Tag 1: Fachvorträge

Motto des diesjährigen Events

SIL versus PL

Vorträge

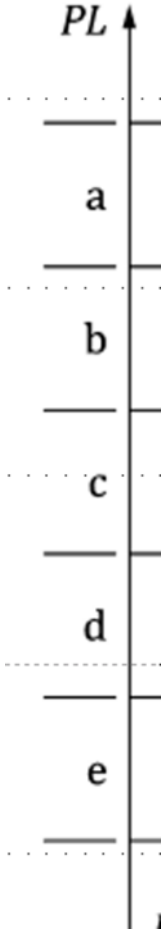
1. Normenvergleich IEC 61508, IEC 61511, ISO 13849
2. Sicherheitsgerichtete Alarme in SIL - Möglich oder nicht?
3. Übersetzung SIL↔PL – wo geht's schief
4. VDI-Richtlinie "Gebrauchsdauer"
5. Zusammenhang zwischen Markov-Modellen, PFD und PFH
6. Digitalisierung und KI im Safety Lifecycle aus Betreiber-Sicht – 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!

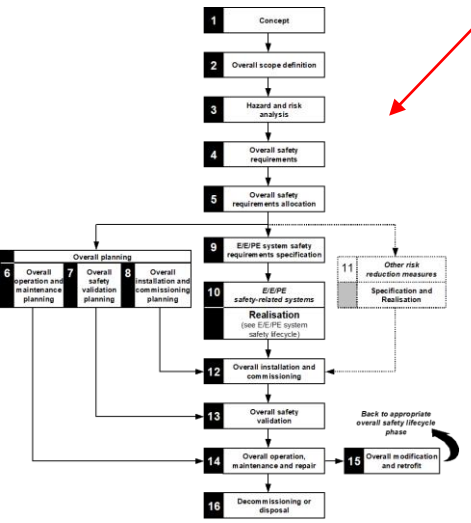
Performance Level required PL_r

a: niedrige Risikominderung

e: hohe Riskominderung



SIL Sprechstunde 2023 – Die Säulen der funktionalen Sicherheit



Fehlervermeidung durch den Functional Safety Lifecycle

Begrenzung der zufälligen Hardwareausfälle über die Schätzung der Ausfallwahrscheinlichkeit

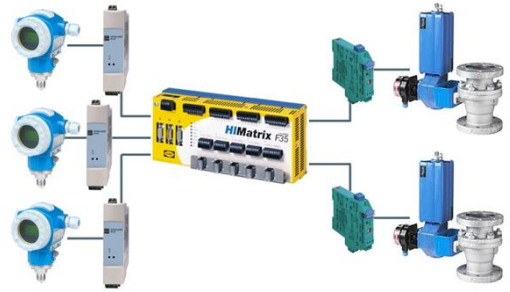
Systemtoleranz über Architekturanforderungen

Techniken und Maßnahmen unterstützen die Einhaltung dieser Prinzipien

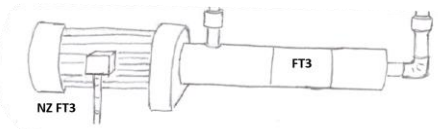
Betrachtung der gesamten Sicherheitskette – “from pipe to pipe”

in tne 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):

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

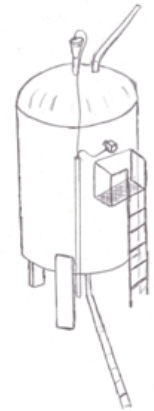


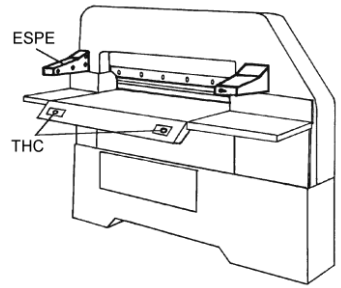
Ingo Rolle, February 2023
Bilder von Pixabay and Wikimedia

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**
   - **Architekturanforderungen (Systemtoleranz)**





Damit werden natürlich nur die grundsätzlichen Vorgehensweisen der Normen verglichen.
Für Einzelheiten muss bitte in diesen selbst nachgesehen werden.

Ingo Rolle, im September 2022
Bilder: IFA, Pixabay, IEC

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.

h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES
fbeit
FACHBEREICH ELEKTROTECHNIK
UND INFORMATIONSTECHNIK

Vergleich von Normen zur funktionalen Sicherheit

Vorstellung des Semesterprojekts im Fernstudiengang Zuverlässigkeitsingenieurwesen der Hochschule Darmstadt

Alexandra Platte, Stephan Radke
Frankfurt, 15. Mai 2019

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 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

Ingo Rolle, im September 2022

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 Perfomance 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).

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)

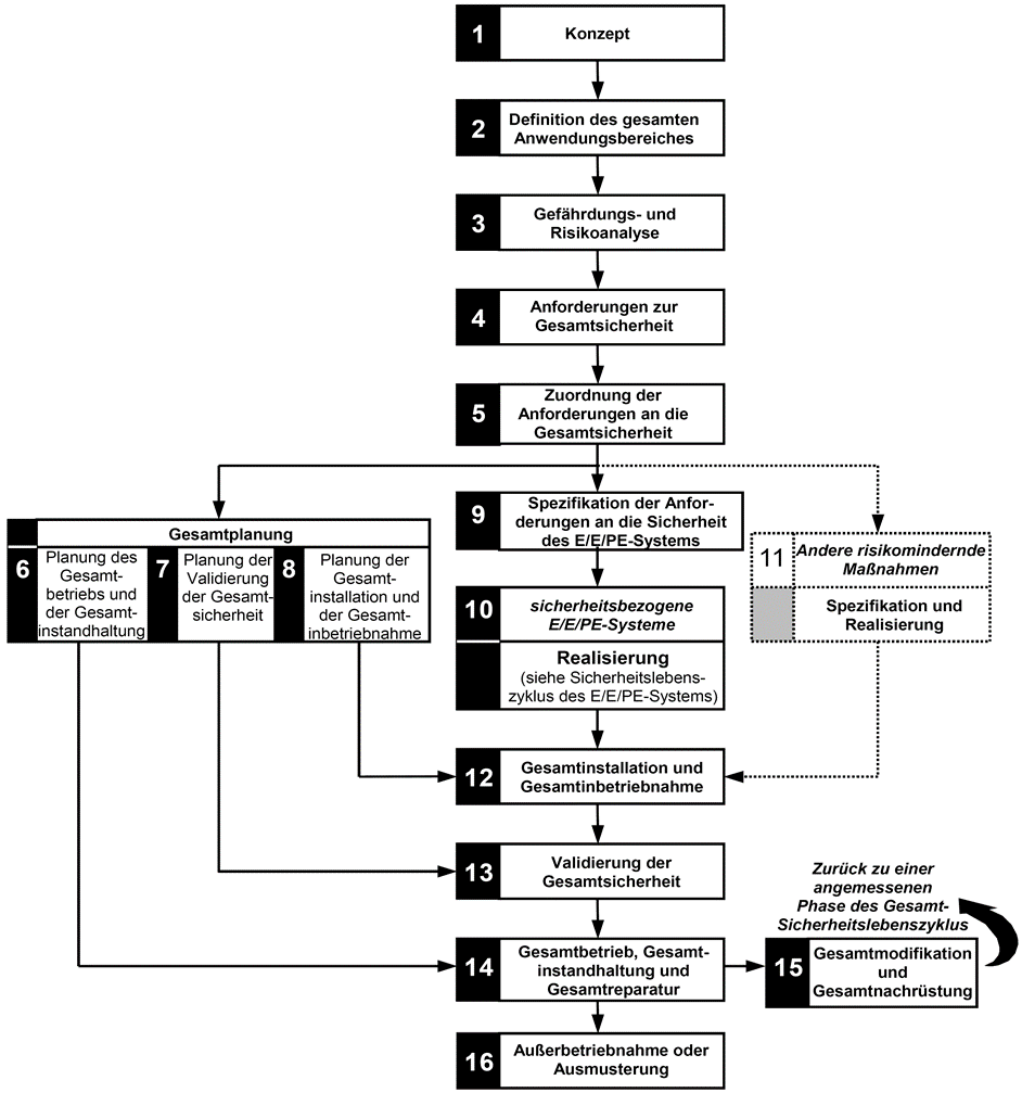
Es wird also die gesamte Sicherheitskette detailliert behandelt, mit Pneumatik und Hydraulik, auch im Teil 2. Die IEC 61508 bezieht die Aktorik zwar mit ein, gibt aber keine Anweisungen dazu. Auch in der IEC 61511 und ISO 26262 sind die Anforderungen hierzu nicht besonders detailliiert.

