

Tag 1: Fachvorträge

Motto des diesjährigen
Events

SIL versus
PL

2023
SIL Sprechstunde
PEPPERL+FUCHS



Vorträge

- 1. Normenvergleich IEC 61508, IEC 61511, ISO 13849**
- 2. Sicherheitsgerichtete Alarme in SIL - Möglich oder nicht?**
- 3. Übersetzung SIL \leftrightarrow PL – wo geht's schief**
- 4. VDI-Richtlinie "Gebrauchsdauer"**
- 5. Zusammenhang zwischen Markov-Modellen, PFD und PFH**
- 6. Digitalisierung und KI im Safety Lifecycle aus Betreiber-Sicht – Spannung – Potential – Erdung ...**
- 7. Praktische Erfahrung in Auslegung und Betrieb von PLT-Sicherheitseinrichtungen**

SIL-Sprechstunde 2023 – Grundsätzliche Gemeinsamkeiten und Unterschiede der Normen IEC 61508, IEC 61511, ISO 13849, ISO 26262 – Es sind nicht nur die Metriken!



IEC 61508-1

Edition 2.0 2010-04

INTERNATIONAL STANDARD

NORME INTERNATIONALE

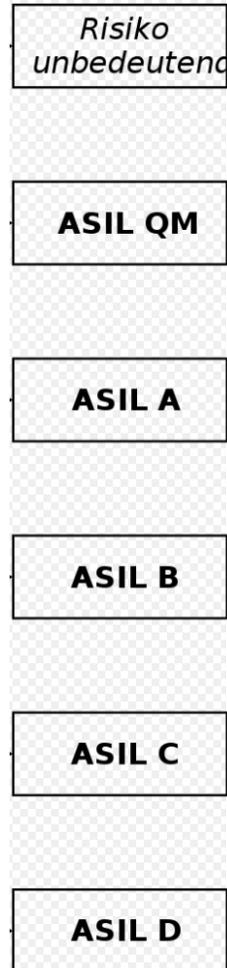
BASIC SAFETY PUBLICATION
PUBLICATION FONDAMENTALE DE SÉCURITÉ

Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements

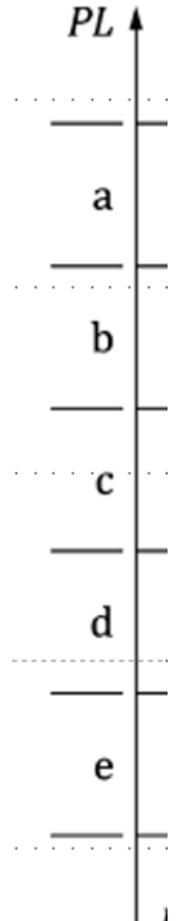
Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 1: Exigences générales



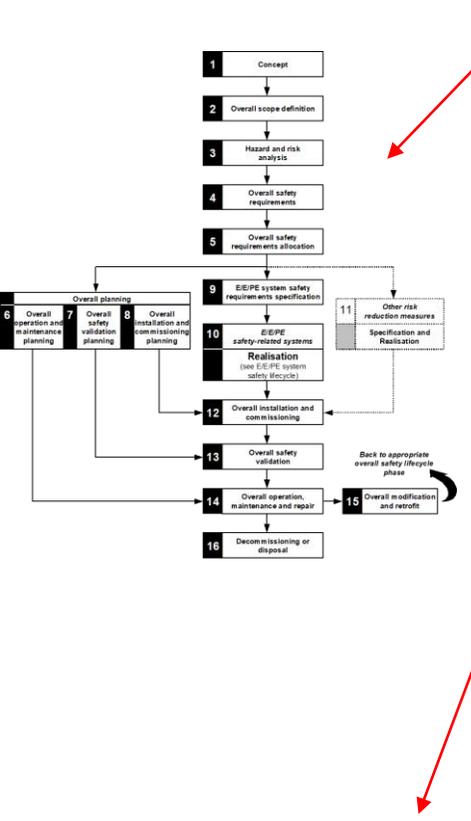
SIL 1-4



Performance Level required PL_r
a: niedrige Risikominderung
e: hohe Risikominderung

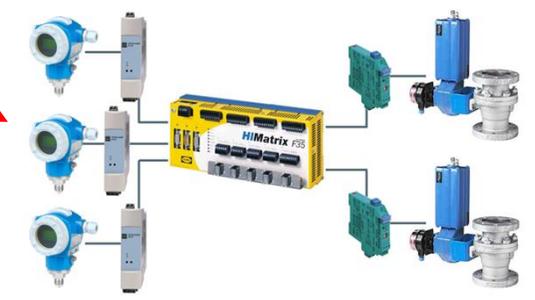


SIL Sprechstunde 2023 – Die Säulen der funktionalen Sicherheit

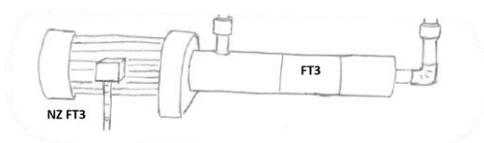


in the power part now.) Since only the failures in opening prevent the safety function to be carried out, we get for λ_{DU} (and the probability of failure per hour):

$$\lambda_{DU} = 6 \times 10^{-9} \text{ 1/h} \times 0,73 = 4,5 \times 10^{-9} \text{ 1/h}$$



Technique/measure	See IEC 61508-7	SIL 1
Measures against voltage breakdown, voltage variations, overvoltage, low voltage and other phenomena such as a.c. power supply frequency variation that can lead to dangerous failure	A.8	M low
Separation of electrical energy lines from information lines (see Note 4)	A.11.1	M



Normen zur funktionalen Sicherheit: IEC 61508 und sektorspezifische Ausprägungen – Wie vergleichen wir?

Um etwas Ordnung in diese Komplexität zu bringen, werden wir einen Vergleich anhand der folgenden Kriterien vornehmen:

1. Anwendungsbereiche

2. Terminologie

3. Aufbau der Lebenszyklen und zugrundeliegende Rollenmodelle

4. Risikoanalyse, mit den Unterpunkten:

- Wahl des Betrachtungsgegenstandes
- Auffindung der Gefährdungen
- Bewerten der damit verbundenen Risiken

5. Festlegung der Anforderungen (Sicherheitsfunktionen), insbesondere:

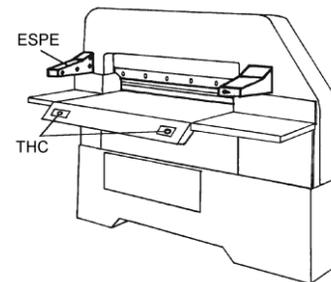
- Zuordnung zu Systemen und
- Bestimmung der notwendigen Risikominderung

6. Realisierung, mit den Unterpunkten

- Anforderungen und Wahl der Lösung
- Begrenzung der zufälligen Ausfälle (Schätzung der Ausfallwahrscheinlichkeit) und
- Architekturansforderungen (Systemtoleranz)

Damit werden natürlich nur die grundsätzlichen Vorgehensweisen der Normen verglichen.

Für Einzelheiten muss bitte in diesen selbst nachgesehen werden.



Normen zur funktionalen Sicherheit: IEC 61508 und sektorspezifische Ausprägungen

In diese Ausarbeitung sind die Ergebnisse von studentischen Arbeiten eingeflossen, die an der Hochschule Darmstadt angefertigt wurden.



Normenvergleich zwischen DIN EN 61508:2011 und ISO 26262:2018

Teamprojekt im Modul M8 im Studiengang Zuverlässigkeitsingenieurwesen
Wintersemester 2019/2020

Projektteam

- Thomas Becker
- Fabian Dorn
- Johannes Schmidt
- Andreas Weber

Betreuung: Ingo Rolle, Lehrbeauftragter im Fachbereich EIT

Projektbericht vom 29. Februar 2020

Vergleich von Normen zur funktionalen Sicherheit

Vorstellung des Semesterprojekts im Fernstudiengang Zuverlässigkeitsingenieurwesen
der Hochschule Darmstadt

Alexandra Platte, Stephan Radke
Frankfurt, 15. Mai 2019

Ingo Rolle, im September 2022

Vergleich von Lebenszyklen in Normen der funktionalen Sicherheit und der dazugehörigen Rollenmodelle für verschiedene Branchen in Bezug auf die Risikoanalyse

Teamprojekt im Modul M8 des Studiengangs Zuverlässigkeitsingenieurwesen
Sommersemester 2020

Projektteam:

Eddaoui, Mustapha
El Achabi, Younes

Betreuung: Ingo Rolle,
Lehrbeauftragter im Fachbereich EIT

Normen zur funktionalen Sicherheit: IEC 61508 und sektorspezifische Ausprägungen – 1. Anwendungsbereiche – IEC 61508-Reihe

IEC 61508 Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme

Diese Internationale Norm behandelt diejenigen Gesichtspunkte, die zu betrachten sind, wenn elektrische/elektronische/programmierbare elektronische (E/E/PE) Systeme zur Ausführung von Sicherheitsfunktionen eingesetzt werden.

Ein Hauptziel dieser Norm ist es, die Entwicklung produkt- und anwendungsspezifischer Internationaler Normen durch die für ein Produkt- und Anwendungsgebiet verantwortlichen Technischen Komitees zu unterstützen.....

Ein zweites Ziel dieser Norm ist es, die Entwicklung sicherheitsbezogener E/E/PE-Systeme zu ermöglichen, für die keine produkt- oder anwendungsspezifischen Internationalen Normen bestehen.

.....

Der Anwendungsbereich der IEC 61508 umfasst fast 2 Seiten!

Die Norm gilt also für die gesamte Sicherheitskette, nicht nur für die Elektronik! Obwohl der Titel etwas anderes vermuten lässt.

Die IEC 61508 ist eine Sicherheitsgruppennorm für Normungskomitees („eine generische Norm“) und nicht zur direkten Anwendung gedacht.

Nur wenn es keine Produktnorm gibt, soll sie direkt angewendet werden.

Normen zur funktionalen Sicherheit: IEC 61508 und sektorspezifische Ausprägungen— 1. Anwendungsbereiche – IEC 61511-Reihe

IEC 61511 FUNCTIONAL SAFETY – SAFETY INSTRUMENTED SYSTEMS FOR THE PROCESS INDUSTRY SECTOR

This part of IEC 61511 gives requirements for the specification, design, installation, operation and maintenance of a safety instrumented system (SIS), so that it can be confidently entrusted to achieve or maintain a safe state of the process. IEC 61511-1 has been developed as a process sector implementation of IEC 61508:2010.

....

c) defines the relationship between IEC 61511 and IEC 61508 (see Figures 2 and 3)

.....

u) specifies requirements for all parts of the SIS from sensor to final element(s);



Für die Verfahrenstechnik, hauptsächlich chemische Verfahrenstechnik, aber auch z.B. Kraftwerke.

Das bedeutet, dass Gerätezulieferungen nach IEC 61508 behandelt werden müssen.

Sie bezieht die gesamte Sicherheitskette mit ein. In der Verfahrenstechnik nennt man das „pipe-to-pipe principle“.

Normen zur funktionalen Sicherheit: IEC 61508 und sektorspezifische Ausprägungen – 1. Anwendungsbereiche – ISO 13849 -Reihe

DIN EN ISO 13849-1:2016-06; Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen

Die Norm DIN EN ISO 13849-1 stellt Sicherheitsanforderungen und einen Leitfaden für die Prinzipien der Gestaltung und Integration sicherheitsbezogener Teile von Steuerungen bereit. Für diese Teile werden spezielle Eigenschaften einschließlich des Performance Level festgelegt, die zur Ausführung der entsprechenden Sicherheitsfunktionen erforderlich sind.

Sie ist anzuwenden auf sicherheitsbezogene Teile von Steuerungen ungeachtet der verwendeten Technologie und Energie (elektrisch, hydraulisch, pneumatisch, mechanisch).



Ingo Rolle, im September 2022

Für den Maschinenbau. Die Norm ist im Amtsblatt der Europäischen Gemeinschaften entsprechend angegeben und unterstützt die Erfüllung der grundlegenden Anforderungen der EU-Maschinenrichtlinie.
(Das macht auch die IEC 62061)

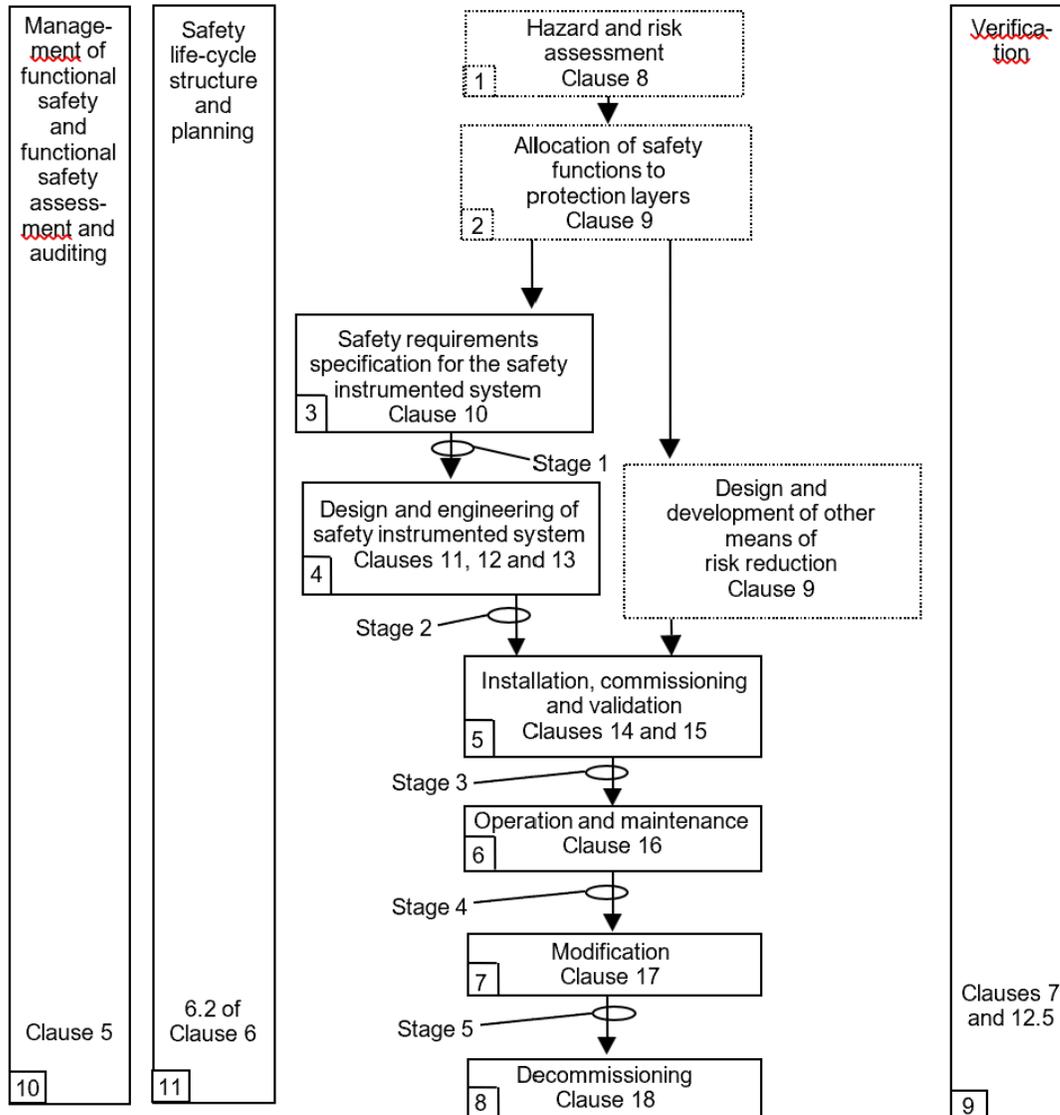
Es wird also die gesamte Sicherheitskette detailliert behandelt, mit Pneumatik und Hydraulik, auch im Teil 2. Die IEC 61508 bezieht die Aktorik zwar mit ein, gibt aber keine Anweisungen dazu. Auch in der IEC 61511 und ISO 26262 sind die Anforderungen hierzu nicht besonders detailliert.

Die ISO 13849-Reihe gibt detaillierte Anweisungen zu Pneumatik und Hydraulik, im Gegensatz zu den anderen genannten Normen.

Normen zur funktionalen Sicherheit: IEC 61508 und sektorspezifische Ausprägungen – 2. Terminologie

Begriff	IEC 61508	IEC 61511	ISO 13849	ISO 26262
Betrachtetes (physikalisches) System, auf dem die Risikoanalyse ausgeführt wird	EUC = Equipment under Control	process	Maschine	item
Betriebliches Leitsystem	EUC control system	BPCS = basic process control system	Control system	
Sicherheitsgerichtetes System	E/E/PES safety-related system	safety instrumented system	SRP/CS = safety-related part of a control system	
Technische Aufgabenstellung, die das Risiko mindert	Sicherheitsfunktion, safety function	Safety instrumented function	safety function	Safety goal
Zugeliefertes Gerät mit sicherheitstechnischen Eigenschaften	Conformant object	Gerät	Sicherheitsbauteil (nach Maschinenrichtlinie)	Element out of context

Normen zur funktionalen Sicherheit: IEC 61508 und sektorspezifische Ausprägungen – 3. Lebenszyklen und Rollenmodelle – IEC 61511



Dem Lebenszyklus der IEC 61511 liegt folgendes Rollenmodell zu Grunde:

- **Betreiber** (z.B. eine Chemiefabrik)
- **Integrator** (z.B. ein Ingenieurbüro)
- **Gerätelieferanten** (z.B. von Sensoren, Leitsystem, Ventilen)

Die im Lebenszyklus definierten Tätigkeiten lassen sich auch als Rollen auffassen, die jemand übernehmen muss. Es gibt in der Branche Verfahrenstechnik hierfür Usancen und gesetzliche Vorschriften (Rollenmodell). Z.B. übernimmt der Betreiber die Risikoanalyse, die Validierung und den Betrieb, oder er wird sich hier zumindest einbringen. Der Integrator übernimmt Entwurf und Realisierung des sicherheitsgerichteten Systems (safety integrated system).

Der Lebenszyklus ist gegenüber der IEC 61508 vereinfacht dargestellt. Die Festlegung des Untersuchungsbereichs wird der Risikoanalyse zugeschlagen.

Normen zur funktionalen Sicherheit: IEC 61508 und sektorspezifische Ausprägungen – 3. Lebenszyklen und Rollenmodelle – ISO 13849

Die ISO 12100 beschreibt den Prozess der Risikoanalyse (Typ A-Norm), während die ISO 13849-1 den Entwurf eines sicherheitsgerichteten Systems beschreibt (Typ B1-Norm). ISO 13849-2 beschreibt die Validierung.

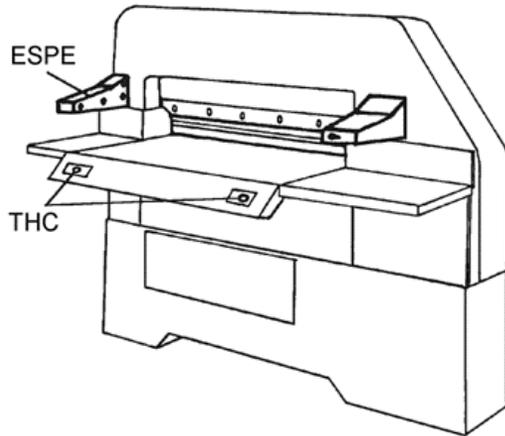
Ein Lebenszyklus, der an ein Functional Safety Management System gebunden ist, ist weder in der ISO 12100 noch in der ISO 13849 enthalten. Die entsprechenden Tätigkeiten sind in den Normen aber beschrieben und können vom Hersteller eines Steuerungssystems in sein Qualitätsmanagementsystem eingebunden werden, um systematische Fehler zu vermeiden.

ISO 13849-1:2023 empfiehlt in Anhang G.5 ein Functional Safety Managementsystem zur Vermeidung systematischer Fehler. In Unterabschnitt 7.1 wird für die Entwicklung der sicherheitsgerichteten SW ein V-Modell vorgeschrieben, auch für Anwendersoftware.

Das Rollenmodell von ISO 12100/ISO 13849 beruht auf demjenigen der europäischen Maschinenrichtlinie und umfasst:

- dem Maschinenhersteller, der die Risikoanalyse durchführt
- dem Betreiber
- der Überwachungsbehörde
- dem Zulieferer von Sicherheitsbauteilen

Normen zur funktionalen Sicherheit: IEC 61508 und sektorspezifische Ausprägungen – 4. Risikoanalyse – ISO 13849 - Wahl des Betrachtungsgegenstandes, Auffinden der Gefährdungen, Risikobewertung



Die für die Anwendung der ISO 13849 erforderliche Risikoanalyse ist in der ISO 12100 beschrieben. Der Untersuchungsgegenstand ist hier stets „die Maschine“, so wie sie in der europäischen Maschinenrichtlinie definiert ist.

Als Methode zum Auffinden der Gefährdungen ist als Beispiel das Abarbeiten eine Checkliste angegeben. Diese ist die Liste der Gefährdungen aus dem Anhang A.1 der europäischen Maschinenrichtlinie.

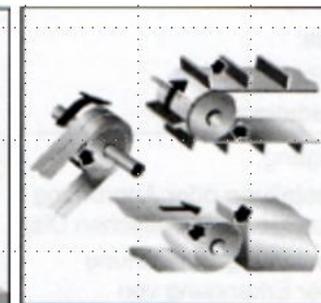
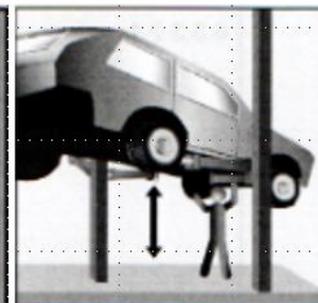
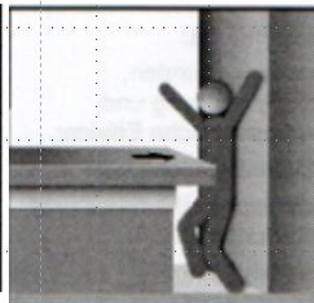
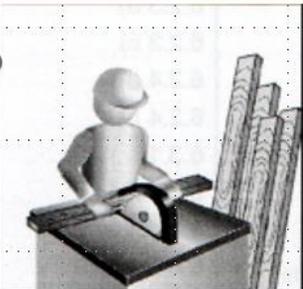
Die Risikobewertung ist in der ISO 12100 rein qualitativ vorgeschrieben.

cutting

moving parts

gravitation

getting caught
and pulled in

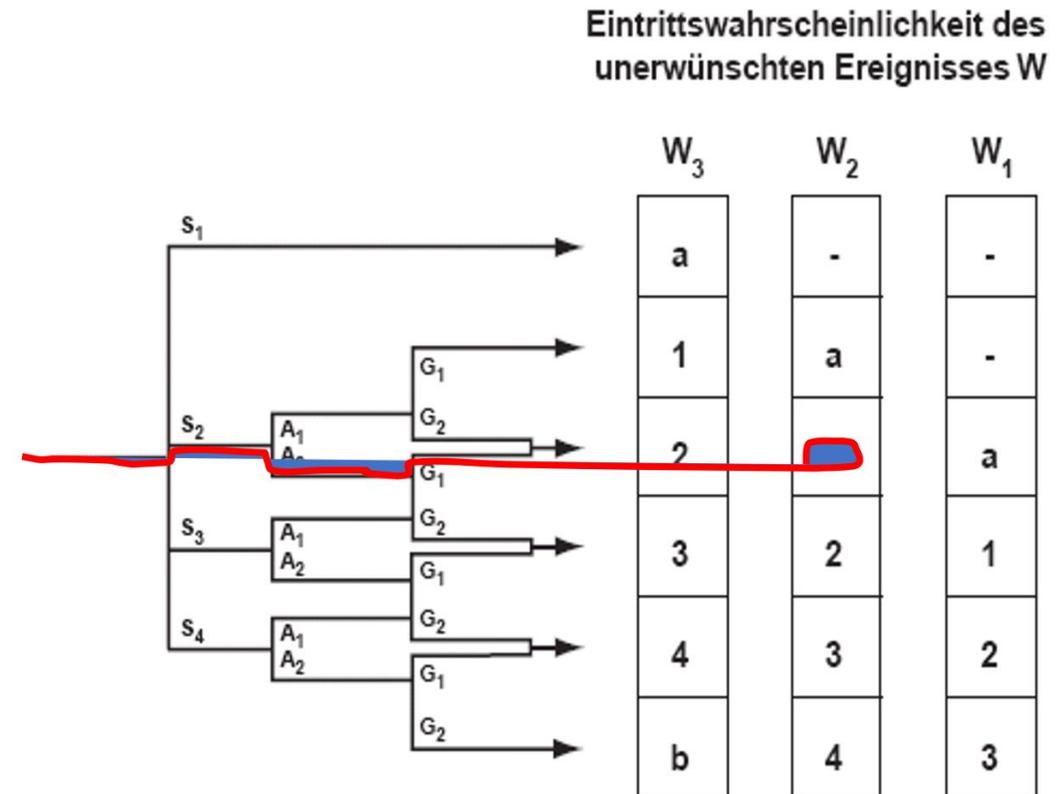


Normen zur funktionalen Sicherheit: IEC 61508 und sektorspezifische Ausprägungen – 5. Festlegen der Anforderungen – IEC 61508, IEC 61511, ISO 13849

Zur Feststellung der Risikominderung in SIL (oder PL nach ISO 13849-1), die die Sicherheitsfunktion herbeiführen soll, wird in keinem der genannten Normen ein Verfahren normativ vorgeschrieben. Üblich sind der Risikograph, Matrix-Methoden (ähnlich der ISO 26262), LOPA oder ALARP.

Dabei wird ein Gedankenexperiment durchgeführt. Man stellt sich vor, die Sicherheitsfunktion wäre nicht wirksam und bestimmt das Risiko der ungeschützten Anlage. Dies wird mit der zu erreichenden Risikominderung gleichgesetzt.

- Risikoparameter
- Schadensausmaß
 - S₁ leichte Verletzung oder leichter Schaden
 - S₂ schwere, irreversible Verletzung oder Tod einer Person, temporärer schwerer Schaden
 - S₃ Tod mehrerer Personen, langfristiger Schaden
 - S₄ viele Tode, katastrophale Auswirkungen
- Häufigkeit/Aufenthaltsdauer
 - A₁ seltener bis häufiger Aufenthalt im Gefahrenbereich
 - A₂ häufiger bis dauernder Aufenthalt im Gefahrenbereich
- Gefahrenabwendung
 - G₁ möglich
 - G₂ nicht abwendbar, kaum möglich
- Eintrittswahrscheinlichkeit des unerwünschten Ereignisses
 - W₁ sehr gering, kaum
 - W₂ gering
 - W₃ hoch, häufig



- 1, 2, 3, 4 = Sicherheits-Integritätslevel, SIL
- = tolerierbares Risiko, keine Sicherheitsanforderungen
- a = keine besonderen Sicherheitsanforderungen
- b = ein einzelnes E/E/PE-System reicht nicht aus

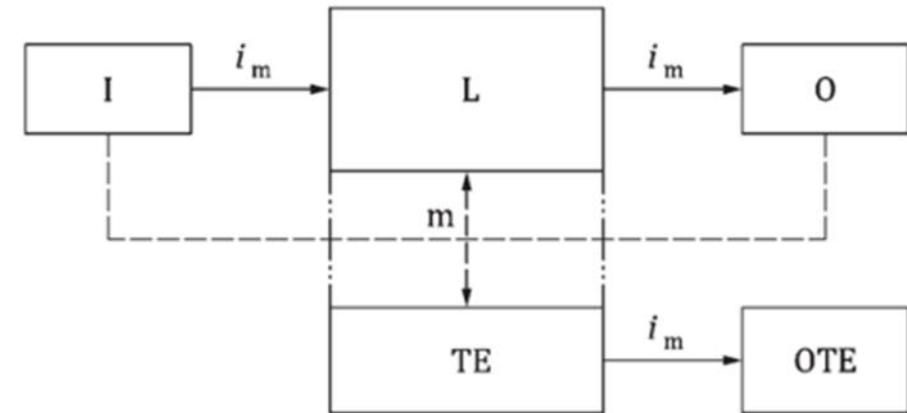
Normen zur funktionalen Sicherheit: IEC 61508 und sektorspezifische Ausprägungen – 6. Realisierung, Anforderungen und Wahl der Lösung

Alle Normen verlangen,

- dass die Anforderungen weiter heruntergebrochen werden zu einer Anforderungsspezifikation,
- dass ein sicherheitsgerichtetes System entworfen wird
- und nachgewiesen wird, dass dieser Entwurf den Anforderungen der Anforderungsspezifikation und denen der Norm genügt.

Einzig die ISO 13849-1 schreibt Lösungsansätze als sogenannte Kategorien mit vorgesehenen Architekturen vor. Sie sollen logisch, nicht physikalisch, umgesetzt werden.

Im Bereich der übrigen Normen wird das Vorgeben von Lösungen auf die Ebene informativer Literatur oder Werknormen verlagert. Diese Lösungsansätze werden oft „Typicals“ genannt.



Legende:

i_m : interconnecting means, z.B. Sicherheits-Feldbus

I: input device, z.B. Sensor

L: logic, z.B. Sicherheits-SPS

m: monitoring/testing

O: output device, z.B. Schütz

TE: test equipment

OTE: Ausgang der TE

Ein Beispiel:

Die Kategorie 2 nach ISO 13849-1:2006. Sie ist üblicherweise einsetzbar bis Performance Level (PL) C, was mit SIL 2 vergleichbar ist. (Bei Nachweis eines hohen Diagnosedeckungsgrades der Testeinrichtung TE kann auch Performance Level D angesetzt werden.)

Normen zur funktionalen Sicherheit: IEC 61508 und sektorspezifische Ausprägungen – 6. Realisierung, Begrenzung der zufälligen HW-Ausfälle – IEC 61508

Die IEC 61508 verlangt, dass die Ausfallwahrscheinlichkeit des Systems, das die Sicherheitsfunktion ausführt, geschätzt, d.h. vorhergesagt wird. Sie muss unter einer SIL-abhängigen Grenze liegen. (Das SIL ergab sich aus der Risikoanalyse).

Safety integrity level	Low demand mode of operation (Average probability of failure to perform its design function on demand)
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

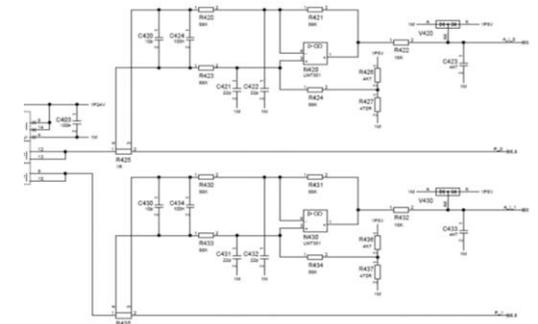
Die Vorgehensweise zur Schätzung gliedert sich in zwei Schritte:

- von der Bauteilebene auf die Geräteebene („Elemente“)
- von der Geräteebene auf das Gesamtsystem.

Safety integrity level	High demand or continuous mode of operation (Probability of a dangerous failure per hour)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

Dies beruht auf dem verwendeten HW-Modell mit Bauteilen, Elementen, Teilsystemen und Gesamtsystem.

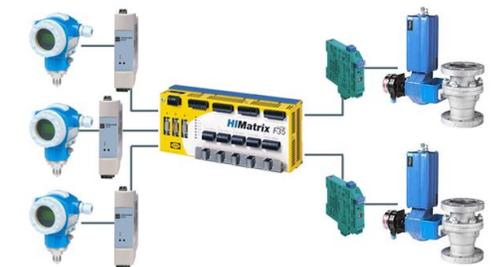
Für den ersten Schritt wird FMEA/FMEDA eingesetzt, erlaubt ist auch eine statistische Beobachtung auf Geräteebene. Für den zweiten Schritt werden z.B. die Methoden Reliability Block Diagram oder Markow eingesetzt.



NOT MEASUREMENT SENSITIVE
MIL-HDBK-217F
2 DECEMBER 1991
SUPERSEDED BY
MIL-HDBK-217E, Notice 1
2 January 1990

MILITARY HANDBOOK
RELIABILITY PREDICTION OF
ELECTRONIC EQUIPMENT

component designation	failure rate λ [1/h]	failure mode	fraction	effect	λ_{sub} [1/h]	λ_{su} [1/h]
resistor R3	10^{-9}	short	10%	S	1×10^{-10}	
		interruption	70%	D		7×10^{-10}
		Drift	20%	D		2×10^{-10}
relay RI	6×10^{-9} $= 60 \times 10^{-10}$	failure to open	73%	D		15×10^{-10}
		failure to close	25%	S	45×10^{-10}	
		sum (results from the previous sheets in parenthesis)			$(8 + 13,5 + 46) \times 10^{-10} = 67,5 \times 10^{-10} = 6,8 \times 10^{-9}$	$(12 + 16,5 + 24) \times 10^{-10} = 52,5 \times 10^{-10} = 5,3 \times 10^{-9}$



Normen zur funktionalen Sicherheit: IEC 61508 und sektorspezifische Ausprägungen – 6. Realisierung, Begrenzung der zufälligen HW-Ausfälle, Architektur Anforderungen – IEC 61508

Die IEC 61508 verlangt die Berechnung folgender Kennziffern:

λ_s Rate der sicheren Ausfälle

λ_{dd} Rate der gefährlichen entdeckten Ausfälle

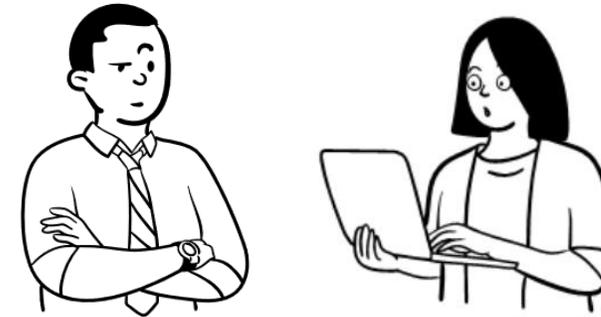
λ_{du} Rate der gefährlichen, unentdeckten Ausfälle. Sie wird für das Kriterium „Begrenzung der zufälligen Hardwareausfälle“ verwendet.

Der Anteil sicherer Ausfälle = safe failure fraction = SFF . Diese Kennziffer wird für das Kriterium „Architekturbeschränkungen“ verwendet. Sie ist pro „Element“ zu berechnen. (Ein Element ist ein Gerät oder eine Zusammenstellung von Geräten)

$$\text{SFF} = \frac{\lambda_s + \lambda_{dd}}{\lambda}$$

Ingo Rolle, im
September 2023

Diese Vorschrift ist mit dem Argument kritisiert worden, dass sichere Ausfälle für die Zuverlässigkeit der Ausführung einer Sicherheitsfunktion nicht relevant sind.



Einige sektorspezifische Normen verwenden daher nicht die SFF, sondern definieren andere Kriterien zur Einhaltung von Architekturbeschränkungen.

Normen zur funktionalen Sicherheit: IEC 61508 und sektorspezifische Ausprägungen – 6. Realisierung, Architektur Anforderungen – das Kriterium der IEC 61508

Die IEC 61508-1 verlangt für jedes Element, dass in die Ausführung einer Sicherheitsfunktion eingebunden ist, die Einhaltung der folgenden Tabellen



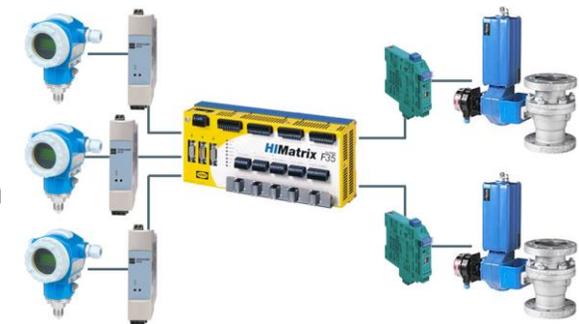
Safe failure fraction of an element	Hardware fault tolerance		
	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3
60 % – < 90 %	SIL 2	SIL 3	SIL 4
90 % – < 99 %	SIL 3	SIL 4	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

Hardware Fault Tolerance (HFT) = 0 bedeutet, dass nach Ausfall eines Kanals noch 0 übrig bleiben, um die Sicherheitsfunktion auszuführen. Bei HFT 1 bleibt nach einem Ausfall noch ein Kanal übrig.

Safe failure fraction of an element	Hardware fault tolerance		
	0	1	2
<60 %	nicht erlaubt	SIL 1	SIL 2
60 % – <90 %	SIL 1	SIL 2	SIL 3
90 % – <99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

Die obere Tabelle gilt für einfache Bauteile, deren Ausfallverhalten bekannt und statistisch dokumentiert ist, z.B. Relais.

Die untere Tabelle gilt für komplexe Elemente, deren Ausfallverhalten nicht vorhersagbar ist, z.B. eingebettete Systeme.



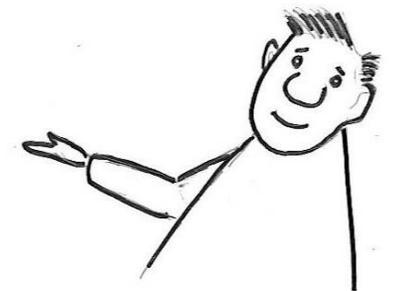
Normen zur funktionalen Sicherheit: IEC 61508 und sektorspezifische Ausprägungen – 6. Realisierung, Anforderungen und Wahl der Lösung – Überlegungen, die bei der Entstehung der ISO 13849 eine Rolle gespielt haben mögen

Die Norm soll nur Anforderungen vorgeben – zur Begrenzung der zufälligen Hardwareausfälle und für die Architekturansforderungen. Der Projektierer muss eine Lösung wählen und schauen, ob er die Anforderungen damit einhält. In der Praxis werden Lösungskataloge entstehen, in der Fachliteratur und in den Firmen. Der Projektierer wird dann lernen, welche Lösungen er nehmen kann.



