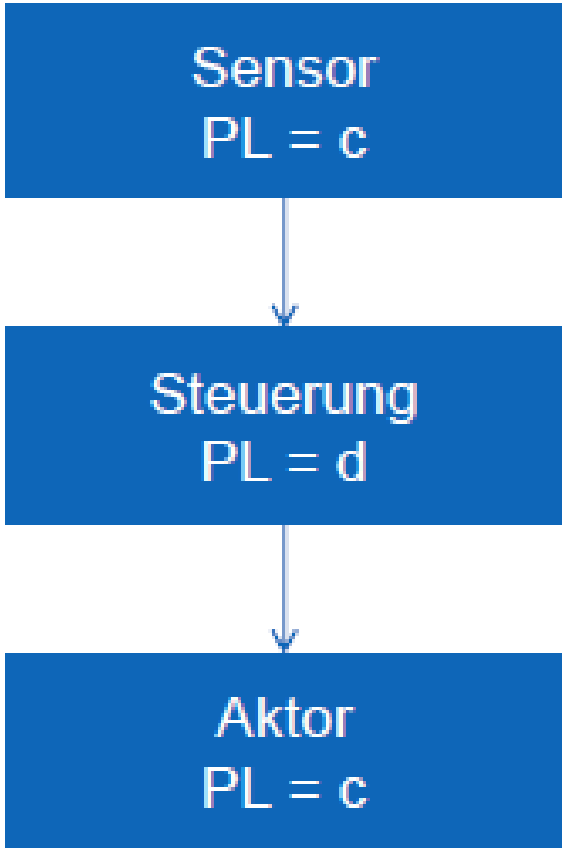
Ermittlung PL bei mehreren Bauteilen

- Zunächst Bestimmung des niedrigsten PL
- Bestimmung der Bauteile mit dem niedrigsten PL (n)
- Nachschlagen des Gesamt-PL

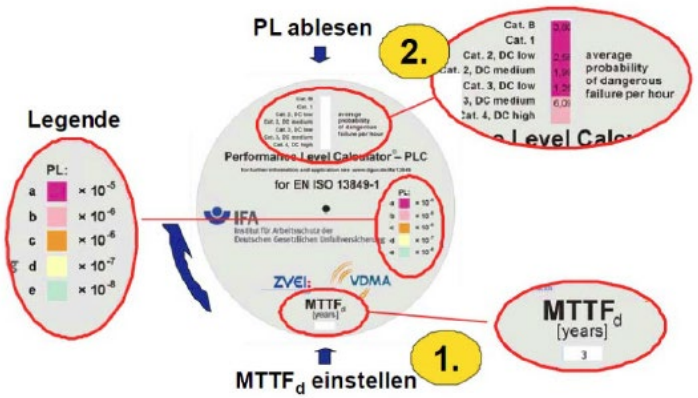
$PL_{niedrig}$	$N_{niedrig}$	PL
a	> 3	kein, nicht erlaubt
	≤ 3	a
b	> 2	a
	≤ 2	b
c	> 2	b
	≤ 2	c
d	> 3	c
	≤ 3	d
e	> 3	d
	≤ 3	e