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
Betrachtes (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 61508



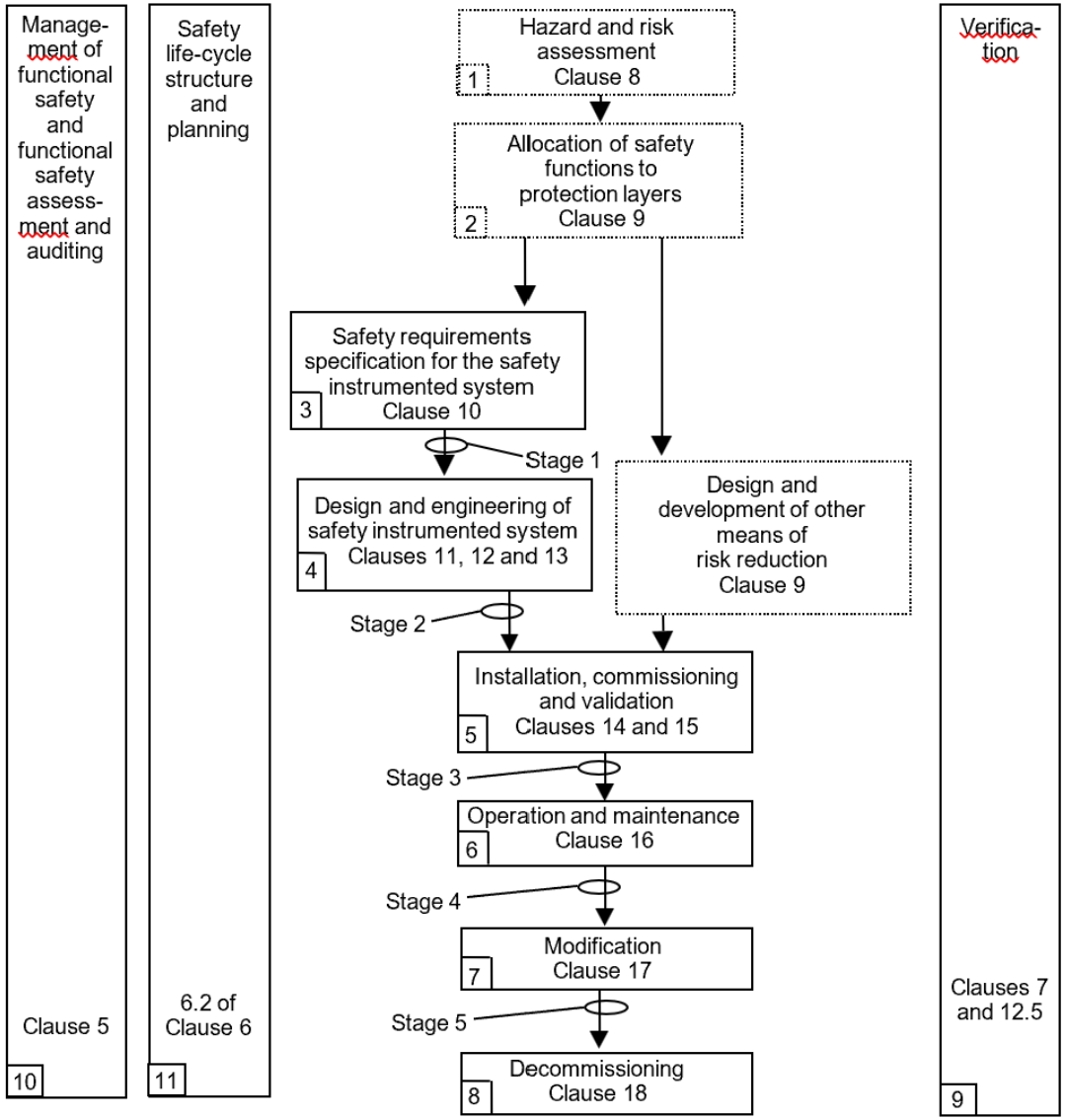
Der Lebenszyklus der IEC 61508 zeigt, wie eine Instanz untersucht wird und hierfür das sicherheitsgerichtete System (E/E/PE safety-related system) definiert, realisiert, validiert, betrieben, und instandgehalten wird. Plus Änderung und Abbau. Dieser Lebenszyklus passt gut zu Einzelanlagen.
Die Verifikation findet für jeden Schritt statt und ist hier nicht dargestellt. Ähnliches gilt für die Beurteilung.

Wer welche Schritte durchzuführen hat, beschreibt die IEC 61508 nicht (keine Rollenfestlegungen, kein Rollenmodell). Es wird nicht ausgesagt, wer die Risikoanalyse durchführen soll und es wird keine Vorstellung zur Arbeitsteilung geäußert.

Als Norm, die Normungskomitees bei der Erstellung von sektorspezifischen Normen anleiten soll, kann die IEC 61508 dies auch nicht liefern.

Meine Meinung: Der Versuch, einen Lebenszyklus zu definieren, der auf alle Branchen passt, wäre vergeblich. Von einem Normungskomitee kann erwartet werden, dass es diesen Lebenszyklus auf seine Branche anpasst.

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.

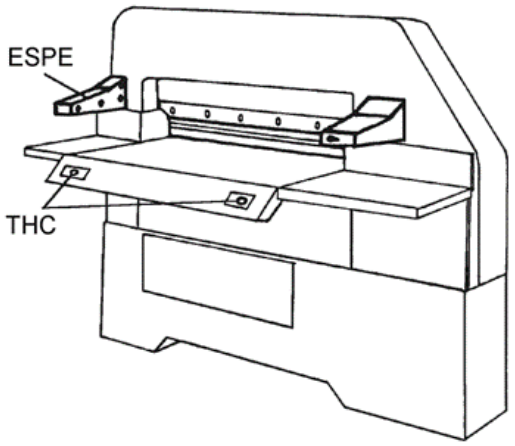
Ein Lebenszyklus, der an ein Functional Safety Management System gebunden ist, ist weder in der ISO 12100 noch in der ISO 13849 enthalten. Die entsprechenden Tätigkeiten sind in den Normen aber beschrieben und können vom Hersteller eines Steuerungssystems in sein Qualitätsmanagementsystem eingebunden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

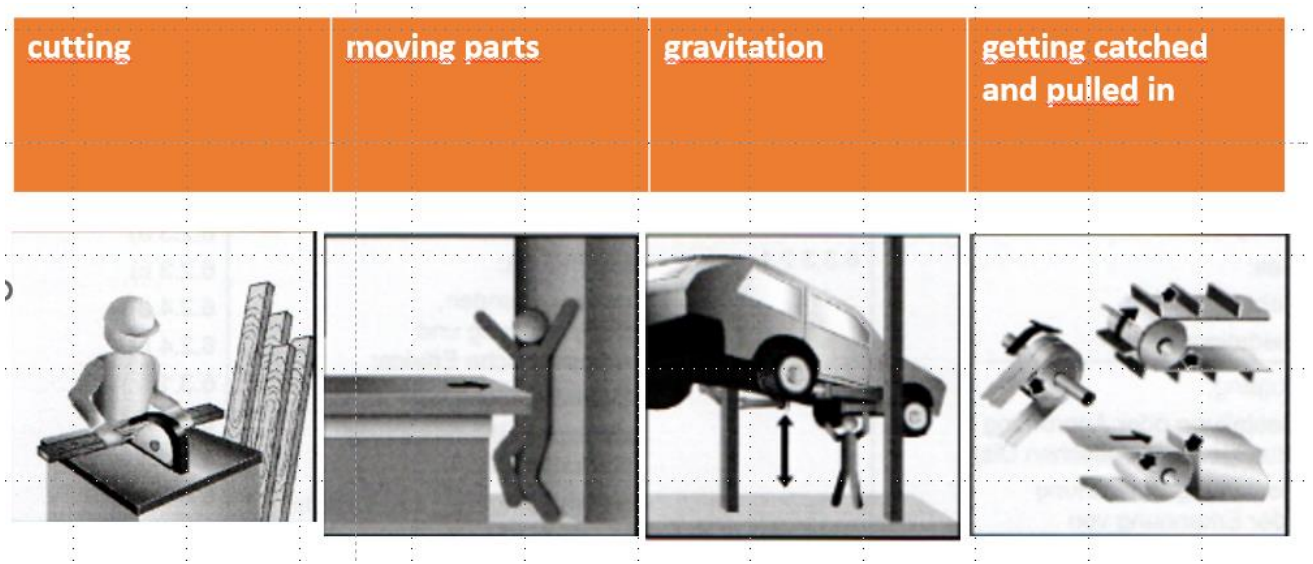
Normen zur funktionalen Sicherheit: IEC 61508 und sektorspezifische Ausprägungen – 4. Risikoanalyse – ISO 13849 - Wahl des Betrachtungsgegenstandes, Auffinden der Gefährdungen, Risikobewertung



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.



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

- S_1 leichte Verletzung oder leichter Schaden
- S_2 schwere, irreversible Verletzung oder Tod einer Person, temporärer schwerer Schaden
- S_3 Tod mehrerer Personen, langfristiger Schaden
- S_4 viele Tode, katastrophale Auswirkungen

Häufigkeit/Aufenthaltsdauer

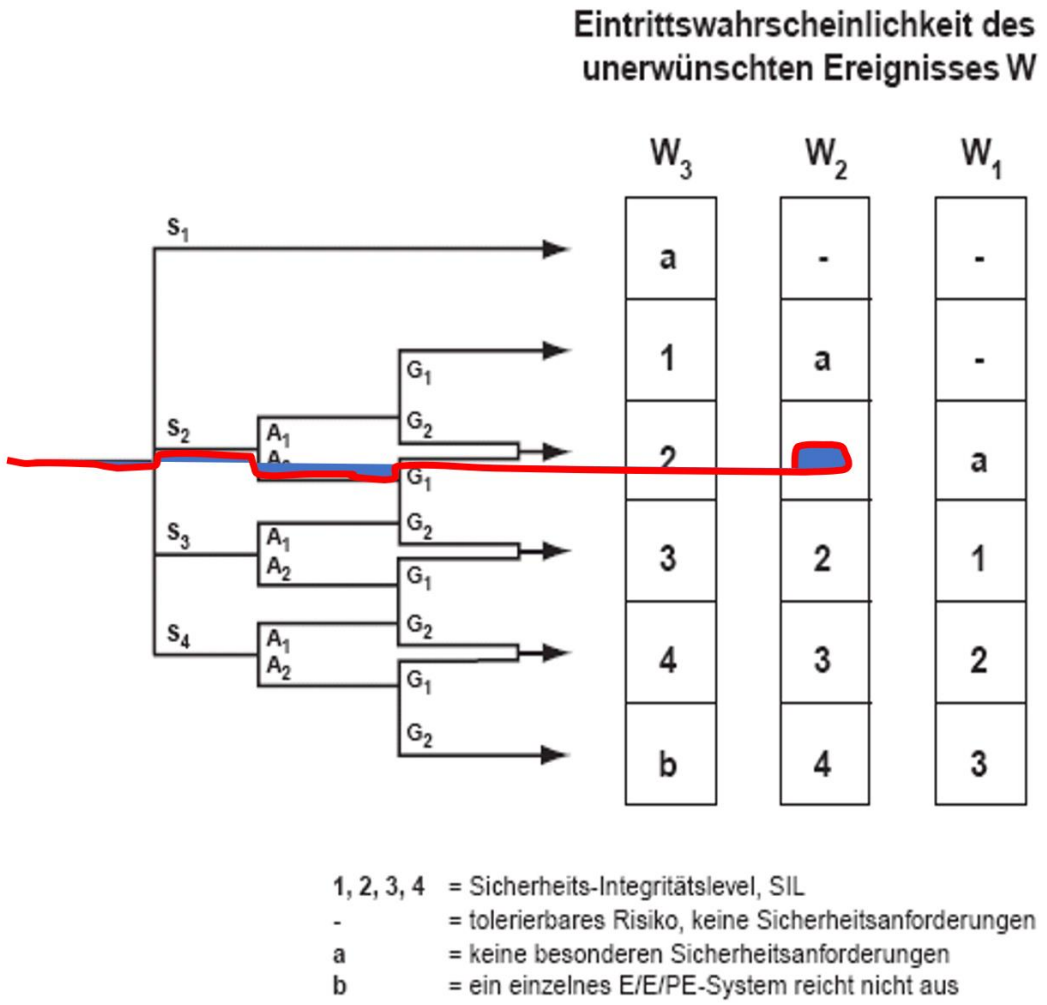
- A_1 seltener bis häufiger Aufenthalt im Gefahrenbereich
- A_2 häufiger bis dauernder Aufenthalt im Gefahrenbereich