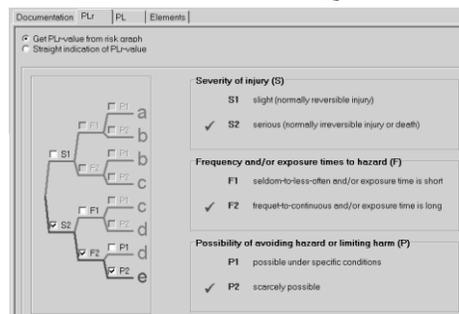
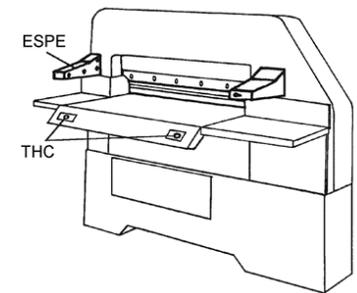
IEC 61508

Nein, wir können den Steuerungsbauer im mittelständischen Maschinenbau nicht im Regen stehen lassen. Die Norm muss ihn zur richtigen Lösung führen. Auch muss er den Anschluss an die Kategorien der EN 954 finden. Und es muss einen einfachen Weg geben, den Entwurf gegen die Anforderungen zu verifizieren.



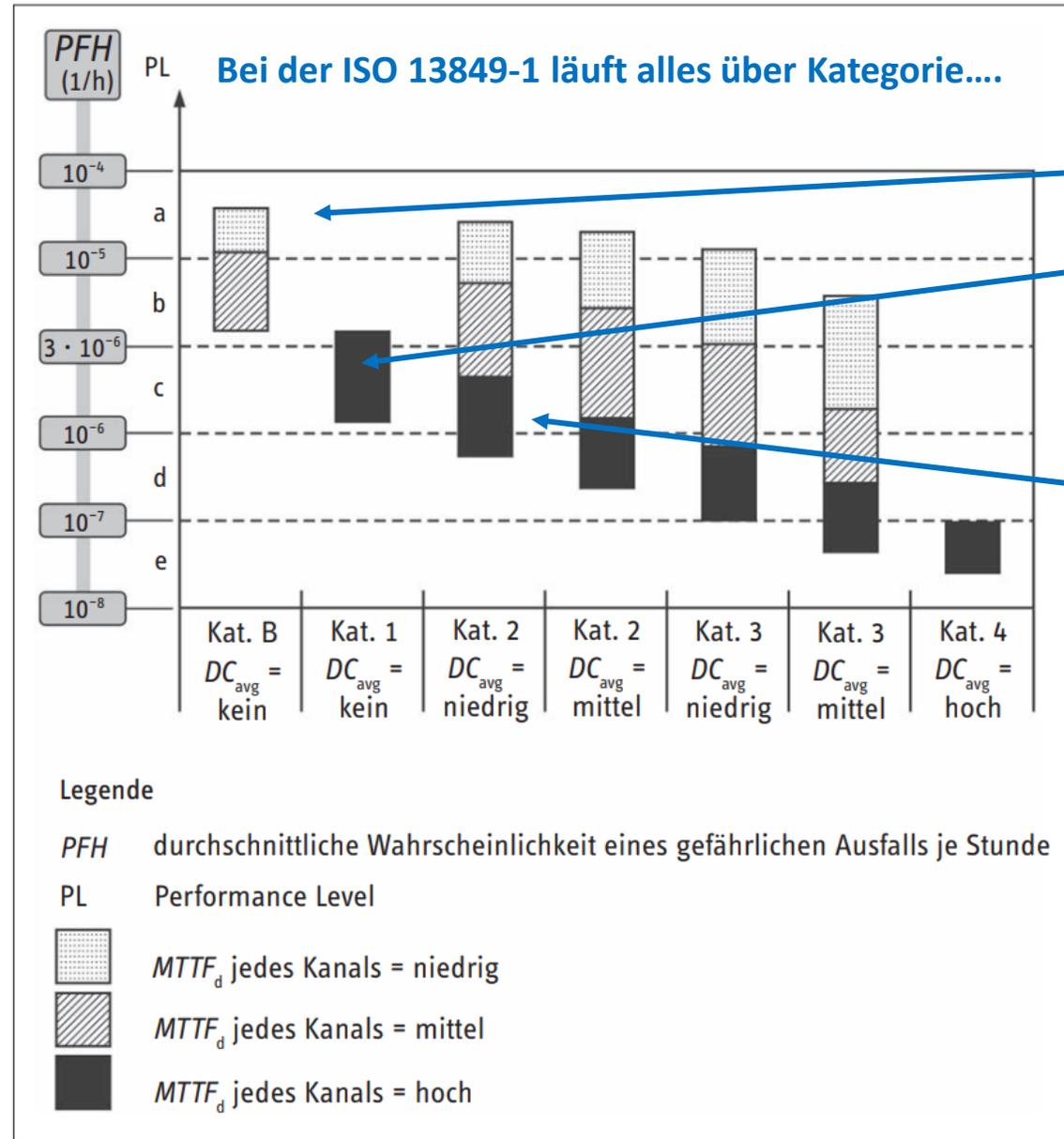
ISO 13849

Normen zur funktionalen Sicherheit: IEC 61508 und sektorspezifische Ausprägungen – 6. Realisierung, Begrenzung der zufälligen Ausfälle, Architektur Anforderungen – ISO 13849



Für eine bestimmte Sicherheitsfunktion ergab der Risikograph z.B. PL c, d.h die PFH liegt zwischen 10^{-6} und 3×10^{-6} .

Ingo Rolle, im September 2023

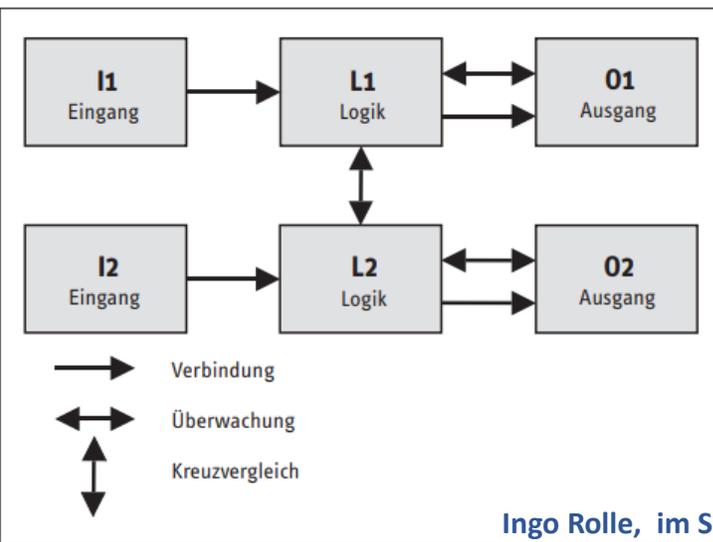
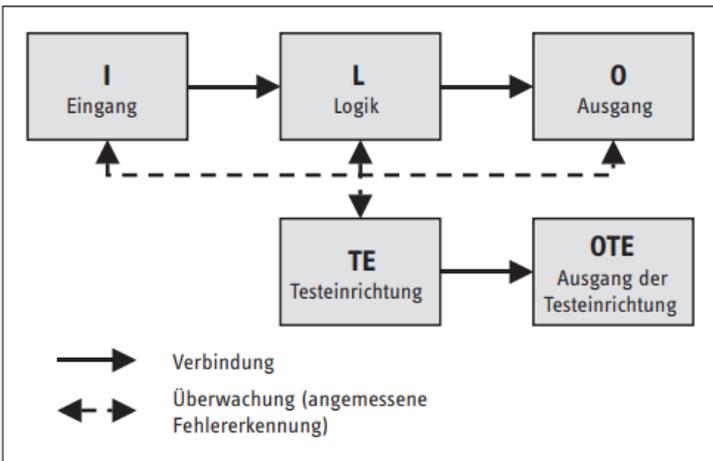
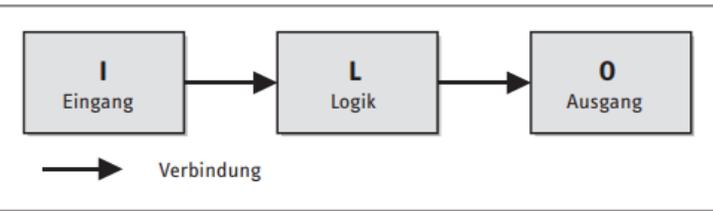


Das lässt sich erreichen

- mit Kategorie B gar nicht
- mit Kategorie 1, sofern der Nachweis gelingt, dass die $MTTF_d$ hoch ist (mean time to dangerous failure)
- mit Kategorie 2 mit $MTTF_d$ mittel bis hoch und DC (diagnostic coverage) niedrig bis mittel
- mit Kategorie 3 usw

das Säulendiagramm

Normen zur funktionalen Sicherheit: IEC 61508 und sektorspezifische Ausprägungen – 6. Realisierung, Begrenzung der zufälligen Ausfälle, Architektur Anforderungen – ISO 13849



Das sind die Kategorien:

viele Begriffe zur Qualifikation von Bauteilen und Geräten

- Kategorie B. Erfüllt maximal PL b = SIL 1. Qualifikation über Auswahl der Bauelemente (grundlegende Sicherheitsprinzipien, Einhaltung der Betriebsbeanspruchungen).
- Kategorie 1. Erfüllt maximal PL c = SIL 1. Qualifikation über Auswahl der Bauelemente (grundlegende und bewährte Sicherheitsprinzipien, bewährte Bauteile, für komplexe elektron. Bauteile meist nicht erreichbar). Nachweis, dass die $MTTF_d$ hoch ist (mean time to dangerous failure)
- Kategorie 2. Erfüllt maximal PL d = SIL 2. Qualifikation über Testeinrichtung (Diagnose). Anforderungen an Bauelemente, $MTTF_d$, CCF-Verhinderung und DC (diagnostic coverage).
- Kategorie 3. Erfüllt maximal PL e = SIL 3. Qualifikation über Redundanz. Anforderungen an Bauelemente, $MTTF_d$, CCF-Verhinderung und DC (diagnostic coverage).
- Kategorie 4. Erfüllt maximal PL e = SIL 3. Qualifikation über Redundanz und erhöhtes DC und $MTTF_d$.

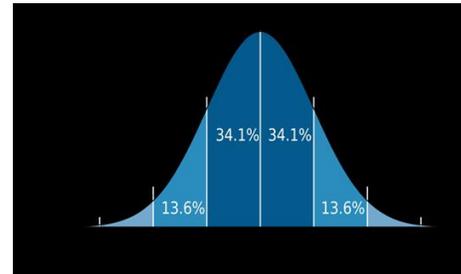
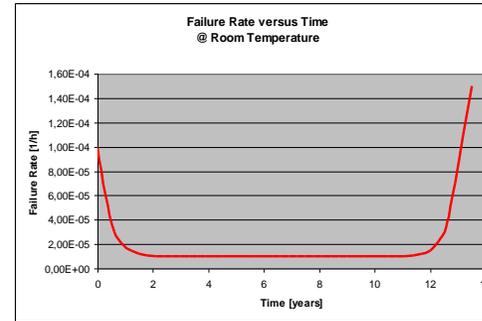
Alle BSB sind prinzipiell gemeint, physikalische Realisierung kann anders aussehen

Normen zur funktionalen Sicherheit: IEC 61508 und sektorspezifische Ausprägungen – 6. Realisierung, Begrenzung der zufälligen Ausfälle, Architektur Anforderungen – ISO 13849

ISO 13849-1:2023, 6.1.4 verlangt die Begrenzung zufälliger Hardwareausfälle und die Festlegung einer Ausfallwahrscheinlichkeit. Als Maßzahl wird die $MTTF_d$ verwendet, d.h. die mittlere Zeit bis zum Auftreten eines gefährlichen Fehlers.

Sie ist folgendermaßen zu bestimmen, mit Vorrang für die erstgenannte Maßnahme (ISO 13849-1:2023, 6.1.4):

- Verwendung von Herstellerdaten aus Datenblättern
- Nachsehen in einer kleinen Datensammlung in ISO 13849-1:2023, Anhang C mit Rechenformeln für elektromechanische Bauelemente
- Felddaten mit baugleichen Komponenten
- 10 Jahre ansetzen



Auch zur Ermittlung des DC gibt es ein vereinfachtes Verfahren: im informativen Anhang E wird für jede Diagnosemethode ein DC geschätzt. Anschließend kann aus allen DC der Mittelwert gebildet werden. (Zweifelloos ein kühner Schritt.) Alternativ kann FMEA angewendet werden (eigentlich FMEDA).

Auch die Einhaltung der Architektur Anforderungen erledigt aus Sicht des Normenanwenders also das Säulendiagramm mit der passenden Kategorie.

- Als Rechenmethode, um von der Ebene der Bauteile auf die Ebene der Geräte, hier eines gesamten Kanals, zu schließen, darf die Parts-Count-Methode eingesetzt werden. Hierbei werden alle Ausfälle als gefährlich angenommen und alle Ausfallwahrscheinlichkeiten addiert. Dies ergibt einen zu hohen und damit konservativen Wert.
- Der Schluss von der Ebene der Kanäle auf das Gesamtsystem ergibt sich aus Sicht des Normenanwenders durch die Kategorie und das Säulendiagramm. Wenn die Werte für die Kanäle in den vorgegebenen Grenzen liegen, sind die Voraussetzungen für die Kategorie erfüllt und das Gesamtsystem erfüllt den PL.

Normen zur funktionalen Sicherheit: IEC 61508 und sektorspezifische Ausprägungen – 6. Realisierung, Architekturbeschränkungen – das Kriterium der IEC 61511

Die IEC 61511-1:2010 verlangt für Geräte, für die keine Betriebsbewährung ausgesprochen werden kann, die Erfüllung der Anforderungen der IEC 61508, also auch die Erfüllung derer Anforderungen zur Architektur.

Für die Teilsysteme (oder das Gesamtsystem) wird zusätzlich die Einhaltung der Tabelle 6 gefordert, welche keine Eigenschaften der Geräte berücksichtigt.



SIL	Minimum required HFT
1 (any mode)	0
2 (low demand mode)	0
2 (continuous mode)	1
3 (high demand mode or continuous mode)	1
4 (any mode)	2

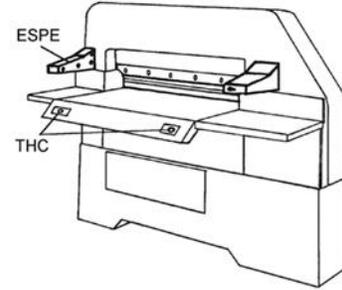
Normen zur funktionalen Sicherheit: IEC 61508 und sektorspezifische Ausprägungen – Ergebnis des Vergleichs

Kriterium	IEC 61508	IEC 61511	ISO 13849	ISO 26262
Anwendungsbereich	Für Normausschüsse	Verfahrenstechnik, Geräte nach IEC 61508	Maschinen, Anweisung für Pneumatik + Hydraulik	Automobile
Lebenszyklen & Rollenmodell	Für einzelne Anlagen	Für einzelne Anlagen	nicht beschrieben	Für Serienproduktion
Anwendungsbereich der Risikoanalyse	Alles in Zusammenhang mit der EUC	Alles in Zusammenhang mit der Anlage	Alles in Zusammenhang mit der Maschine	Alle Fehlfunktionen in Zusammenhang mit der betrachteten Funktion
Vorgehensweise bei der Risikoanalyse	Auffinden gefährlicher Situationen, Risikobewertung, Entscheidung über Risikominderung	Auffinden gefährlicher Situationen, Risikobewertung, Entscheidung über Risikominderung	Auffinden gefährlicher Situationen, Risikobewertung, Entscheidung über Risikominderung	Auffinden gefährlicher Situationen, Risikobewertung, gefährliche Situation mit ASIL klassifizieren
Spezifikation der Sicherheitsfunktion	Spezifiziere Sicherheitsfunktion mit SIL	Spezifiziere Sicherheitsfunktion mit SIL	Spezifiziere Sicherheitsfunktion mit PL	Spezifiziere Safety Goal, übernehme ASIL der Gefährdung

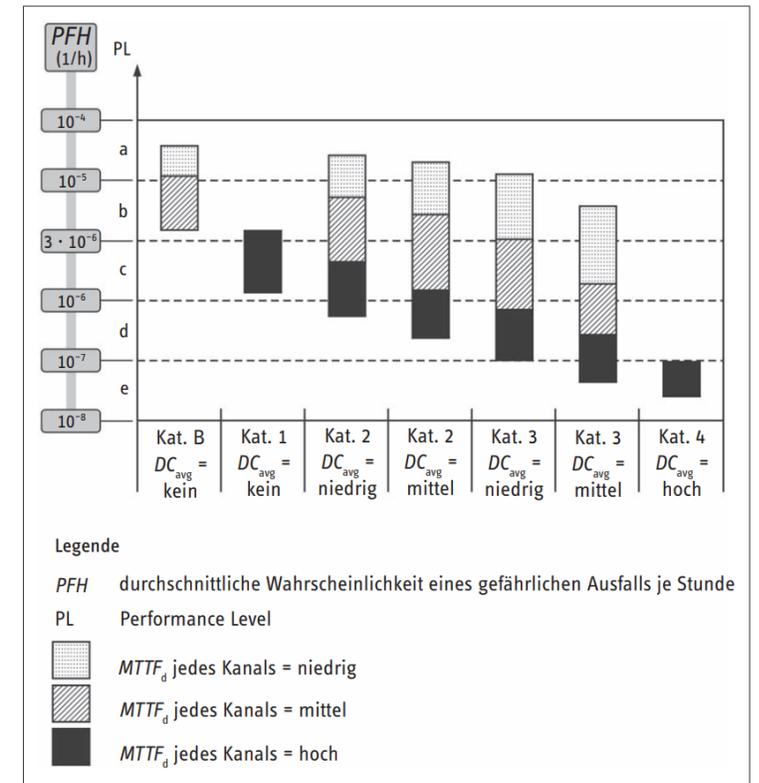
Normen zur funktionalen Sicherheit: IEC 61508 und sektorspezifische Ausprägungen – Ergebnis des Vergleichs

Kriterium	IEC 61508	IEC 61511	ISO 13849	ISO 26262
Lösungsansatz Steuerungsarchitektur	Nach Erfahrung des Projektierers	Nach Erfahrung des Projektierers	Ergibt sich aus dem PL	Nach Erfahrung des Projektierers
Begrenzung zufälliger HW-Ausfälle	Schätzung der PFH oder PFD durch zweistufigen Ansatz	Schätzung der PFD (PFH) durch zweistufigen Ansatz	Schätzung der $MTTF_D$ durch speziellen zweistufigen Ansatz	Durch spezielle Rechenvorschrift (Metrik), einstufiger Ansatz, keine Gesamt-PFH
Architektur-anforderungen	Durch Anteil sicherer Ausfälle (SFF)	Durch SIL-abhängige Tabelle	Ergibt sich durch die vorgesehene Architektur	Durch besondere Rechenvorschrift (Metrik)
Techniken & Maßnahmen	Auswahl durch SIL-abhängige Tabelle	Anforderungen im Text	Zur Validierung in ISO 13849-2	Auswahl durch SIL-abhängige Tabelle
Regelmäßige Prüfung	Informative Anleitung	Wiederkehrende Prüfungen gefordert	Erwähnt als Instandhaltungstätigkeit	Nicht erwähnt

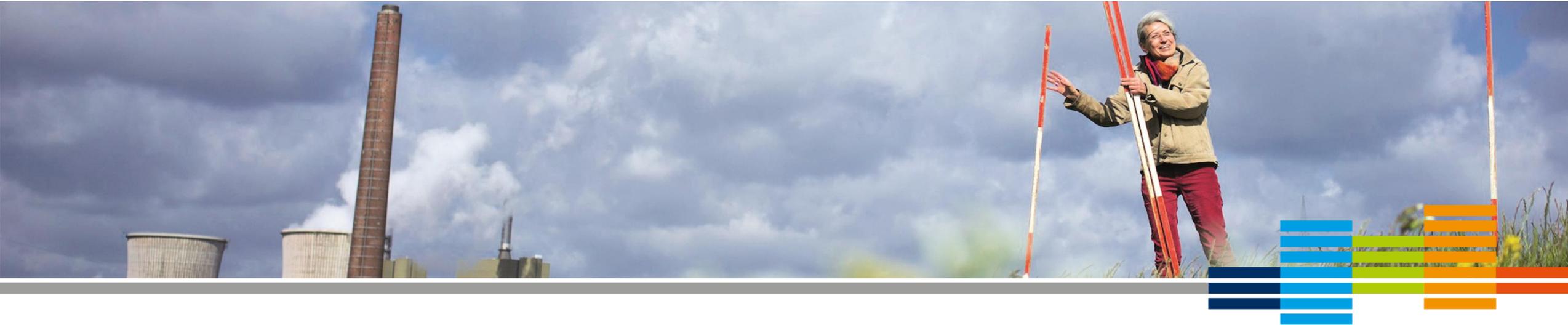
Normen zur funktionalen Sicherheit: IEC 61508 und sektorspezifische Ausprägungen — IEC 61511 - ISO 13849



Das ist auch funktionale Sicherheit – hat aber durch die Kategorien und Rechenhilfen einen anderen Rechnungsgang als bei uns. Aber ist es wirklich einfacher?



Ingo Rolle, im September 2023
 Bilder: VDE und IFA in der DGUV



Sicherheitsgerichtete Alarme in SIL

Möglich oder nicht?

Ludwig Schenk, LANUV NRW, FB 74

17.10.2023

Kurze Vorstellung



Ludwig Schenk

Lebenslauf

- | | |
|-------------|--|
| 2006 – 2011 | Studium Chemieingenieurwesen, TU Dortmund |
| 2011 – 2018 | Projektingenieur und Leiter Instandhaltung der Acetylen-Anlage/Butandiol-Anlage im Chemiepark Marl |
| 2018 – 2019 | Betriebsleiter PE2 & PE3 Rütgers Germany GmbH, Castrop-Rauxel |
| Seit 2019 | Dezernent für Anlagensicherheit beim LANUV FB 74 |

Schwerpunkte: Funktionale Sicherheit,
Explosionsschutz



Meine Tätigkeit

- Erstellung eines Sachverständigengutachten nach § 13 Abs. 1 der 9.BImSchV
- Prüfung des Sicherheitsberichts im Rahmen eines Genehmigungsverfahrens
- Teilbereich: störfallverhindernde Maßnahmen durch sicherheitsrelevante Anlagenteile aufgrund ihrer Funktion
- Zuständigkeit für alle 4er Anlagen in NRW – Chemie und Mineralölraffination
- Spezialisierung auf PLT-Sicherheitseinrichtungen



Aus der Erfahrung

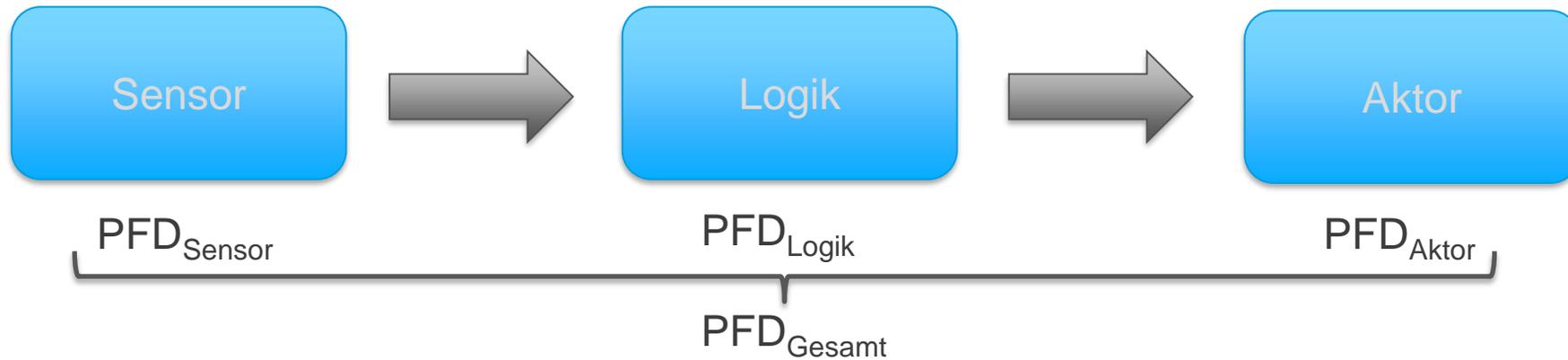
- Beispiel einer Gefahrenanalyse:

Abweichung	Ursache	Auswirkungen	Risikograph	Not. Risiko-reduzierung	Sicherheitsfunktion
W1004: Temperatur hoch	Fehlerhafte Temperaturregelung	Temperaturerhöhung ggf. bis zur Zersetzung, Überschreitung der mechanischen Integrität, Explosion	S2-A2-G1-W2	SIL2	A++ alarmiert Temperatur zu hoch im Tafelfeld. Handlung nach Betriebsanweisung

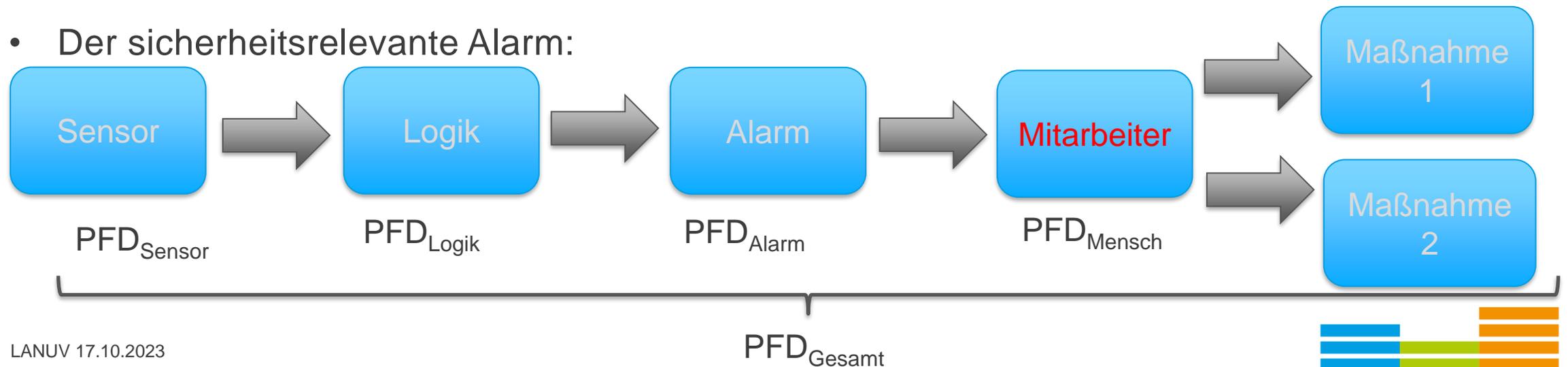


Sicherheitsrelevante Alarme?

- Die Wirkkette der PLT-Sicherheitseinrichtung:

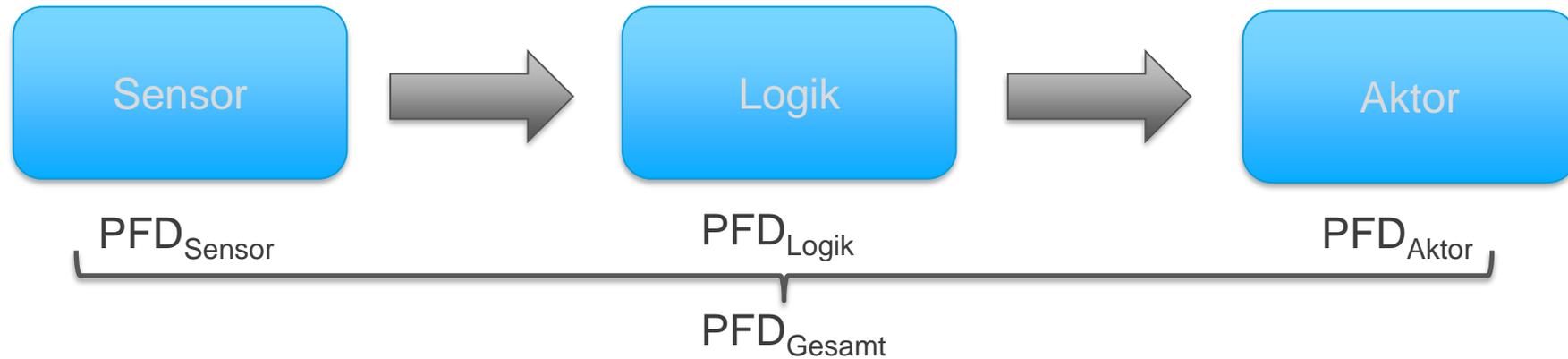


- Der sicherheitsrelevante Alarm:

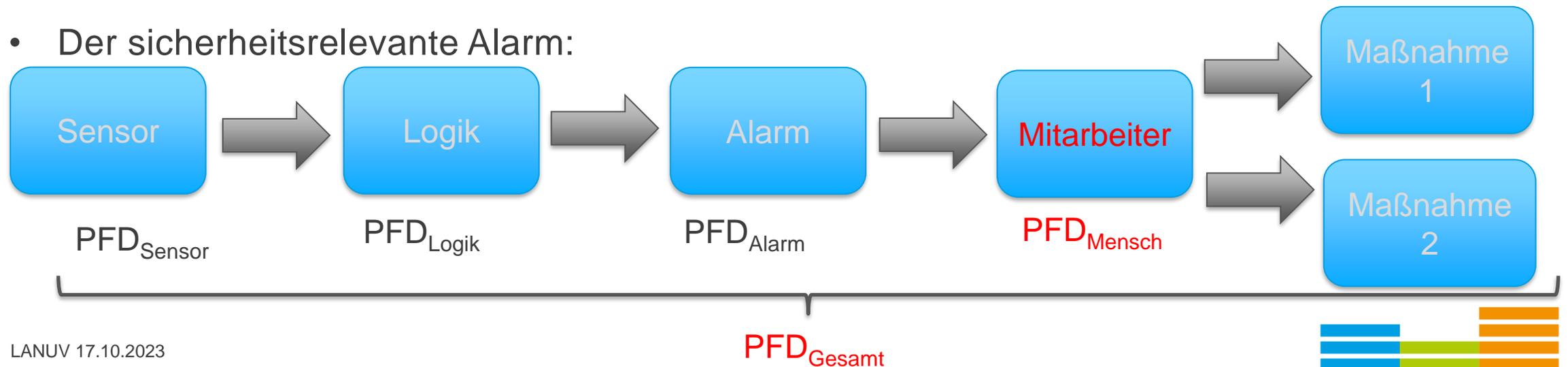


PFD-Mensch

- Die Wirkkette der PLT-Sicherheitseinrichtung:



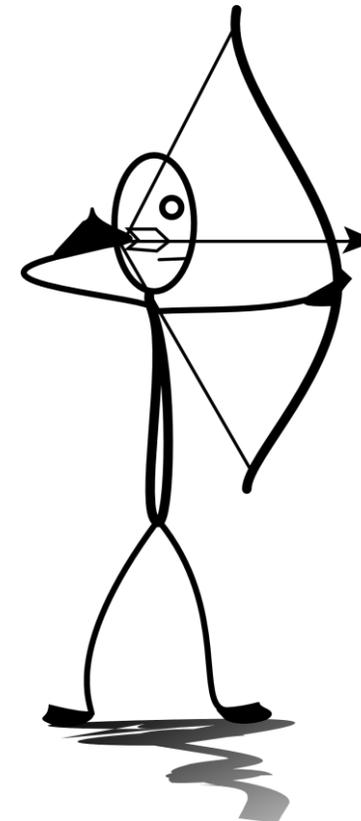
- Der sicherheitsrelevante Alarm:



PFD-Mensch

- Erkenntnisse aus der VDI 4006 Blatt 2 (2017)
- HEP (Human Error Probability) = Anzahl fehlerhafte Handlung / Anzahl aller Handlungen

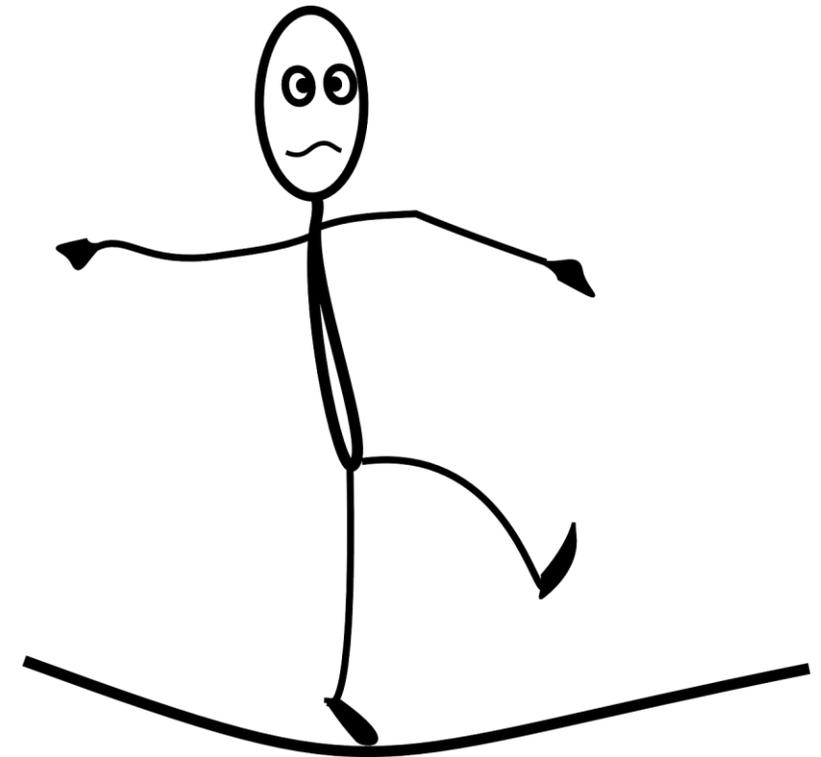
Aufgabenbeschreibung in Abhängigkeit von den situativen Anforderungen und der kognitiven Belastung	Fehlerwahrscheinlichkeit (Streubreite)
Einfache und häufig durchgeführte Aufgaben bei geringem Stress und genügend zur Verfügung stehender Zeit in gewohnten Situationen ohne Zielkonflikte	$1 \cdot 10^{-3}$ ($k = 10$)
Komplexe und häufig durchgeführte Aufgaben ohne Zielkonflikte in gewohnten Situationen mit geringem Stress und genügend zur Verfügung stehender Zeit, wobei eine gewisse Sorgfalt bei der Durchführung notwendig ist	$1 \cdot 10^{-2}$ ($k = 10$)
Komplexere und regelmäßig durchgeführte Aufgaben in ungewohnten Situationen bei hohem Stress, geringer zur Verfügung stehender Zeit oder Situationen, in denen unterschiedliche Ziele abgeglichen werden müssen	$1 \cdot 10^{-1}$ ($k = 3$)



PFD-Mensch

- Erkenntnisse aus der VDI 4006 Blatt 2 (2017)
- HEP (Human Error Probability) = Anzahl fehlerhafte Handlung / Anzahl aller Handlungen

Komplexere und selten durchgeführte Aufgaben in ungewohnten Situationen (z.B. ablenkende oder störende Einflüsse, unzureichende Rückmeldung), bei hohem Stress oder geringer zur Verfügung stehender Zeit oder ein bestehender Zielkonflikt (Widerspruch zwischen zwei oder mehreren Handlungsoptionen) innerhalb des Arbeitssystems verleiten den Operateur, eine andere als die vorgesehene Aufgabe durchzuführen.	$3 \cdot 10^{-1}$ ($k = 3$)
Hochkomplexe oder sehr selten durchgeführte Aufgaben in ungewohnten Situationen (z.B. viele unbekannte ablenkende oder störende Einflüsse, unpassende Rückmeldung), bei sehr hohem Stress oder geringer zur Verfügung stehender Zeit oder Zielkonflikte, bei denen das nicht sicherheitsgerichtete Ziel aus der Situation heraus als eindeutig plausibler erscheint	$\sim 1 \cdot 10^{-0}$



VDI/VDE 2180

- Blatt 1 - Funktionale Sicherheit in der Prozessindustrie:

PLT-Betriebsfunktion (prozessleittechnische Betriebsfunktion)

Funktion, die im →bestimmungsgemäßen Betrieb einer Anlage agiert

Beispiele: Messen, Steuern, Regeln, Überwachen, Melden und Registrieren

Anmerkung: Dazu gehören auch Funktionen, die auf Störungen des bestimmungsgemäßen Betriebs hinweisen (z.B. durch Alarmieren oder Schalten).



VDI/VDE 2180

- Blatt 1 - Funktionale Sicherheit in der Prozessindustrie:

PLT-Sicherheitsfunktion (prozessleittechnische Sicherheitsfunktion)

Funktion, die für ein bestimmtes gefährliches Ereignis einen sicheren Zustand für den Prozess erreichen oder aufrechterhalten soll

Anmerkung 1: PLT-Sicherheitsfunktionen verhindern durch einen selbsttätigen Eingriff in den Prozess eine Störung des →bestimmungsgemäßen Betriebs oder veranlassen im begründeten Ausnahmefall das Bedienpersonal durch eine Meldung zu einem Eingreifen oder sie begrenzen im Fall des Eintritts eines →gefährlichen Ereignisses die möglichen Auswirkungen dieses Ereignisses.

VDI/VDE 2180

- Blatt 1 - Funktionale Sicherheit in der Prozessindustrie:

Im Ausnahmefall können auch organisatorische Sicherheitsmaßnahmen (z. B. manuelle Bedieneingriffe nach optischen oder akustischen Alarmen) zum Einsatz kommen, wenn eine technische Maßnahme nicht möglich oder nicht sinnvoll einsetzbar ist (z. B. Raumluftüberwachung mit Alarmierung beim Überschreiten festgelegter Grenzwerte und anschließender Bedienertätigkeit). Diese organisatorischen Maßnahmen sind in der Sicherheitsbetrachtung mit zu bewerten.

VDI/VDE 2180

- Blatt 2 – Planung, Errichtung und Betrieb von PLT-Sicherheitseinrichtungen:

Bei PLT-Sicherheitsfunktionen, die eine Tätigkeit des Bedienpersonals beinhalten (z. B. Betätigen eines Stellglieds), ist dieser Teil der PLT-Sicherheitseinrichtung und muss in der Sicherheitsspezifikation vorgegeben und in einer Betriebsanweisung geregelt sein. Eine erforderliche Alarmierung (akustischer/optischer Alarm) ist als Teil der PLT-Sicherheitsfunktion auszuführen und muss sich von betrieblichen Meldungen deutlich unterscheiden.