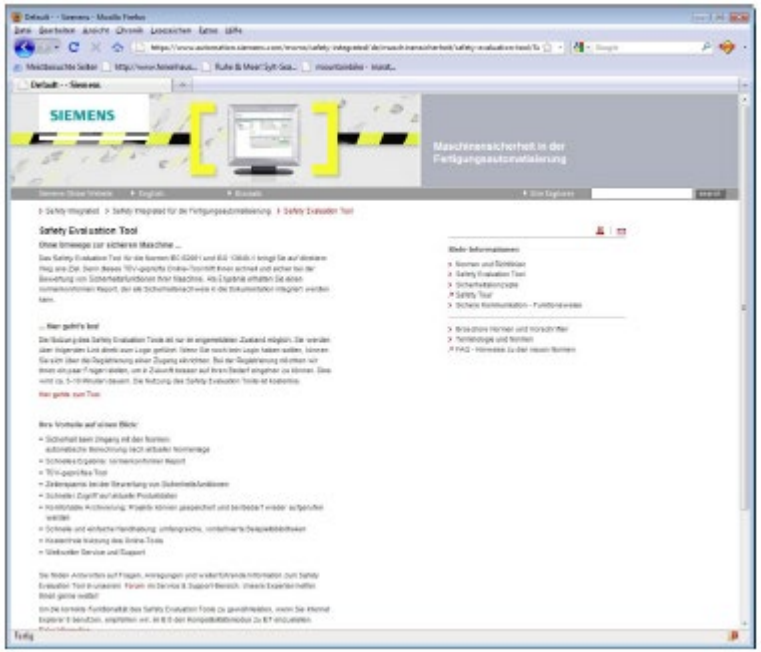
Ermittlung PL: Beispiel

- PL (niedrig) = c
- N (niedrig) = 2
- Tabelle anwenden
- **PL (gesamt) = c**



Ermittlung PL: Hilfsmittel





z.B. Performance Level Calculator,
Sistema, Siemens Safety Evaluation Tool

Sicherheitstechnik: Beispiel Erreichung PL

MTTFd	
Bezeichnung für jeden Kanal	Bereich für jeden Kanal
niedrig	3 Jahre ≤ $MTTF_d$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_d$ < 30 Jahre
hoch	30 Jahre ≤ $MTTF_d$ ≤ 100 Jahre

ANMERKUNG 1 Die Wahl der $MTTF_d$-Bereiche eines Kanals basiert nach dem in der Praxis vorgefundenen Stand der Technik auf einer logarithmischen Skala, die sich der logarithmischen Skala des PL anpasst. Es wird nicht angenommen, dass ein $MTTF_d$-Wert eines Kanals für ein reales SRP/CS kleiner als drei Jahre gefunden werden kann, denn das würde bedeuten, dass nach einem Jahr etwa 30 % aller Systeme auf dem Markt defekt sind und ersetzt werden müssten. Ein $MTTF_d$-Wert eines Kanals größer als 100 Jahre wird nicht akzeptiert, denn ein SRP/CS für hohe Risiken sollte nicht von der Zuverlässigkeit von Bauteilen alleine abhängig sein. Um ein SRP/CS gegen systematische und zufällige Fehler zu ertüchtigen, sind zusätzliche Mittel wie Redundanzen und Tests erforderlich. Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf drei beschränkt. Die Beschränkung des $MTTF_d$-Wertes jedes Kanals auf ein Maximum von 100 Jahren bezieht sich auf den einzelnen Kanal des SRP/CS, der die Sicherheitsfunktion ausführt. Höhere $MTTF_d$-Werte können für einzelne Bauteile verwendet werden (siehe Tabelle D.1).

ANMERKUNG 2 Für die gezeigten Grenzwerte der Tabelle 5 wird eine Genauigkeit von 5 % angenommen.

	Grundlegende und bewährte Sicherheitsprinzipien nach ISO 13849-2:2003	Andere relevante Normen	Typische Werte: $MTTF_d$ (Jahre) B_{10d} (Zyklus)
Mechanische Bauteile	Tabellen A.1 und A.2	—	$MTTF_d$ = 150
Hydraulische Bauteile	Tabellen C.1 und C.2	EN 982	$MTTF_d$ = 150
Pneumatische Bauteile	Tabellen B.1 und B.2	EN 983	B_{10d} = 20 000 000
Relais und Hilfsschütze mit geringer Last (mechanische Belastung)	Tabellen D.1 und D.2	EN 50205 IEC 61810 IEC 60947	B_{10d} = 20 000 000
Relais und Hilfsschütze mit maximaler Belastung	Tabellen D.1 und D.2	EN 50205 IEC 61810 IEC 60947	B_{10d} = 400 000
Näherungsschalter mit geringer Last (mechanische Belastung)	Tabellen D.1 und D.2	IEC 60947 EN 1088	B_{10d} = 20 000 000
Näherungsschalter mit maximaler Belastung	Tabellen D.1 und D.2	IEC 60947 EN 1088	B_{10d} = 400 000
Schütze mit geringer Last (mechanische Belastung)	Tabellen D.1 und D.2	IEC 60947	B_{10d} = 20 000 000
Schütze mit nominaler Last	Tabellen D.1 und D.2	IEC 60947	B_{10d} = 2 000 000