Gefahrenabwendung

- G_1 möglich
- G_2 nicht abwendbar, kaum möglich

Eintrittswahrscheinlichkeit des unerwünschten Ereignisses

- W_1 sehr gering, kaum
- W_2 gering
- W_3 hoch, häufig

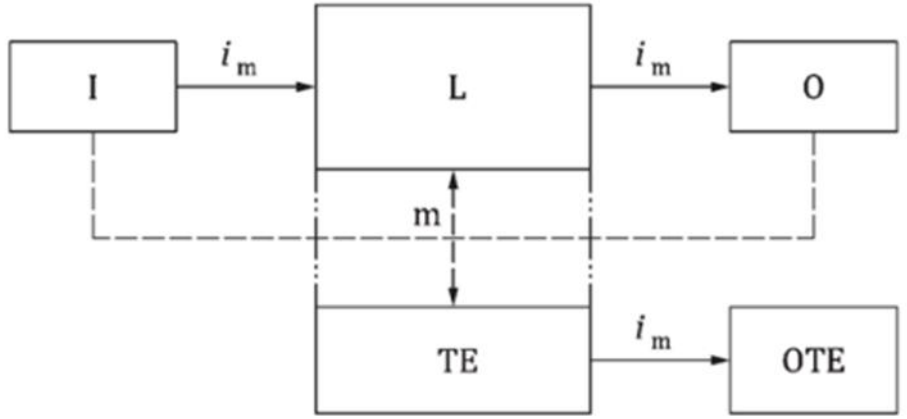


Normen zur funktionalen Sicherheit: IEC 61508 und sektorspezifische Ausprägungen – 6. Realisierung, Anforderungen und Wahl der Lösung

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 Werksnormen 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).

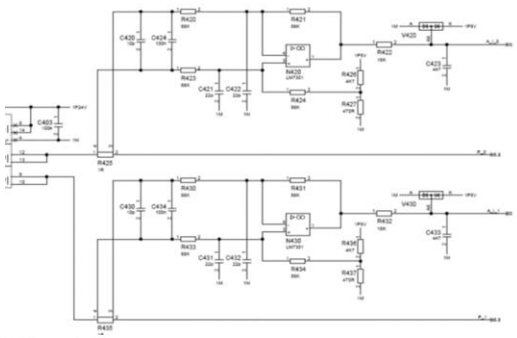
Safety integrity level	Low demand mode of operation (Average probability of failure to perform its design function on demand)
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

Safety integrity level	High demand or continuous mode of ope (Probability of a dangerous failure per h
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 $< 10^{-5}$

Die Vorgehensweise zur Schätzung gliedert sich in zwei Schritte:

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

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.

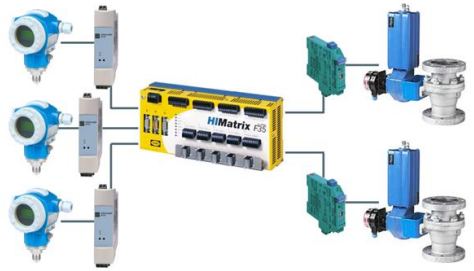


NOT MEASUREMENT SENSITIVE
MIL-HDBK-217F
2 DECEMBER 1991
SUPERSEDING
MIL-HDBK-217E, Notice 1
2 January 1990

MILITARY HANDBOOK

RELIABILITY PREDICTION OF ELECTRONIC EQUIPMENT

com-ponent	desig-nation	failure rate λ [1/h]	failure mode	frac-tion	effect	λ_{safe} [1/h]	λ_{du} [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	$6 \times 10^{-9} = 60 \times 10^{-10}$	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, Architekturanforderungen – 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)

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

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, Architekturanforderungen – das Kriterium der IEC 61508

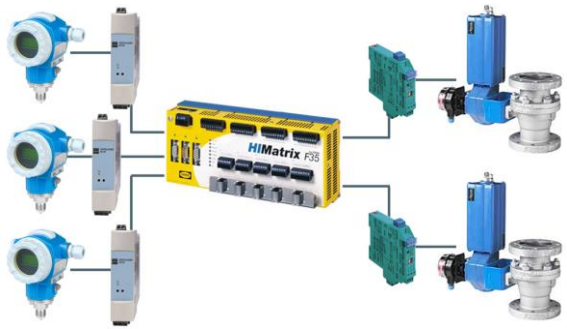
Die IEC 61508-1 verlangt für jedes Element, dass in die Ausführung einer Sicherheitsfunktion eingebunden ist, die Einhaltung der folgenden Tabellen

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.



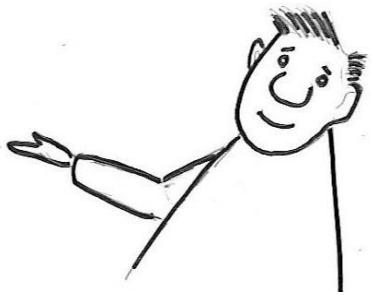
Ingo Rolle, im November 2022
Bilder: Wikimedia, Endress + Hauser, HIMA, Arca, Pepperl + Fuchs

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 Architekturanforderungen. 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.

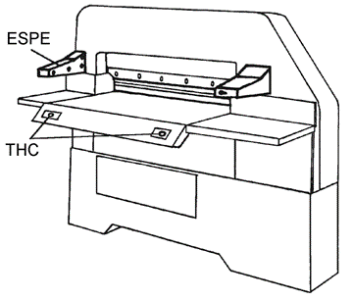
IEC 61508

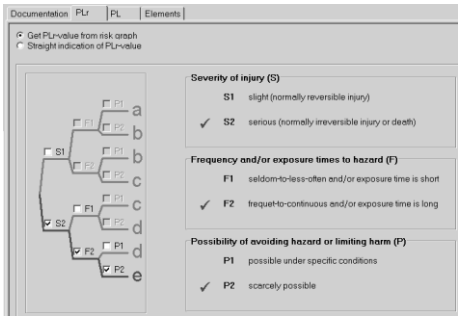
Nein, wir können den Steuerungsbauer im mittelständischen Maschinenbau nicht im Regen stehen lassen. Die Norm muss ihn zur richtigen Lösung führen. Auch muss er den Anschluss an die Kategorien der EN 954 finden.
Und es muss einen einfachen Weg geben, den Entwurf gegen die Anforderungen zu verifizieren.



ISO 13849

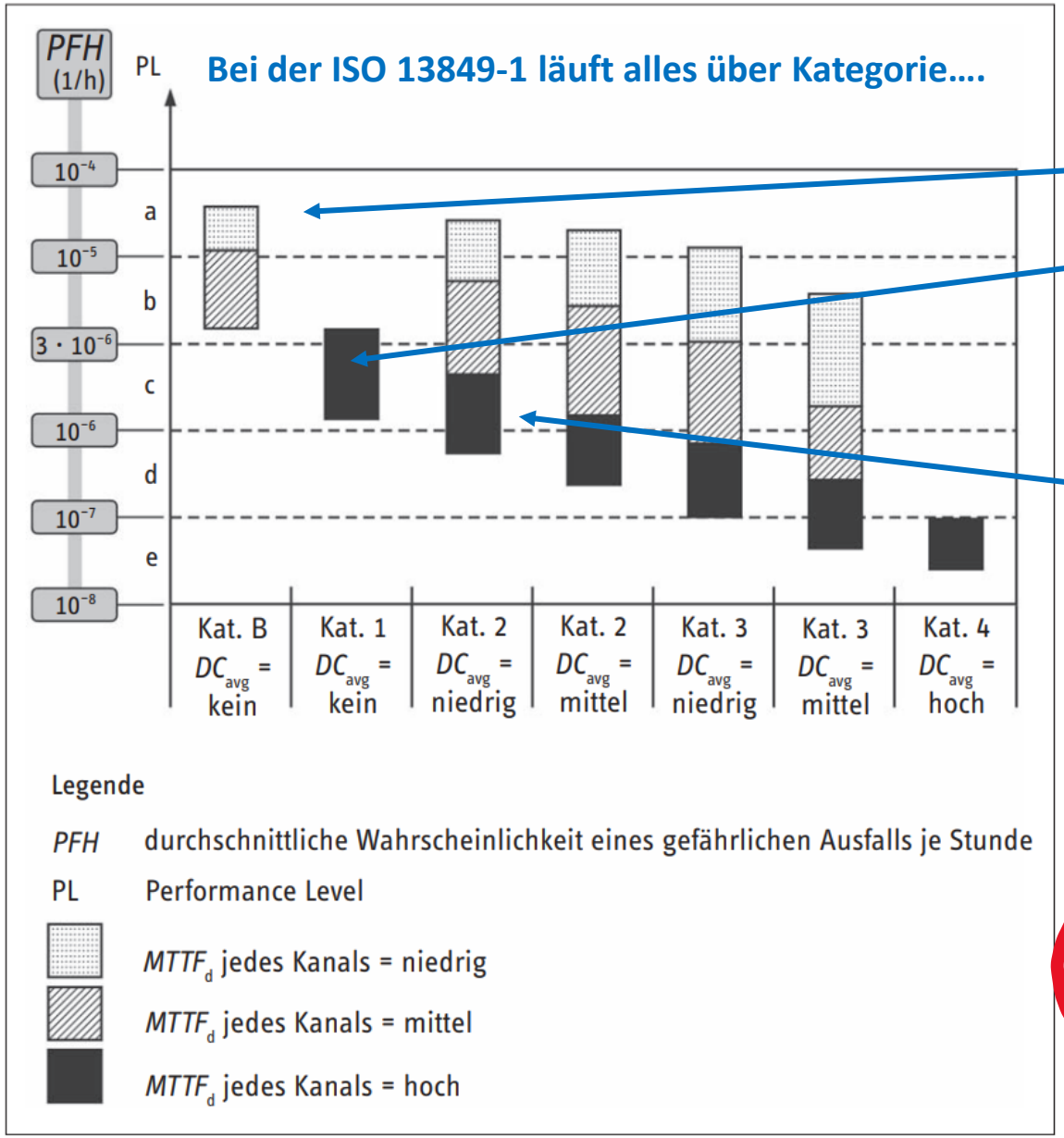
Normen zur funktionalen Sicherheit: IEC 61508 und sektorspezifische Ausprägungen – 6. Realisierung, Begrenzung der zufälligen Ausfälle, Architekturanforderungen – ISO 13849