VDI/VDE 2180

- Blatt 3: Nachweis der Ausfallwahrscheinlichkeit im Anforderungsfall

**Keine Nennung von
sicherheitsrelevanten Alarmen
oder menschlichen Eingriffen**



VDI/VDE 2180

- Blatt 3: Nachweis der Ausfallwahrscheinlichkeit im Anforderungsfall

SIL	PFD _{gesamt}
1	$\geq 10^{-2}$ bis $< 10^{-1}$
2	$\geq 10^{-3}$ bis $< 10^{-2}$
3	$\geq 10^{-4}$ bis $< 10^{-3}$

vs.

Aufgabenbeschreibung in Abhängigkeit von den situativen Anforderungen und der kognitiven Belastung	Fehlerwahrscheinlichkeit (Streubreite)
Einfache und häufig durchgeführte Aufgaben bei geringem Stress und genügend zur Verfügung stehender Zeit in gewohnten Situationen ohne Zielkonflikte	$1 \cdot 10^{-3}$ ($k = 10$)
Komplexe und häufig durchgeführte Aufgaben ohne Zielkonflikte in gewohnten Situationen mit geringem Stress und genügend zur Verfügung stehender Zeit, wobei eine gewisse Sorgfalt bei der Durchführung notwendig ist	$1 \cdot 10^{-2}$ ($k = 10$)
Komplexere und regelmäßig durchgeführte Aufgaben in ungewohnten Situationen bei hohem Stress, geringer zur Verfügung stehender Zeit oder Situationen, in denen unterschiedliche Ziele abgeglichen werden müssen	$1 \cdot 10^{-1}$ ($k = 3$)

Kritische Fragen



- Welche Begründung führt zum Ausnahmefall, dass ein sicherheitsrelevanter Alarm der vollautomatisierten Sicherheitseinrichtung vorgezogen wird?
- Wie viele solcher Alarme und entsprechender Betriebsanweisungen sind pro Mitarbeitenden relevant?
- Ist die Handlungsanweisung der Betriebsanweisung ausreichend einfach und überschaubar, dass die Maßnahmen korrekt ausgeführt werden können?
- Herrscht ausreichende Reaktionszeit für die Mitarbeitenden zur Einleitung der Maßnahmen?
- Wie wird sichergestellt, dass solche Alarme bei einem Ereignis z.B. durch Alarmflut nicht übersehen/überhört werden?
- Wie gestaltet die Betreiberin die Funktionsprüfung eines solchen Alarms? Werden dafür Probealarme durchgeführt?



Haben Sie Fragen?



Vielen Dank für Ihre Aufmerksamkeit

Dipl. Ing. Ludwig Schenk

FB 74: Umwelttechnik und Anlagensicherheit für Chemie und Mineralölraffination

Postanschrift: Landesamt für Natur, Umwelt und Verbraucherschutz NRW, 40208 Düsseldorf

Dienstort: Wallneyer Straße 6, 45133 Essen

Telefon: +49 (0)2361 305-1104

Fax: +49 (0)2361 305-1910

E-Mail: Ludwig.schenk@lanuv.nrw.de

www.lanuv.nrw.de

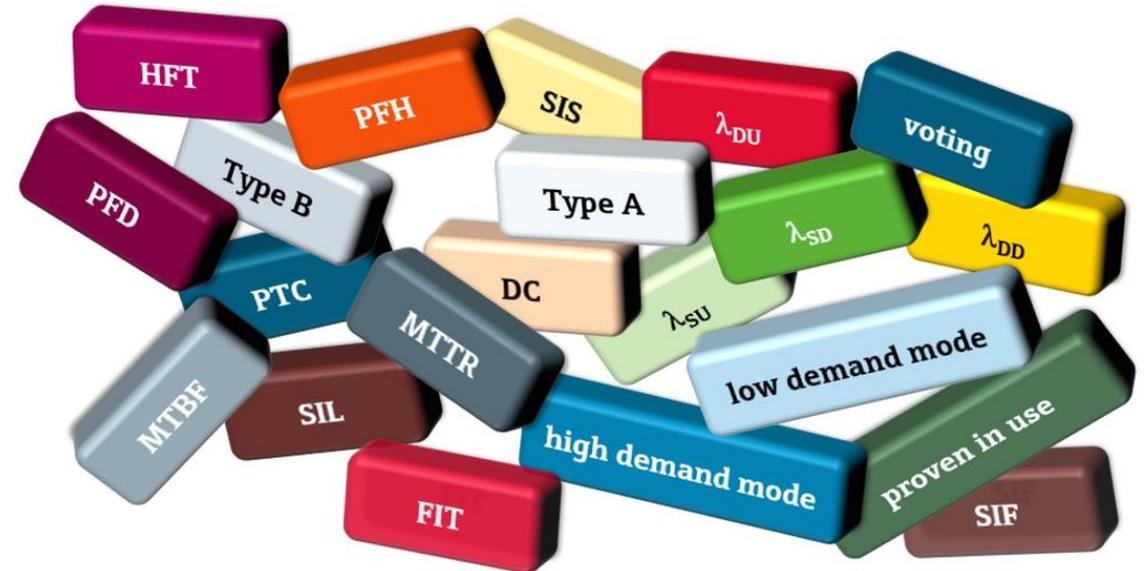
Übersetzung SIL <-> PL – wo geht's schief?

SIL Sprechstunde Mannheim 20./21.09.2023



Übersetzung SIL <-> PL – wo geht's schief?

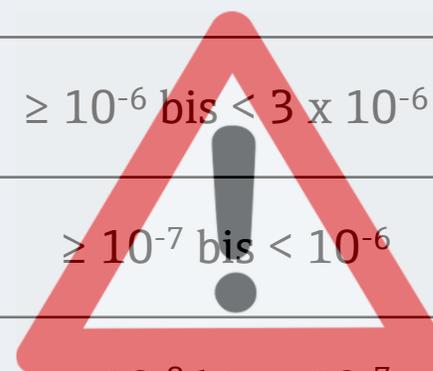
- Kurzer Vergleich funktionale Sicherheit
Prozessindustrie – Maschinensicherheit
- Verwendete Normen: DIN EN ISO13849,
DIN EN 61511, DIN EN 61508
- Praxisbeispiele
 - High Demand Mode – Low Demand Mode
 - Diagnose
 - SIL 2 – PL d
 - Mehrkanalige Strukturen



Übersetzung SIL <-> PL – wo geht's schief?

Beziehung zwischen der Norm „Performance Level [PL]“ und „SIL Level“ auf der Basis der **Ausfallwahrscheinlichkeit**

Performance Level [PL] DIN EN ISO 13849	Mittlere Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde [1/h]	SIL gemäß IEC 61508
a	$\geq 10^{-5}$ bis $< 10^{-4}$	Keine besonderen Anforderungen
b	$\geq 3 \times 10^{-6}$ bis $< 10^{-5}$	SIL1
c	$\geq 10^{-6}$ bis $< 3 \times 10^{-6}$	SIL 1
d	$\geq 10^{-7}$ bis $< 10^{-6}$	SIL 2
e	$\geq 10^{-8}$ bis $< 10^{-7}$	SIL 3



Systemarchitekturen nach IEC 61508 / 61511

Fehlertoleranz des Teilsystems Sensorik

Route 1H
der IEC 61508
Design

Route 2H
der IEC 61508
Proven-in-use

Tabelle 6
der IEC 61511
Prior-use

Table 3 – Maximum allowable safety integrity level for a safety function carried out by a type B safety-related element or subsystem

Safe failure fraction of an element	Hardware fault tolerance		
	0	1	2
<60 %	Not Allowed	SIL 1	SIL 2
60 % – <90 %	SIL 1	SIL 2	SIL 3
90 % – <99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

SIL 3 → 2 kanalig (1oo2)

Table 6 – Minimum HFT requirements according to SIL

SIL	Minimum required HFT
1 (any mode)	0
2 (low demand mode)	0
2 (high demand or continuous mode)	1
3 (any mode)	1
4 (any mode)	2

SIL 3 → 2 kanalig (mit Betriebsbewährung)

Übersetzung SIL <-> PL – wo geht's schief?

- **EN 13849**
 - High-Demand Mode
 - Steuerungen inkl. Hydraulik und Pneumatik
- **Umsetzung von Sicherheitsfunktionen**
 - Systemarchitektur bestimmt durch Kategorie, DC und Massnahmen gegen CCF
 - pfh-Werte
 - Bauteilezuverlässigkeit (MTTF-Werte)
 - Fehlererkennung (DC)
 - Resistenz gegen Fehler mit gemeinsamer Ursache wie EMV, Umwelt, systematische Fehler (CCF)

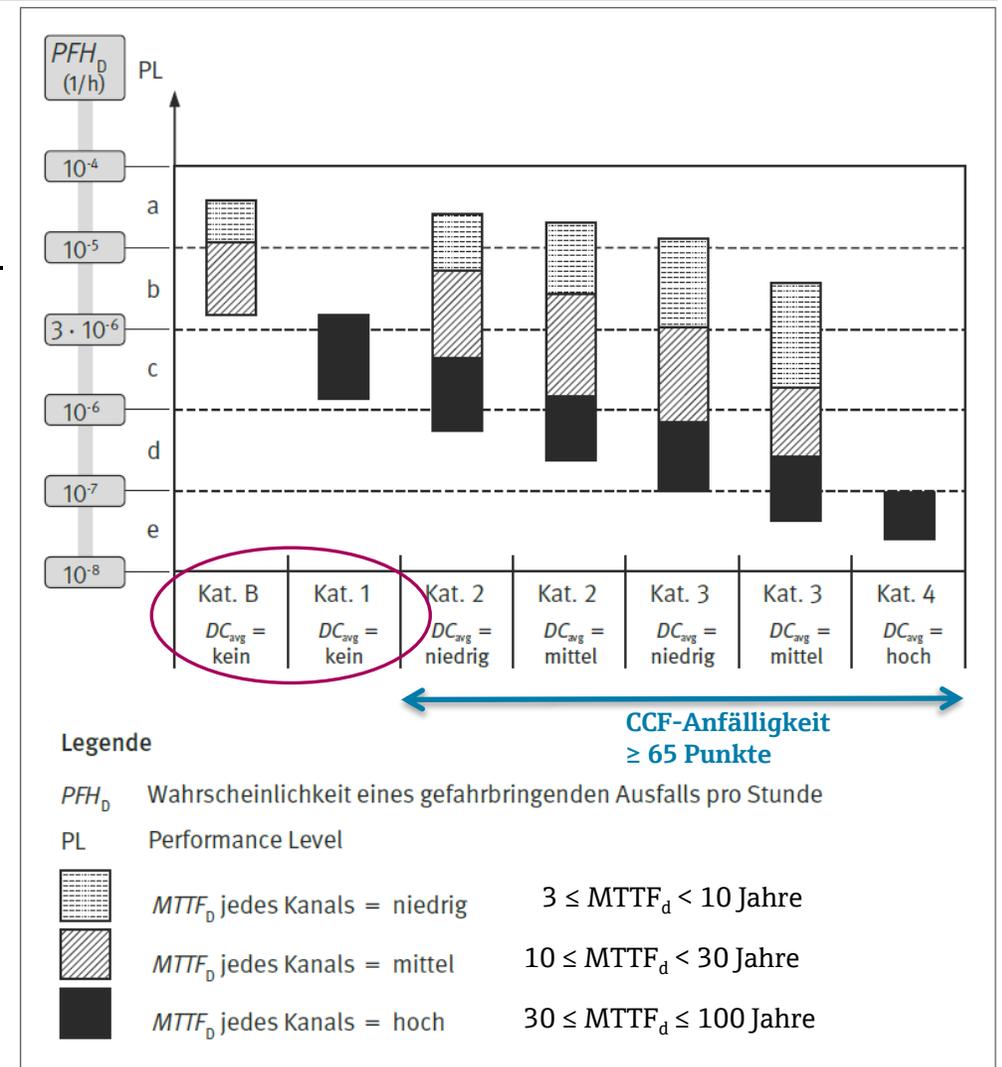
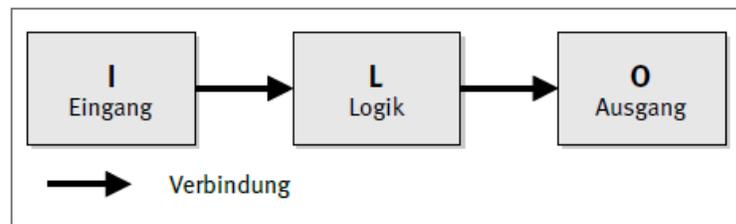
Bewertung und Verifikation z.B. mit SISTEMA

Übersetzung SIL <-> PL – wo geht's schief?

Vorgesehene Architekturen EN 13849

- B: Basiskategorie
- 1: Erhöhte Widerstandsfähigkeit gegen Fehler, sicherheitstechnisch bewährte Bauteile und Prinzipien
- Überwiegend durch BauteilAuswahl charakterisiert
- Beim Auftreten eines Fehlers: Sicherheitsfunktion kann unwirksam werden

Vorgesehene Architektur für Kategorie B und Kategorie 1

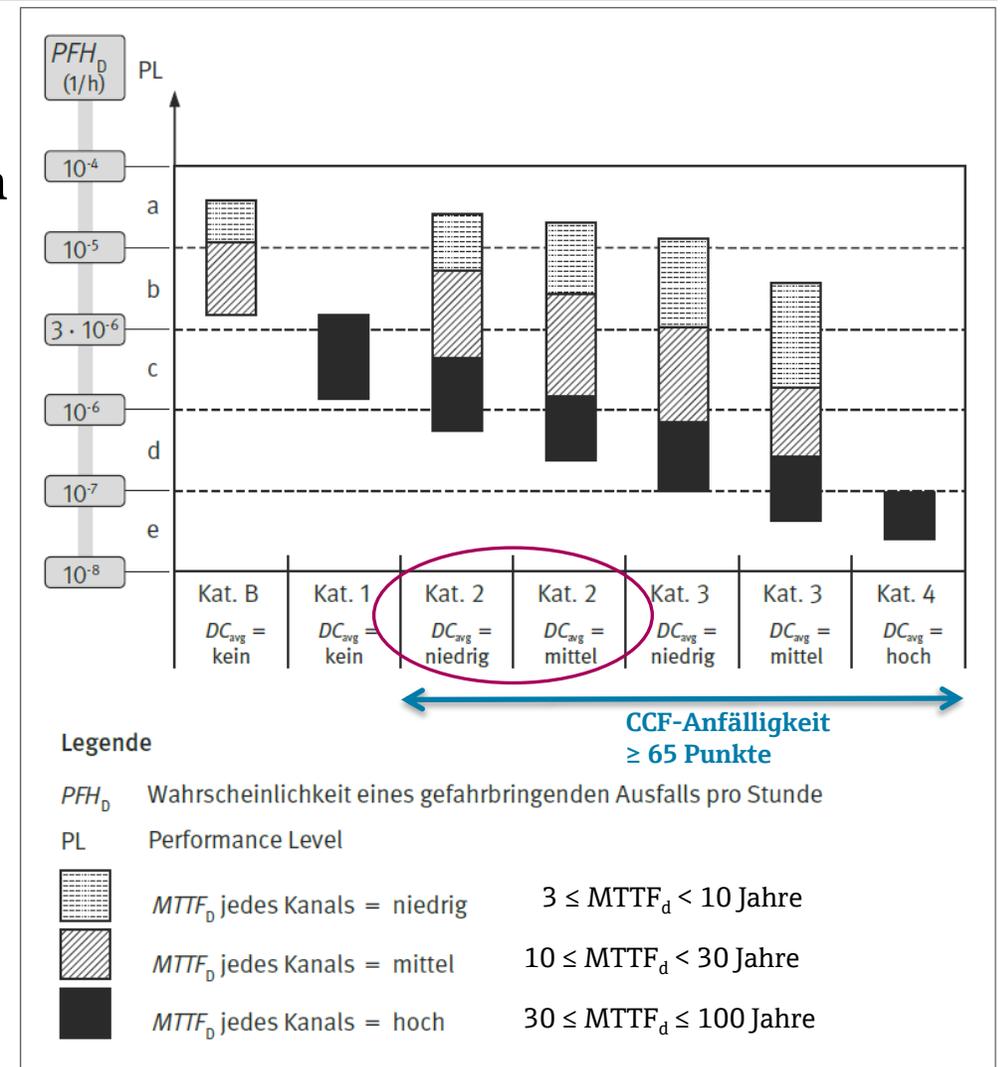
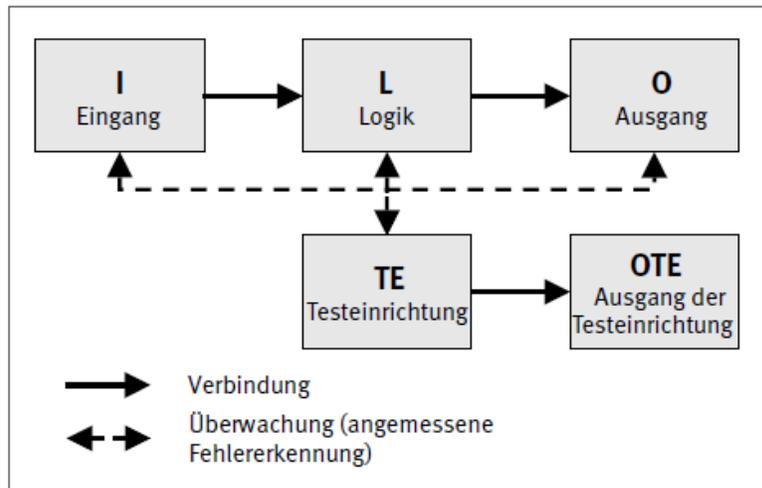


Übersetzung SIL <-> PL – wo geht's schief?

Vorgesehene Architekturen EN 13849

- Überprüfung der Sicherheitsfunktion in regelmässigen Abständen durch Testeinrichtung
- Zwischen den Tests: Sicherheitsfunktion kann ausfallen -> Diagnoseintervall

Vorgesehene Architektur für Kategorie 2; gestrichelte Linien kennzeichnen vernünftigerweise durchführbare Fehlererkennung

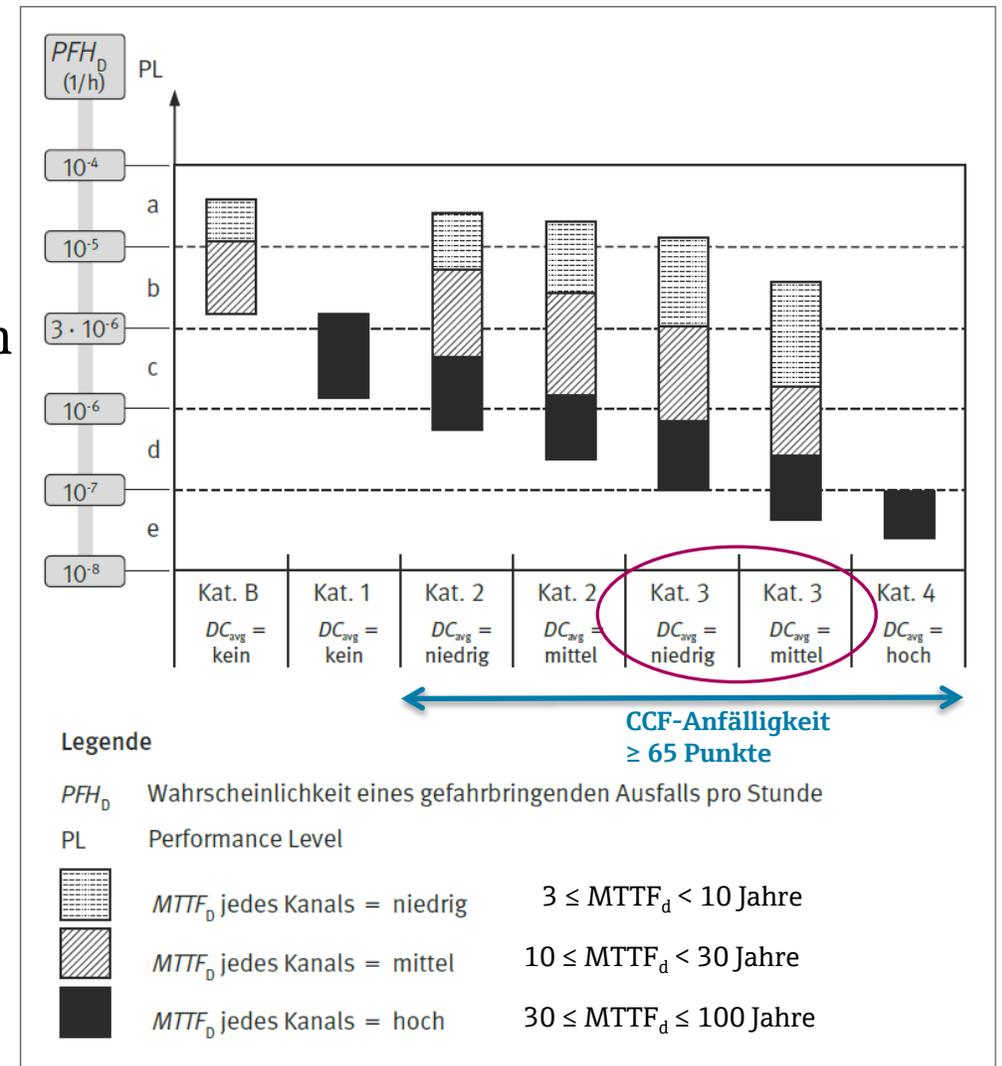
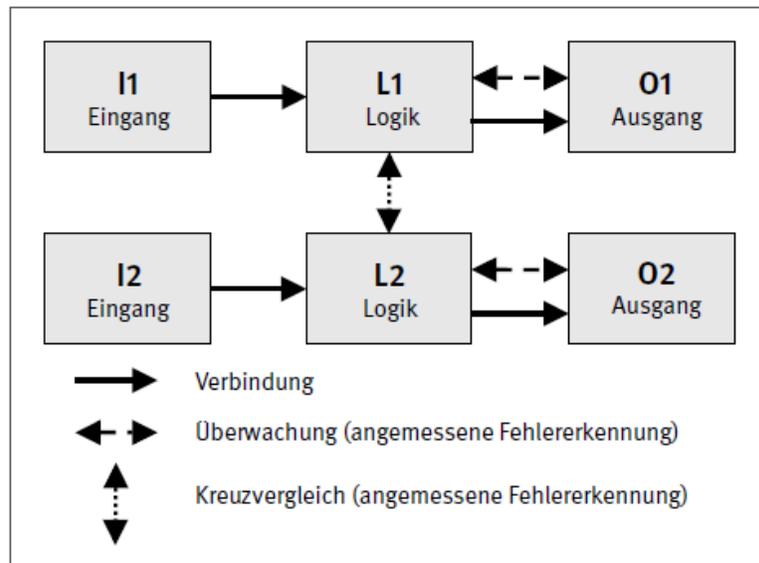


Übersetzung SIL <-> PL – wo geht's schief?

Vorgesehene Architekturen EN 13849

- Selbsttätige Erkennung von Fehlern, wenn angemessen
- Bei Einzelfehlern: Kein Verlust der Sicherheitsfunktion

Vorgesehene Architektur für Kategorie 3: gestrichelte Linien kennzeichnen vernünftigerweise durchführbare Fehlererkennung

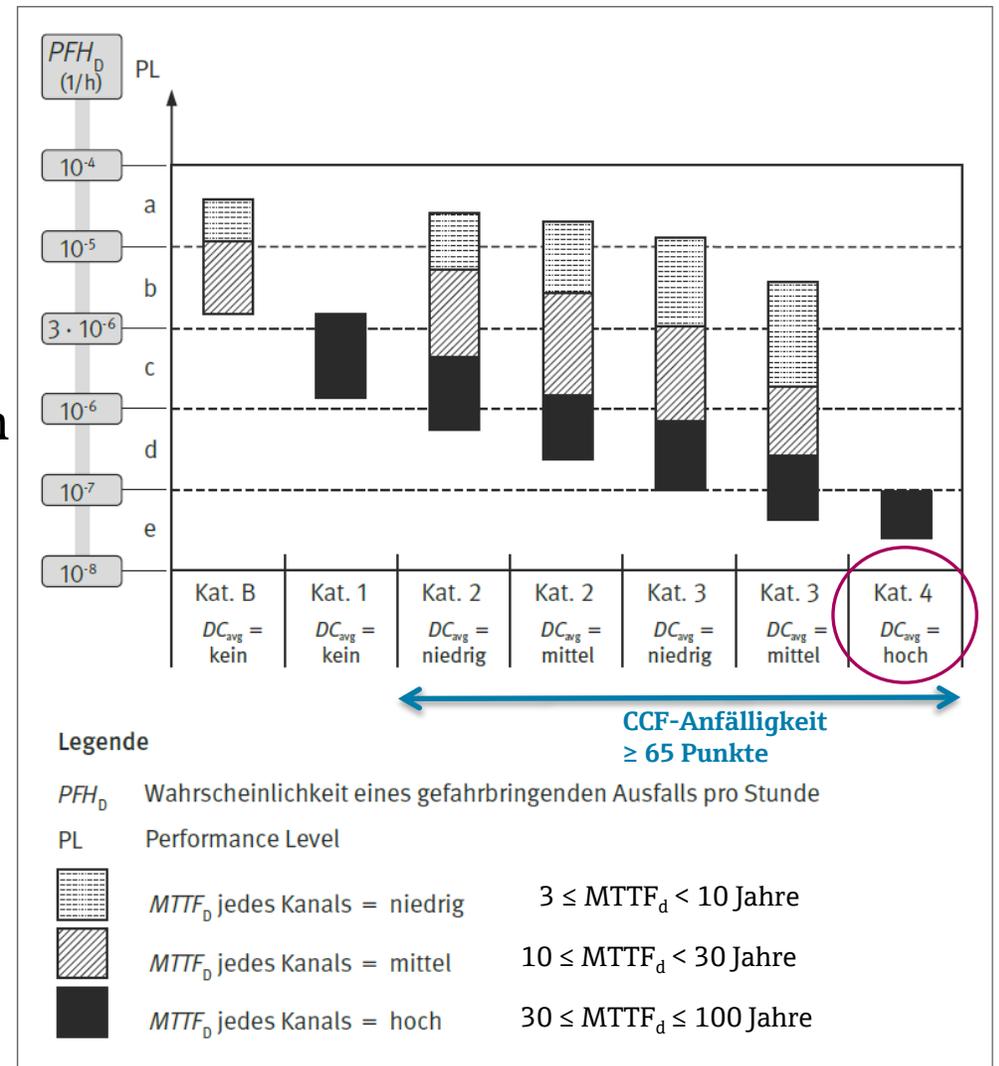
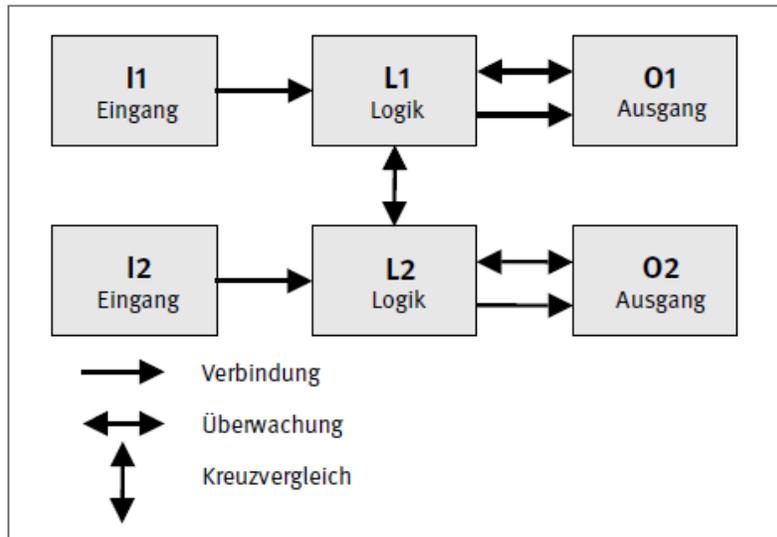


Übersetzung SIL <-> PL – wo geht's schief?

Vorgesehene Architekturen EN 13849

- Selbsttätige Erkennung von Fehlern
- Widerstandsfähigkeit gegenüber Anhäufung unmerkter Fehler
- Bei Einzelfehlern: Kein Verlust der Sicherheitsfunktion

Vorgesehene Architektur für Kategorie 4



Vergleich Sicherheitsnorm der Maschinenrichtlinie / Prozessindustrie

Norm	DIN EN ISO 13849	DIN EN IEC 61511 / 61508
Titel	Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen	Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie
Anwendungsbereich	Steuerungen inkl. Hydraulik und Pneumatik <i>Eher einzelne Maschinen</i>	Elektrische/elektronische/programmierbare elektronische Systeme <i>Meist größere Anlagen</i>
	High Demand Mode	Vorw. Low Demand Mode
Klassifizierung	Performance Level PL a-e	Safety Integrity Level SIL 1-4
Kennzahlen	Kategorie (B, 1-4), MTTF, DC, CCF	PFD, HFT, SFF (nur 61508), (pfh)
Architektur bestimmt durch	PL; vorgeg. Kategorie, DC, CCF	SIL; HFT, SFF (nur 61508)
Sonstiges	Setzt stark auf automatisierte Diagnose, DC	Wiederkehrende Prüfungen

Vergleich Sicherheitsnorm der Maschinenrichtlinie / Prozessindustrie

DIN EN ISO 13849

Kat.	Max. PL *	DC **
B	b	<60%
1	c	<60%
2	d	>60%
3	e	>90%
4	e	≥99%

HFT 0
HFT >0

IEC 61511 (Tab. 6)

HFT	Low / High Demand	SIL
0	L+H	1
0	L	2
1	H	2
1	H	3

HFT 0
HFT >0

IEC 61508 (Tab. 3, Typ B)

HFT	SFF **	SIL
0	<60%	-
0	60..90%	1
0	90..99%	2
0	≥99%	3
1	<60%	1
1	60..90%	2
1	90..99%	3
1	≥99%	4
2	<60%	2
2	60..90%	3
2	90..99%	4
2	≥99%	4

HFT 0
HFT >0

* Unter der Voraussetzung geeigneter MTTF-Werte

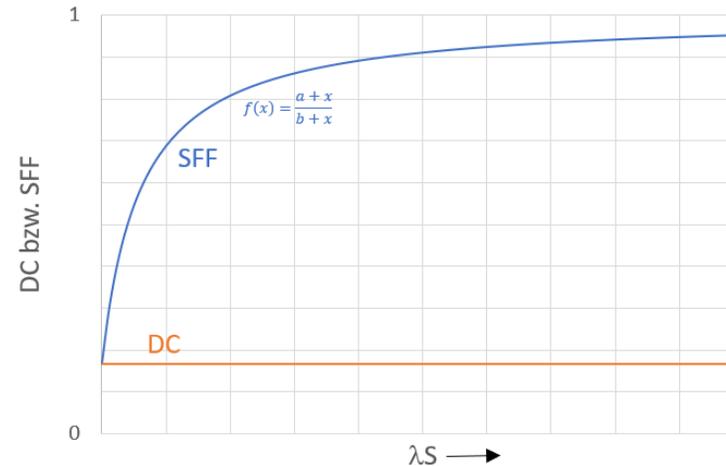
** In praktischen Fällen ist SFF immer höher als DC

Übersetzung SIL <-> PL – wo geht's schief?

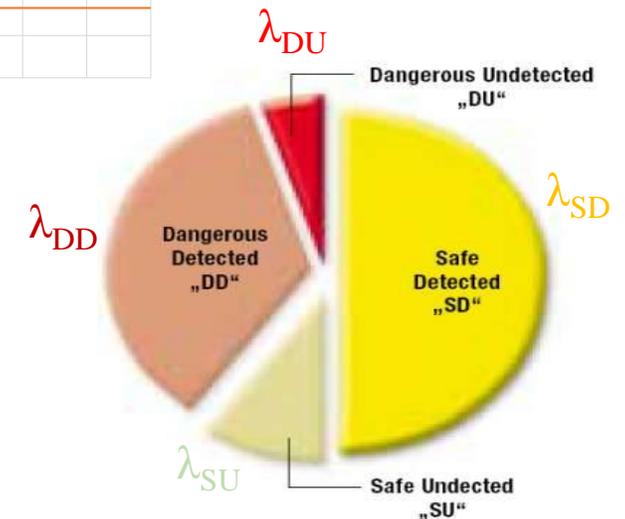
„Vergleich“ DC (Diagnosedeckungsgrad) und SFF (Safe Failure Fraction)

$$DC = \frac{\lambda_{DD}}{\lambda_{DD} + \lambda_{DU}} = \frac{\lambda_{DD}}{\lambda_D}$$

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



- In praktischen Fällen ist SFF immer höher als DC
- SFF „belohnt“ die sicheren Fehler im Entwurf
- DC „bestraft“ das Vorhandensein sicherer Fehler



Übersetzung SIL <-> PL – wo geht's schief?

■ Vergleich FTL81 + FTL825

FMEDA		
Safety function	MIN	MAX
$\lambda_{DU}^{2),3)}$	5 FIT	5 FIT
$\lambda_{DD}^{2),3)}$	120 FIT	120 FIT
$\lambda_{SU}^{2),3)}$	105 FIT	105 FIT
$\lambda_{SD}^{2),3)}$	1280 FIT	1280 FIT
SFF	99,7%	99,7%
$PFD_{avg} (T_1 = 1 \text{ year})^3)$ (single channel architecture)	$2.08 \cdot 10^{-5}$	$2.08 \cdot 10^{-5}$
PFH	$4.74 \cdot 10^{-9} \text{ 1/h}$	$4.74 \cdot 10^{-9} \text{ 1/h}$
PTC ⁴⁾ A / B	90% / 34%	90% / 34%
$\lambda_{total}^{2),3)}$	1510 FIT	1510 FIT
Diagnostic test interval ⁵⁾	$\leq 60 \text{ s} / \leq 30 \text{ min}$	$\leq 60 \text{ s} / \leq 30 \text{ min}$
Fault reaction time ⁶⁾	$\leq 2.5 \text{ s}$	$\leq 2.5 \text{ s}$

SFF = 99,7 % (hoch)

$$DC = \frac{\lambda_{dd}}{\lambda_{dd} + \lambda_{du}} = 96 \% \text{ (mittel)}$$



High-Demand Mode - Low-Demand Mode

→ **Beispiel: In der Prozessindustrie oft Low-Demand Mode, in der Maschinenwelt High-Demand oder Continuous Mode**

- Oft gestellte Frage: Kann man Komponenten, welche für den Low-Demand Mode spezifiziert sind, auch für den High-Demand Mode nutzen?
- Weiterhin Umgang mit den sicherheitstechnischen Kennwerten, welche nach DIN EN ISO 13849 benötigt werden, Ableitung eines PL's
- Und wie verhält es sich mit der Diagnosehäufigkeit?



High-Demand Mode - Low-Demand Mode

- Anwendung von Komponenten im High-Demand Mode, welche für den Low-Demand-Mode spezifiziert sind
- **Beispiel: Cerabar S PMC71**
- Einsatz der Komponente im High-Demand-Mode möglich?
- Umgang mit den sicherheitstechnischen Kennwerten nach IEC 61508 und Ableitung des Performance Levels PL?
- Sicherheitstechnische Kennwerte auch nach EN ISO 13849-1?



High-Demand Mode - Low-Demand Mode

- Generell sind die Sicherheitskennwerte (SIL, Ausfallraten, Safe-Failure-Fraction, Hardwarefehlertoleranz) in der Sonderdokumentation SD für den **Low-Demand-Mode** spezifiziert.
- Hier: *SD00190P, Cerabar S PMC71*
- **Fragen:** Einsatz der Komponente im High-Demand-Mode möglich? Umgang mit den sicherheitstechnischen Kennwerten nach IEC 61508 und Ableitung des Performance Levels PL?

Kenngrößen-Profil A mit Meldung E727 (Druck übersteuert) als Alarm

PMC71 Standard, Ex i

Kenngröße gemäß IEC 61508	Wert		
Sicherheitsfunktionen	MIN, MAX, Bereich		
SIL (Hardware)	<ul style="list-style-type: none"> ■ 2 (einkanalig), ■ 3 (mit SIL 3-fähiger Auswahlschaltung) 		
SIL (Software)	3		
Gerätetyp	B		
Betriebsart	Low demand mode		
Sicherheitsfunktionen	MIN	MAX	Bereich
λ_{zd}	52 FIT	367 FIT	419 FIT
λ_{zu}	392 FIT	392 FIT	392 FIT
λ_{dd}	367 FIT	52 FIT	0 FIT
λ_{du}	80 FIT	80 FIT	80 FIT
$\lambda_{tot}^{1)}$	1128 FIT		
MTBF _{tot} ¹⁾	101 Jahre		
SFF	91,0%		
PF _{avg} für T ₁ = 1 Jahr (einkanalig) ²⁾	3,50 × 10 ⁻⁴		
Diagnose-Testintervall ³⁾	5 min (RAM, ROM, ...), 1 s (Messumformung)		
Fehlerreaktionszeit ⁴⁾	5 min (RAM, ROM, ...), 10 s (Messumformung)		
Einschwingzeit ⁵⁾	→ Technische Information TI00383P/00/DE, Abschnitt "Totzeit, Zeitkonstante (T63)"		

High-Demand Mode - Low-Demand Mode

Vorgehensweise:

- Abprüfen: Sind evtl. Bauteile in der Komponente enthalten, die einem **Verschleiß** unterliegen, z.B. mechanische oder elektromechanische Bauteile wie z.B. Relais?
- *Hier: Beim Cerabar S sind keine elektromechanischen oder mechanischen Bauteile in der Funktionskette, so dass auch im High-Demand-Mode nicht mit Verschleiß zu rechnen ist.*



High-Demand Mode - Low-Demand Mode

- Ohne verschleißbehaftete Bauteile, z.B. bei elektronischen Komponenten, welche ohnehin während des Betriebs dauerhaft in Betrieb sind, muss kein Unterschied zwischen Low-Demand-Mode und High-Demand-Mode gemacht werden, und die spezifizierten Ausfallraten können auch für den High-Demand-Mode verwendet werden.
- Dann ist $pfh_D \approx \lambda_{DU}$ und $MTTF_D \approx \frac{1}{\lambda_{DU}}$
- Oder im schlechtesten Fall: $pfh_D \approx \lambda_{DU} + \lambda_{DD}$
Das entspricht dem Fall, wenn keine Diagnose im Gerät vorhanden wäre, stellt also eine konservative Betrachtungsweise dar.