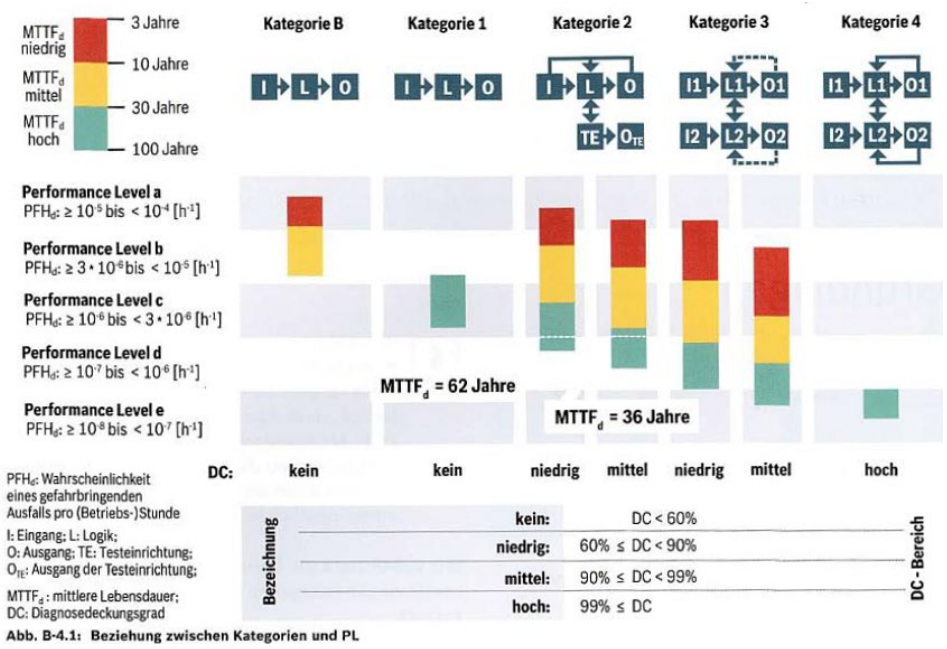


Abb. B-4.1: Beziehung zwischen Kategorien und PL

$PL_{niedrig}$	$N_{niedrig}$	⇒	PL
a	> 3	⇒	kein, nicht erlaubt
	≤ 3	⇒	a
b	> 2	⇒	a
	≤ 2	⇒	b
c	> 2	⇒	b
	≤ 2	⇒	c
d	> 3	⇒	c
	≤ 3	⇒	d
e	> 3	⇒	d
	≤ 3	⇒	e

Sicherheitstechnik: Beispiel Erreichung PL

Gefährdung	Risiko-einschätzung 1	Maßnahmen zur Risikominderung	Risiko-einschätzung 2	Definierter Performance Level	Erreichter Performance Level
Schneiden bzw. Abschneiden von Händen oder Fingern am Spaltkeil beim Auflegen oder Halten von Spaltmaterial und gleichzeitigem Auslösen des Spaltvorgangs.	S = S2, F = F1, O = O3, A = A1, **RI = 3**	1. Zweihandschaltung einbauen. Das Auslösen des Spaltvorgangs darf nur unter Verwendung beider Hände erfolgen können. Zweihandschaltung nach EN 574 gestalten. Die Zwei-handsteuerung muss mindestens Kategorie 1 (DIN EN 954-1) erfüllen. (Forderung aus DIN EN 609-1). 2. Sicherheitshinweise auf der Spaltmaschine: „Vorsicht! Bewegte Maschinenteile!“, „Nur für Betrieb durch 1 Person!“ 3. Hinweis in der Betriebsanleitung: „Warnung! Die Schutzeinrichtung der Spaltmaschine ist nur dann wirksam, wenn die Bedienung durch eine einzelne Person erfolgt. Bedienung niemals durch mehrere Personen!“ 4. Hinweis in der Betriebsanleitung, dass die Schutzeinrichtung regelmäßig auf korrekte Funktion geprüft werden muss.	S = S1, F = F1, O = O1, A = A1, **RI = 1**	S = S2, F = F1, P = P1, **PL = c**	Struktur der Steuerung: Mechanische Ansteuerung des Steuerventils der Zweihandschaltung. Steuerventil: Sicherheitstechnisch bewährtes Hydraulik-Wegeventil 1V3. Daten für das Ventil: MTTF = 150 J (= hoch) Kategorie = 1 PL = c **PL gesamt = c**