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

Ingo Rolle, im September 2023

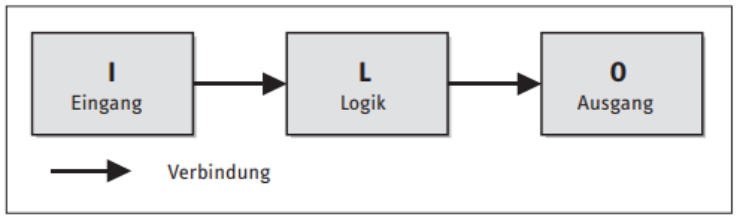


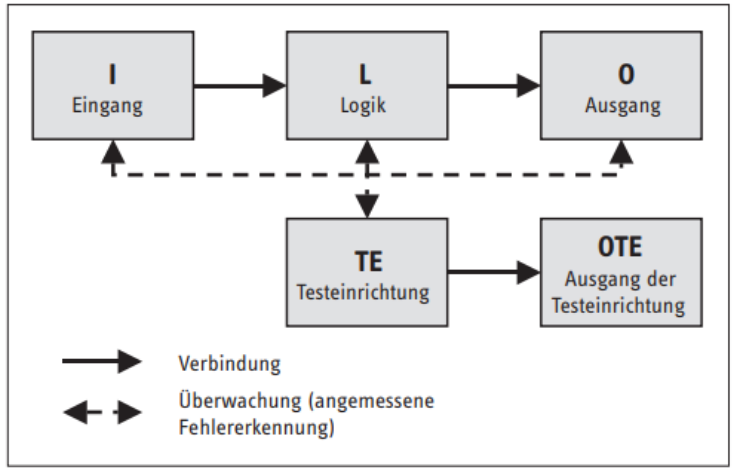
Das lässt sich erreichen

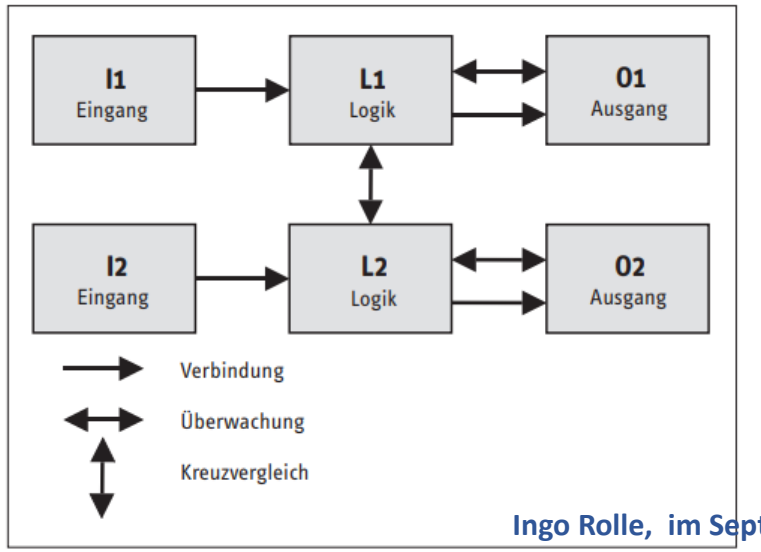
- **mit Kategorie B gar nicht**
- **mit Kategorie 1, sofern der Nachweis gelingt, dass die $MTTF_d$ hoch ist (mean time to dangerous failure)**
- **mit Kategorie 2 mit $MTTF_d$ mittel bis hoch und DC (diagnostic coverage) niedrig bis mittel**
- **mit Kategorie 3 usw**

das Säulendiagramm

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







Das sind die Kategorien:

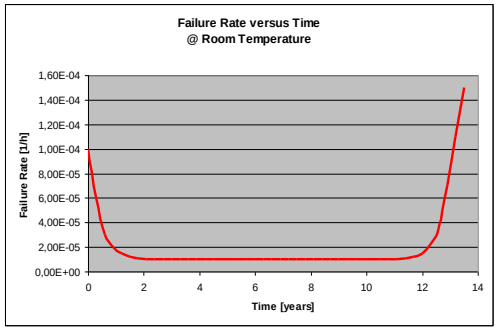
viele Begriffe zur Qualifikation von Bauteilen und Geräten

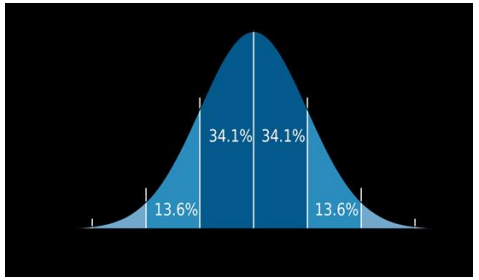
- **Kategorie B. Erfüllt maximal PL b = SIL 1. Qualifikation über Auswahl der Bauelemente (grundlegende Sicherheitsprinzipien, Einhaltung der Betriebsbeanspruchungen).**
- **Kategorie 1. Erfüllt maximal PL c = SIL 1. Qualifikation über Auswahl der Bauelemente (grundlegende und bewährte Sicherheitsprinzipien, 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, Architekturanforderungen – 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. (Zweifellos ein kühner Schritt.) Alternativ kann FMEA angewendet werden (eigentlich FMEDA).
Auch die Einhaltung der Architekturanforderungen 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

Daneben ist noch Route 2H nach IEC 61508-2 möglich.

Ingo Rolle, im November 2022
Bilder: Wikimedia

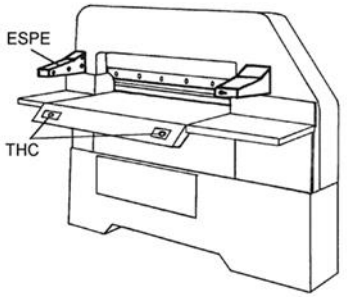
Normen zur funktionalen Sicherheit: IEC 61508 und sektorspezifische Ausprägungen – Ergebnis des Vergleichs

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

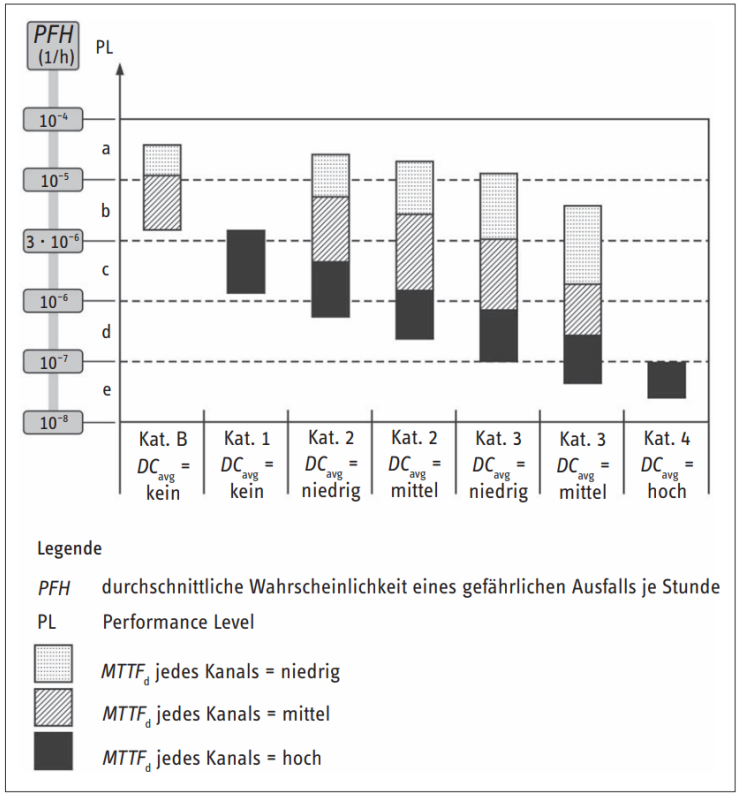
Normen zur funktionalen Sicherheit: IEC 61508 und sektorspezifische Ausprägungen – Ergebnis des Vergleichs

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



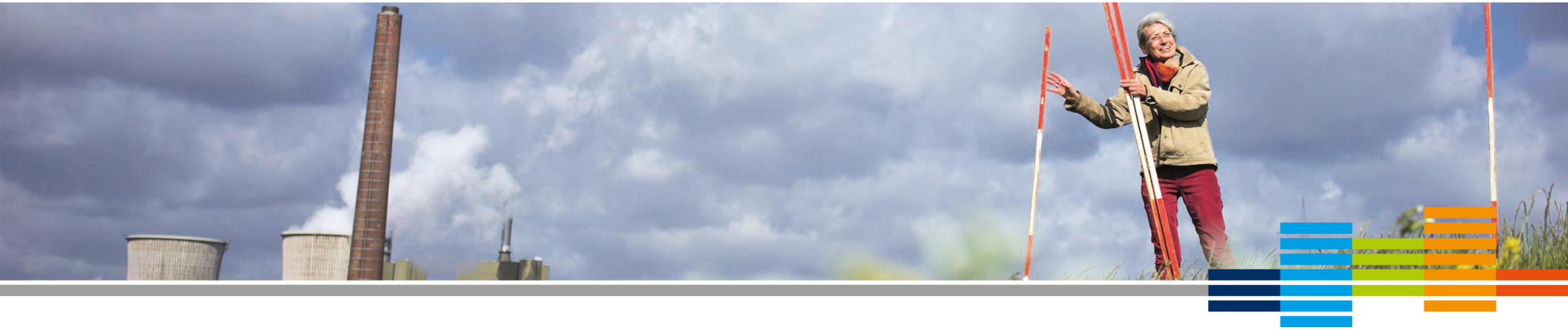
Das ist auch funktionale Sicherheit – hat aber durch die Kategorien und Rechenhilfen einen anderen Rechnungsgang als bei uns. Aber ist es wirklich einfacher?