High-Demand Mode - Low-Demand Mode

- Beispiel Cerabar S:
- *Beim Cerabar S sind keine elektromechanischen oder mechanischen Bauteile in der Funktionskette, so dass auch im High-Demand-Mode nicht mit Verschleiß zu rechnen ist.*

Cerabar S PMC71 Standard, Ex i mit Kenngrößenprofil A mit Meldung „Druck übersteuert“ als Alarm, MIN:

$$pfh_D = \lambda_{DU} + \lambda_{DD} = 80FIT + 367FIT = 4,47 \cdot 10^{-7} \text{ 1/h} \quad (\text{konservative Betrachtung})$$

$$pfh_D = \lambda_{DU} = 80FIT = 8 \cdot 10^{-8} \text{ 1/h}$$

(Diagnose-Testintervall!)

Achtung, hier bei ist unbedingt das
Diagnose-Testintervall zu
berücksichtigen!



High-Demand Mode - Low-Demand Mode

Vorgehensweise:

- Beachtung des **Diagnose-Testintervalls**
In beiden Normen, DIN EN ISO 13849 und IEC 61508-2 muss im High-Demand-Mode für eine wirksame Diagnose die interne Diagnoserate 100x größer sein als die erwartete mittlere Anforderungsrate der Schutzfunktion.
- Dies ist im Anwendungsfall auf Plausibilität zu prüfen, ansonsten ist der konservative Ansatz zu wählen ($pfh_D = \lambda_{DU} + \lambda_{DD}$).

— für Kategorie 2, Anforderungsrate $\leq 1/100$ der Testrate (siehe auch die Anmerkung in Anhang K); oder die Prüfung erfolgt unmittelbar bei Anforderung der Sicherheitsfunktion und die Gesamtzeit zum Erkennen des Ausfalls und zur Überführung der Maschine in einen nicht gefahrbringenden Zustand (in der Regel wird die Maschine angehalten) ist kürzer als die Zeit bis zum Erreichen der Gefährdung (siehe auch ISO 13855); DIN EN ISO 13849-1 4.5.4

High-Demand Mode - Low-Demand Mode

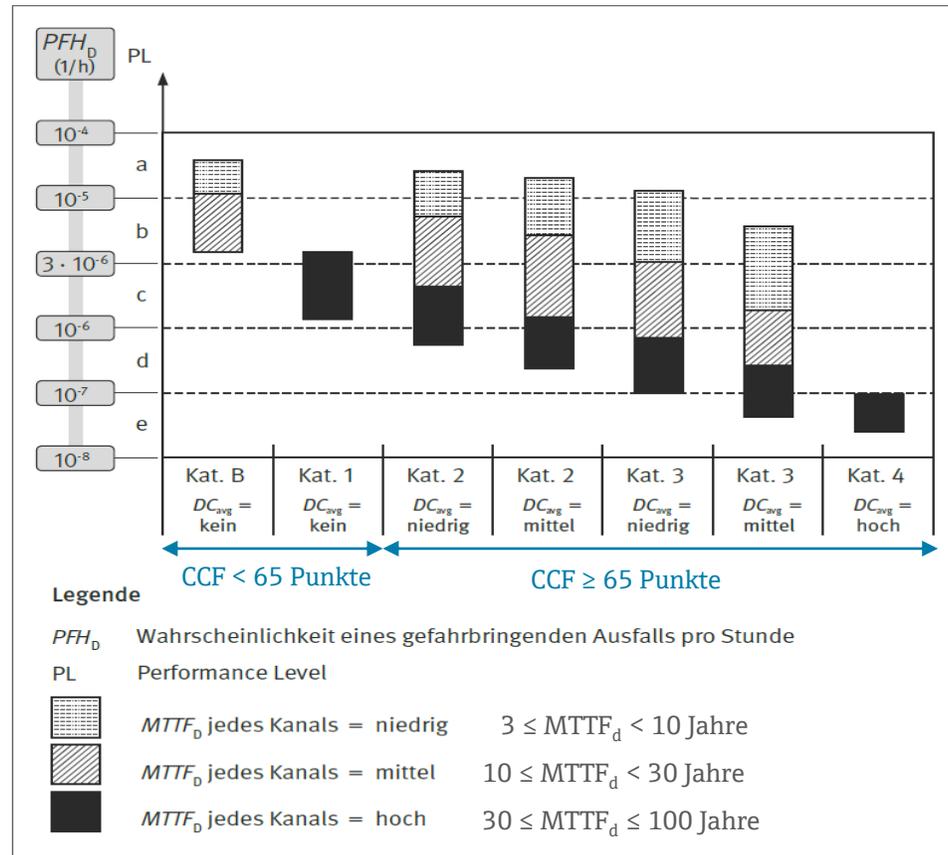
- Beispiel Cerabar S:
- *Im Cerabar S wird die interne Diagnose alle 5 min ausgeführt, die Fehlerreaktionszeit beträgt 5 min, was im schlechtesten Fall 10min ausmacht. Daher darf die Schutzfunktion nicht häufiger als alle 1000 min $\cong 17$ h ausgelöst werden, was im konkreten Anwendungsfall auf Plausibilität zu überprüfen ist. Ansonsten ist der konservative Ansatz zu wählen ($\text{pfh}_D \approx \lambda_{DU} + \lambda_{DD}$).*



High-Demand Mode - Low-Demand Mode

Vorgehensweise:

- Beachtung der Architektur Anforderungen nach DIN EN ISO 13849:



Kategorie	Kanal	DC_{avg}
B	1	kein
1	1	kein
2	1	niedrig ... mittel
3	2	niedrig ... mittel
4	2	hoch

Die **Kategorie** hängt von der Fehlertoleranz (Anzahl redundanter Kanäle) und der Diagnose gefährlicher Fehler ab. Außer bei Systemen der Kategorie B müssen bewährte Bauteile oder Bauteile mit Einhaltung bewährter Sicherheitsprinzipien verwendet werden. Der **Diagnosedeckungsgrad** (DC_{avg}) wird in „niedrig“ ($\geq 60\%$), „mittel“ ($\geq 90\%$) und „hoch“ ($\geq 99\%$) eingeteilt und hängt von den Diagnosemaßnahmen des Systems ab (siehe Tabelle E.1 der DIN EN ISO 13849-1).

$$\text{Oder: } DC = \frac{\lambda_{DD}}{\lambda_{DD} + \lambda_{DU}}$$

High-Demand Mode - Low-Demand Mode

Beispiel Cerabar S:

- Mit $\lambda_{DU} = 80$ FIT ergibt sich ein hoher Wert von $MTTF_D = 1426$ Jahren. (In ISO 13849-1 werden nur 100 Jahre berücksichtigt).
- Mit bewährten Bauteilen und Sicherheitsprinzipien entspricht der Cerabar S der Kategorie 1.
- Nach Tabelle 7 der ISO 13849-1 wird damit ein PL c erreicht.
- Die Architekturanforderungen nach DIN EN ISO 13849 für die komplette Schutzeinrichtung sind durch den Betreiber zu erfüllen.

- *Bemerkung: Die neue Generation Druckmessgeräte Evo 2 ist von vornherein für Low- und High-Demand Mode betrachtet worden. Ebenso sind pfh-Werte angegeben.*



Übersetzung SIL <-> PL – wo geht's schief?

→ Konkret: Sicherheitsfunktionen mit SIL 2 und PL d im Vergleich

- In der Prozessindustrie werden oft Sicherheitsfunktionen mit SIL 2 benötigt.
- Vergleich auf Basis der **Ausfallwahrscheinlichkeit:**

Performance Level (PL)	Durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde (PFH _d) 1/h	SIL (IEC 61508-1, zur Information) hohe / kontinuierliche Betriebsart
a	$\geq 10^{-5}$ bis $< 10^{-4}$	keine Entsprechung
b	$\geq 3 \cdot 10^{-6}$ bis $< 10^{-5}$	1
c	$\geq 10^{-6}$ bis $< 3 \cdot 10^{-6}$	1
d	$\geq 10^{-7}$ bis $< 10^{-6}$	2
e	$\geq 10^{-8}$ bis $< 10^{-7}$	3

- Die Ausfallwahrscheinlichkeiten verleitet zu der Annahme, dass ein SIL 2 immer einem PL d entspricht. Das ist aber nicht der Fall!
- Ausfallwahrscheinlichkeiten sind aber nur ein Aspekt, es fehlt die Systemarchitektur!

Konkret: SIL 2 und PL d im Vergleich

- Systemarchitektur SIL 2 in der Prozessindustrie und PL d in der Maschinenwelt:

Bild 5 der DIN EN ISO 13849-1

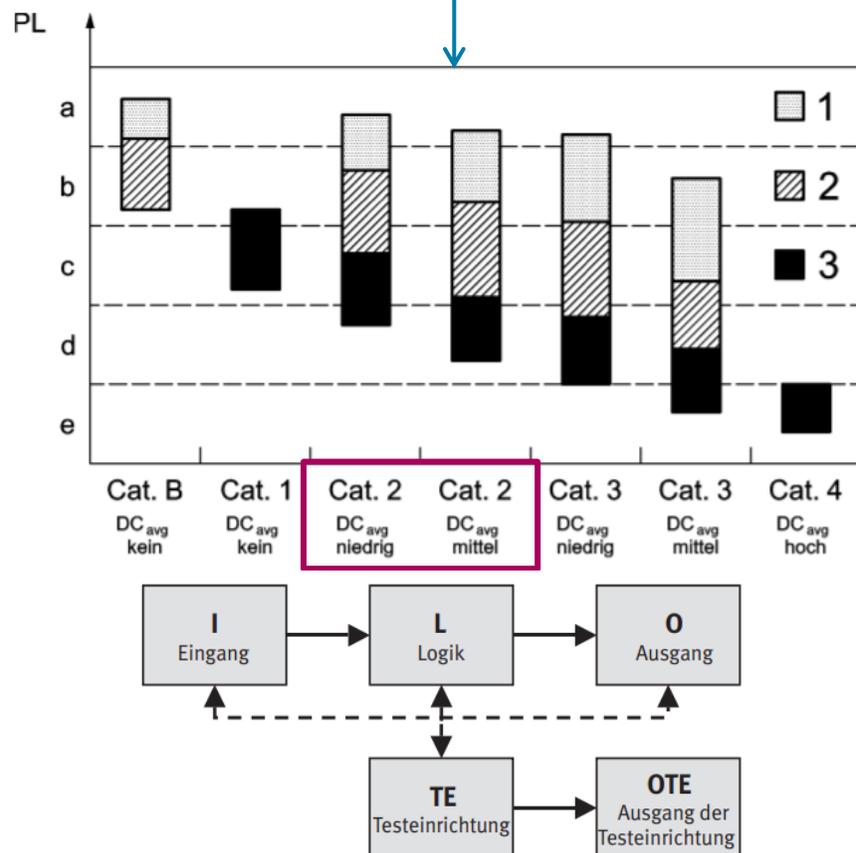
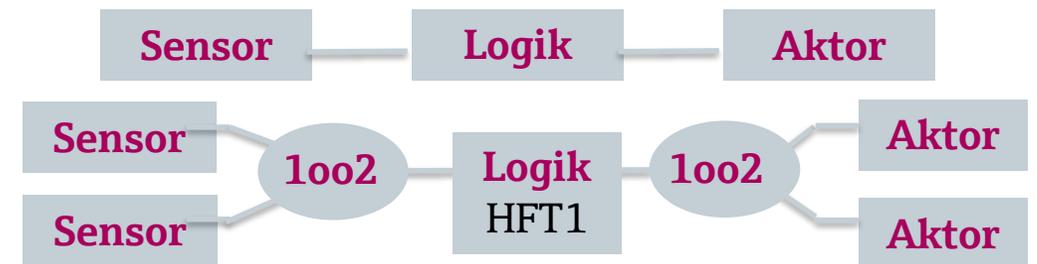


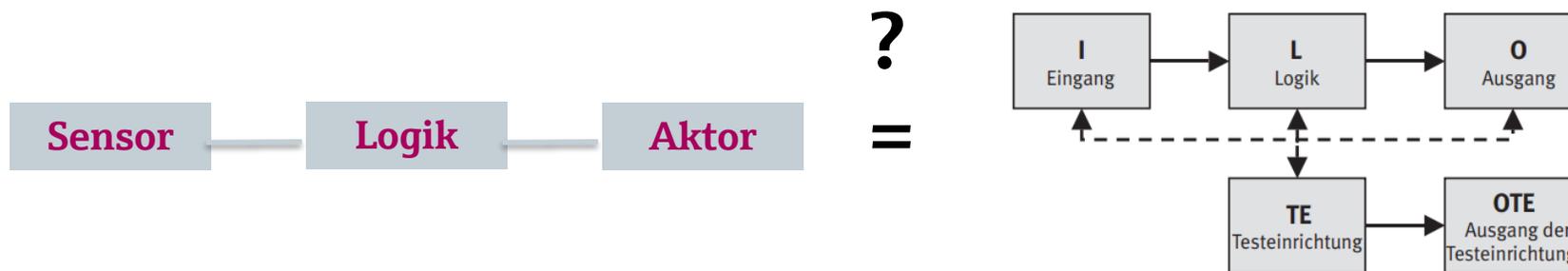
Tabelle 6 der IEC 61511-1

Tabelle 6 – Mindest-HFT in Abh. vom SIL	
SIL	Mindest-HFT
1	0
2 (low demand mode)	0
2 (high demand/continuous mode)	1
3	1
4	2



Konkret: SIL 2 und PL d im Vergleich

- Man könnte jetzt auf die Idee kommen, eine einkanalige Sicherheitseinrichtung mit SIL 2 einen PL d zuordnen zu wollen, indem man die internen Diagnosen der Sicherheitseinrichtung bzw. der einzelnen Komponenten argumentativ als Testeinrichtung nutzt.
- Was ist hierbei zu berücksichtigen?
- Der Testkanal muss mindestens 50% der Zuverlässigkeit des getesteten Kanals aufweisen (DIN EN ISO 13849 4.5.4 und 4.5.5), und mindestens eine MTTF von 10 Jahren aufweisen. Es müssen also MTTF-Werte für den Testkanal vorliegen
 - Weiterhin darf die Diagnose nicht rein softwarebasiert sein.
 - Außerdem muss die Testrate 100x höher sein als die erwartete mittlere Anforderungsrate.



Übersetzung SIL <-> PL – wo geht's schief?

- Herzlichen Dank für Ihre Aufmerksamkeit!





VDI-Handlungsempfehlung

„Gebrauchsdauer in der funktionalen Sicherheit“

Ende der Gebrauchsdauer erreicht – was nun ?

19.09.2023

Firmenvorstellung



Peter Arnold

Entwicklung
CE-Koordinator

Tel.: +49 8196 9000-786

peter.arnold@eichler-service.de

EICHLER GmbH
Elektronik-Service-Center

Unteres Feld 1-3
D-86932 Pürgen
Tel.: +49 8196 9000-0
info@eichler-service.de
www.eichler-service.de





Firmenvorstellung

- Standort: Pürgen, ca. 60km südlich von München, im sogenannten „Lechrain“
- Aktuell ca. 260 Mitarbeiter
- Reparaturdienstleister für Komponenten der Automatisierungstechnik
- Spezialisiert auf drei Hauptbereiche:
 - SPS-Baugruppen
 - HMI-Geräte
 - Frequenzumrichter / Servoantriebe



„Auslöser“ für die VDI-Handlungsempfehlung

- Es mehrten sich die Anfragen, ob die Firma EICHLER GmbH nicht in der Lage wäre, an F-CPU´s einen Proof-Test durchzuführen

„Auslöser“ für die VDI-Handlungsempfehlung

- Es mehrten sich die Anfragen, ob die Firma EICHLER GmbH nicht in der Lage wäre, an F-CPU´s einen Proof-Test durchzuführen
- Nach umfangreicher Recherche wurde festgestellt, dass nicht nur zum Thema „Proof-Test“, sondern auch zum Thema „Gebrauchsdauer“, stark unterschiedliche Meinungen vorhanden waren – selbst in den Fachkreisen

„Auslöser“ für die VDI-Handlungsempfehlung

- Es mehrten sich die Anfragen, ob die Firma EICHLER GmbH nicht in der Lage wäre, an F-CPU's einen Proof-Test durchzuführen
- Nach umfangreicher Recherche wurde festgestellt, dass nicht nur zum Thema „Proof-Test“, sondern auch zum Thema „Gebrauchsdauer“, stark unterschiedliche Meinungen vorhanden waren – selbst in den Fachkreisen
- Problem 1: Betreiber der Maschine/Anlage muss aktuell nach Ablauf der Gebrauchsdauer die entsprechenden Funktionseinheiten austauschen – was nach z.B. 20 Jahren schwierig bis unmöglich ist !!!
 - => durch einen Umbau (Retrofit) könnte er die Maschine/Anlage „am Leben“ erhalten
 - => ist dies technisch oder vor allem wirtschaftlich nicht vertretbar, muss er abschalten !!!
 - => macht er dies nicht, handelt er vorsätzlich

„Auslöser“ für die VDI-Handlungsempfehlung

- Es mehrten sich die Anfragen, ob die Firma EICHLER GmbH nicht in der Lage wäre, an F-CPU's einen Proof-Test durchzuführen
- Nach umfangreicher Recherche wurde festgestellt, dass nicht nur zum Thema „Proof-Test“, sondern auch zum Thema „Gebrauchsdauer“, stark unterschiedliche Meinungen vorhanden waren – selbst in den Fachkreisen
- Problem 1: Betreiber der Maschine/Anlage muss aktuell nach Ablauf der Gebrauchsdauer die entsprechenden Funktionseinheiten austauschen – was nach z.B. 20 Jahren schwierig bis unmöglich ist !!!
 - => durch einen Umbau (Retrofit) könnte er die Maschine/Anlage „am Leben“ erhalten
 - => ist dies technisch oder vor allem wirtschaftlich nicht vertretbar, muss er abschalten !!!
 - => macht er dies nicht, handelt er vorsätzlich
- Problem 2: Ein Großteil der Betreiber weiß darüber nicht Bescheid !!!

„Auslöser“ für die VDI-Handlungsempfehlung

- Es mehrten sich die Anfragen, ob die Firma EICHLER GmbH nicht in der Lage wäre, an F-CPU's einen Proof-Test durchzuführen
- Nach umfangreicher Recherche wurde festgestellt, dass nicht nur zum Thema „Proof-Test“, sondern auch zum Thema „Gebrauchsdauer“, stark unterschiedliche Meinungen vorhanden waren – selbst in den Fachkreisen
- Problem 1: Betreiber der Maschine/Anlage muss aktuell nach Ablauf der Gebrauchsdauer die entsprechenden Funktionseinheiten austauschen – was nach z.B. 20 Jahren schwierig bis unmöglich ist !!!
 - => durch einen Umbau (Retrofit) könnte er die Maschine/Anlage „am Leben“ erhalten
 - => ist dies technisch oder vor allem wirtschaftlich nicht vertretbar, muss er abschalten !!!
 - => macht er dies nicht, handelt er vorsätzlich
- Problem 2: Ein Großteil der Betreiber weiß darüber nicht Bescheid !!!
- Der VDI erklärte sich bereit, hier einen Arbeitskreis ins Leben zu rufen, der sich dieser Problemstellung angenommen hat und Lösungen erarbeitete, welche dem Betreiber es ermöglichen, die Maschine / Anlage noch für einen bestimmten Zeitraum weiter zu betreiben – unter Einhaltung bzw. Durchführung bestimmter Maßnahmen

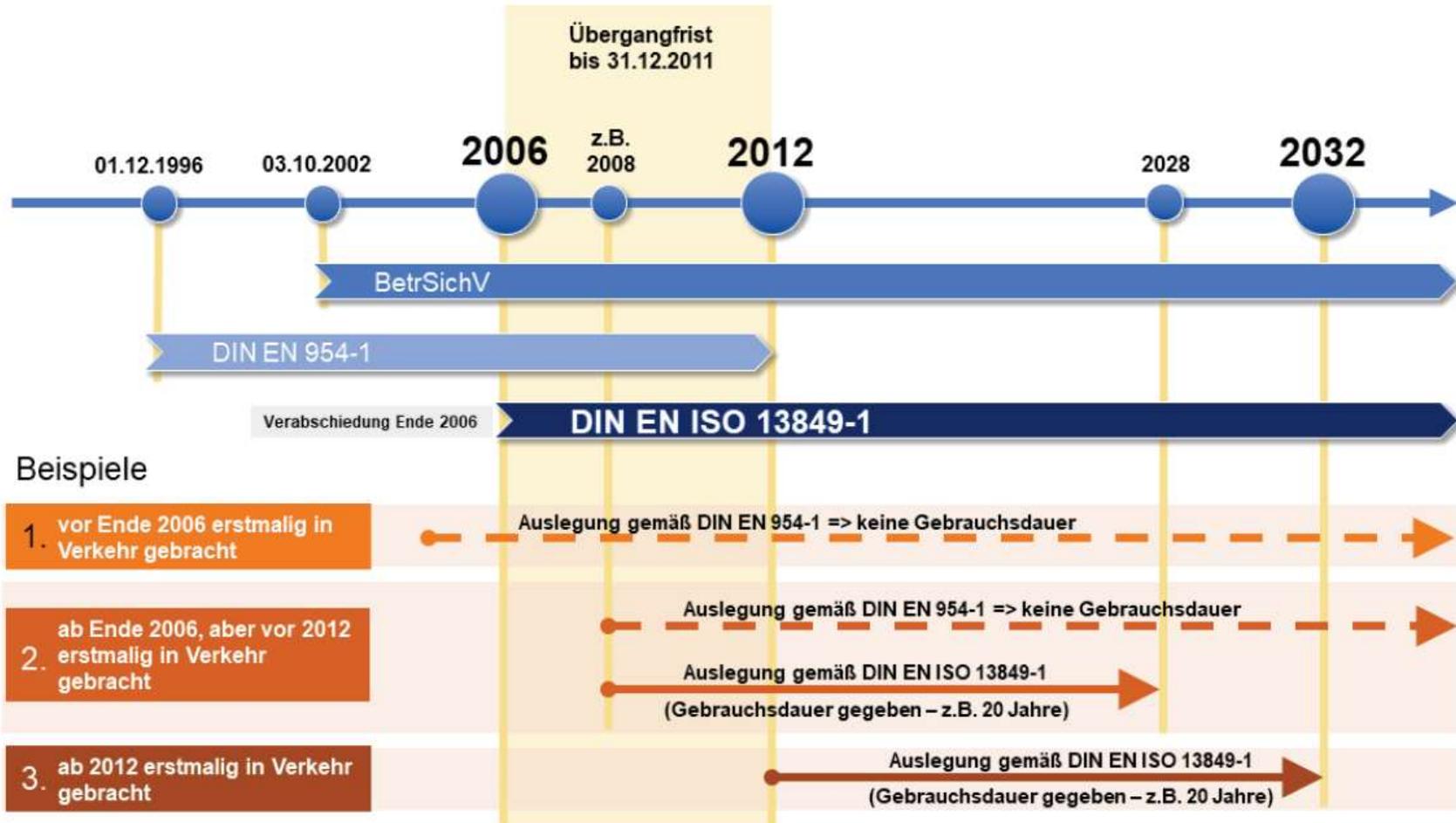
Aktueller Stand der VDI-Handlungsempfehlung

- Die Handlungsempfehlung wurde von der VDI-Redaktion abschließend bearbeitet und wird in den nächsten Tagen als PDF zum Download zur Verfügung stehen
- Link zum PDF-Dokument: <https://www.vdi.de/ueber-uns/presse/publikationen/details/gebrauchsdauer-in-der-funktionalen-sicherheit-ende-der-gebrauchsdauer-erreicht-was-nun>
- Ziel ist es natürlich, dass die VDI-Handlungsempfehlung publik gemacht wird, damit alle Beteiligten auf das Thema „Gebrauchsdauer“ aufmerksam werden und vor allem die Betreiber nicht „ins offene Messer laufen“
- Eine Bitte vom VDI ist es aber, nicht das PDF-Dokument direkt zu verbreiten, sondern immer nur den Link – hat den Hintergrund, dass der VDI die Anzahl der Downloads erfassen möchte um somit das Interesse an dem Thema in Erfahrung zu bringen

Inhalt der VDI-Handlungsempfehlung

- Grundintention der VDI-Handlungsempfehlung:
Betreiber auf das Thema „Gebrauchsdauer“ aufmerksam machen und es ihnen verständlich nahebringen
- Das Dokument ist in zwei Kapitel unterteilt
- Im Kapitel 1:
 - werden alle wichtigen Begriffe und Zusammenhänge zum Thema „Gebrauchsdauer“ erläutert
 - wird dargestellt, wann das Thema „Gebrauchsdauer“ den Betreiber betrifft und wann es für ihn kritisch wird
 - wird erklärt, welche Maßnahmen der Betreiber ergreifen muss bzw. kann, wenn die Gebrauchsdauer abgelaufen ist
- Dieses Kapitel ist für den Betreiber bestimmt. Hier wurde speziell darauf geachtet, dass die „fachliche Flughöhe“ niedrig gehalten wurde, damit es für alle verständlich bleibt
- Kapitel 2 ist ausgerichtet für den fachlich Interessierten => beinhaltet weiterführende Informationen und Erläuterungen (muss zum Verständnis der Thematik nicht zwingend gelesen werden)

Wann betrifft das Thema „Gebrauchsdauer“ den Betreiber ?



Definition „Funktionseinheit“



Laserscanner



Schütz



Relais



Näherungs-
sensor



Verriegelung
mit Zuhaltung



Frequenzumrichter



Not-Halt-
Sicherheitsschaltgerät



induktiver
Sensor



Näherungs-
schalter



Zweihand-
Steuerungsventil



Pneumatik-Ventil



Sicherheits-SPS



Lichtgitter



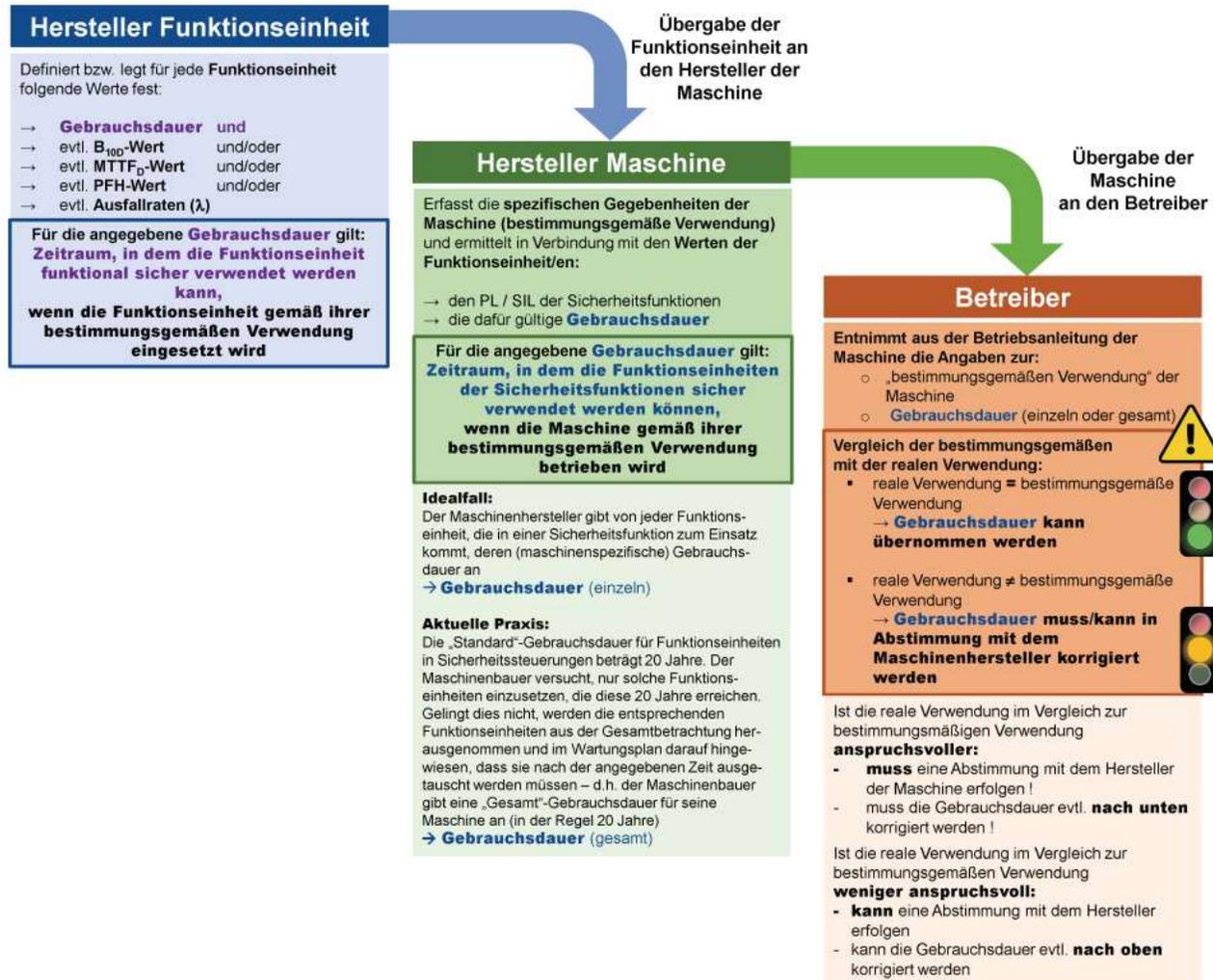
mechanischer
Positionsschalter



elektronischer
Sicherheitssensor

Einheit aus Hardware mit oder ohne Software, die zur Durchführung einer angegebenen Aufgabe geeignet ist und die üblicherweise **als Ganzes vom Betreiber selbst** ausgetauscht werden kann. Eine Funktionseinheit kann ein Gerät, eine Komponente, eine Baugruppe, etc. sein

Gebrauchsdauer – ein Begriff, zwei Bedeutungen



Wann „startet“ die Gebrauchsdauer ?

- Nach Herstellung der Funktionseinheit ?
- Bei Kauf der Maschine ?
- Bei Inbetriebnahme der Maschine ?
- Was ist mit Lagerzeiten ?
- Bestimmungsgemäße Verwendung beachtet (sowohl von der Funktionseinheit, als auch der Maschine) ?
- Wann wurden die einzelnen Bauteile einer Funktionseinheit hergestellt ?

Wann „startet“ die Gebrauchsdauer ?

- **Pragmatischer Ansatz:**

Funktionseinheiten, die für Sicherheitsfunktionen vorgesehen sind, kann eine gute industrielle Qualität unterstellt werden. Hinzu kommt, dass Hersteller dieser Funktionseinheiten bei deren Entwicklung das Prinzip der „guten Ingenieurspraxis“ anwenden. Deshalb kann davon ausgegangen werden, dass standardmäßige Produktions- und Lagerzeiten – sowohl von einzelnen Funktionseinheiten, als auch von Maschinen – mitberücksichtigt sind

- **Bedeutet für den Betreiber:**

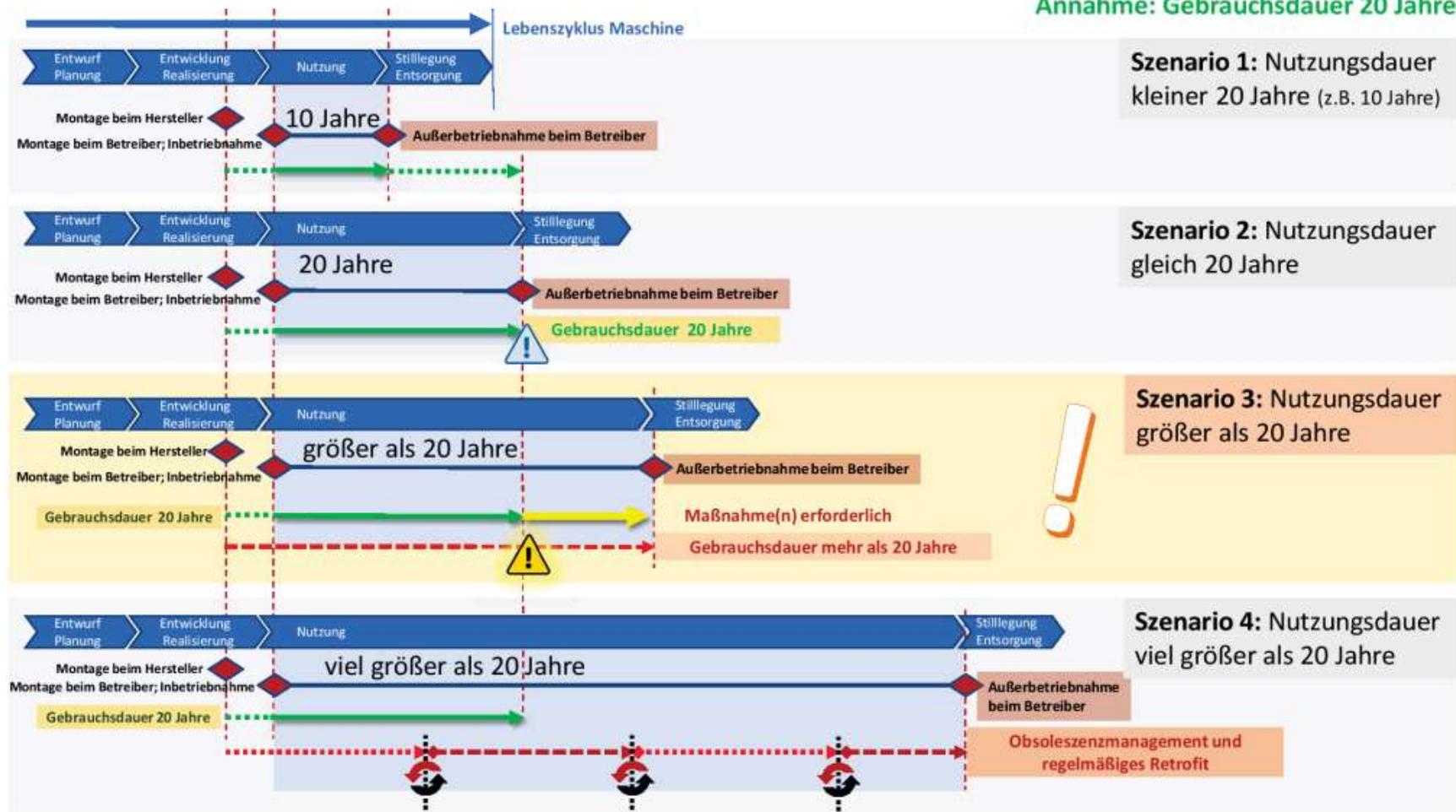
- beim Kauf einer Maschine:
erstmalige bestimmungsgemäße Verwendung (Inbetriebnahme) der Maschine
- beim Kauf einer einzelnen Funktionseinheit (z.B. als Ersatzteil):
entweder der Zeitpunkt der Anlieferung der Funktionseinheit (und Einlagerung) oder der Zeitpunkt der (Wieder-)Inbetriebnahme der Maschine (nach dem Einbau)

- **Ergänzender Hinweis:**

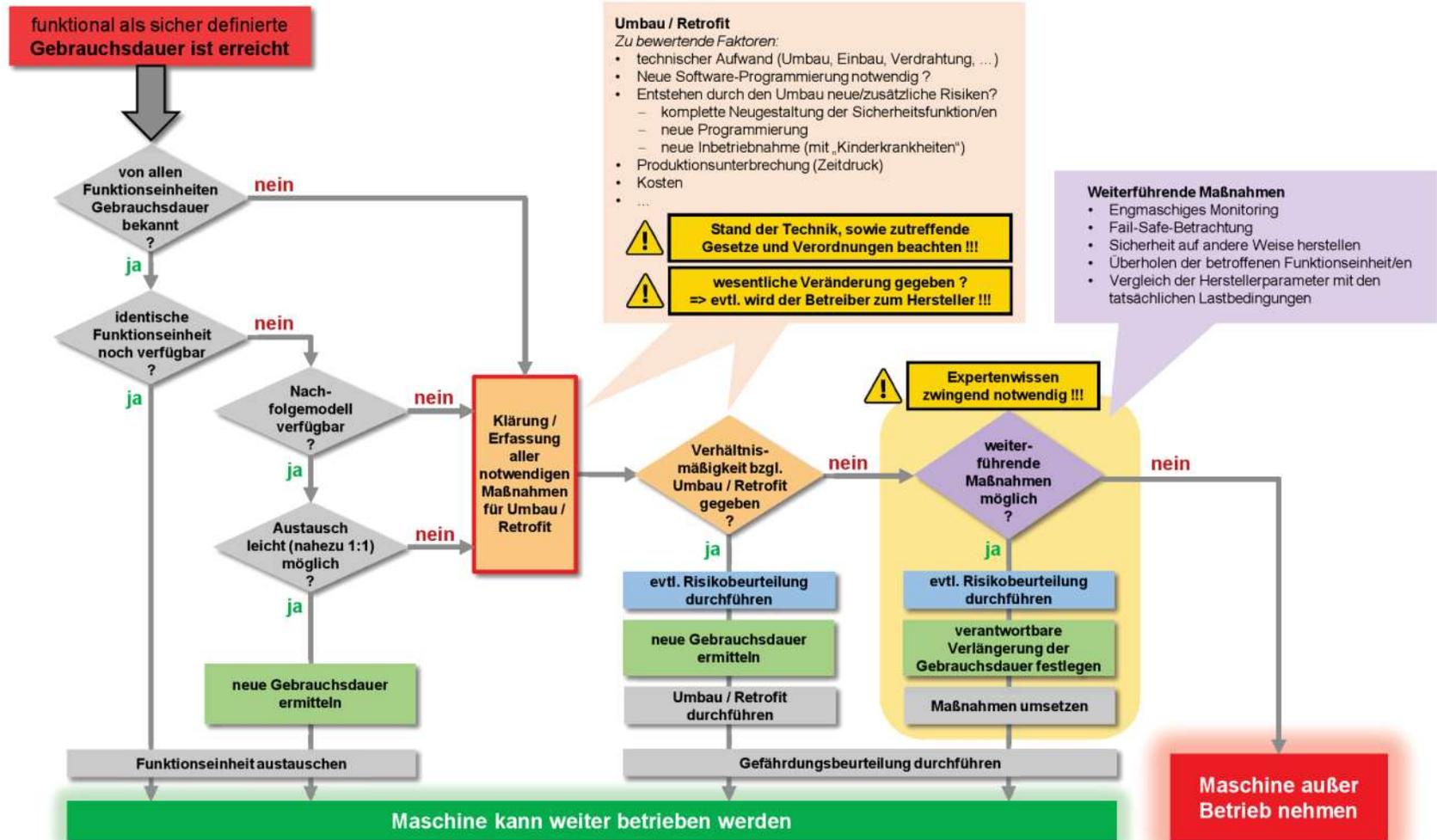
Kommt es zu längeren Lagerzeiten – sowohl einzelner Funktionseinheiten als auch von Maschinen, in denen Funktionseinheiten in Sicherheitsfunktionen eingesetzt sind – muss dies bei der Festlegung der Gebrauchsdauer mit berücksichtigt werden!