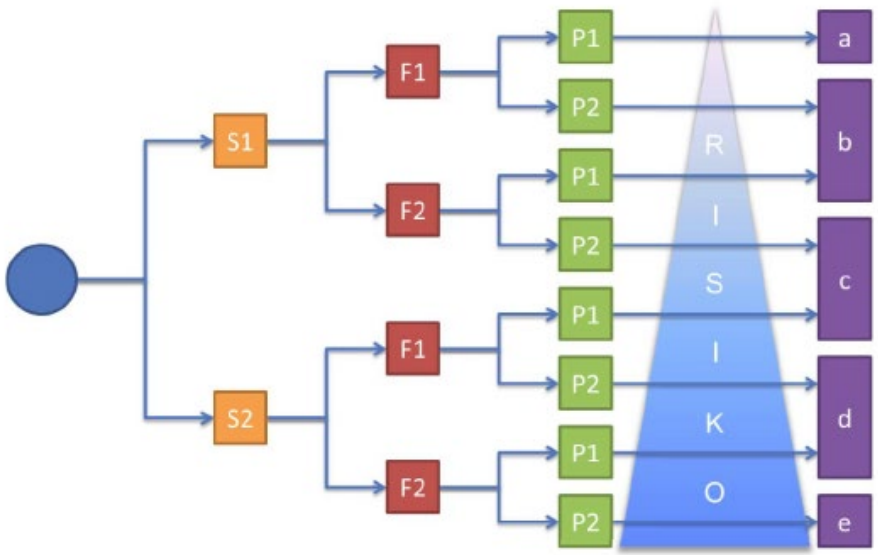
Beispiel

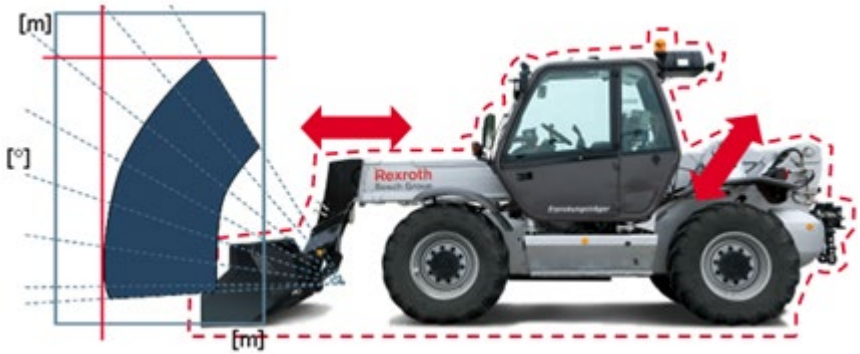
1. Risikobeurteilung und –minderung
2. Identifikation der Sicherheitsfunktionen
3. Bestimmen des PL_r
4. **Auswahl der Systemarchitektur**
5. Modellieren des Systems als Blockdiagramm
6. Fehler und Diagnose
7. Bestimmen des PL
8. Bewerten der Robustheit der Steuerung - Fehlervermeidung
9. Software-Anforderungen
10. Verifizieren und Validieren

Quelle: Nach [4]

Beispiel

Prevent unexpected start-up of the telescopic movement





Measure	SIL	PL_r
e.g. safety function (SF)	3	e
e.g. safety function (SF)	2	d
e.g. safety function (SF)	1	c
Other measure or SF	-	b
Other measure or SF	-	a

Quelle: Nach [4]