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

LANUV
Kompetenz für ein lebenswertes Land

Landesamt für Natur,
Umwelt und Verbraucherschutz
Nordrhein-Westfalen



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

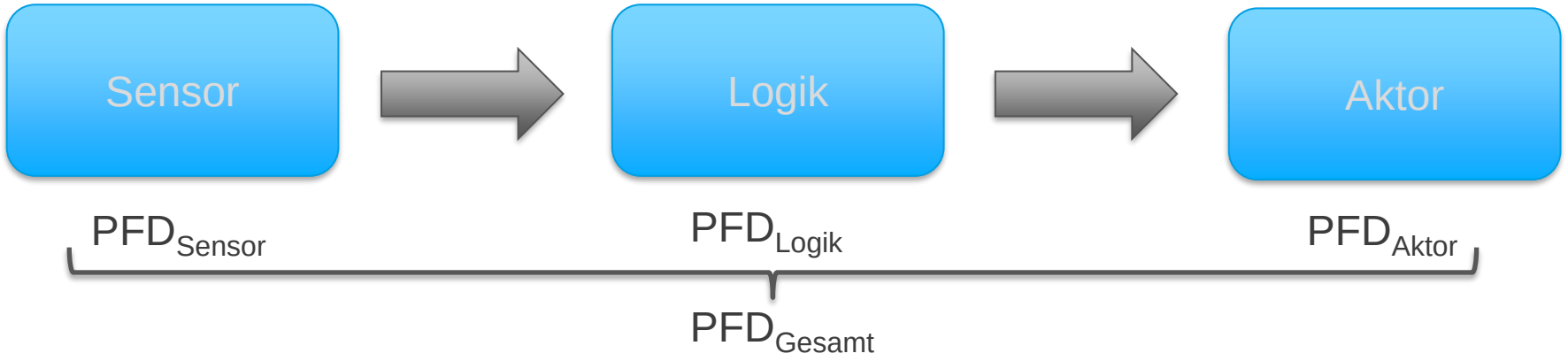
Aus der Erfahrung

- Beispiel einer Gefahrenanalyse:

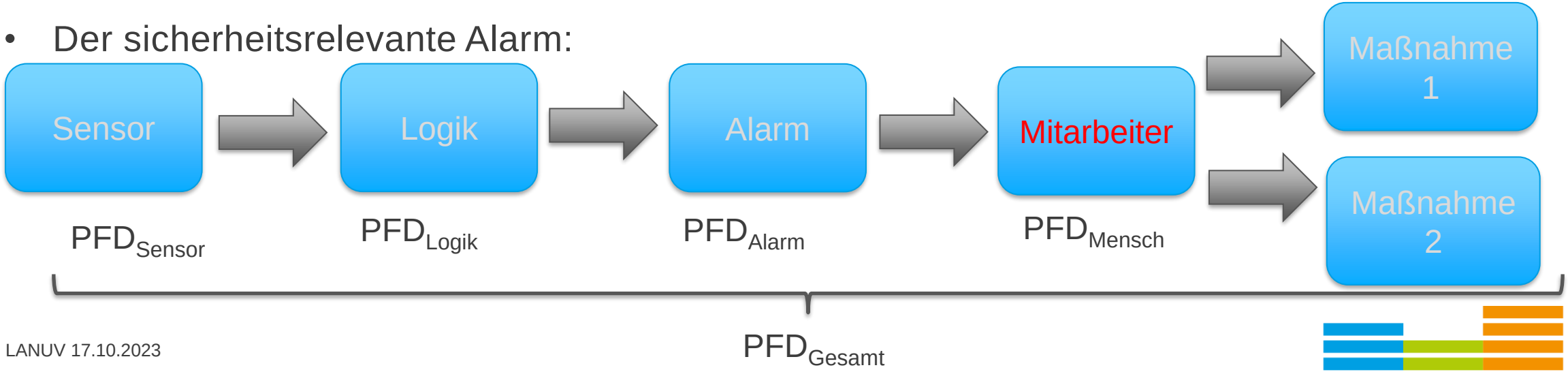
Abweichung	Ursache	Auswirkungen	Risikograph	Not. Risiko-reduzierung	Sicherheitsfunktion
W1004: Temperatur hoch	Fehlerhafte Temperaturregelung	Temperaturerhöhung ggf. bis zur Zersetzung, Überschreitung der mechanischen Integrität, Explosion	S2-A2-G1-W2	SIL2	A++ alarmiert Temperatur zu hoch im Tafelfeld.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

Sicherheitsrelevante Alarme?

- Die Wirkkette der PLT-Sicherheitseinrichtung:

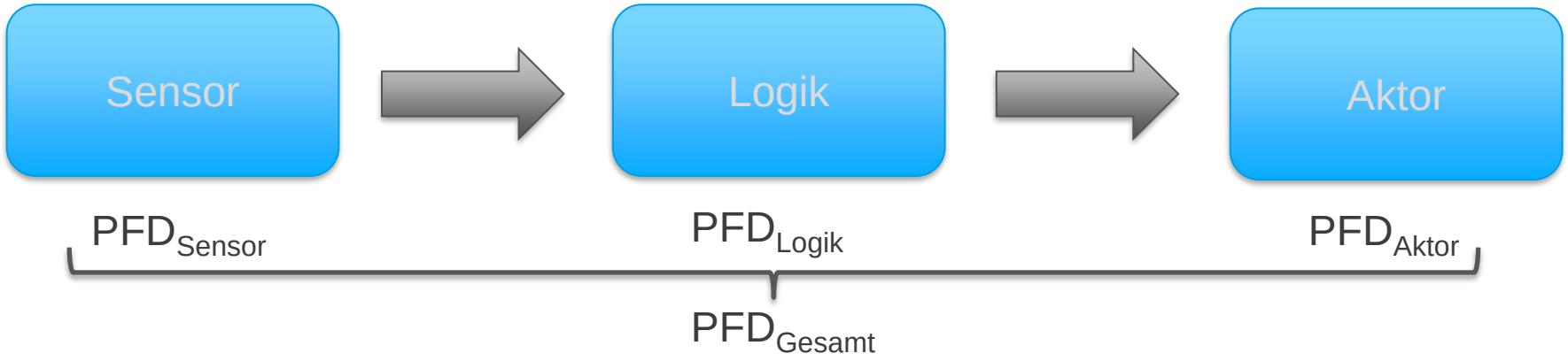


- Der sicherheitsrelevante Alarm:

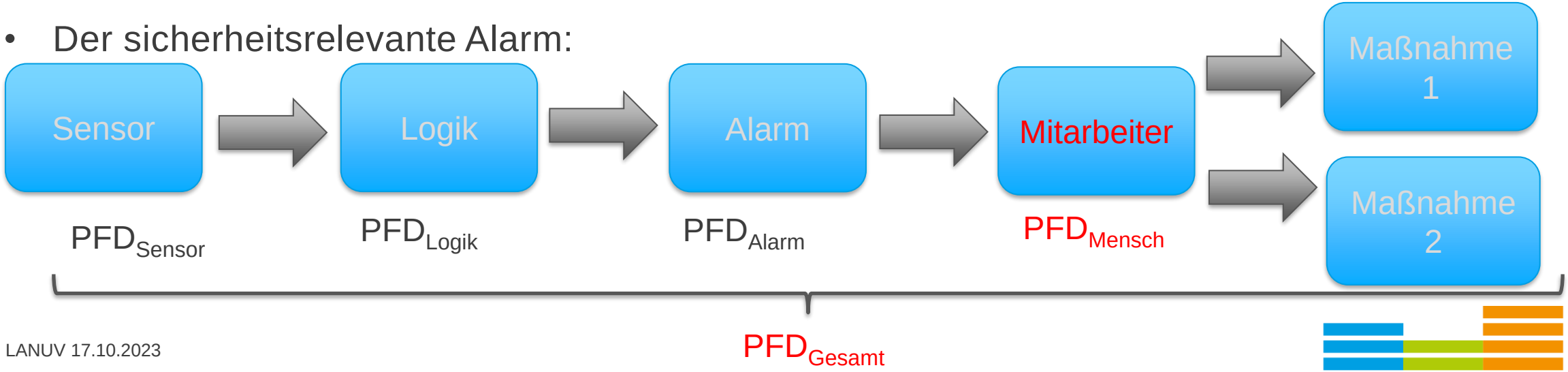


PFD-Mensch

- Die Wirkkette der PLT-Sicherheitseinrichtung:



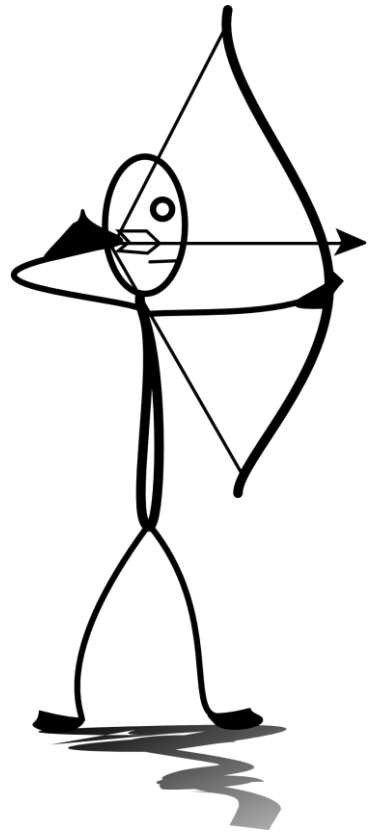
- Der sicherheitsrelevante Alarm:



PFD-Mensch

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

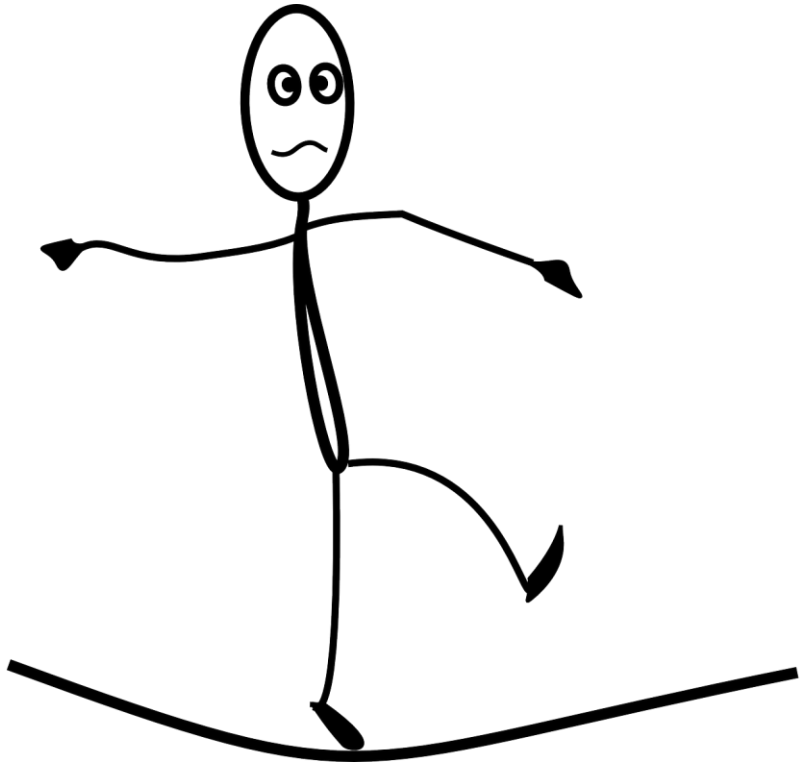
Aufgabenbeschreibung in Abhängigkeit von den situativen Anforderungen und der kognitiven Belastung	**Fehlerwahrscheinlichkeit** (Streubreite)
Einfache und häufig durchgeführte Aufgaben bei geringem Stress und genügend zur Verfügung stehender Zeit in gewohnten Situationen ohne Zielkonflikte	$1 \cdot 10^{-3}$ (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

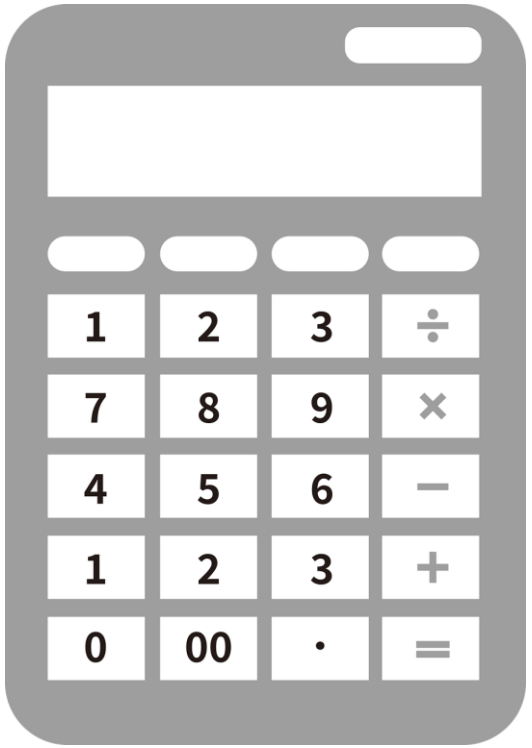
- Blatt 2 – Planung, Errichtung und Betrieb von PLT-Sicherheitseinrichtungen:

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?

LANUV
Kompetenz für ein lebenswertes Land

Landesamt für Natur,
Umwelt und Verbraucherschutz
Nordrhein-Westfalen

Haben Sie Fragen?

17.10.2023

LANUV
Kompetenz für ein lebenswertes Land

Landesamt für Natur,
Umwelt und Verbraucherschutz
Nordrhein-Westfalen

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

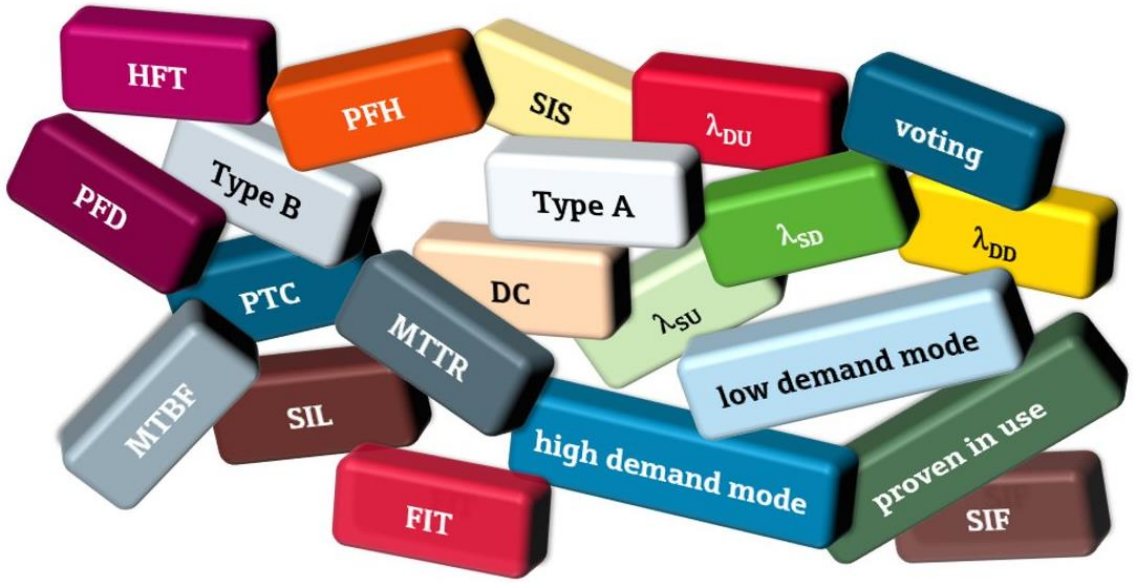
17.10.2023

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

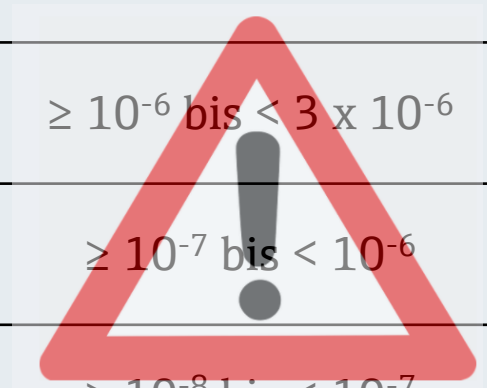


Endress+Hauser

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

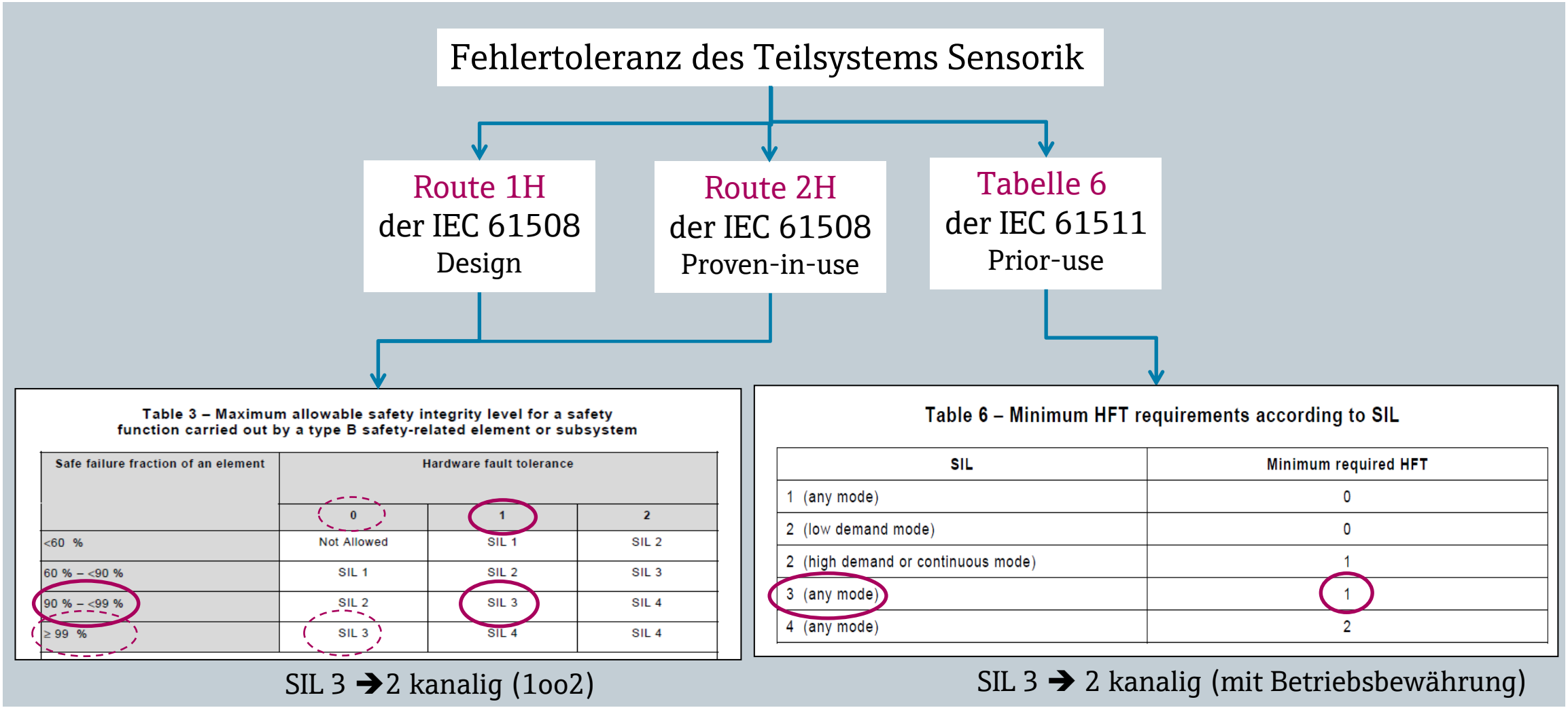


Table 3 – Maximum allowable safety integrity level for a safety function carried out by a type B safety-related element or subsystem