Wann wird es für den Betreiber kritisch

Annahme: Gebrauchsdauer 20 Jahre



Entscheidungswege für den Betreiber



Hinweis

- Dieses Dokument ist eine Handlung**empfehlung**, erarbeitet von Fachleuten unterschiedlichster Hersteller und Institutionen
- Das Dokument ist aber **keine VDI-Richtlinie, keine Norm, kein Gesetz, keine Verordnung**
=> andere Kreise können zu einzelnen Punkten durchaus eine andere Meinung haben
- Die gezeigten Abbildungen entsprechen nicht zu 100% dem endgültigen Stand:
 - inhaltlich absolut identisch
 - Gestaltung wurde noch etwas angepasst

„Wunschliste“ für eine Betriebsanleitung

Für einen Betreiber wären folgende Informationen absolut wichtig:

- Welche Sicherheitsfunktionen sind in einer Maschine vorhanden?
- Wie können/müssen diese Sicherheitsfunktionen getestet werden?
- Welche Funktionseinheiten sind in diesen Sicherheitsfunktionen verbaut?
- Welche Gebrauchsdauer hat jede dieser Funktionseinheiten?



**Vielen Dank für
Ihre Aufmerksamkeit**

Relationship between Markov Models, PFD and PFH

Frank Schiller¹, Jürgen Mottok², Patrick Gehlen³

¹IEC/TC 65/WG 12, Beckhoff Automation GmbH & Co. KG;

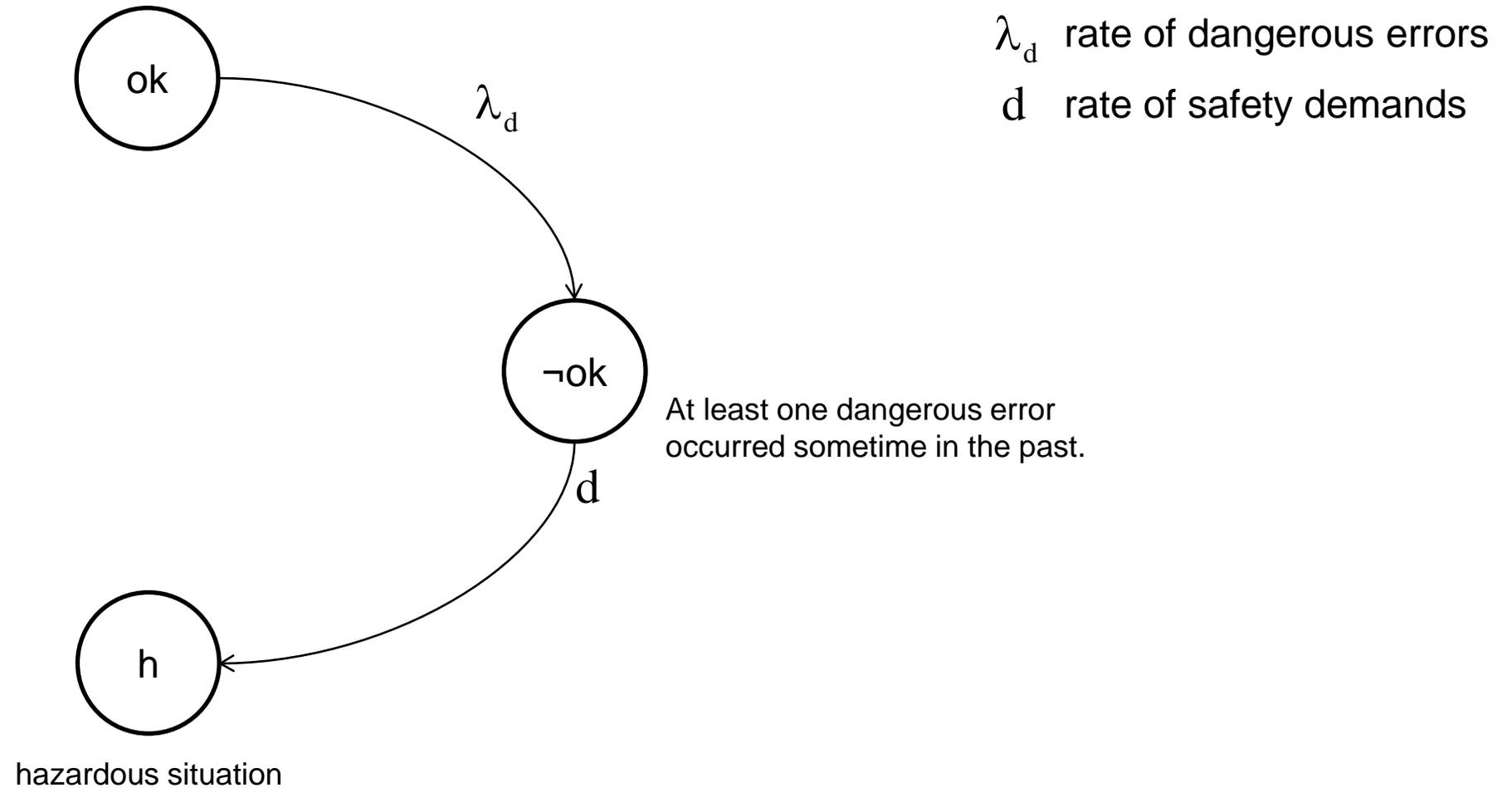
²Laboratory for Safe and Secure Systems, Ostbayerische Technische Hochschule Regensburg;

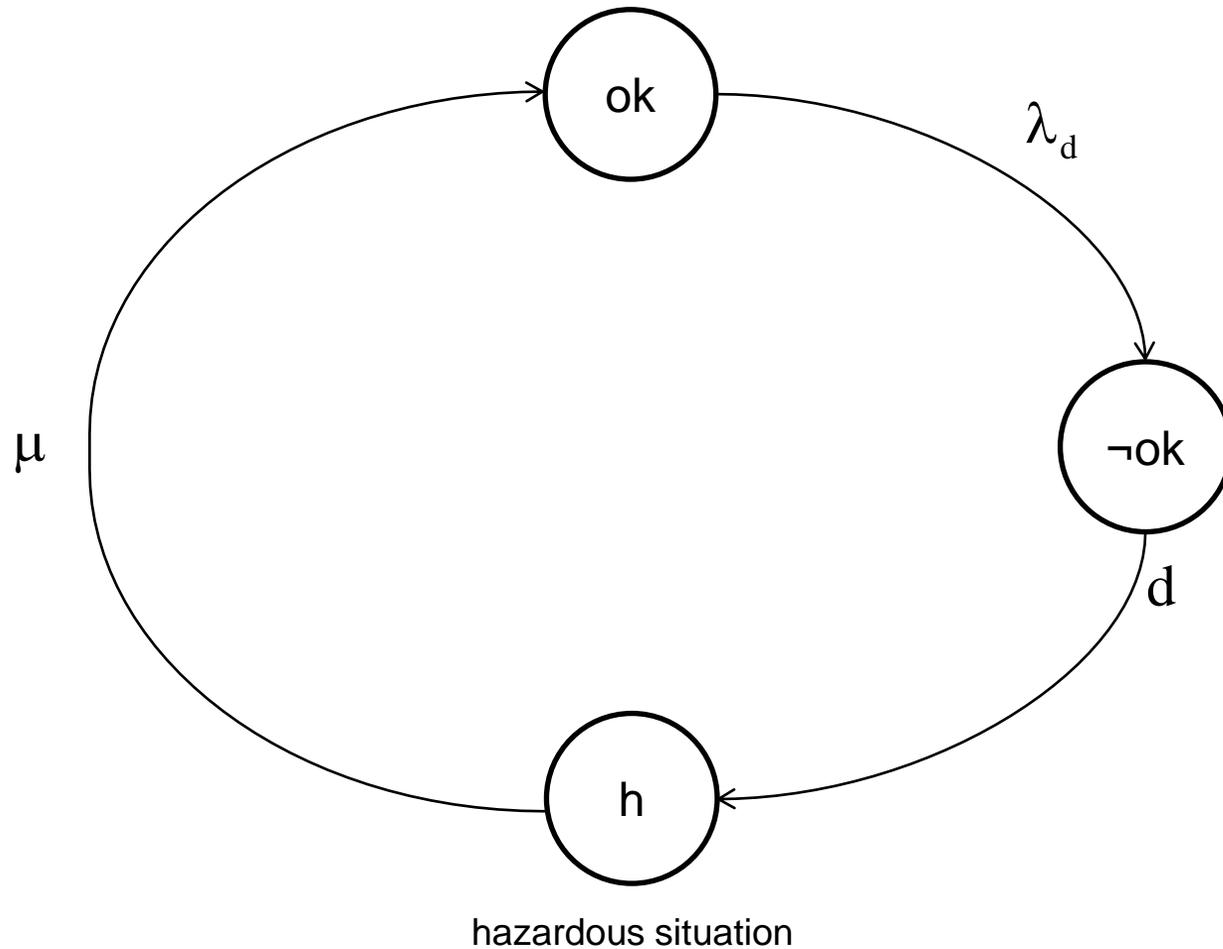
³IEC/TC 44, Siemens AG

- Motivation
- Markov Models
- PFD
- PFH
- Discussion
- Summary

- Safety functions are distinguished acc. to demand: low demand, high demand, continuous operation.
- Demand is not always known in the whole life cycle:
 - Demand rate changes, e.g., by attacks.
Then, the safety function reacts acc. to its specification and avoids hazards – but are the calculations still correct?
 - Characteristic of demand changes, e.g., random demand vs. cyclic demand.

- Motivation
- Markov Models
- PFD
- PFH
- Discussion
- Summary



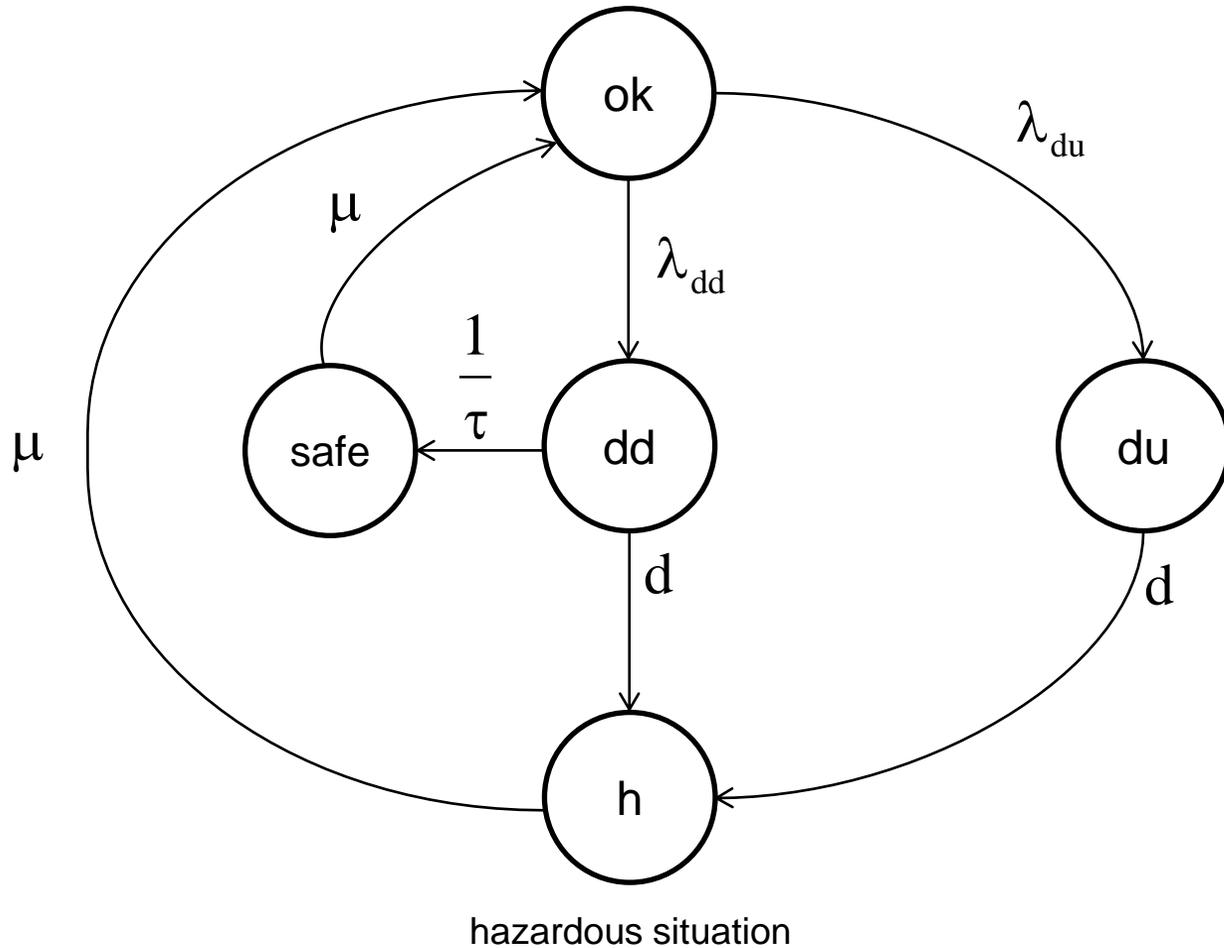


λ_d rate of dangerous errors

d rate of safety demands

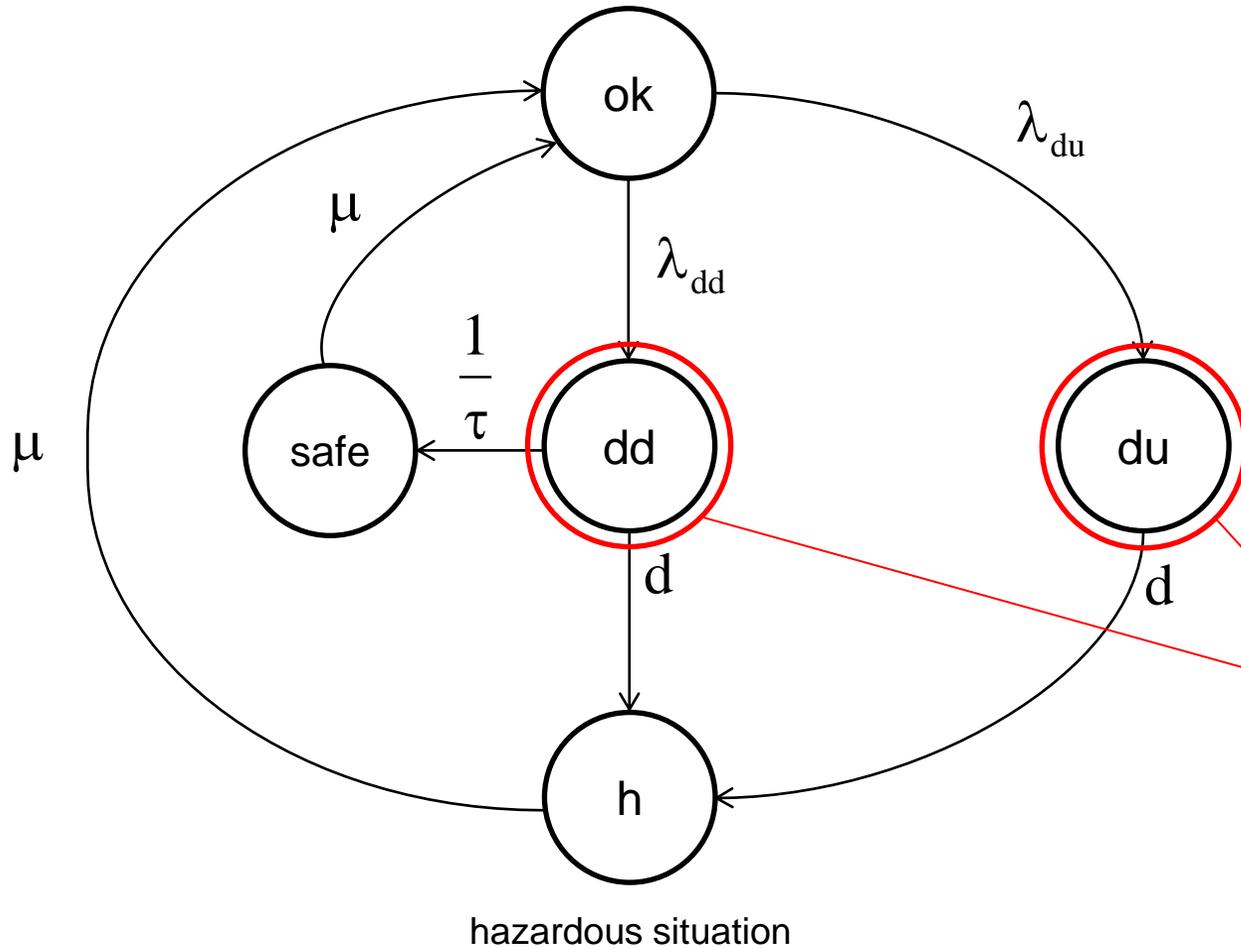
μ repair “rate”

At least one dangerous error occurred after the system was ok.



- λ_{du} rate of undetectable dang. errors
- λ_{dd} rate of detectable dang. errors
- d rate of safety demands
- μ repair "rate"
- $1/\tau$ rate of error detection algorithm

At least one dangerous undetectable error occurred after the system was ok.

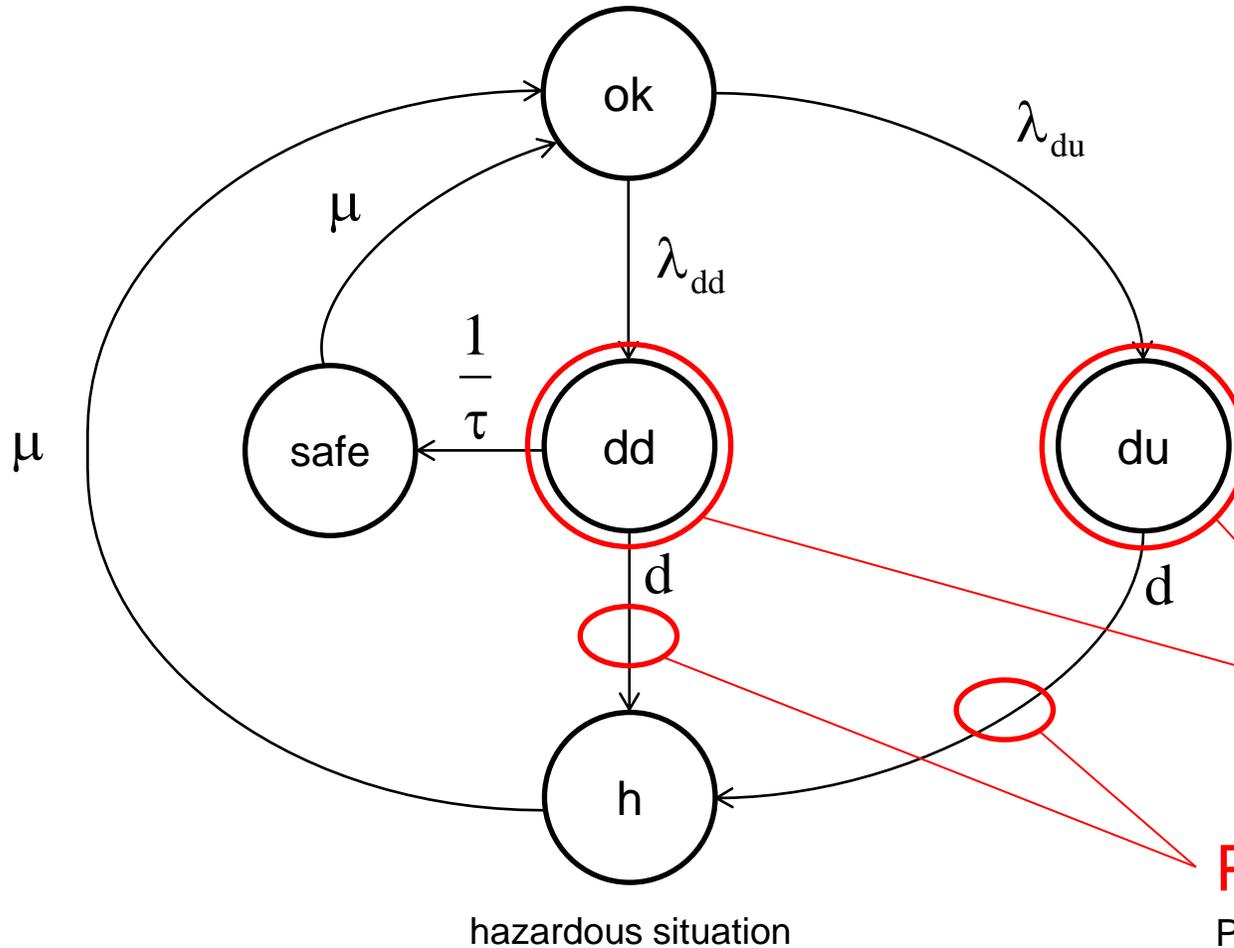


- λ_{du} rate of undetectable dang. errors
- λ_{dd} rate of detectable dang. errors
- d rate of safety demands
- μ repair "rate"
- $1/\tau$ rate of error detection algorithm

At least one dangerous undetectable error occurred after the system was ok.

PFD

Probability of dangerous Failure on Demand

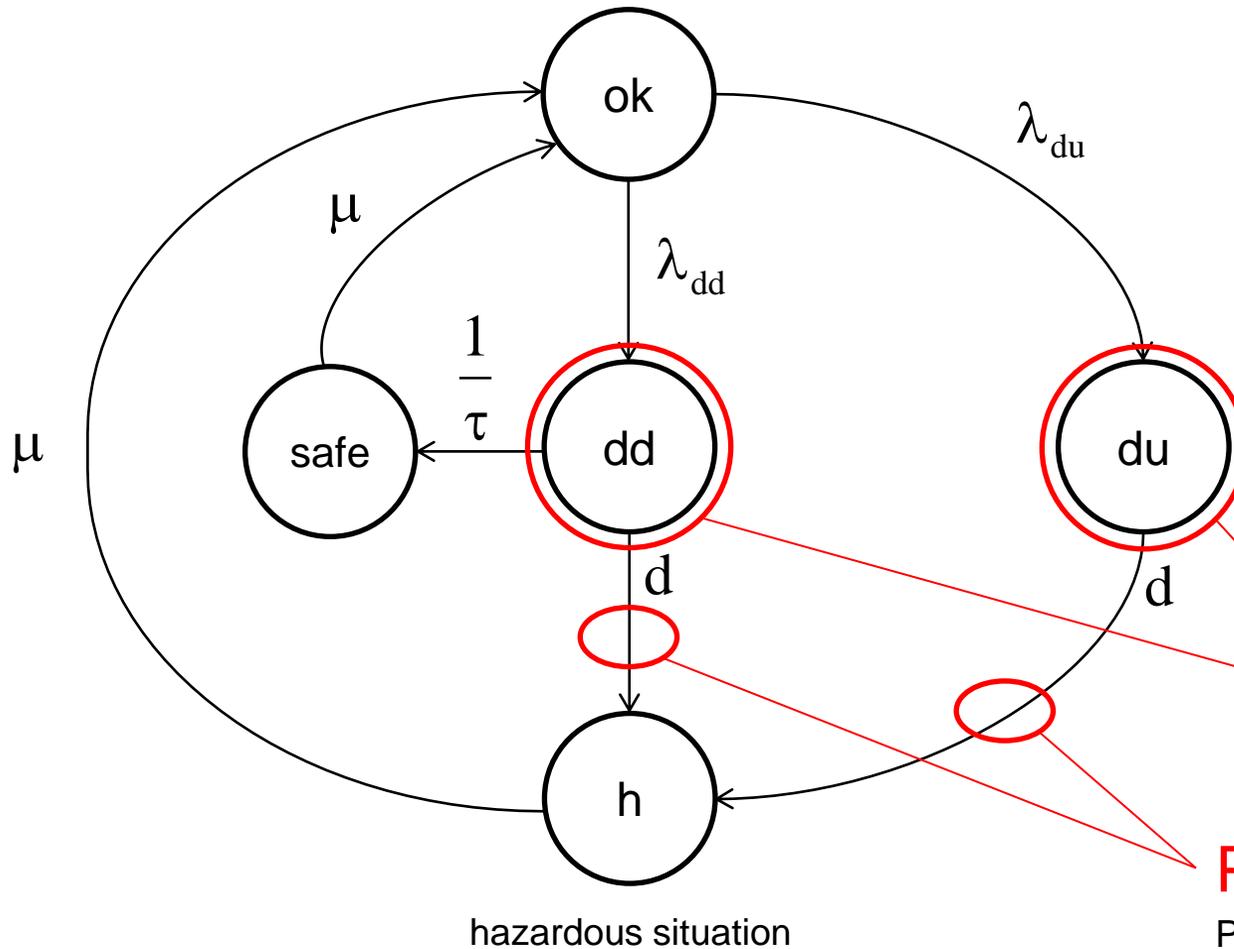


- λ_{du} rate of undetectable dang. errors
- λ_{dd} rate of detectable dang. errors
- d rate of safety demands
- μ repair "rate"
- $1/\tau$ rate of error detection algorithm

At least one dangerous undetectable error occurred after the system was ok.

PFD
Probability of dangerous Failure on Demand

PFH
Probability of dangerous Failure per Hour



- λ_{du} rate of undetectable dang. errors
- λ_{dd} rate of detectable dang. errors
- d rate of safety demands
- μ repair "rate"
- $1/\tau$ rate of error detection algorithm

At least one dangerous undetectable error occurred after the system was ok.

PFD

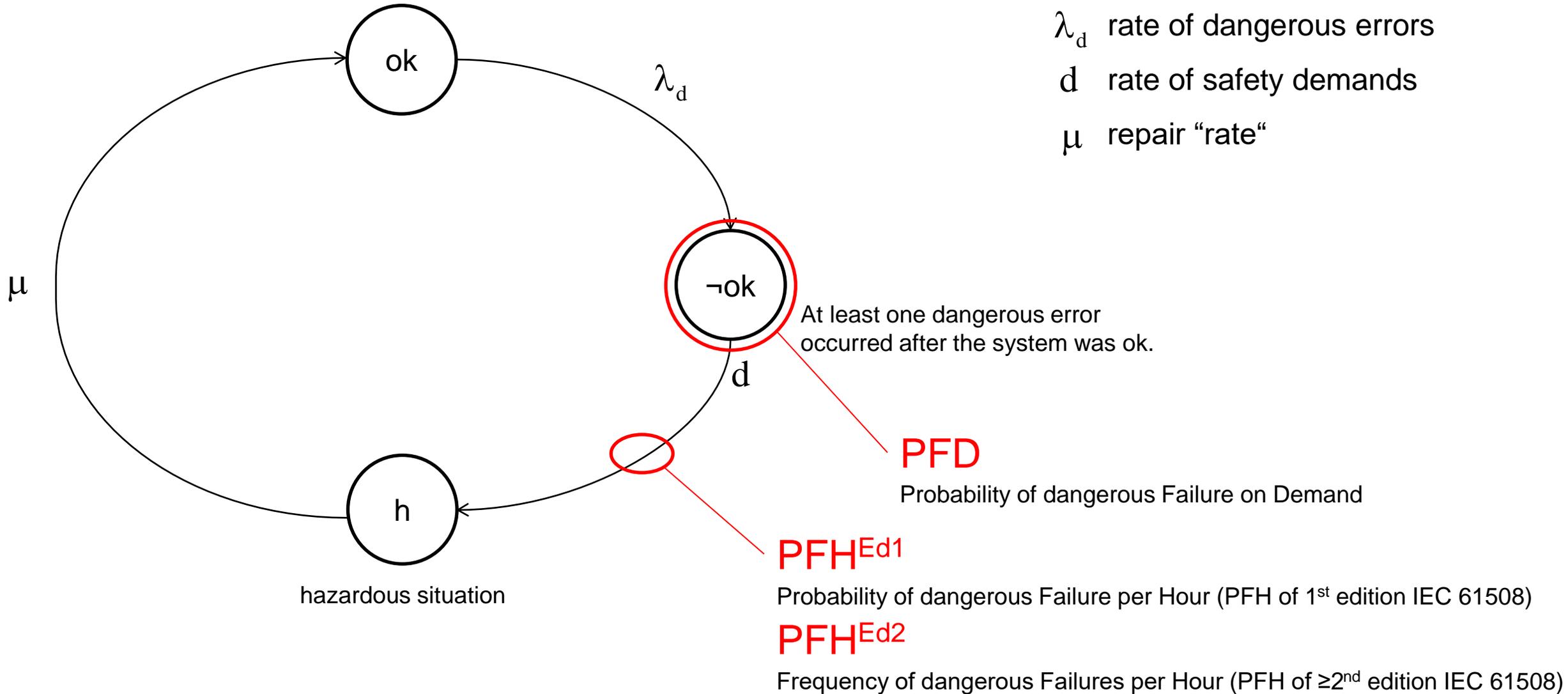
Probability of dangerous Failure on Demand

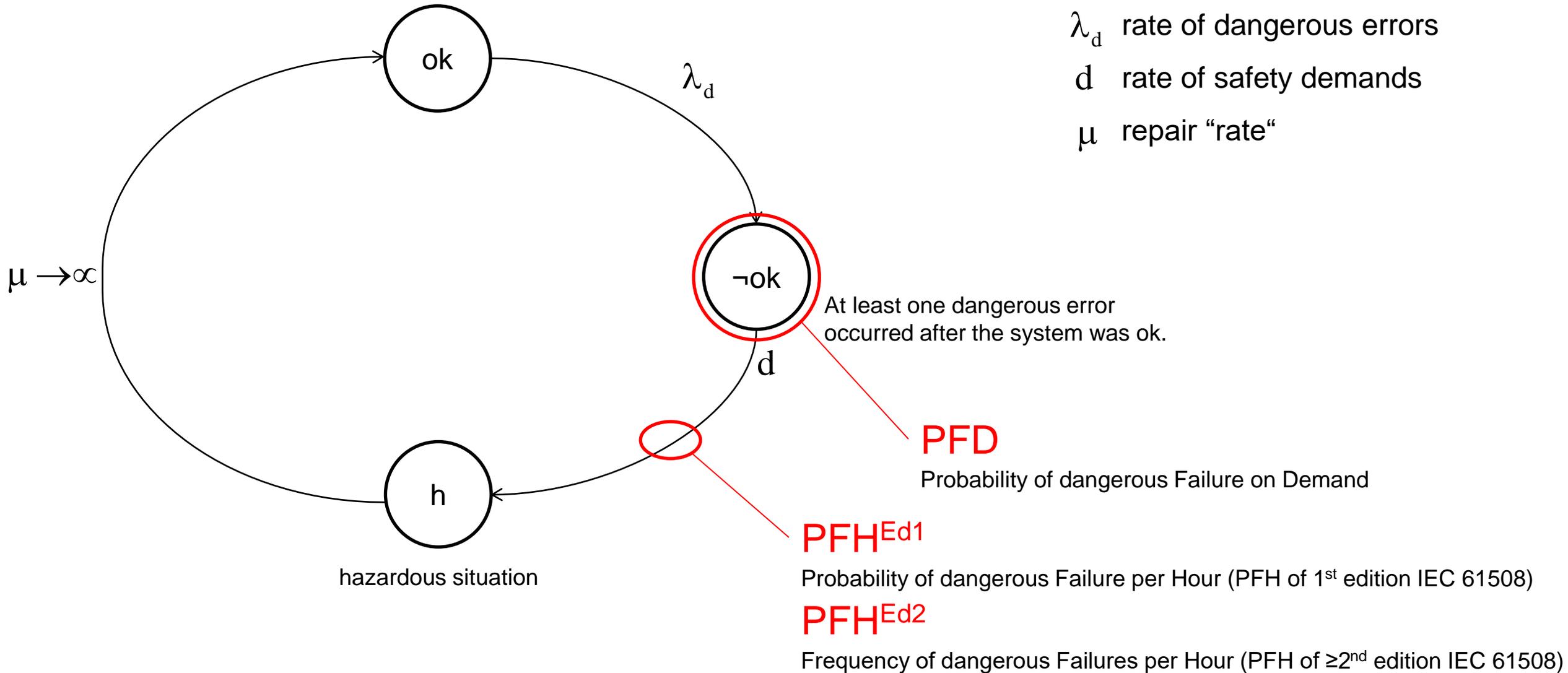
PFH^{Ed1}

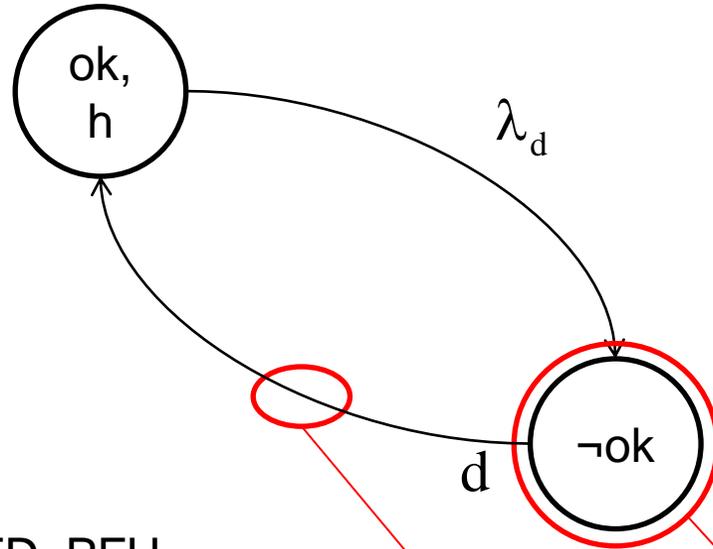
Probability of dangerous Failure per Hour (PFH of 1st edition IEC 61508)

PFH^{Ed2}

Frequency of dangerous Failures per Hour (PFH of $\geq 2^{\text{nd}}$ edition IEC 61508)







λ_d rate of dangerous errors

d rate of safety demands

$\mu \rightarrow \infty$

Disadvantage:

- Greater values for PFD, PFH

Advantage:

- No assumption about repair necessary

At least one dangerous error occurred after the system was ok.

PFD

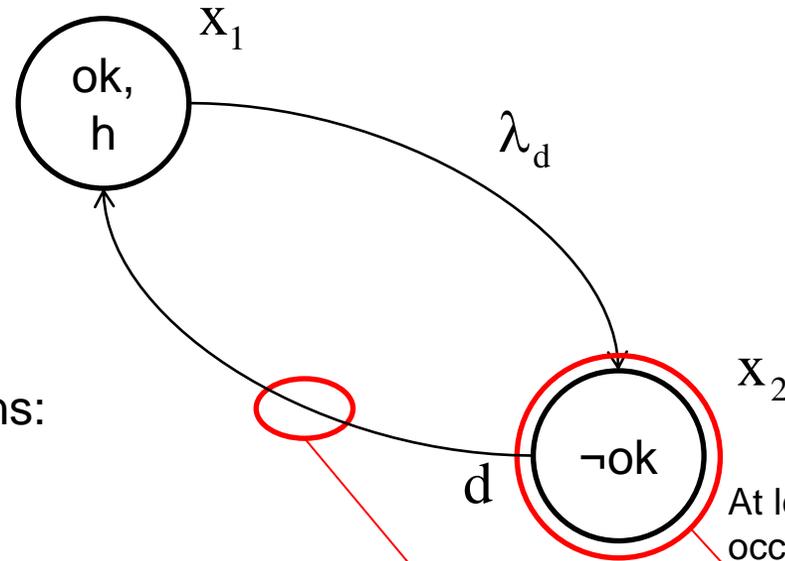
Probability of dangerous Failure on Demand

PFH^{Ed1}

Probability of dangerous Failure per Hour (PFH of 1st edition IEC 61508)

PFH^{Ed2}

Frequency of dangerous Failures per Hour (PFH of $\geq 2^{\text{nd}}$ edition IEC 61508)



λ_d rate of dangerous errors

d rate of safety demands

Set of differential equations:

$$\dot{x}_1 = -\lambda_d \cdot x_1 + d \cdot x_2$$

$$\dot{x}_2 = \lambda_d \cdot x_1 - d \cdot x_2$$

$$x_1(0) = 1, x_2(0) = 0$$

$$x_1 + x_2 = 1$$

At least one dangerous error occurred after the system was ok.