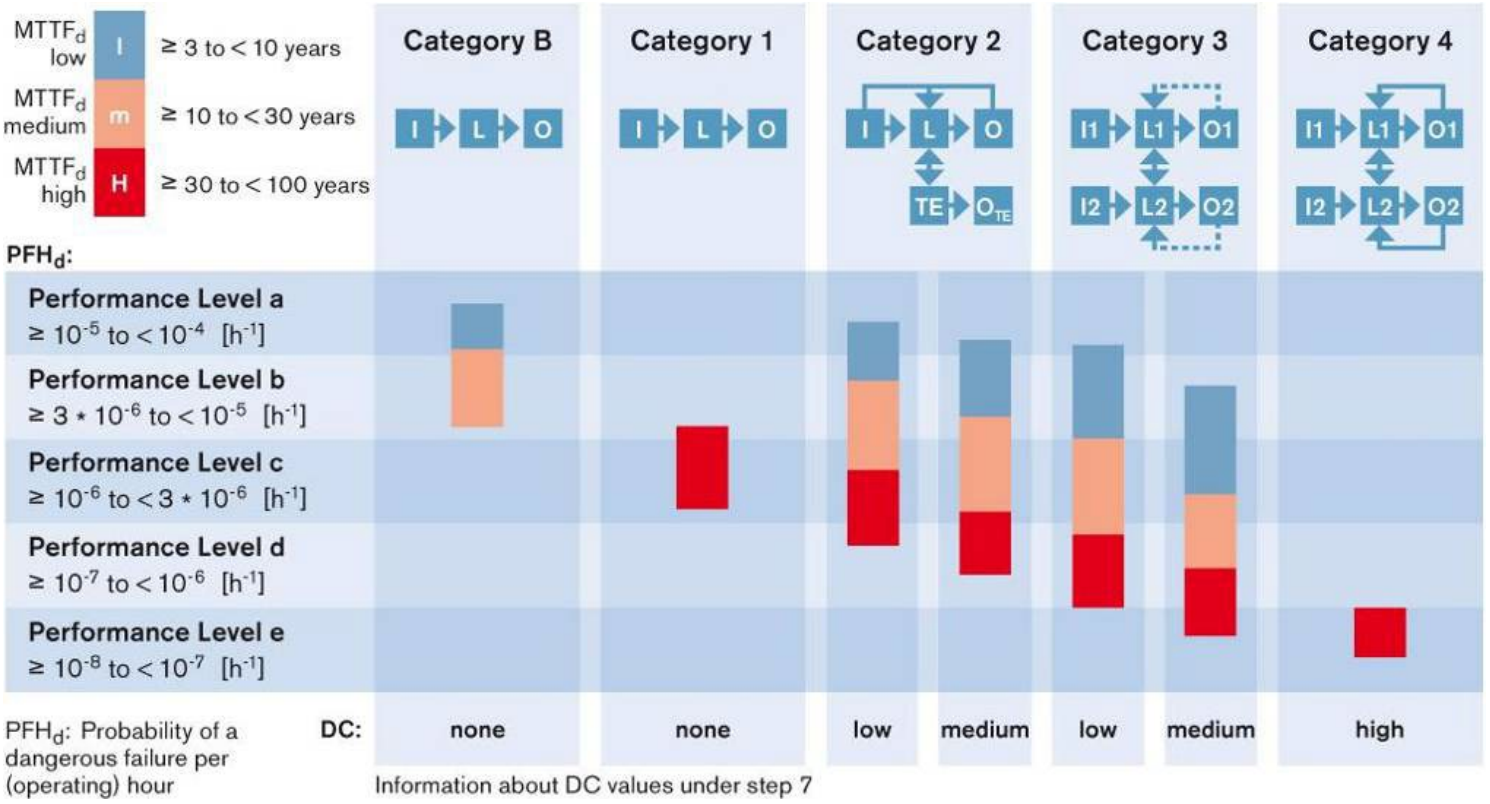
Beispiel

c + d + c = c

Joystick Kat. 2

Controller Kat. 2

Ventil Kat. 1



Beispiel

1. Risikobeurteilung und –minderung
2. Identifikation der Sicherheitsfunktionen
3. Bestimmen des PL_r
4. Auswahl der Systemarchitektur
5. **Modellieren des Systems als Blockdiagramm**
6. **Fehler und Diagnose**
7. Bestimmen des PL
8. Bewerten der Robustheit der Steuerung - Fehlervermeidung
9. Software-Anforderungen
10. Verifizieren und Validieren