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)

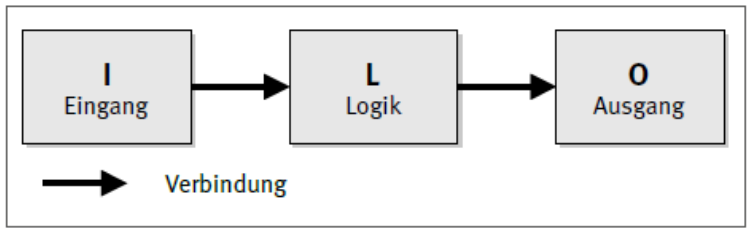
Bewertung und Verifikation z.B. mit SISTEMA

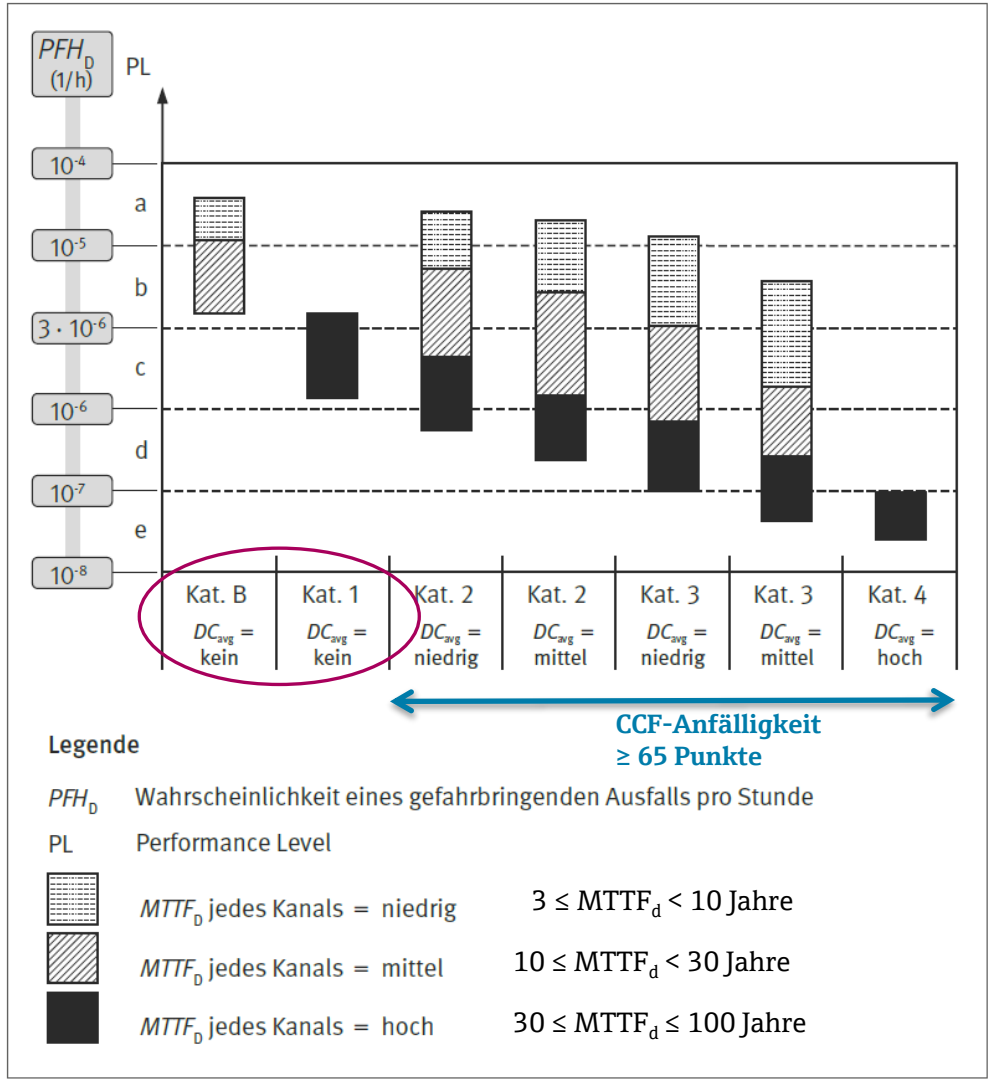
Übersetzung SIL <-> PL – wo geht‘s schief?

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





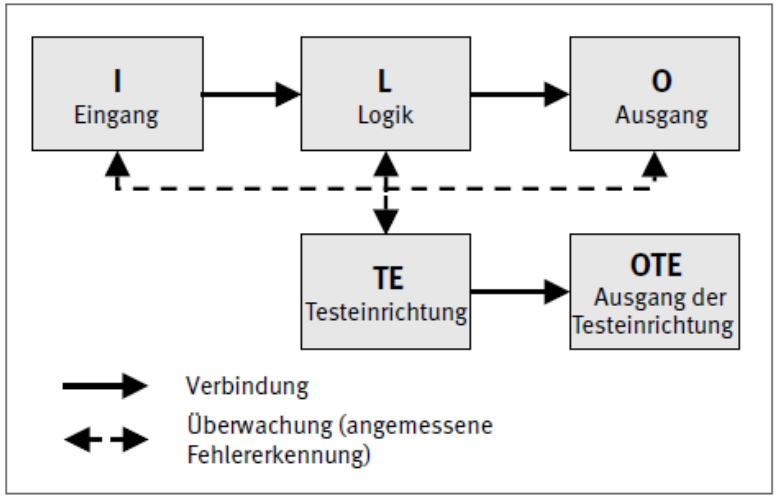
Endress+Hauser

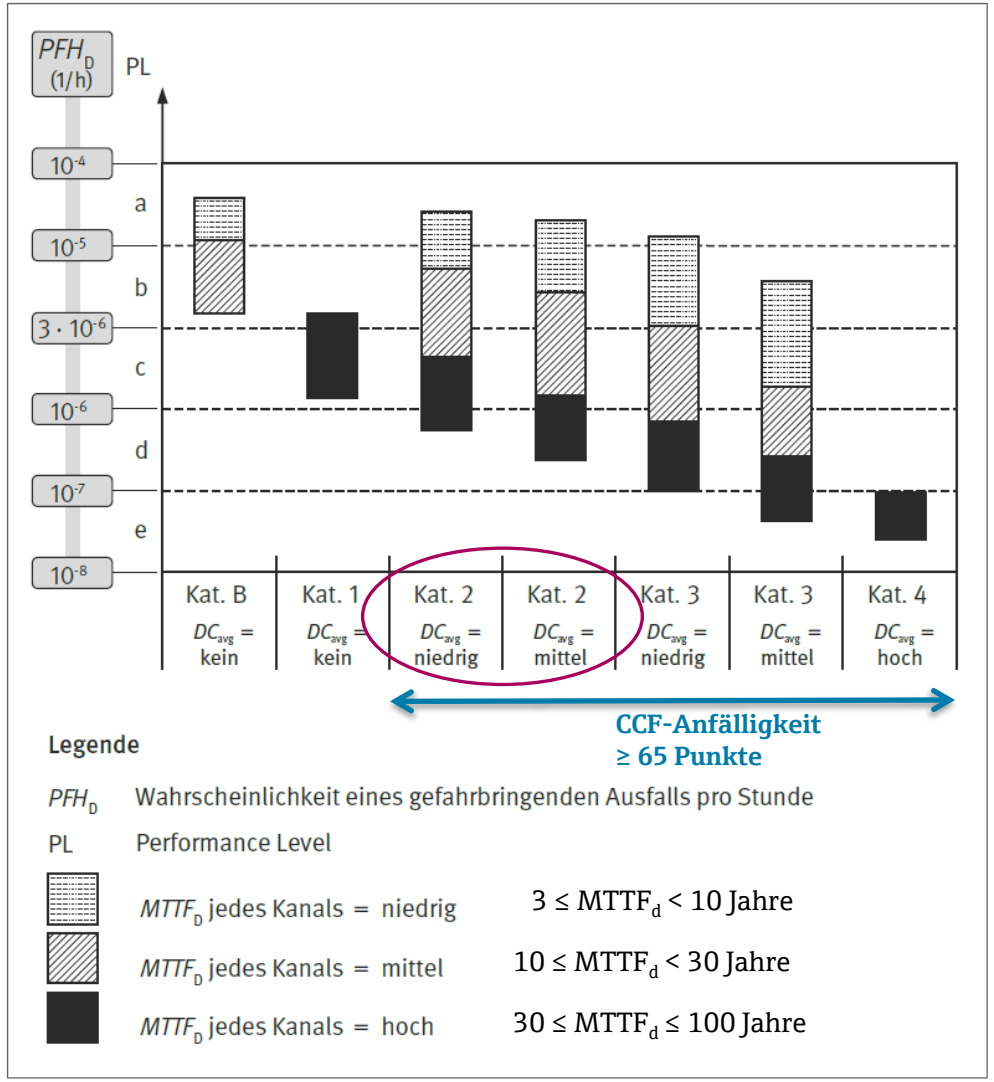
Übersetzung SIL <-> PL – wo geht‘s schief?