PFD

Probability of dangerous Failure on Demand

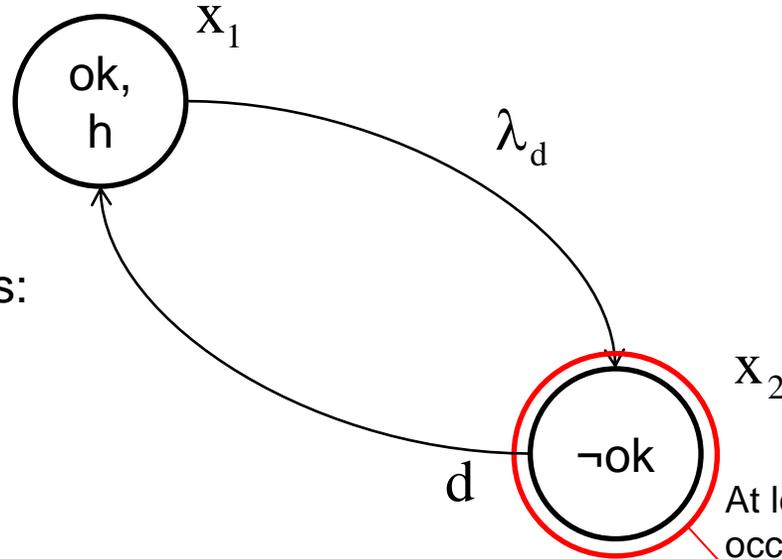
PFH^{Ed1}

Probability of dangerous Failure per Hour (PFH of 1st edition IEC 61508)

PFH^{Ed2}

Frequency of dangerous Failures per Hour (PFH of $\geq 2^{\text{nd}}$ edition IEC 61508)

- Motivation
- Markov Models
- PFD
- PFH
- Discussion
- Summary



λ_d rate of dangerous errors
 d rate of safety demands

Set of differential equations:

$$\dot{x}_1 = -\lambda_d \cdot x_1 + d \cdot x_2$$

$$\dot{x}_2 = \lambda_d \cdot x_1 - d \cdot x_2$$

$$x_1(0) = 1, x_2(0) = 0$$

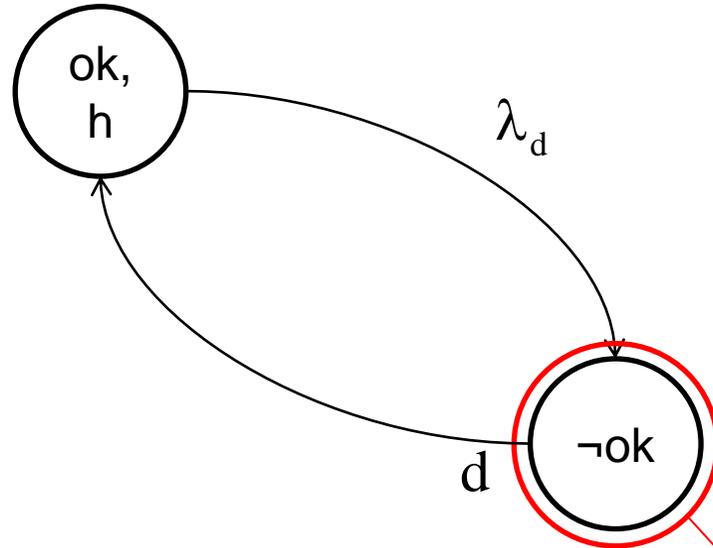
$$x_1 + x_2 = 1$$

At least one dangerous error occurred after the system was ok.

PFD

Probability of dangerous Failure on Demand

$$\text{PFD}(t) = x_2(t) = \frac{\lambda_d}{\lambda_d + d} \cdot (1 - e^{-(\lambda_d + d) \cdot t})$$



λ_d rate of dangerous errors

d rate of safety demands

At least one dangerous error occurred after the system was ok.

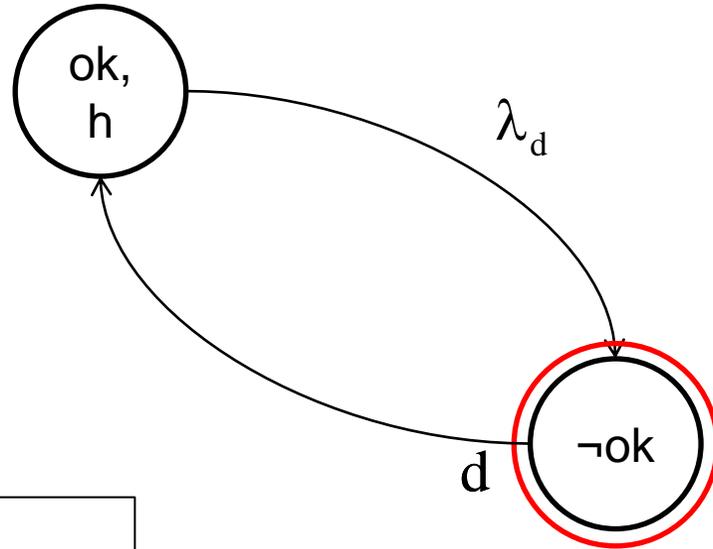
PFD

Probability of dangerous Failure on Demand

$$PFD(t) = \frac{\lambda_d}{\lambda_d + d} \cdot (1 - e^{-(\lambda_d + d) \cdot t})$$

$$PFD_{avg}(T) = \frac{\lambda_d}{\lambda_d + d} \cdot \left(1 - \frac{1}{(\lambda_d + d) \cdot T} \cdot (1 - e^{-(\lambda_d + d) \cdot T}) \right)$$

Worst case demand?



λ_d rate of dangerous errors

d rate of safety demands

$$\text{PFD}(t) \leq \text{PFD}(t, d = 0)$$

$$\text{PFD}_{\text{avg}}(T) \leq \text{PFD}_{\text{avg}}(T, d = 0)$$

$$\text{PFD}(t, d = 0) = 1 - e^{-\lambda_d \cdot t}$$

$$\text{PFD}_{\text{avg}}(T, d = 0) = 1 - \frac{1}{\lambda_d \cdot T} \cdot (1 - e^{-\lambda_d \cdot T})$$

$d = 0$

Disadvantage:

- Greater value for PFD

Advantage:

- No assumption about demand necessary, neither its rate nor its characteristic.

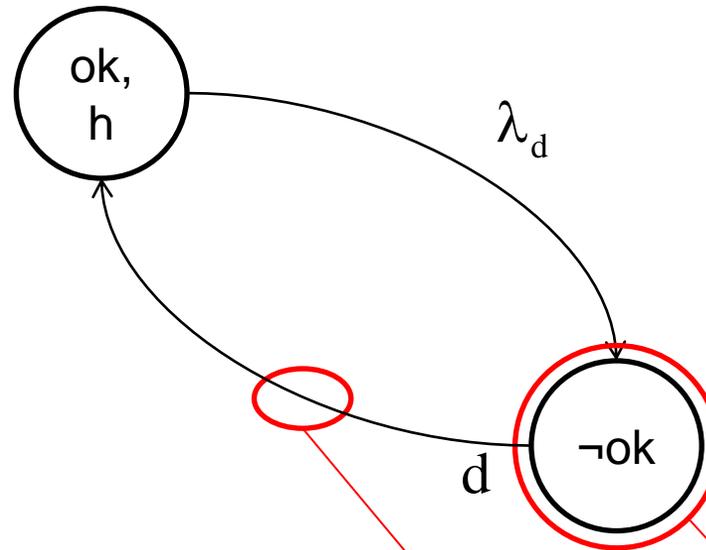
- Motivation
- Markov Models
- PFD
- PFH
 - PFH^{Ed2}
 - PFH^{Ed1}
- Discussion
- Summary

$$PFH^{Ed2}(t) = PFD(t) \cdot d$$

$$PFH^{Ed2}(t) = \frac{\lambda_d}{\lambda_d + d} \cdot (1 - e^{-(\lambda_d + d) \cdot t}) \cdot d$$

$$PFH_{avg}^{Ed2}(T) = \frac{\lambda_d}{\lambda_d + d} \cdot \left(1 - \frac{1}{(\lambda_d + d) \cdot T} \cdot (1 - e^{-(\lambda_d + d) \cdot T}) \right) \cdot d$$

Worst case demand?



λ_d rate of dangerous errors

d rate of safety demands

PFD

Probability of dangerous Failure on Demand

PFH^{Ed2}

Frequency of dangerous Failures per Hour
(PFH of $\geq 2^{nd}$ edition IEC 61508)

$$PFH^{Ed2}(t) = PFD(t) \cdot d$$

$d \rightarrow \infty$

$$PFH^{Ed2}(t) \leq \lambda_d$$

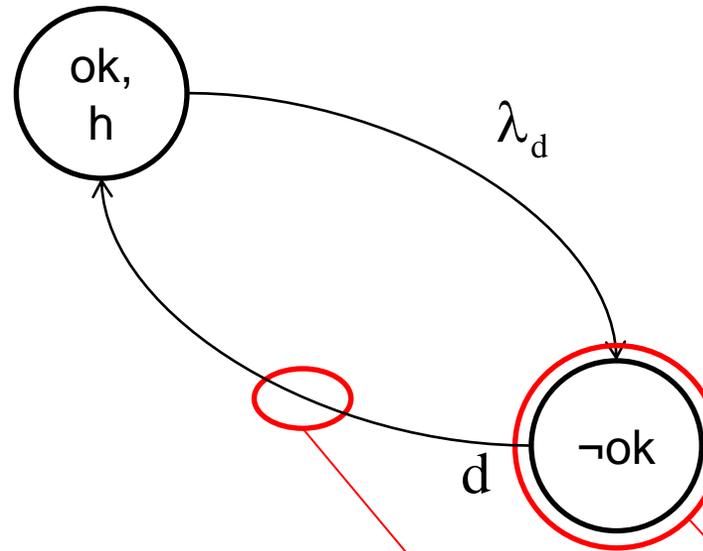
$$PFH_{avg}^{Ed2}(T) \leq \lambda_d$$

Disadvantages:

- Greater value for PFH

Advantages:

- No assumption about demand necessary, neither its rate nor its characteristic.



λ_d rate of dangerous errors

d rate of safety demands

PFD

Probability of dangerous Failure on Demand

PFH^{Ed2}

Frequency of dangerous Failures per Hour
(PFH of $\geq 2^{nd}$ edition IEC 61508)

$$PFH^{Ed2}(t) = \underline{PFD(t)} \cdot d$$

$$PFD(t) \leq PFD(t, d = 0)$$

$$PFH^{Ed2}(t) \leq PFD(t, d = 0) \cdot d$$

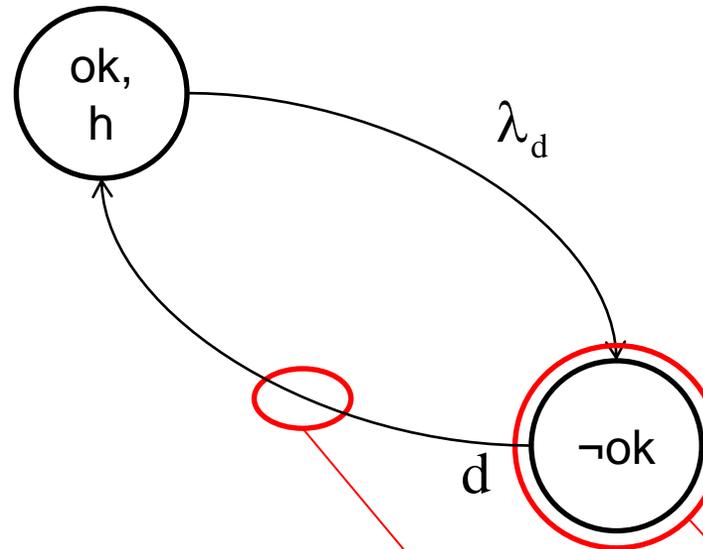
$$PFH_{avg}^{Ed2}(T) \leq PFD_{avg}(T, d = 0) \cdot d$$

Disadvantage:

- Greater value for PFH

Advantage:

- Characteristic of demand is not an inherent part of the math. model. Its characteristic is transferred to PFH.



λ_d rate of dangerous errors

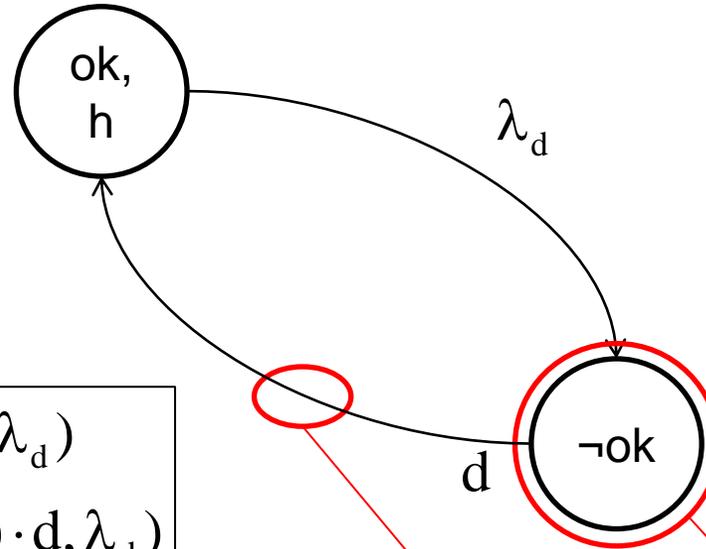
d rate of safety demands

PFD

Probability of dangerous Failure on Demand

PFH^{Ed2}

Frequency of dangerous Failures per Hour
(PFH of ≥2nd edition IEC 61508)



λ_d rate of dangerous errors

d rate of safety demands

$$PFH^{Ed2}(t) \leq \min(PFD(t, d = 0) \cdot d, \lambda_d)$$

$$PFH_{avg}^{Ed2}(T) \leq \min(PFD_{avg}(T, d = 0) \cdot d, \lambda_d)$$

Disadvantage:

- Greater value for PFH

Advantage:

- Characteristic of demand is not an inherent part of the math. model. Its characteristic is transferred to PFH.

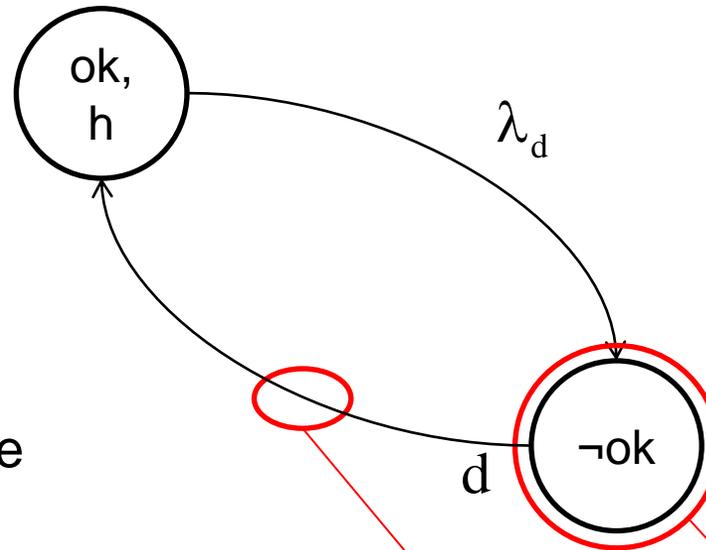
PFD

Probability of dangerous Failure on Demand

PFH^{Ed2}

Frequency of dangerous Failures per Hour
(PFH of $\geq 2^{nd}$ edition IEC 61508)

- Motivation
- Markov Models
- PFD
- PFH
 - PFH^{Ed2}
 - PFH^{Ed1}
- Discussion
- Summary



λ_d rate of dangerous errors

d rate of safety demands

Probability that a dangerous failure occurs in one hour.

= Probability that at least one dangerous failure occurs within one hour.

= Probability that a safety system is in state “¬ok” (“dangerous undetectable” and “dangerous detectable”) within one hour and at least one demand occurs within that hour.

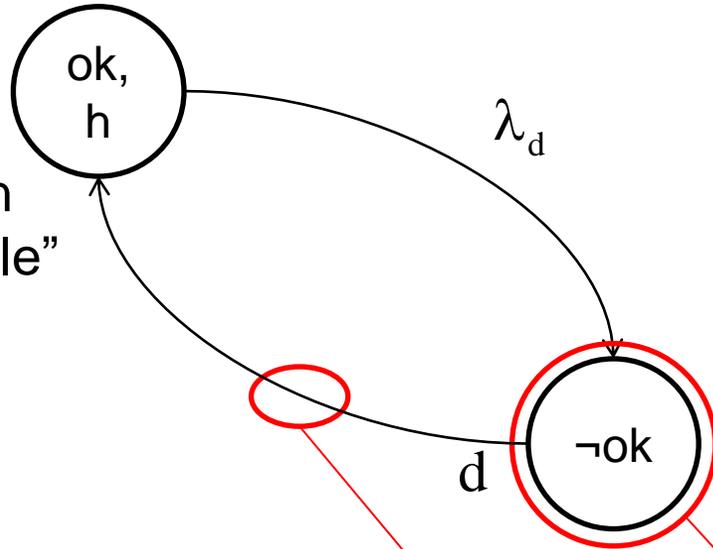
PFD

Probability of dangerous Failure on Demand

PFH^{Ed1}

Probability of dangerous Failure per Hour (PFH of 1st edition IEC 61508)

Probability that a safety system is in state “¬ok” (“dangerous undetectable” and “dangerous detectable”) within one hour and at least one demand occurs within that hour.



λ_d rate of dangerous errors
 d rate of safety demands

$$PFH^{Ed1}(t..t+1h) = PFD(t..t+1h) \cdot P(d(t..t+1h))$$

$$\leq \underline{PFD(t..t+1h, d = 0)} \cdot P(d(t..t+1h))$$

1. Average within that hour:
 $PFD(t..t+1h, d = 0) \approx PFD_{avg}(t..t+1h, d = 0)$
2. Maximum within that hour (worst case):
 $PFD(t..t+1h, d = 0) \leq PFD(t+1h, d = 0)$

PFD
 Probability of dangerous Failure on Demand

PFH^{Ed1}
 Probability of dangerous Failure per Hour
 (PFH of 1st edition IEC 61508)

$$PFH^{Ed1}(t..t+1h) = PFD(t..t+1h) \cdot P(d(t..t+1h))$$

$$\leq PFD(t..t+1h, d=0) \cdot \underline{P(d(t..t+1h))}$$

Random demand (here):
Characteristic like λ_d such that the state variables are exponentially distributed.

1. Random demand:

$$\dot{x}_1 = -d \cdot x_1$$

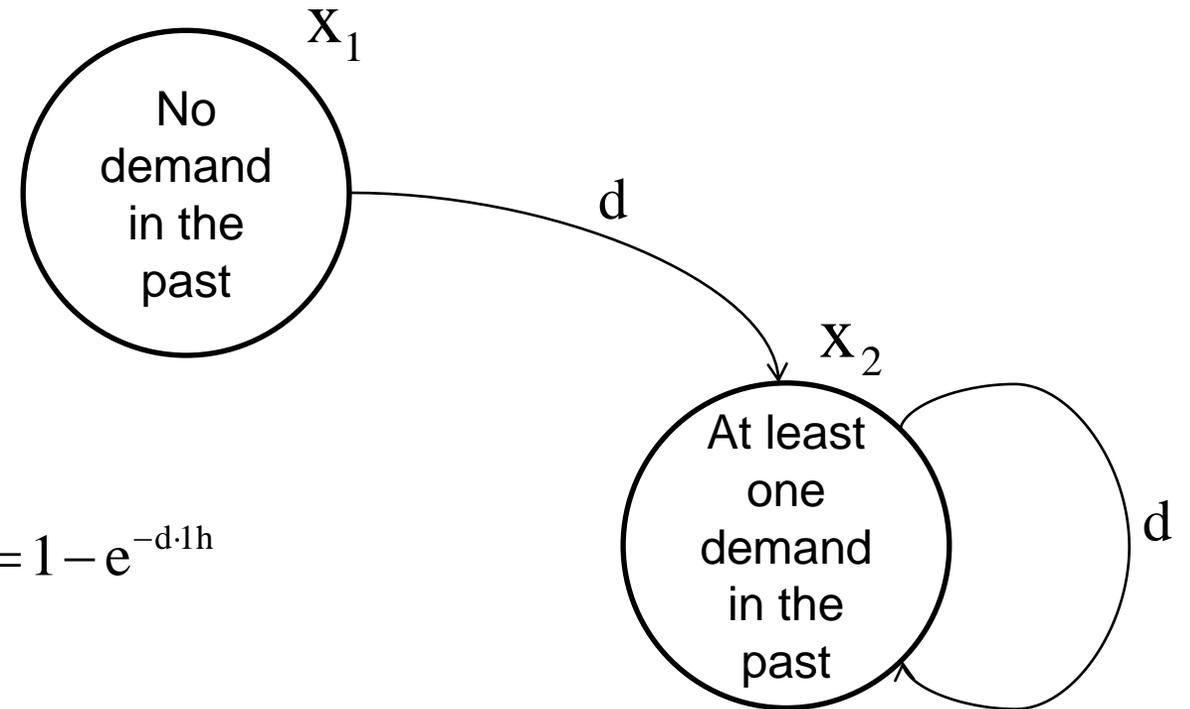
$$\dot{x}_2 = d \cdot x_1$$

$$x_1 + x_2 = 0$$

$$x_1(t_0) = 1, x_2(t_0) = 0$$

$$x_2(t) = 1 - e^{-d \cdot (t-t_0)}$$

$$P(d(t..t+1h)) = 1 - e^{-d \cdot 1h}$$



$$\begin{aligned} \text{PFH}^{\text{Ed1}}(t..t+1h) &= \text{PFD}(t..t+1h) \cdot P(d(t..t+1h)) \\ &\leq \text{PFD}(t..t+1h, d=0) \cdot \underline{P(d(t..t+1h))} \end{aligned}$$

2. Cyclic demand:

$$P(d(t..t+1h)) = \min(d \cdot 1h, 1)$$

Examples:

$$d = \frac{1}{1h} \Rightarrow P(d(t..t+1h)) = d \cdot 1h = 1$$

$$d = \frac{1}{2h} \Rightarrow P(d(t..t+1h)) = d \cdot 1h = 0.5$$

$$d = \frac{2}{1h} \Rightarrow P(d(t..t+1h)) = \min(d \cdot 1h, 1) = 1$$

$$\begin{aligned}
 \text{PFH}^{\text{Ed1}}(t..t+1h) &= \text{PFD}(t..t+1h) \cdot \text{P}(d(t..t+1h)) \\
 &\leq \text{PFD}(t..t+1h, d=0) \cdot \underline{\text{P}(d(t..t+1h))} \\
 &\leq \max(\underbrace{1 - e^{-d \cdot 1h}}_{\leq d \cdot 1h}, \min(d \cdot 1h, 1)) \\
 &\leq \min(d \cdot 1h, 1)
 \end{aligned}$$

$$\begin{aligned}
 \text{PFH}^{\text{Ed1}}(t..t+1h) &\leq \text{PFD}(t+1h, d=0) \cdot \min(d \cdot 1h, 1) \\
 \text{PFH}_{\text{avg}}^{\text{Ed1}}(T..T+1h) &\leq \text{PFD}_{\text{avg}}(T+1h, d=0) \cdot \min(d \cdot 1h, 1)
 \end{aligned}$$

$$\begin{aligned}
 \text{PFH}^{\text{Ed1}}(t..t+1h) &\leq \text{PFD}(t+1h, d=0) \\
 \text{PFH}_{\text{avg}}^{\text{Ed1}}(T..T+1h) &\leq \text{PFD}_{\text{avg}}(T+1h, d=0)
 \end{aligned}$$

Advantages:

- Characteristic of demand is not an inherent part of the math. model. Its characteristic is transferred to PFH.
- Reasonable upper limit.
- Continuous operation is manageable.

Advantages:

- No assumption about demand necessary, neither its rate nor its characteristic.
- Continuous operation is manageable.

- Motivation
- Markov Models
- PFD
- PFH
 - PFH^2
 - PFH^1
- Discussion
- Summary

$$\text{PFH}^{\text{Ed1}}(t..t + 1h) \leq \text{PFD}(t+1h, d = 0) \cdot \min(d \cdot 1h, 1)$$

$$\text{PFH}^{\text{Ed2}}(t) \leq \min(\text{PFD}(t, d = 0) \cdot d, \lambda_d)$$

For low demand systems, $d \leq \frac{1}{a}$ holds:

$$\begin{aligned} \text{PFH}^{\text{Ed1}}(t, t + 1h) &\leq \text{PFD}(t+1h, d = 0) \cdot \frac{1}{365 \cdot 24h} \cdot 1h \\ &\leq \text{PFD}(t+1h, d = 0) \cdot 1.1 \cdot 10^{-4} \end{aligned}$$

$$\begin{aligned} \text{PFH}^{\text{Ed2}}(t) &\leq \text{PFD}(t, d = 0) \cdot \frac{1}{365 \cdot 24h} \\ &\leq \text{PFD}(t, d = 0) \cdot 1.1 \cdot 10^{-4} \text{h}^{-1} \end{aligned}$$

Since a demand rate of once per year is assumed for low demand systems, PFH could be applied to low demand systems, too.

For example: $d = \frac{1}{2a}$ PFD applies
PFH applies with $d = \frac{1}{a}$ } same SIL

$$\begin{aligned}
 \text{PFH}^{\text{Ed1}}(t..t+1h) &= \text{PFD}(t..t+1h) \cdot P(d(t..t+1h)) \\
 &\leq \text{PFD}(t+1h, d=0) \cdot \min(d \cdot 1h, 1) \\
 &\leq \min(\underline{\text{PFD}(t+1h, d=0) \cdot d \cdot 1h}, \text{PFD}(t+1h, d=0))
 \end{aligned}$$

≈

$$\begin{aligned}
 \text{PFH}^{\text{Ed2}}(t) &= \text{PFD}(t) \cdot d \\
 &\leq \min(\underline{\text{PFD}(t, d=0) \cdot d}, \lambda_d)
 \end{aligned}$$

Different measuring units of the underlined parts, but (almost) equal numeric upper values that are differently limited by the minimum operation.

- Motivation
- Markov Models
- PFD
- PFH
 - PFH^{Ed2}
 - PFH^{Ed1}
- Discussion
- Summary

- Different worst-case approaches to PFD and PFH w.r.t. demand.
- Different PFH definitions in IEC 61508 editions with almost equal numerical values.
- Unknown demand (rate and characteristic) is manageable incl. continuous operation.
- One of the parameters, PFD or PFH, is sufficient.

$$\text{PFD}(t) \leq \text{PFD}(t, d = 0)$$

$$\text{PFD}(t, d = 0) = 1 - e^{-\lambda_d \cdot t}$$

$$\text{PFD}_{\text{avg}}(T) \leq \text{PFD}_{\text{avg}}(T, d = 0)$$

$$\text{PFD}_{\text{avg}}(T, d = 0) = 1 - \frac{1}{\lambda_d \cdot T} \cdot (1 - e^{-\lambda_d \cdot T})$$

$$\text{PFH}^{\text{Ed}2}(t) = \text{PFD}(t) \cdot d$$

$$\text{PFH}_{\text{avg}}^{\text{Ed}2}(T) = \text{PFD}_{\text{avg}}(T) \cdot d$$

$$\text{PFH}^{\text{Ed}2}(t) \leq \min(\text{PFD}(t, d = 0) \cdot d, \lambda_d)$$

$$\text{PFH}_{\text{avg}}^{\text{Ed}2}(T) \leq \min(\text{PFD}_{\text{avg}}(T, d = 0) \cdot d, \lambda_d)$$

$$\text{PFH}^{\text{Ed}1}(t..t + 1h) \leq \text{PFD}(t + 1h, d = 0) \cdot \min(d \cdot 1h, 1)$$

$$\text{PFH}_{\text{avg}}^{\text{Ed}1}(T..T + 1h) \leq \text{PFD}_{\text{avg}}(T + 1h, d = 0) \cdot \min(d \cdot 1h, 1)$$

- [1] IEC 61508: *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems*, Edition 1, 1998.
- [2] IEC 61508: *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems*, Edition 2, 2010.
- [3] Rausand, M.: *Reliability of Safety-Critical Systems – Theory and Applications*, Wiley, 2014.
- [4] Hauke, M. et. al.: *Functional Safety of Machine Controls*, BGIA Report 2/2008e, 2008.

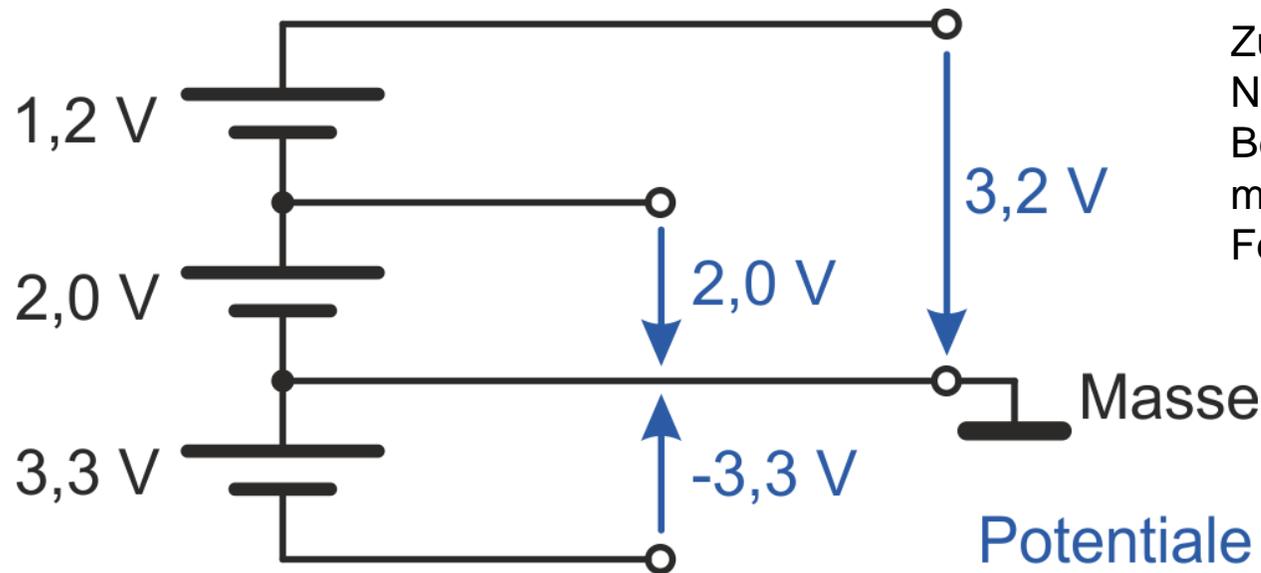
**„DIGITALISIERUNG UND KI IM SAFETY LIFECYCLE
AUS BETREIBER-SICHT –
SPANNUNG - POTENTIAL – ERDUNG...“**

www.yncoris.com

YNCORIS
Industrial Services

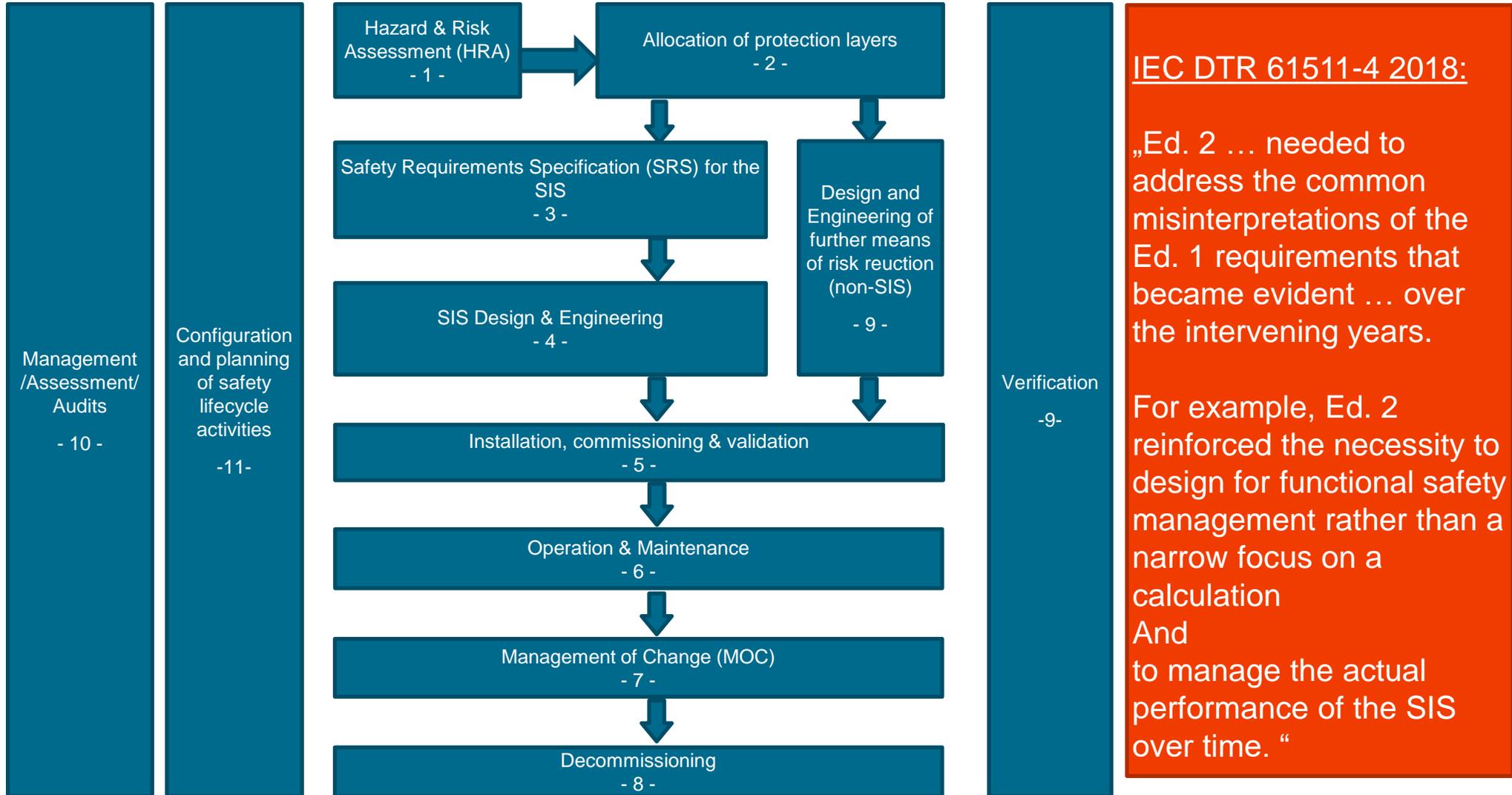
Das elektrische **Potential**, auch Coulomb-Potential, ist eine physikalische Größe in der klassischen Elektrodynamik. Es beschreibt die Fähigkeit eines elektrischen Feldes, Arbeit an einer elektrischen Ladung zu verrichten.

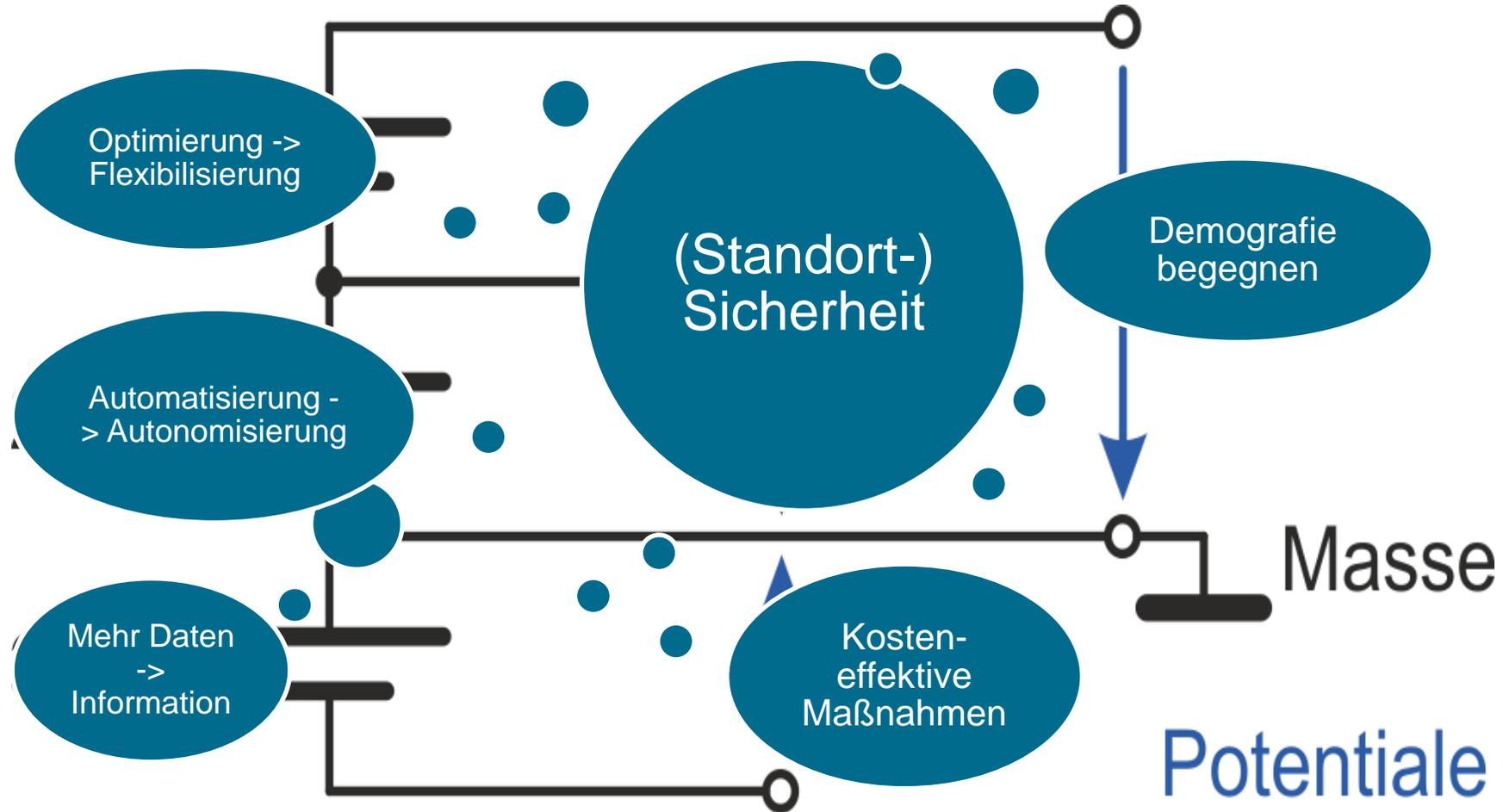
Die **Differenz der Potentiale** zwischen zwei Punkten wird als elektrische Spannung bezeichnet

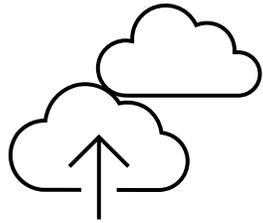


Zur Eindeutigkeit wird ein **Bezugspunkt** P0 festgelegt, der das Nullpotential erhält. [...] In der Elektrotechnik wird der Bezugspunkt auf dasjenige Leiterstück gelegt, das mit „Masse“ bezeichnet wird; **in der Theorie** der elektrischen Felder wird der Bezugspunkt oft „**ins Unendliche**“ gelegt.