Quelle: Nach [4]

Beispiel

5. Modellieren des Systems: $MTTF_d$-Daten

- $MTTF_d$-Wert: Erwartungswert der durchschnittlichen Zeit bis zu einem gefährlichen Ausfall
- Voraussetzung: Komponentenhersteller bestätigt die anwendbaren grundlegenden und bewährten Sicherheitsprinzipien (abhängig von spezifiziertem Einsatz)
- Elektronik: Berechnung nach Abstimmung des Einsatzes (z.B. Temperaturprofil) möglich
- Priorität nach ISO 13849:

Daten des Komponentenherstellers

↓

Standardisierte Werte in ISO 13849 mit zusätzlichen qualitativen Anforderungen, z.B. 150 Jahre für hydraulische Komponenten (zukünftig: 150-1200 Jahre je nach n_{Op})

↓

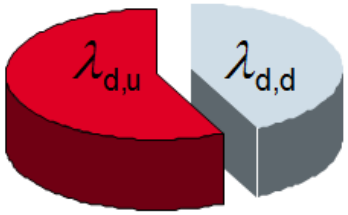
Pessimistische zehn Jahre

Beispiel

6. Fehler und Diagnose

- Der erreichbare PL hängt neben $MTTF_d$ und Kategorie vom Diagnosedeckunggrad ab.
- Der Diagnosedeckungsgrad (diagnostic coverage, DC) ist das Verhältnis

$$\frac{\text{unentdeckte gefährliche Fehlerrate}}{\text{gesamte gefährliche Fehlerrate}} = \frac{\lambda_{du}}{\lambda_d} = \frac{\lambda_{du}}{\lambda_{du} + \lambda_{dd}}$$



- Der DC ist auf Subsystemebene relevant, sollte aber mit Komponentenexperten gemeinsam bestimmt werden.
- Rexroth stellt möglichen DC bereit: Steuergeräte-Sicherheitshandbuch
- Beispiel möglicher Sicherheitsmechanismen aus ISO 13849:

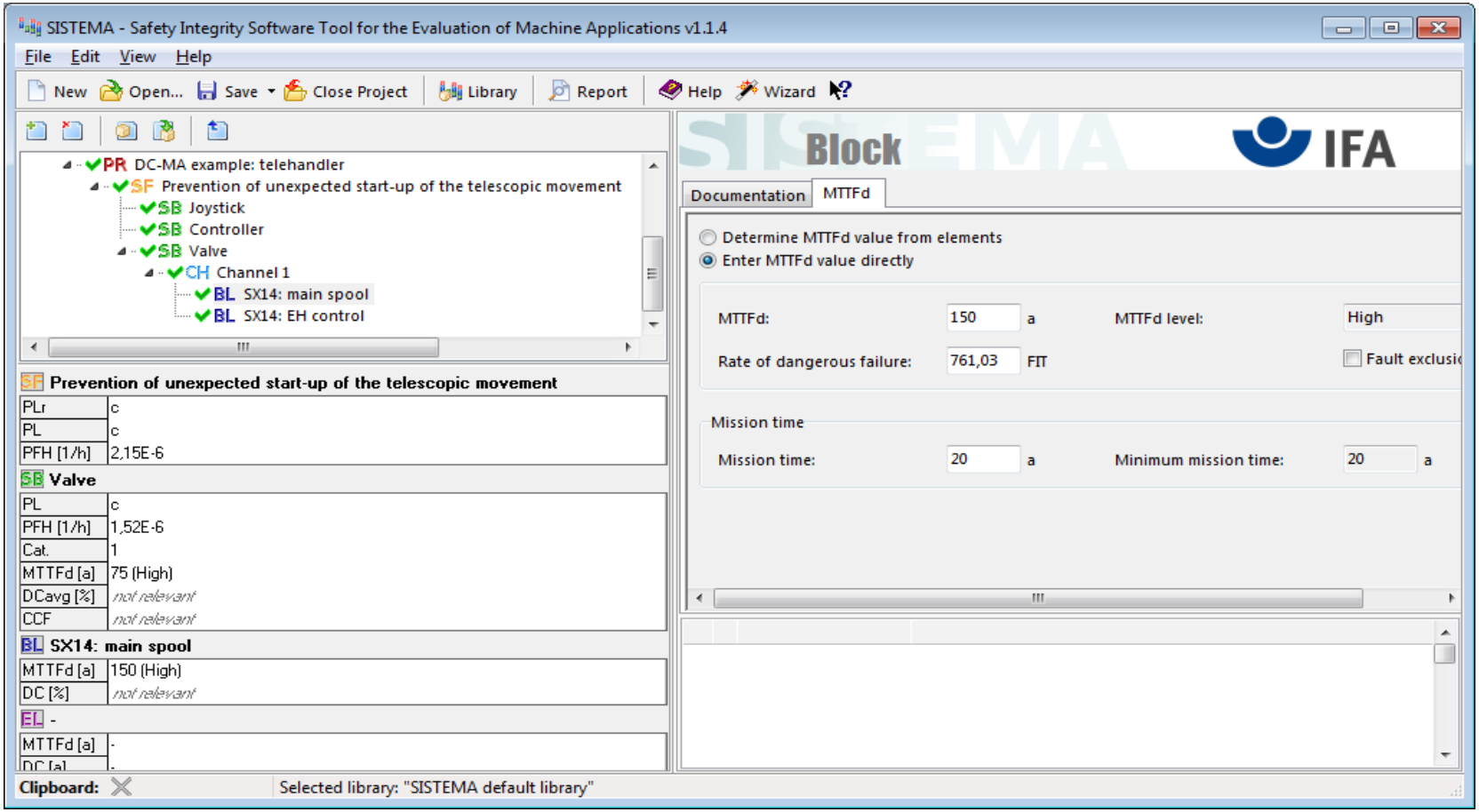
Maßnahme	Technologie	DC
Process (zyklischer Test)	Fluidtechnik	0% ≤ DC < 99%
Kreuzüberwachung (2 Kanäle)	Elektronik	DC = 99%
Indirekte Überwachung (z.B. Druck)	Fluidtechnik	90% ≤ DC < 99%
Direkte Positionsüberwachung	Fluidtechnik	DC = 99%

Beispiel

1. Risikobeurteilung und –minderung
2. Identifikation der Sicherheitsfunktionen
3. Bestimmen des PL_r
4. Auswahl der Systemarchitektur
5. Modellieren des Systems als Blockdiagramm
6. Fehler und Diagnose
7. **Bestimmen des PL**
8. Bewerten der Robustheit der Steuerung - Fehlervermeidung
9. Software-Anforderungen
10. Verifizieren und Validieren

Quelle: Nach [4]

Beispiel


SISTEMA - Safety Integrity Software Tool for the Evaluation of Machine Applications v1.1.4
File Edit View Help
New Open... Save Close Project Library Report Help Wizard
PR DC-MA example: telehandler
SF Prevention of unexpected start-up of the telescopic movement
SB Joystick
SB Controller
SB Valve
CH Channel 1
BL SX14: main spool
BL SX14: EH control
SF Prevention of unexpected start-up of the telescopic movement
PLr c
PL c
PFH [1/h] 2,15E-6
SB Valve
PL c
PFH [1/h] 1,52E-6
Cat. 1
MTTFd [a] 75 (High)
DCavg [%] not relevant
CCF not relevant
BL SX14: main spool
MTTFd [a] 150 (High)
DC [%] not relevant
EL -
MTTFd [a] -
Block
IFA
Documentation MTTFd
Determine MTTFd value from elements
Enter MTTFd value directly
MTTFd: 150 a
MTTFd level: High
Rate of dangerous failure: 761,03 FIT
Mission time
Mission time: 20 a
Minimum mission time: 20 a
Clipboard:
Selected library: "SISTEMA default library"