Erdung hat zum Ziel, ein **definiertes Bezugspotential** [...] herzustellen. Als Bezugspotential (engl. reference potential) bezeichnet man in der Elektrotechnik einen Punkt in einer Schaltungsanordnung, auf den alle anderen elektrischen Potentiale bezogen werden. Dies ist meistens das Erdpotential







Nutzen/
Zukunftsfähigkeit

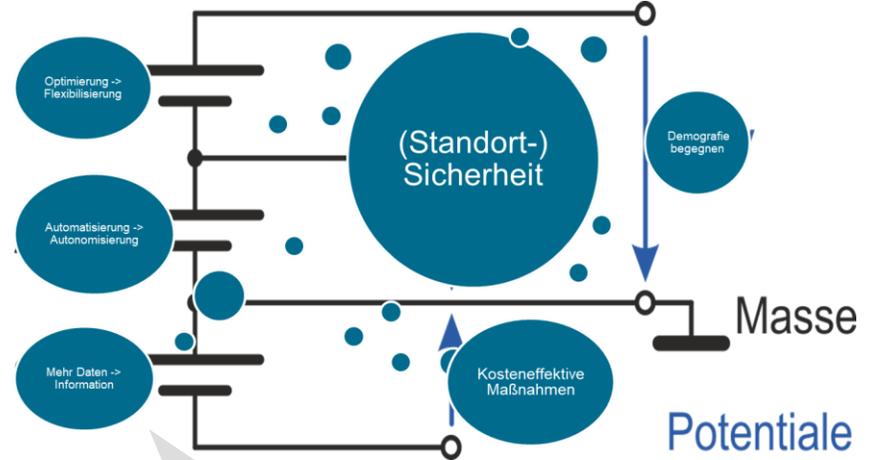


Wir machen das

<p>manuelle Aufwände reduzieren</p> <p>Diagnose als Teil flexibler Prüfkonzepte</p> <p>erhöhte Granularität -> noch genauere Auswertung möglich -> Optimierung</p> <p>Stördatenerhebung und Unterstützungsmöglichkeit für Betriebsbewährungsprozesse</p>	<p>Mehr ist nicht besser</p> <p>Die Arbeit bleibt doch bei mir hängen</p> <p>das hat schon mal nicht geklappt</p> <p>Die Verantwortung kann ich nicht abgeben</p>
--	---

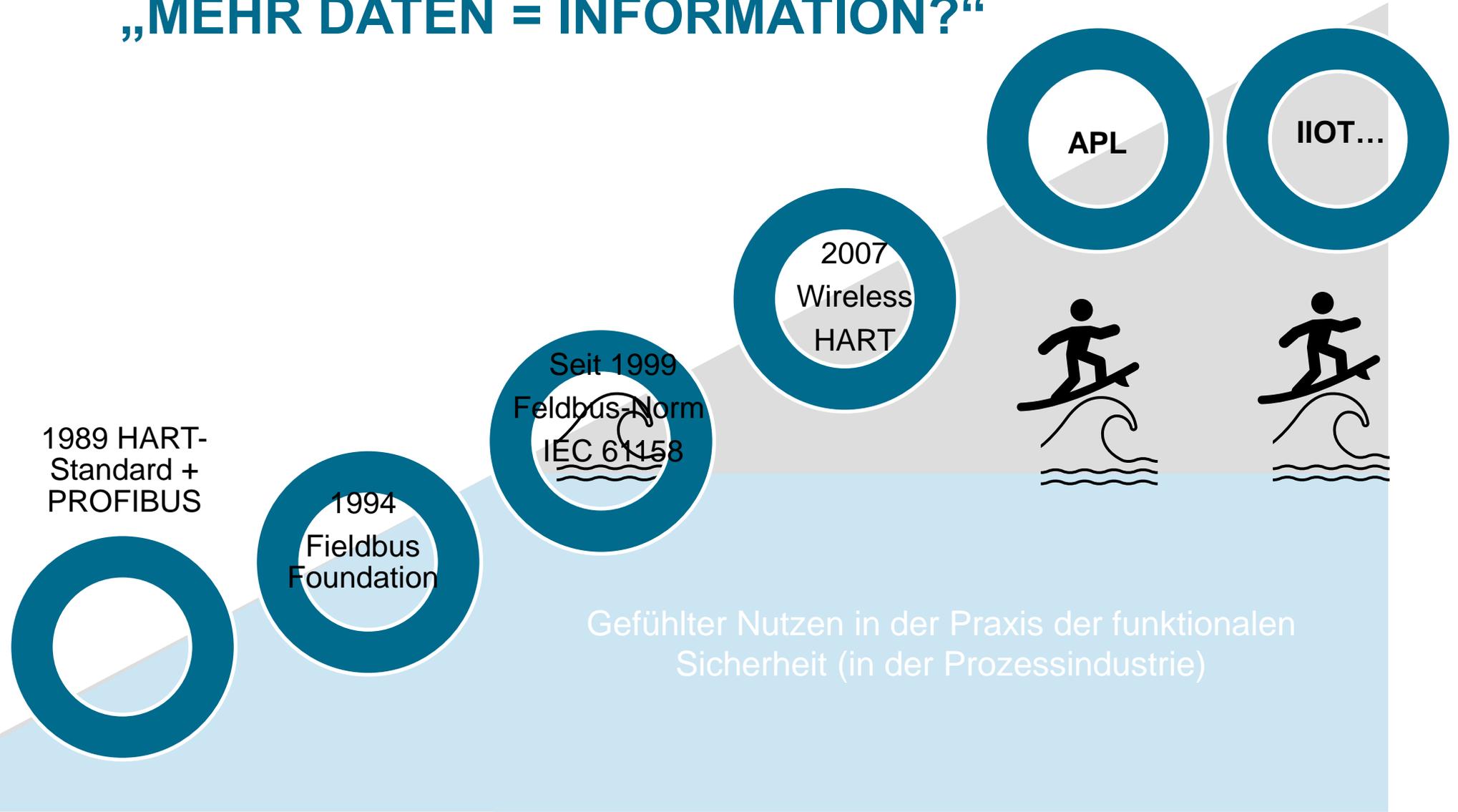
Wir lassen das

Kosten/
Risiko

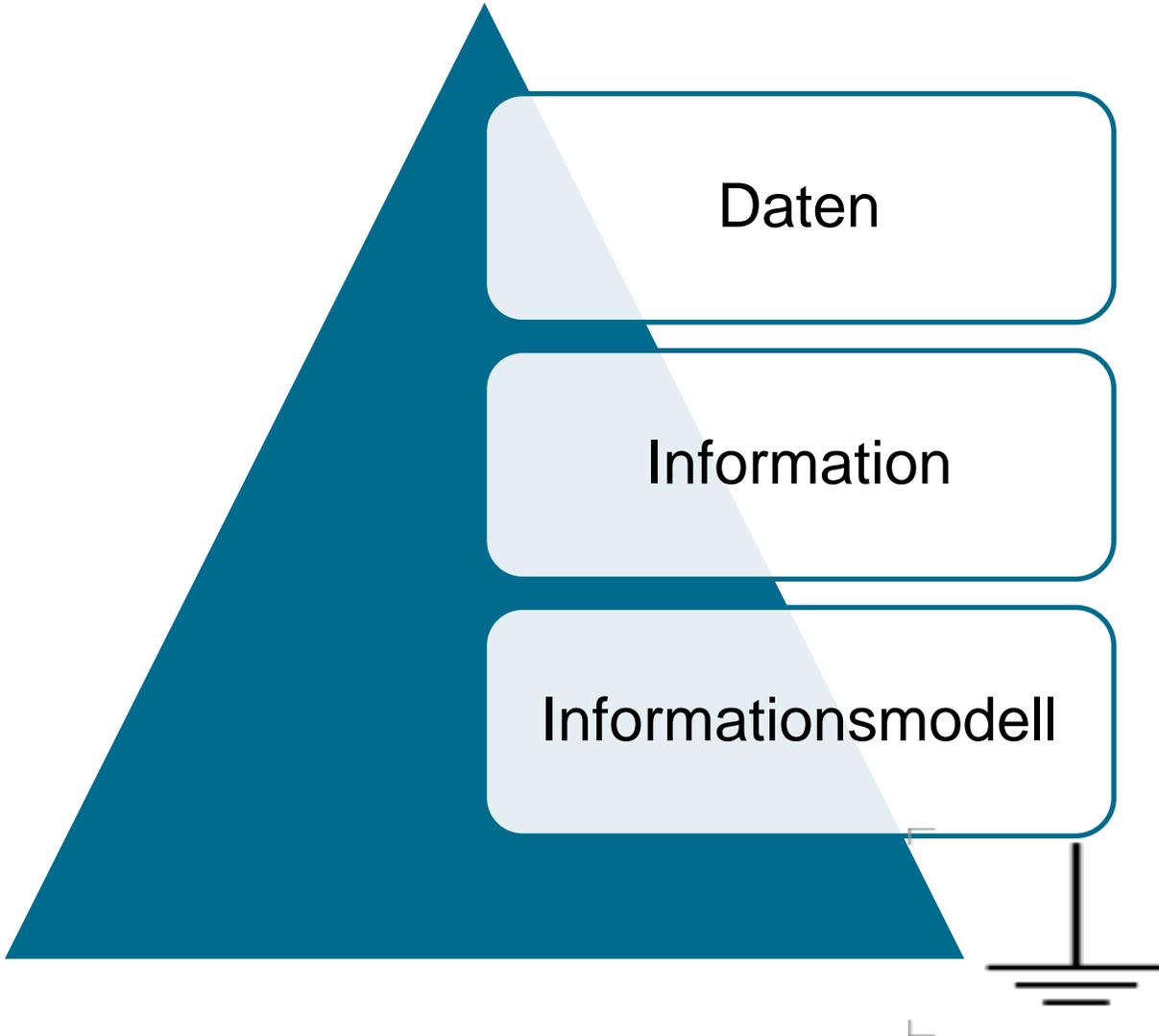


Mehr Daten -> Information

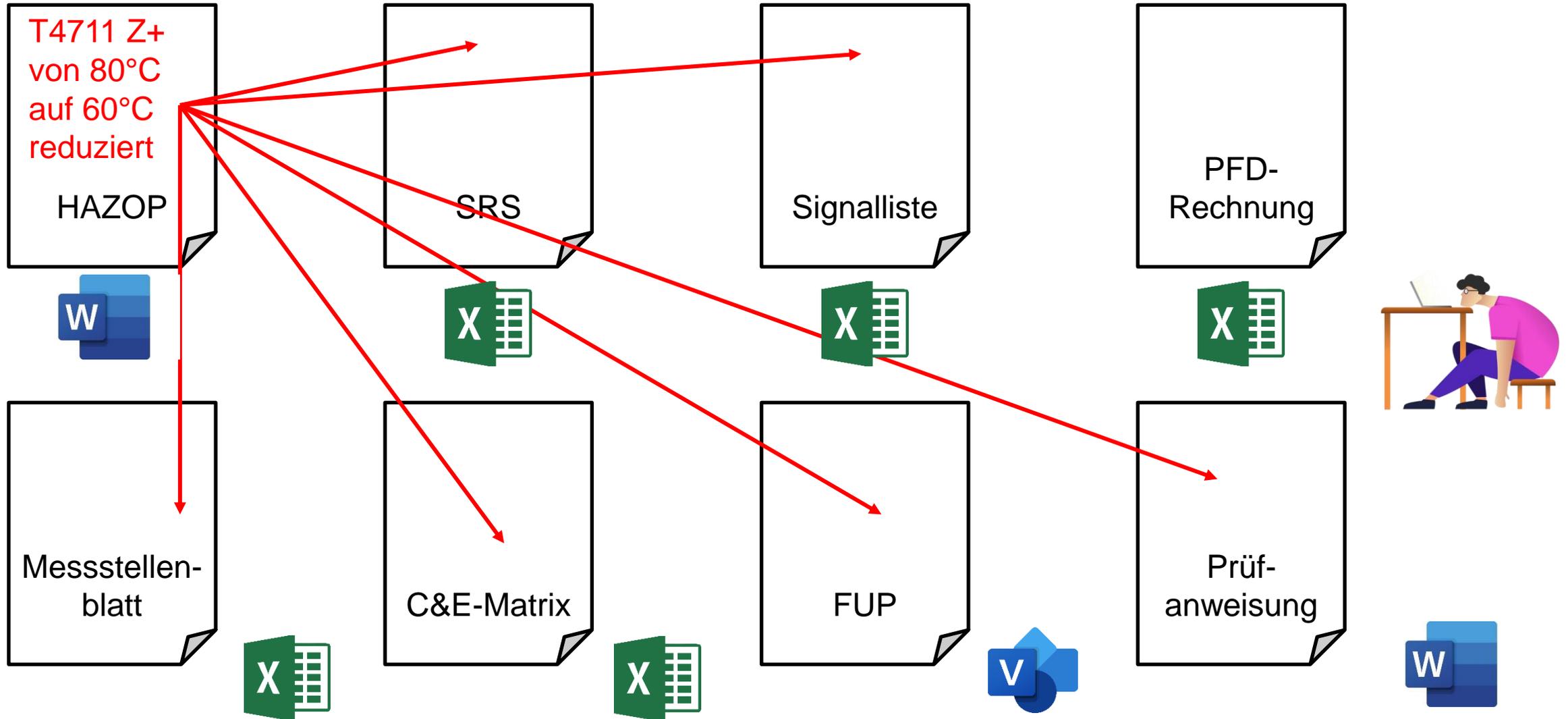
INTELLIGENTE/SMARTE DIGITALISIERUNG – MIT SPANNUNG ERWARTET... AM BEISPIEL „MEHR DATEN = INFORMATION?“



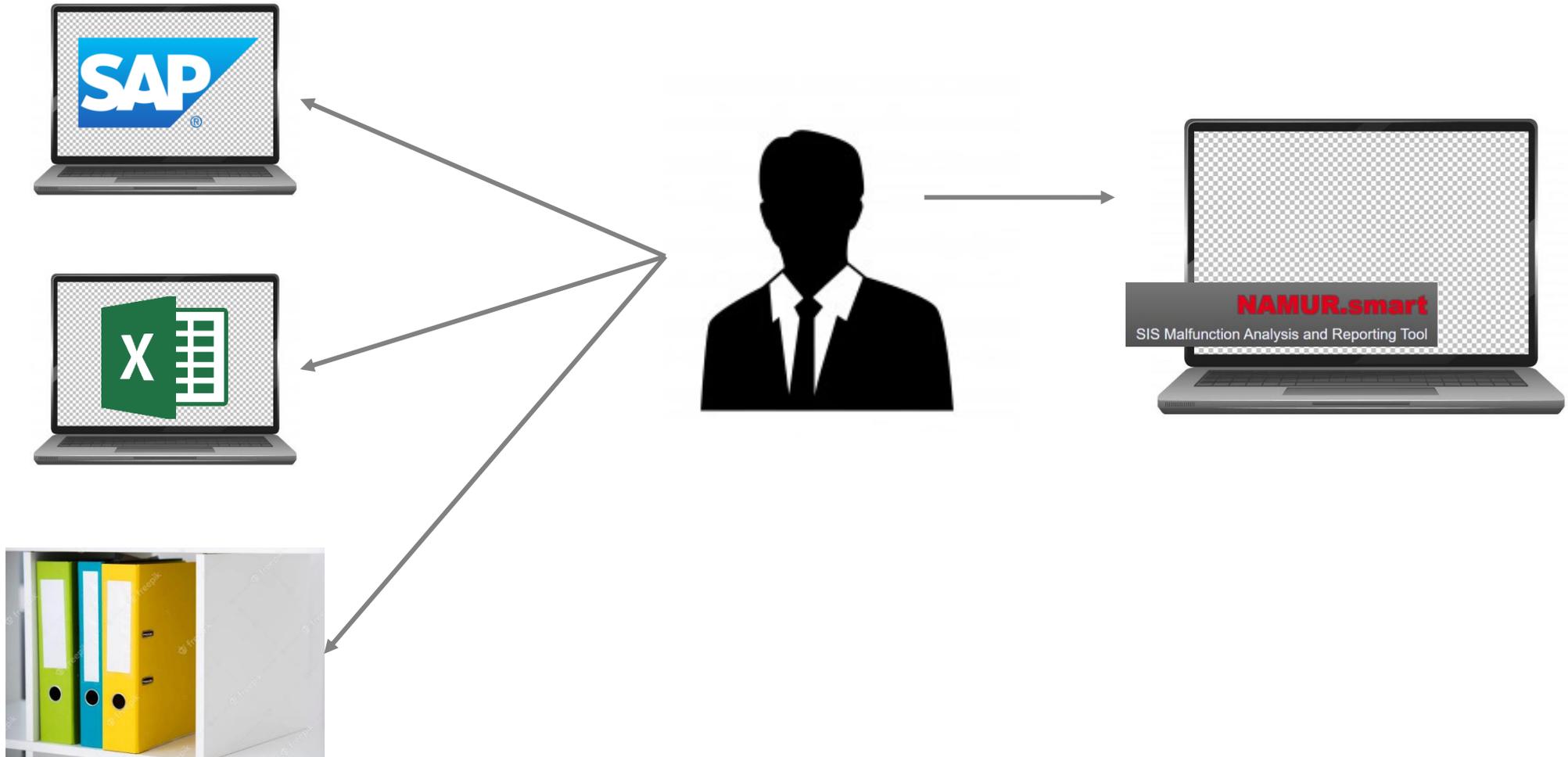
ERDUNG...INFORMATIONSMODELLE ALS DEFINIERTES BEZUGSPOTENTIAL?



Beispiel SIF-Engineering: TS der neuen Pumpe ist geringer

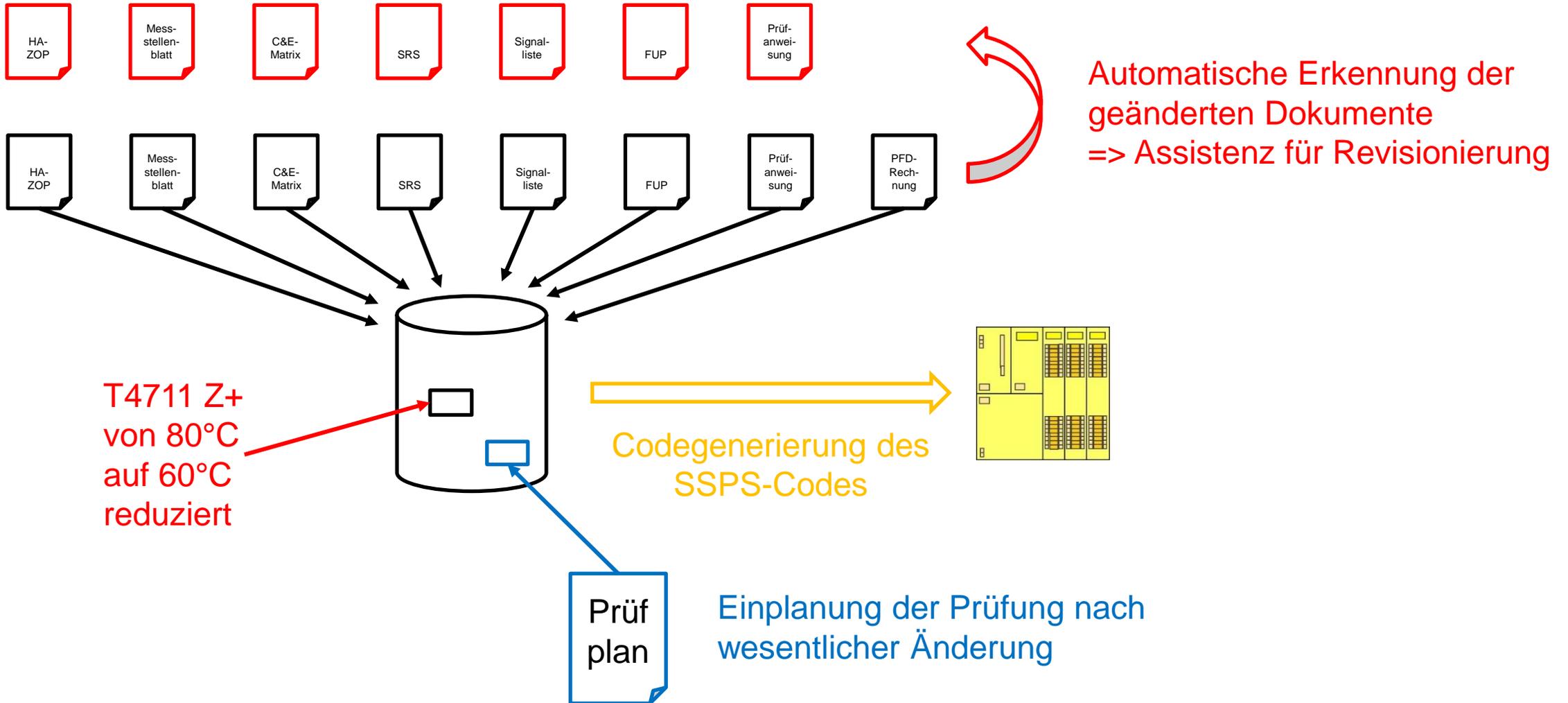


Klassische Ermittlung der Informationen



"Bild: Freepik.com". Diese Folie wurde mit Ressourcen von Freepik.com erstellt.

Vision: TS der neuen Pumpe ist geringer

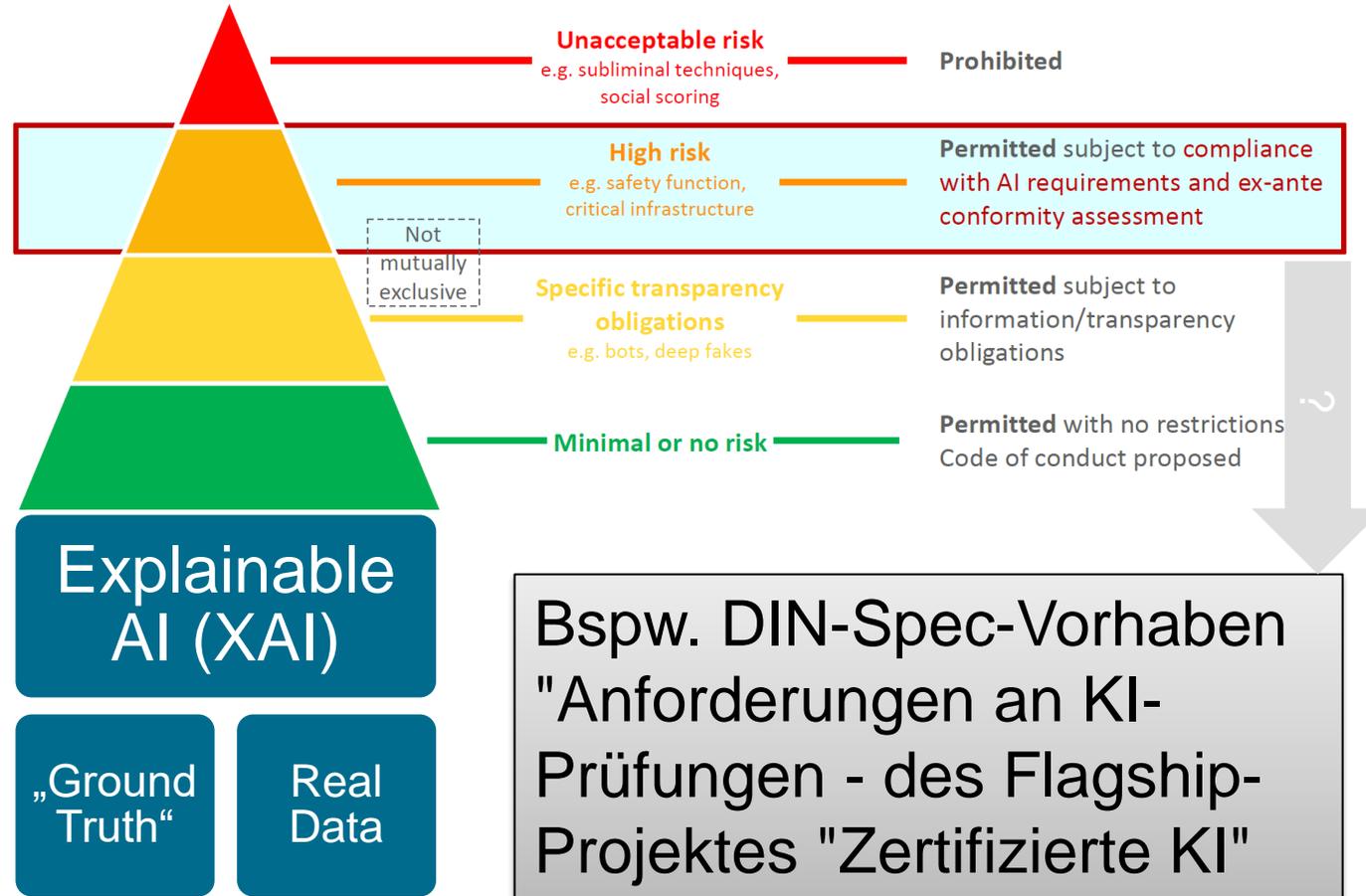


- Informationsmodelle können/müssen die funktionale Sicherheit sinnvoll unterstützen
- Entlang des Lebenszyklus werden Daten konsistent an die benötigten Stellen weitergegeben
- Dadurch wird die Qualität und die Sicherheit erhöht
- Beispiel NAMUR.smart
 - manueller Aufwand deutlich reduzieren
 - erhöhte Granularität -> noch genauere Auswertung möglich
 - Der gute Datenstand kann noch weiter verbessert werden
 - Unterstützungsmöglichkeit für Betriebsbewährungsprozesse

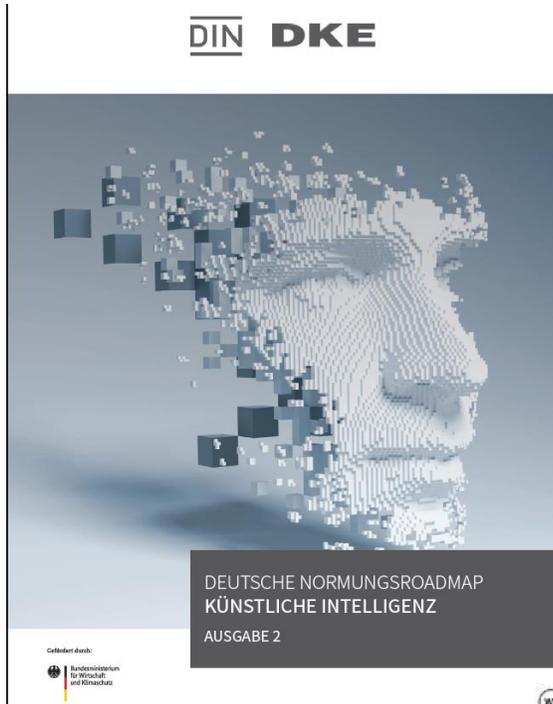


NRM KI (2.0) – PRÜFBARE KI (4 SAFETY)

Risk-based approach of AI regulation



SICHER NAVIGIEREN AUF DER NORMUNGSMAP (NRM) KI



- „Mit der Normungsroadmap wird eine Maßnahme der KI-Strategie der Bundesregierung umgesetzt und damit ein wesentlicher Beitrag zur „KI – Made in Germany“ geleistet.
- Die Normung ist Teil der KI-Strategie und ein strategisches Instrument zur Stärkung der Innovations- und Wettbewerbsfähigkeit der deutschen und europäischen Wirtschaft. Nicht zuletzt deshalb spielt sie im geplanten europäischen Rechtsrahmen für KI, dem **Artificial Intelligence Act**, eine besondere Rolle. [...]

Risk-based approach of AI regulation

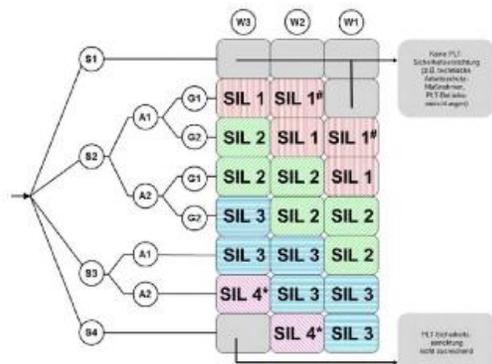
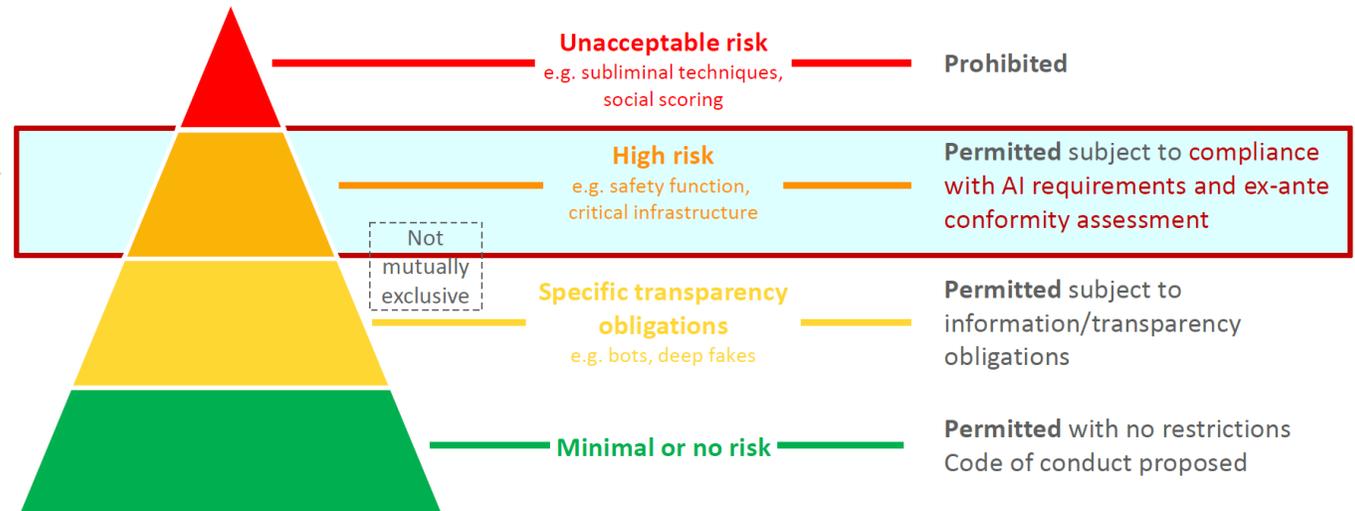


Bild 1 Risikograph und Beziehung zwischen den Sicherheits-Integritätslevel (SIL) gemäß VDI/VDE 2190 Blatt 1 - # PLT-BS in VDI 2190, jedoch Umsetzung in SIL 1 empfohlen



SICHER NAVIGIEREN AUF DER NORMUNGSROADMAP (NRM) KI

DIN DKE

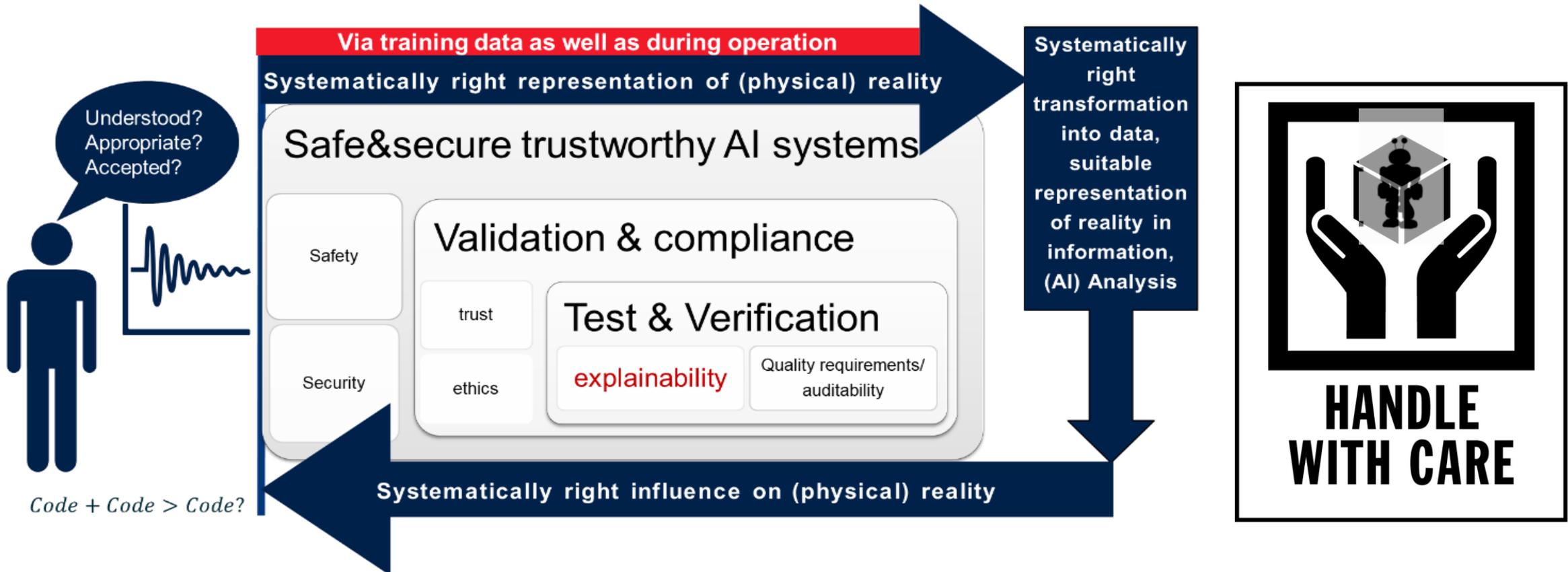


- „Mit der Normungsroadmap wird eine Maßnahme der KI-Strategie der Bundesregierung umgesetzt und damit ein wesentlicher Beitrag zur „KI – Made in Germany“ geleistet.
- Die Normung ist Teil der KI-Strategie und ein strategisches Instrument zur Stärkung der Innovations- und Wettbewerbsfähigkeit der deutschen und europäischen Wirtschaft. Nicht zuletzt deshalb spielt sie im geplanten europäischen Rechtsrahmen für KI, dem **Artificial Intelligence Act**, eine besondere Rolle. [...]
- Für eine breite Nutzung von KI-Lösungen spielt die **Sicherheit von KI-Systemen** eine entscheidende Rolle. Nur eine tiefgehende Betrachtung von Anforderungen beispielsweise an die Betriebs- und Informationssicherheit kann einen umfassenden Einsatz von KI-Systemen in Wirtschaft und Gesellschaft ermöglichen.
- Ein weiteres Schwerpunktthema und Grundlage für einen breiten Markterfolg von KI sind die **Prüfung und Zertifizierung**. Hierfür braucht es verlässliche Qualitätskriterien und reproduzierbare Prüfverfahren, mit denen sich die Eigenschaften von KI-Systemen überprüfen lassen. Sie sind eine Schlüsselvoraussetzung für die Bewertung der Qualität von KI-basierten Anwendungen und tragen maßgeblich zur **Erklärbarkeit und Nachvollziehbarkeit** bei – zwei Faktoren, die **Vertrauen und Akzeptanz** schaffen.

HANDLE WITH CARE...

„Die Möglichkeiten sind grenzenlos – und doch sollte sich eine so einflussreiche Technologie innerhalb bestimmter Grenzen bewegen, damit sie uns tatsächlich hilft. Eine zuverlässige, funktionale und vor allem sichere KI braucht gewisse Regeln: zunächst ein gemeinsames Verständnis und eine einheitliche Sprache, sodass alle vom Gleichen reden. [...] Normen und Standards spielen dabei eine wichtige Rolle.