Sicherheitstechnik: Übung 4
PL bestimmen und Kategorie auswählen

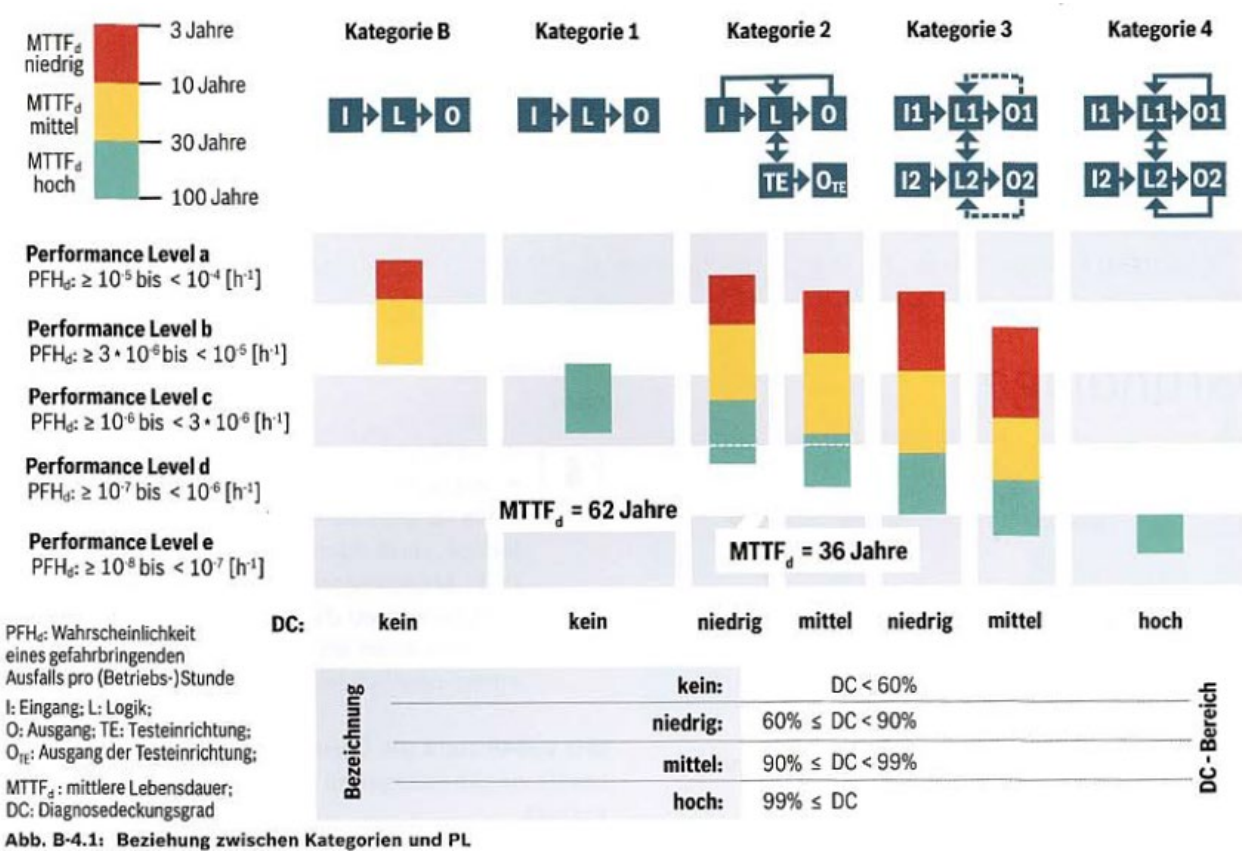


Abb. B-4.1: Beziehung zwischen Kategorien und PL

Sicherheitstechnik: Lösung Übung 4

Gefährdung	Definierter Performance Level	Erreichter Performance Level
Verletzung von Personen durch Quetschen oder Stoßen	S = 2 F = 2 P = 1 **PL = d**	**Kategorie = 2 für elektronische Systeme, Kategorie = 3 für hydraulische und pneumatische Systeme** **PL = d**