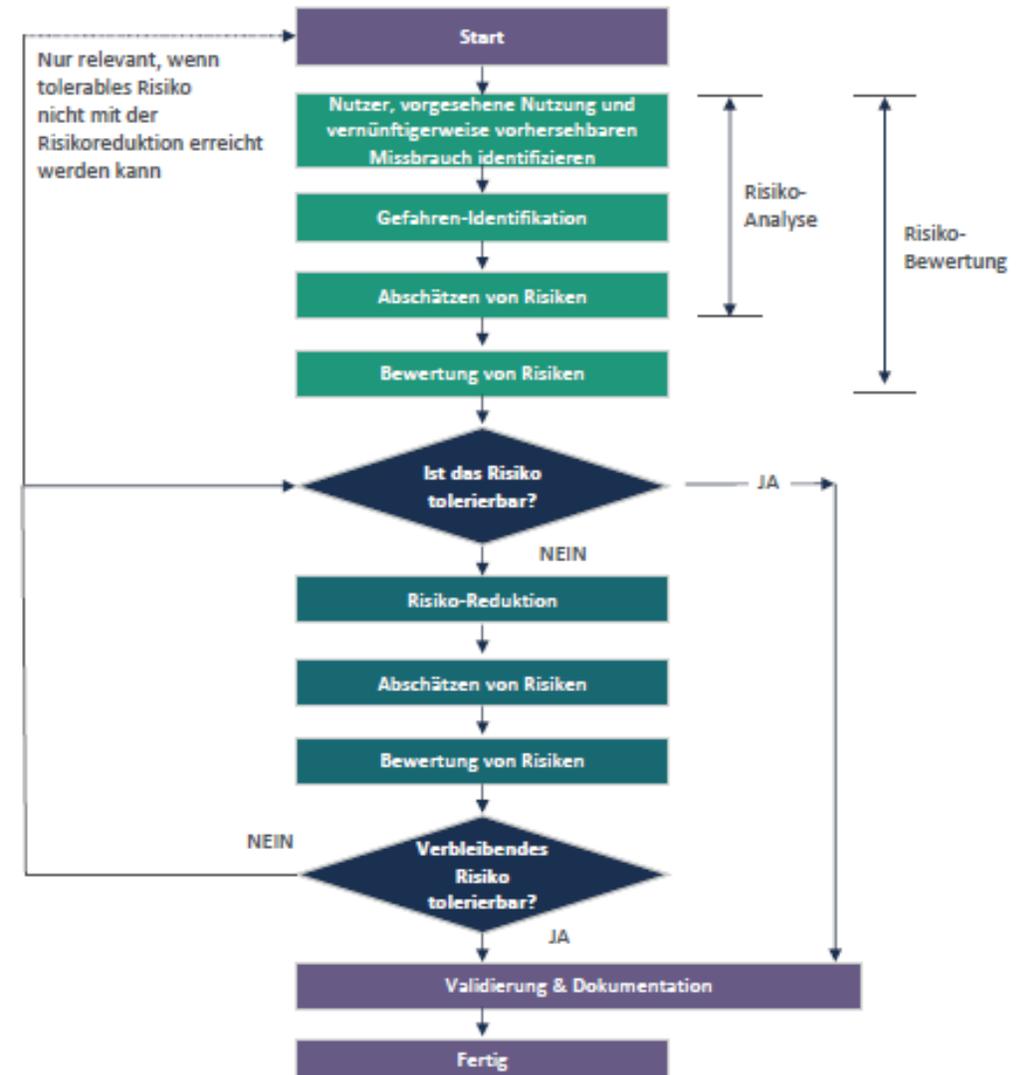
Sie ermöglichen eine zuverlässige und sichere Anwendung von KI-Technologien und tragen zur Erklärbarkeit und Nachvollziehbarkeit bei. Das wiederum macht sie zu Schlüsselfaktoren für die Akzeptanz von KI-Anwendungen.“ (Einleitung, 2. Ausgabe NRM KI)



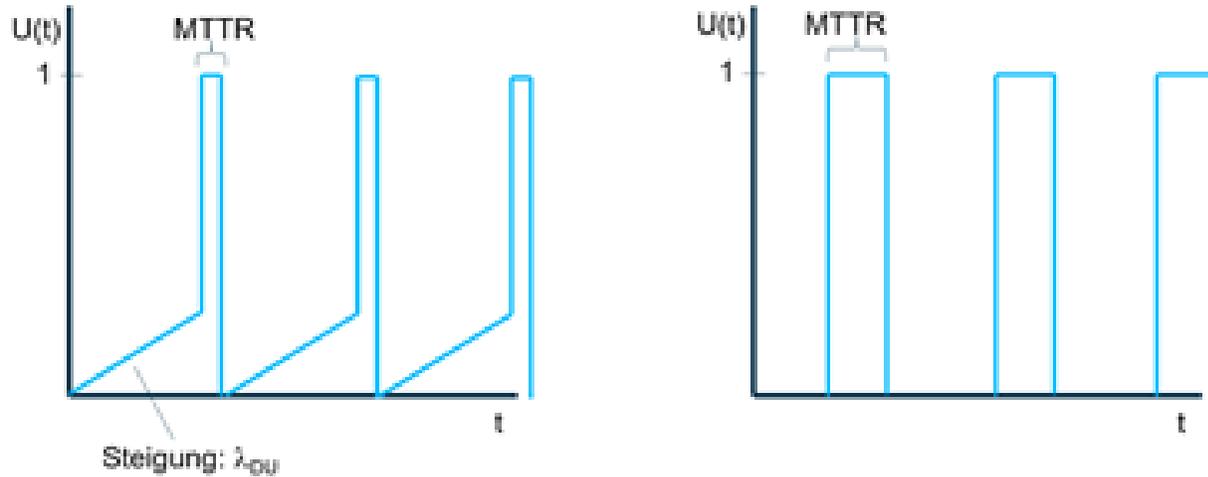


Ohne Ziel ist jeder Weg falsch.

Konfuzius, chinesischer Philosoph



PERFEKTE DIAGNOSE IM DIGITALISIERTEN SICHERHEITSLEBENSZYKLUS = PERFEKTE SICHERHEIT?



Lambda_D = 1 in X Jahren
 die perfekte Diagnose-
 Einrichtung(100% DC) macht daraus
 Lambda_DU = 0 -> PFD = 0?
 Unverfügbarkeit = 0?

-> Unverfügbarkeit im Hinblick auf
 Lambda_DD und MTTR wird zum
 entscheidenden Kriterium anstatt wie
 gewohnt das Lambda_DU

Generell ist die Unverfügbarkeit von Komponenten i bezogen auf gefährliche entdeckte Fehler λ_{DD} (nach [1], für große Zeiten t):

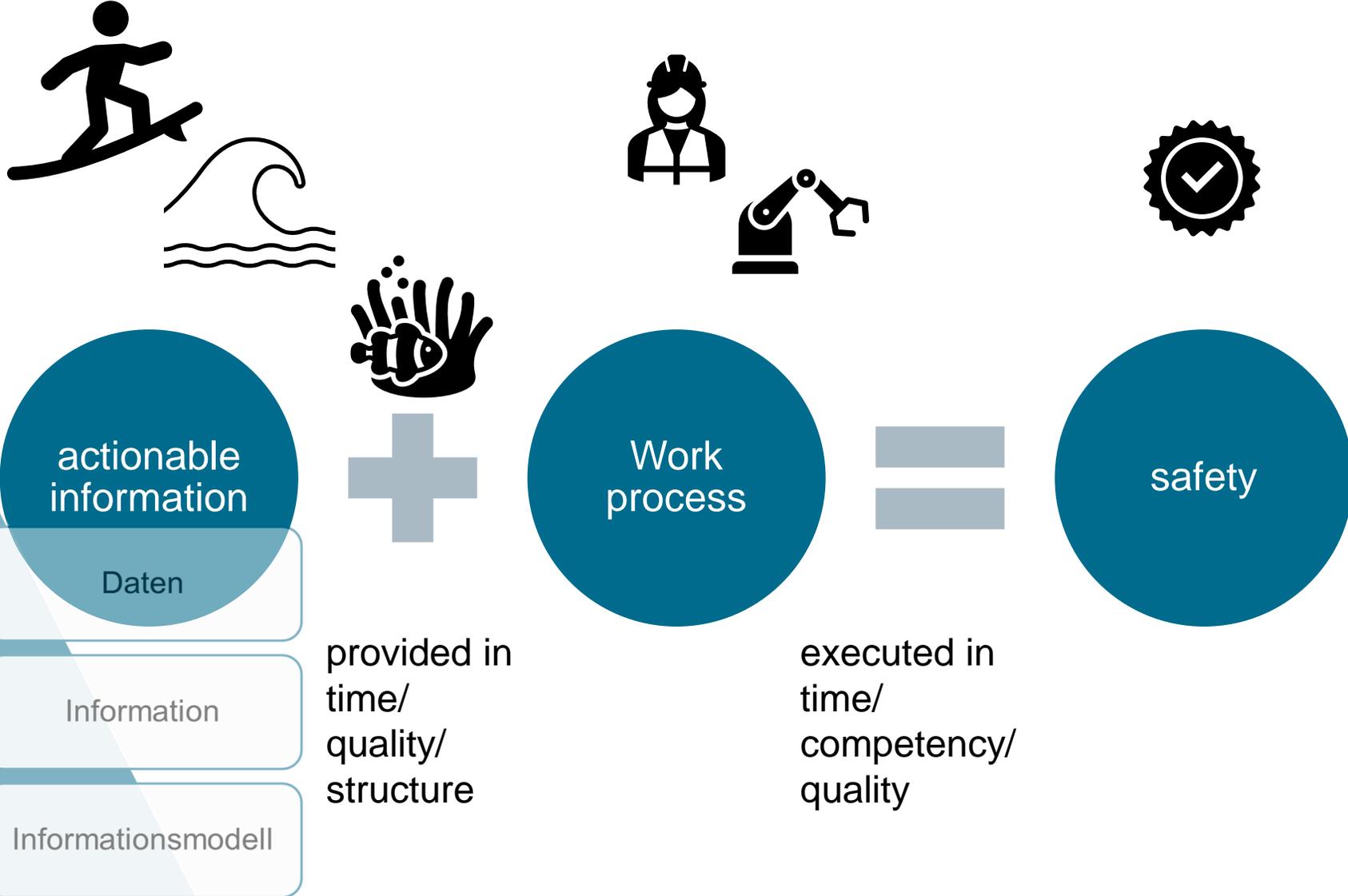
$$U_{DD, i}(t) = \frac{\lambda_{DD, i}}{\lambda_{DD, i} + \mu} (1 - e^{-(\lambda_i + \mu)t}) \approx \frac{\lambda_{DD, i}}{\lambda_{DD, i} + \mu}$$

Die Reparaturrate μ ist hierbei der Kehrwert der mittleren Systemausfalldauer MTTR (Mean Time to Restoration).

Quelle: NE146

Damit theoretisch dem „Zufall“ keine Chance gelassen, aber systematisch richtig umso mehr auf entsprechende Reparaturzeit MTTR zum Erreichen möglichst geringer Unverfügbarkeit angewiesen.

FELDGLEICHUNG...



NAMUR@
LinkedIn



NAMUR
Homepage

**THANKS FOR YOUR ATTENTION AND A
PRODUCTIVE DISCUSSION**

Marco Knödler

- NAMUR WG 4.5 – VDI/VDE-GMA FA 2.18 & 3.22
- DIN NA 003-01-01 AA - CEN/TC 69/WG 1 -
- DKE STD_1941.0.8 - SCI 4.0 Expert Panel AI in Industrial Applications





Praktische Erfahrungen in Auslegung von PLT-Sicherheitseinrichtungen

Persönliche Vorstellung

Persönliche Vorstellung:

Malika Mast

Geschäftsführerin RAMSYS GmbH

- FSCEA (Functional Safety Certified Engineer Application)
A031_01255/18 (TÜV Nord)
- FS Eng für Maschinen
14527/17 (TÜV Rheinland)
- FS Eng im Arbeitsgebiet Explosion Protection
Id.-Nr.: 0328/2019 (TÜV Süd)

Kontaktdaten:

Hervester Straße 36

46286 Dorsten

Tel.: +49 (0)2369 / 74593-10

m.mast@ramsys.org

www.ramsys.org



Agenda

I. Auslegung in der Theorie

- (1) Functional Safety Managementsystem
- (2) Prozessanschluss
- (3) Zusammenspiel Engineering / FuSi

II. In der Praxis

- (1) Kommunikation Projektteams / Betrieb
- (2) SIL? Und jetzt?
- (3) Projektablauf inklusive FuSi
- (4) Einkauf von Dienstleistern
- (5) Entwicklung der PFD-Berechnung

III. Dokumentation

- (1) FuSi-Dokumentation
- (2) Ablagemanagement

I. Auslegung in der Theorie

- (1) Functional Safety Managementsystem
- (2) Prozessanschluss
- (3) Zusammenspiel Engineering / FuSi

(1) FSM

- Regelt den Ablauf des Sicherheitslebenszyklus in einem Unternehmen
 - Schnittstellenmanagement
 - Arbeitsanweisungen
 - Prozessbeschreibungen
 - Formblätter
 - Etc.

BESCHEINIGUNG ♦ ATTESTAZIONE
BESCHEINIGUNG ♦ ATTESTAZIONE ♦ CONSTANCIA ♦ СВИДЕТЕЛЬСТВО ♦ 証明書 ♦ ATTESTATION



BESCHEINIGUNG

Hiermit wird bescheinigt, dass das Unternehmen

RAMSYS GmbH
Hervester Straße 36
46286 Dorsten
Deutschland

für die durch das Unternehmen durchgeführten Tätigkeiten, die den Sicherheitslebenszyklus eines Sicherheitstechnischen Systems betreffen, insbesondere

Planung, Programmierung, Montagebegleitung sowie Inbetriebnahmeunterstützung

ein Managementsystem der Funktionalen Sicherheit gem.

**DIN EN 61511-1, Abschnitt 5 u.
DIN EN 61508-1, Abschnitt 6**

eingeführt hat und anwendet.

Dauer der Gültigkeit
siehe Auditbericht Br-ET-2946-2019-01 vom 23.09.2019

TÜV SÜD Industrie Service GmbH
Niederlassung Regensburg
Abteilung Elektro- und Gebäudetechnik

Regensburg, 2019-09-23



Christian Eberle

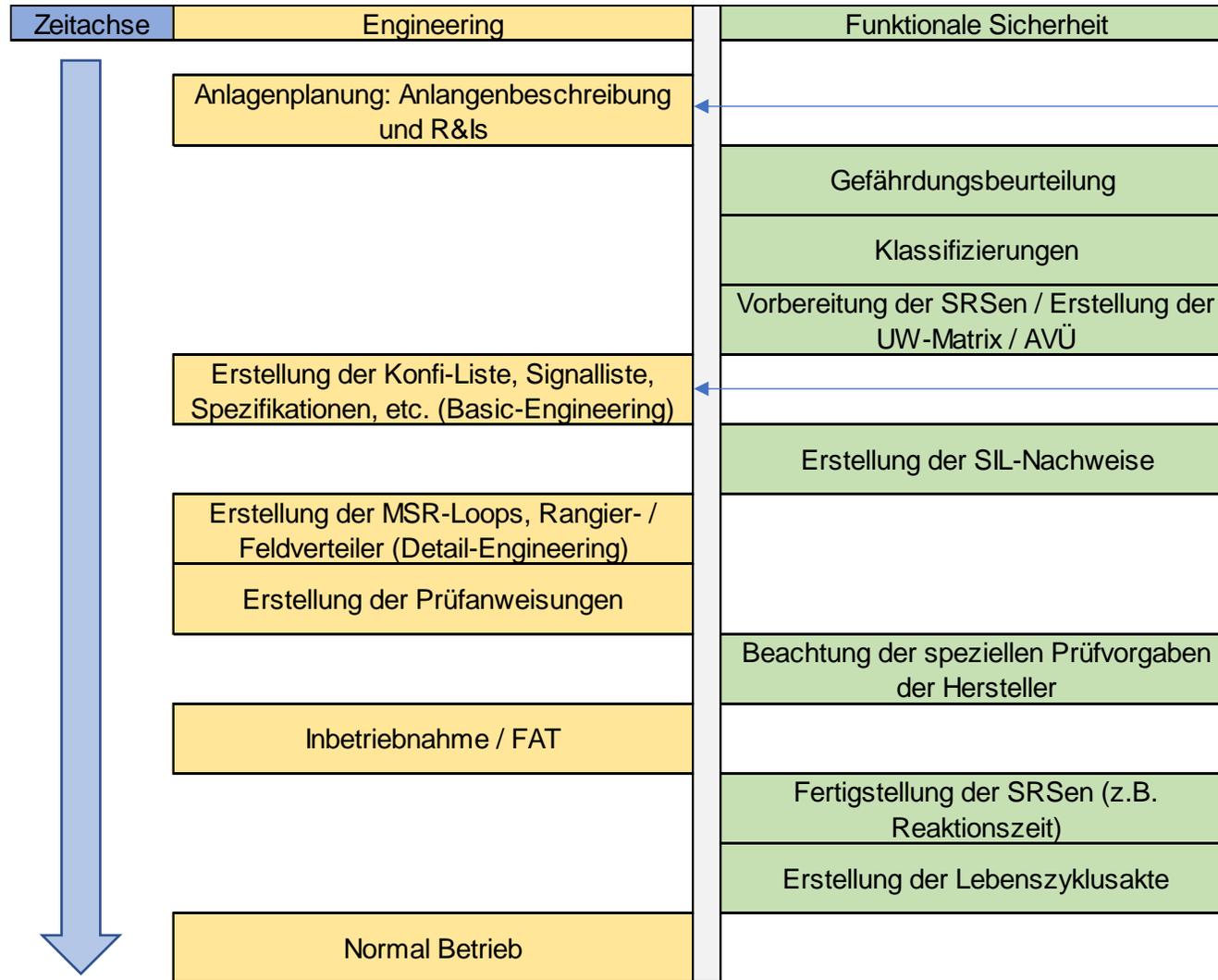
TUV®

(2) Prozessanschluss

- ◆ Prozessdaten und zusätzliche Anforderungen (SIL, Ex, Werksstandards, etc.) Spezifikationen / SRS
- ◆ Eignung der Geräte
- ◆ SSPS ist nicht gleich PLS
- ◆ Verschaltung der Geräte
- ◆ Kennzeichnung in der Dokumentation
- ◆ Besondere Anforderungen an das Prüfkonzept
- ◆ Prozesssicherheitszeit und Reaktionszeit



(3) Zusammenspiel Engineering / FuSi



Ablauf kann je nach Firma / Projekt variieren

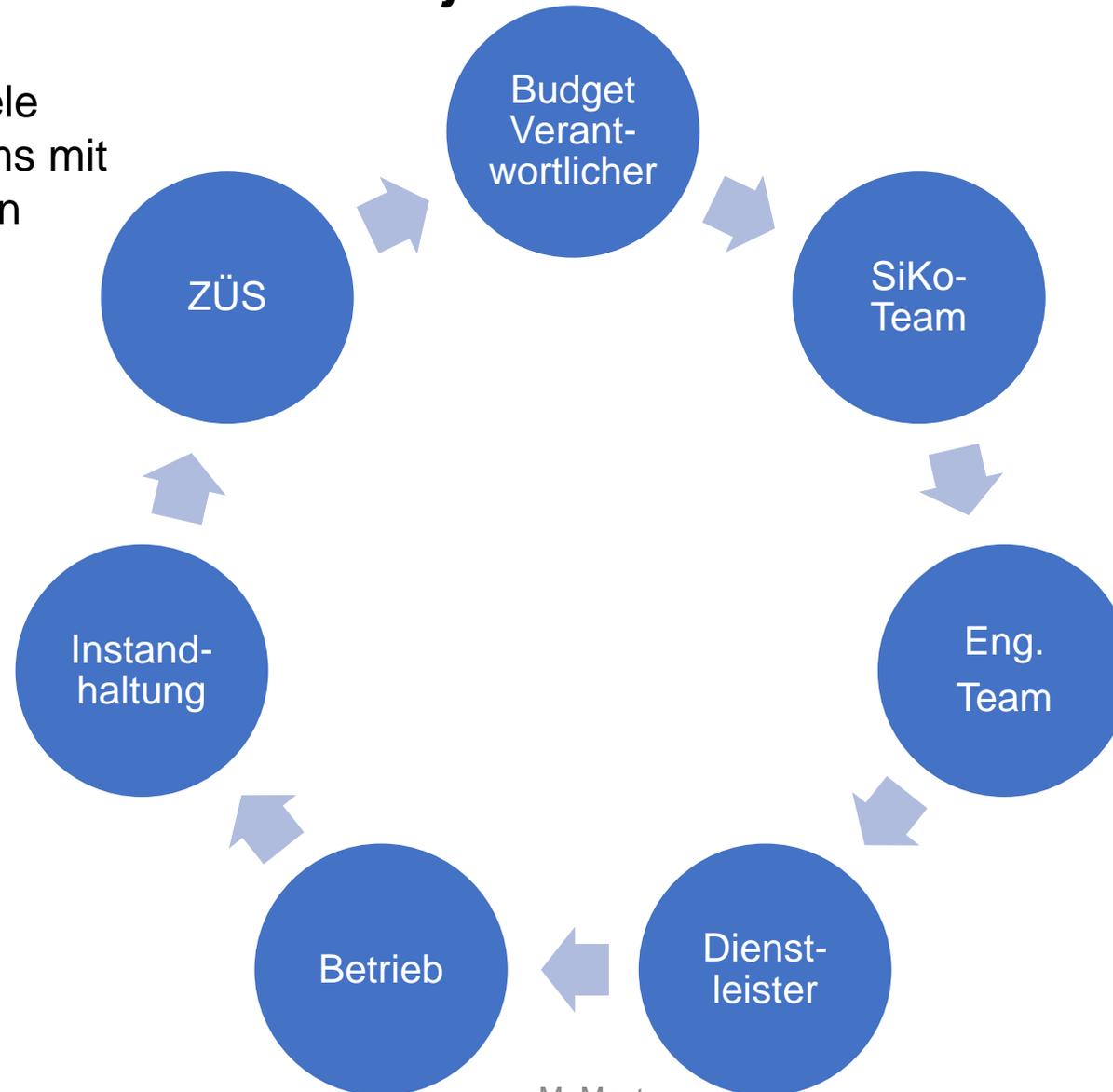
- Funktionale Sicherheit
- Engineering

II. In der Praxis

- (1) Kommunikation Projektteams / Betrieb
- (2) SIL? Und jetzt?
- (3) Projektablauf inklusive FuSi
- (4) Einkauf von Dienstleistern
- (5) Entwicklung der PFD-Berechnung

(1) Kommunikation Projektteams / Betrieb

In der Praxis gibt es viele Schnittstellen und Teams mit unterschiedlichen Zielen



(2) SIL? Und jetzt?

- ◆ Man spricht gerne bei der Realisierung von Maßnahmen und Anforderungen davon, diese nach aktuellem Stand der Technik umzusetzen
- ◆ „Der Stand der Technik“ ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Anlagen, die die praktische Eignung einer Maßnahme zum Schutz der Gesundheit und Sicherheit der Beschäftigten gesichert erscheinen lässt
- ◆ Der Stand der Technik wird in anerkannten Regelwerken festzulegen, z.B.
 - ◆ Normen
 - ◆ Richtlinien
 - ◆ Technische Regeln
 - ◆ Verordnungen

Klingt doch sehr gut und sehr einfach, oder nicht?

(2) SIL? Und jetzt?

Prozessindustrie

Transportmittel

Maschinen

Verordnungen

Sonstiges

DIN EN 61508

DIN EN 50400

MDI

EN 61511

DGRL

DIN EN 61511

DIN EN 60601

VDI / VDE 218

DIN EN 62304

DIN EN 746-2

DIN EN 61513

DIN EN 12952

DIN ISO 15998

DIN EN 12953

DIN ISO 25119

NE 130

DIN EN 16590

NE 93

DIN EN 12999

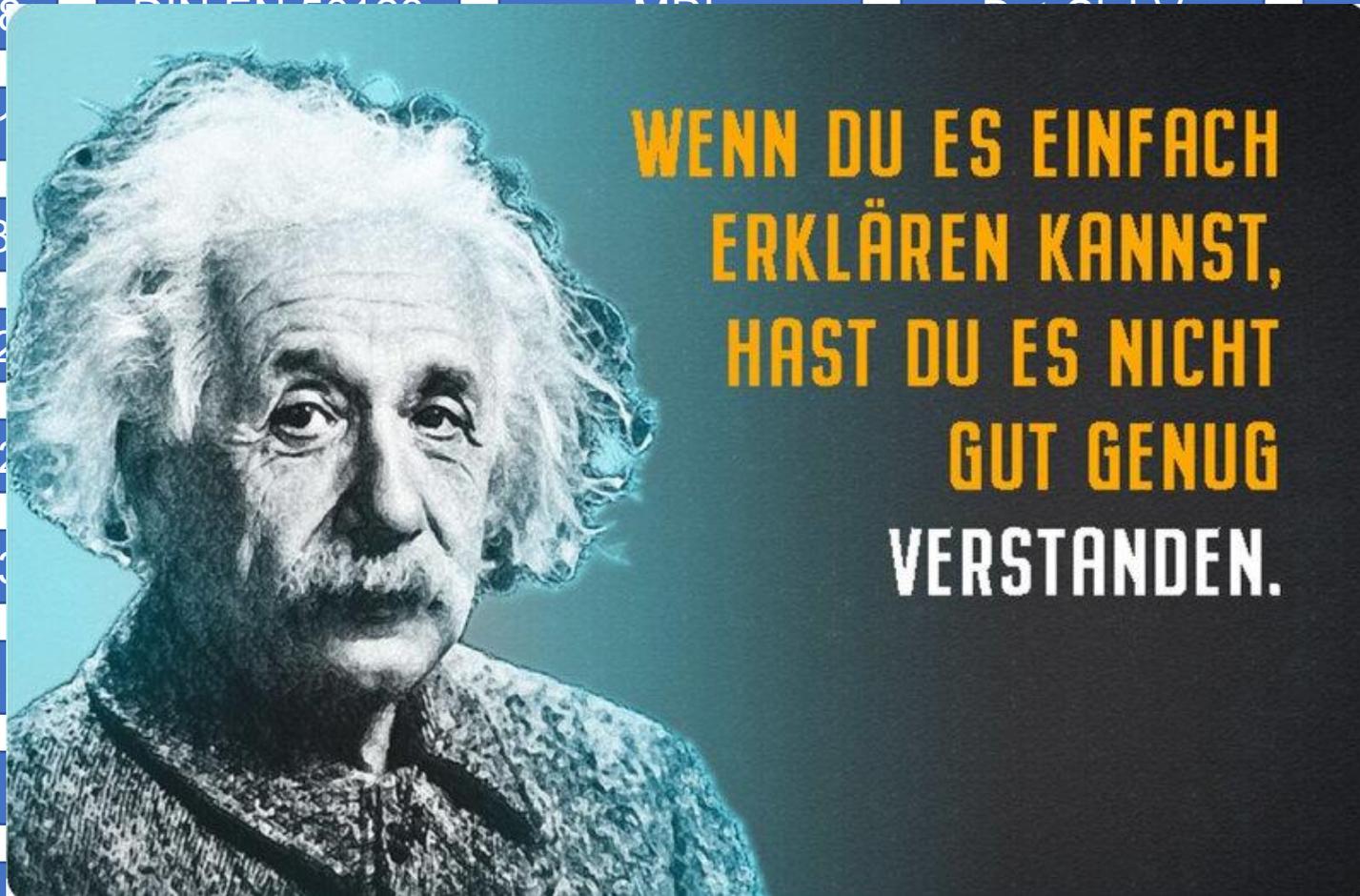
NA 106

BoStrab

CE-Konformität

DIN EN 61511

DIN IEC 60880



(3) Projektablauf inklusive FuSI: Praxis / Theorie



(4) Einkauf von Dienstleistern

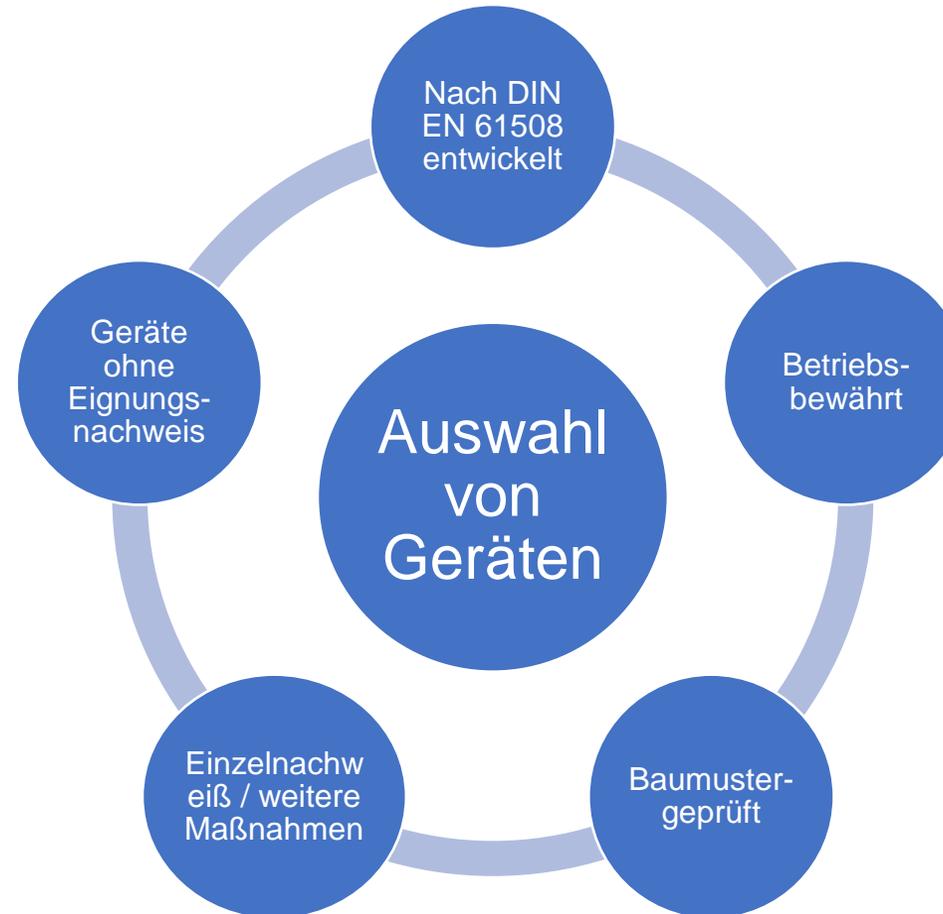
- Wie entscheide ich wer für mich arbeitet?
 - Liegt ein implementiertes FSM vor? (Eigentlich sollte dann auch ein QM vorliegen)
 - Besitzen die Mitarbeiter die entsprechende Qualifikation?
 - FSE (Engineering), SSPS-Zertifikat (Programmierer)

5 ANZEICHEN FÜR DEN RICHTIGEN DIENSTLEISTER



(5) Entwicklung der PFD-Berechnung

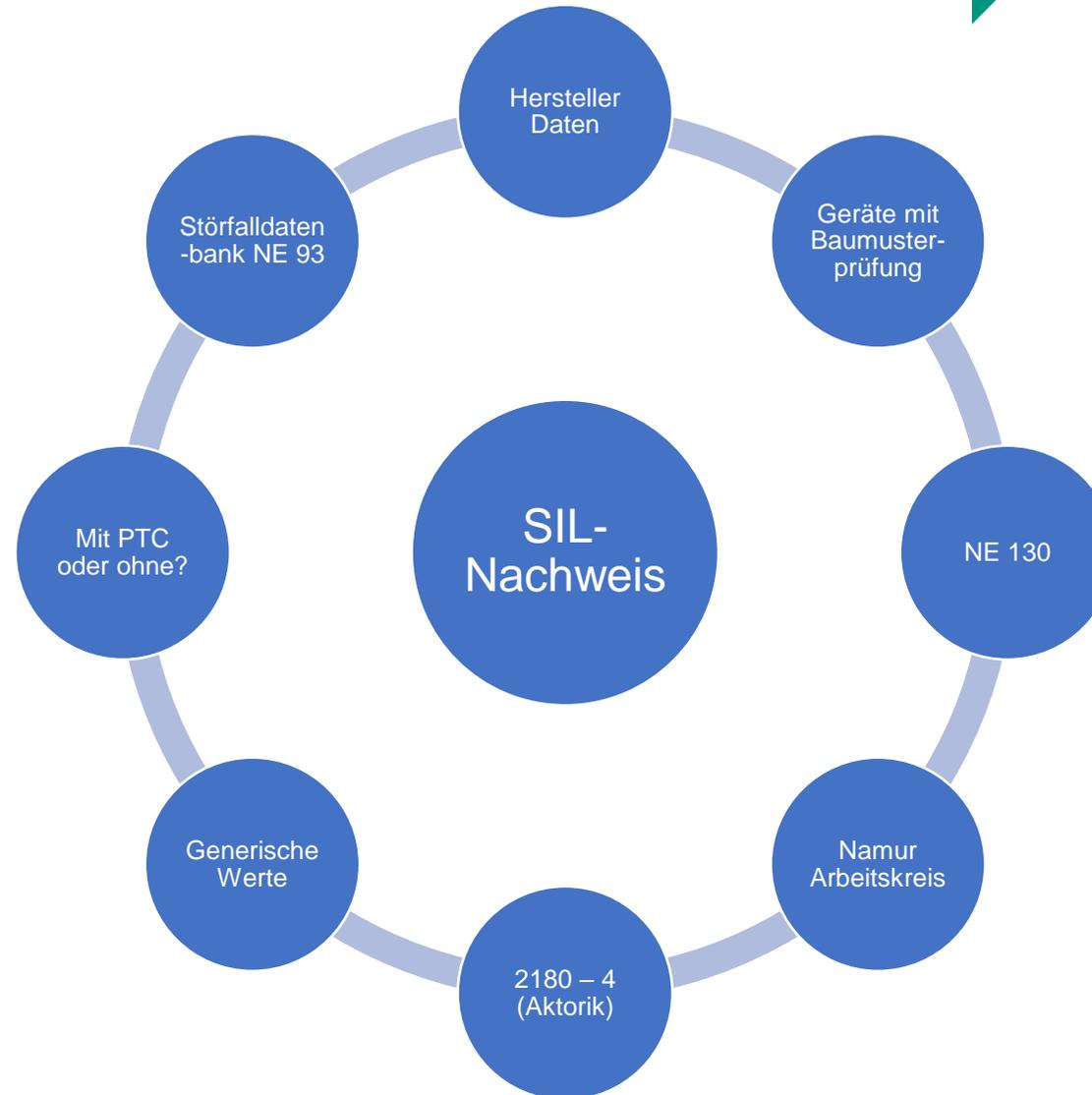
- Einzelne Tätigkeiten in den Normen der Funktionalen Sicherheit können auf unterschiedlichste Art und Weise geleistet werden. Beispiel VDI / VDE 2180:



- Eine Trennung zwischen neu Anlagen und Modifikationen / alt Anlagen fehlt langsam. Die Funktionale Sicherheit ist mittlerweile so etabliert, dass bei Neuanlagen die Geräte entsprechend entwickelt sein sollten

(5) Entwicklung in der PFD-Berechnung

Wie entscheide ich, wonach ich rechne?



III. Dokumentation

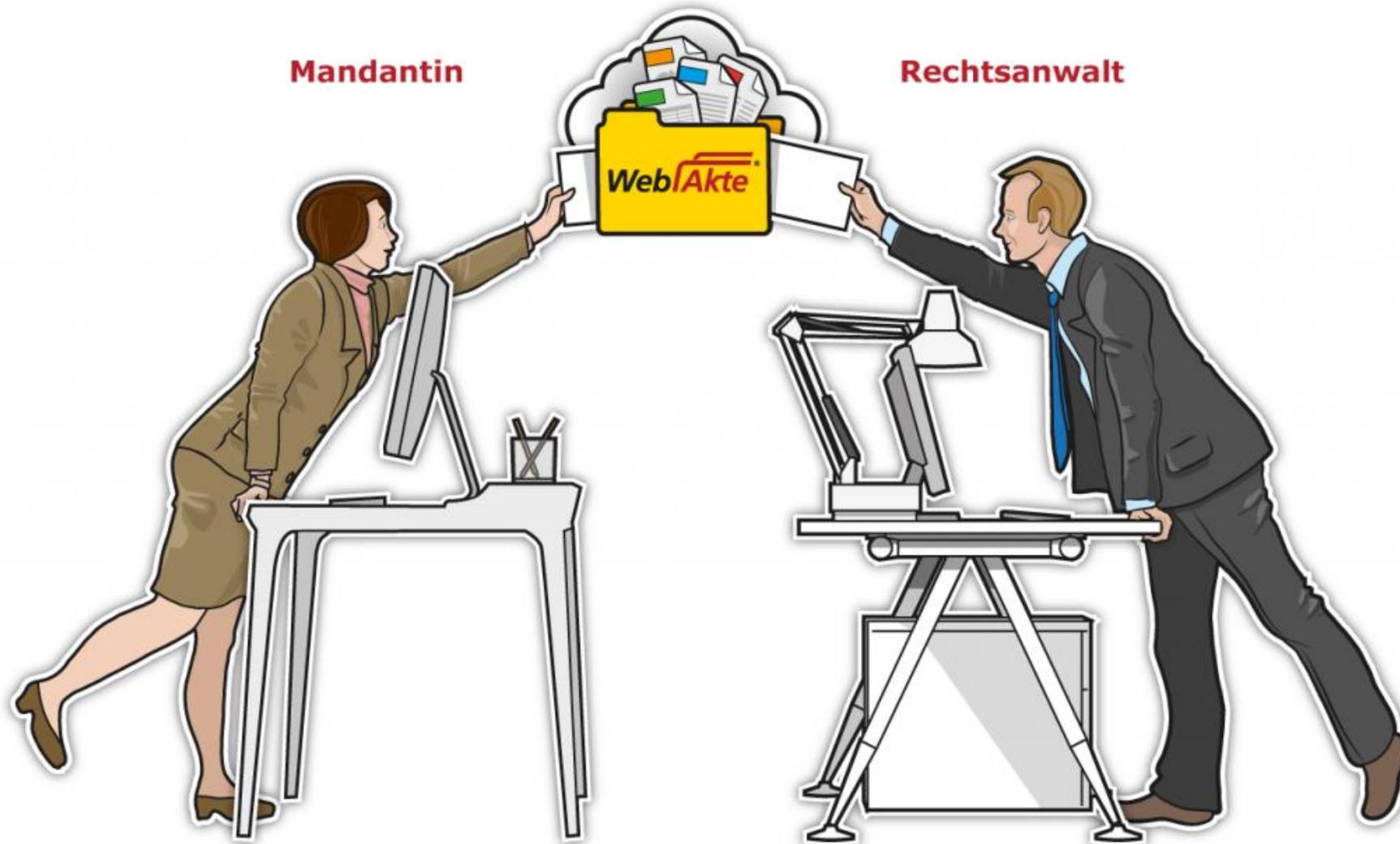
- (1) FuSi - Dokumentation
- (2) Ablagemanagement

(1) FuSi-Dokumentation

Notwendige Dokumentation (Prozessindustrie) nach Durchlaufen des Sicherheitslebenszyklus

Dienstleister	ZÜS / TAS	Interne Prüfung	Geräte-Doku	Betreiber
Nachweis FSM	Abnahme Protokoll	Validierungsberichte	Sicherheitshandbuch	Gefährdungsbeurteilung
Qualifikationsnachweise der Mitarbeiter	Prüfbericht	Verifizierungsberichte	SIL-Zertifikat	Klassifizierung
		Auditberichte	Handbuch	SRS
			Technische Inf.	SIL-Nachweis
			Konformitätserkl.	UW-Matrix
			Bedienungsanleit.	Prüfkonzept
			Montageanleit.	FAT-Doku
				SSPS-Doku

(2) Ablagemanagement



Vielen Dank für Ihre Aufmerksamkeit

Malika Mast Dipl. Ing / Geschäftsführerin

E-Mail: M.Mast@ramsys.org

Tel.-Nr.: 0 23 69 / 745 93 10

Mobil: 0171 / 3037392