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





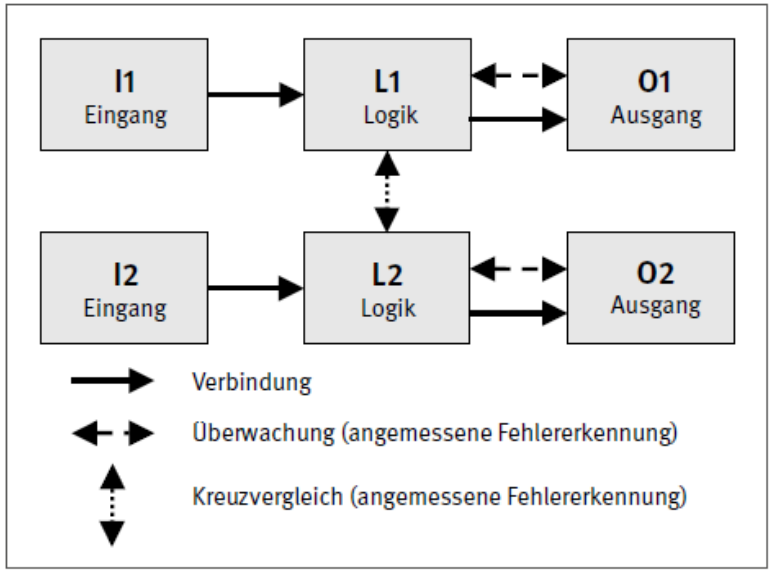
Endress+Hauser

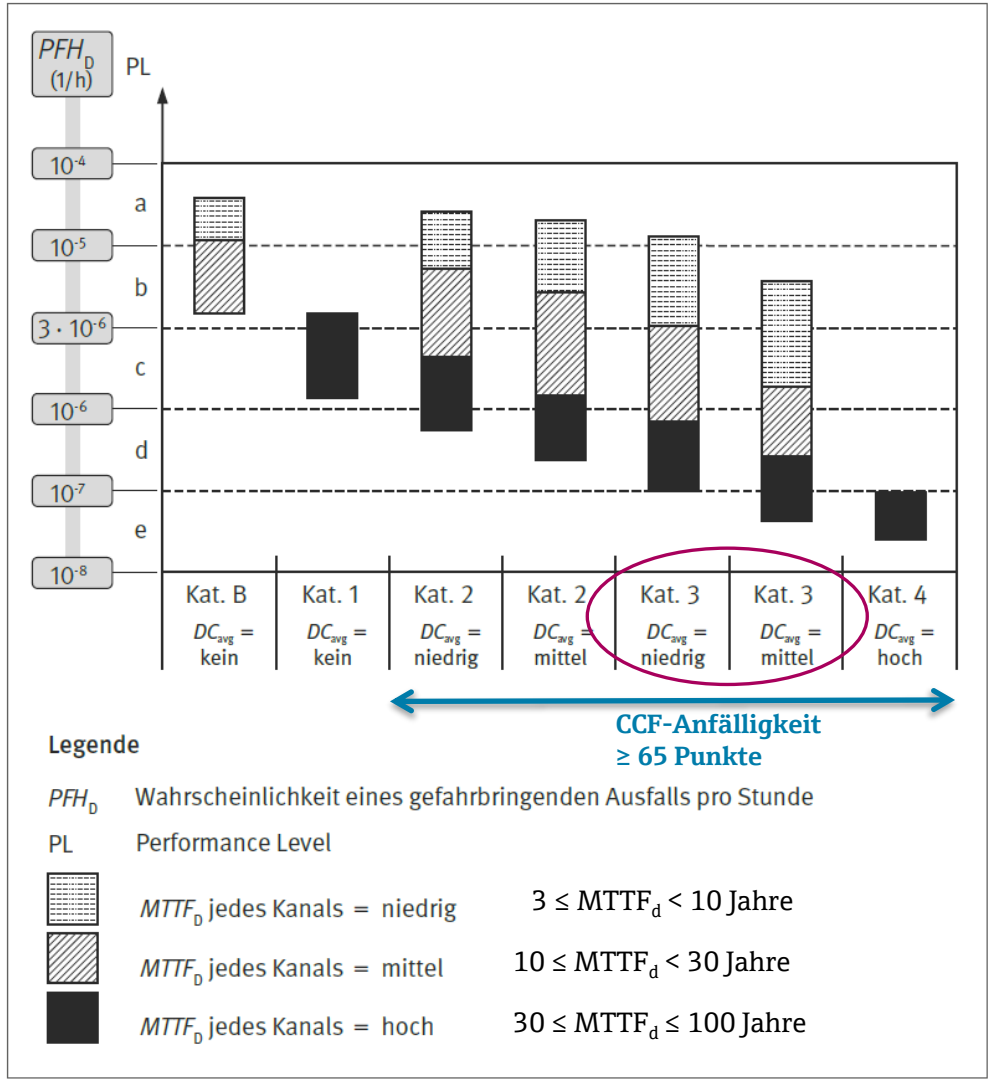
Übersetzung SIL <-> PL – wo geht‘s schief?

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





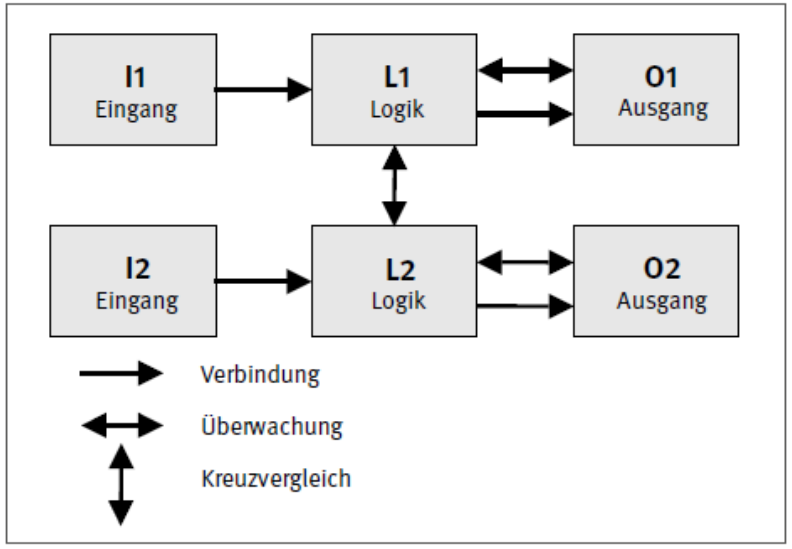
Endress+Hauser

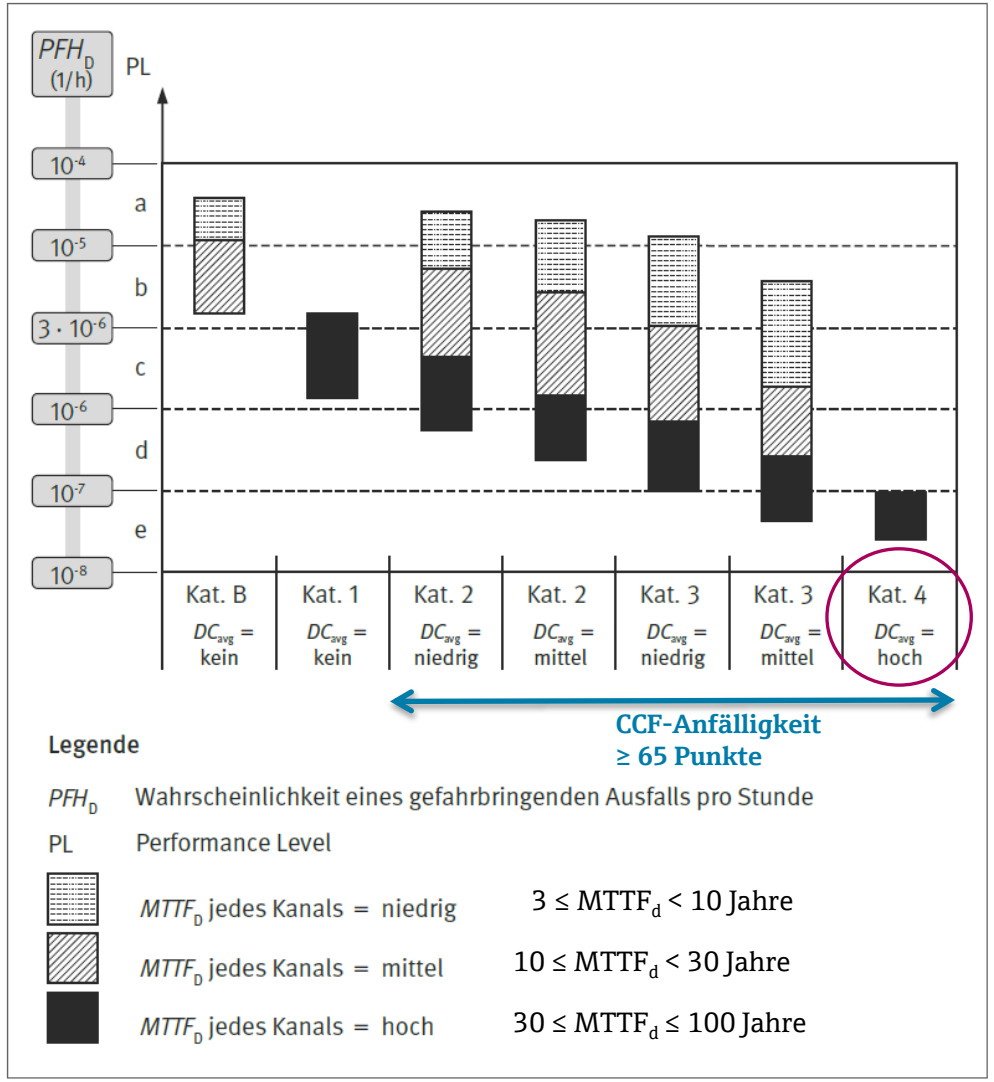
Übersetzung SIL <-> PL – wo geht‘s schief?

Vorgesehene Architekturen EN 13849

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

Vorgesehene Architektur für Kategorie 4





Endress+Hauser

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
Anwendungs-bereich	Steuerungen inkl. Hydraulik und Pneumatik *Eher einzelne Maschinen*	Elektrische/elektronische/program-mierbare elektronische Systeme *Meist größere Anlagen*
	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

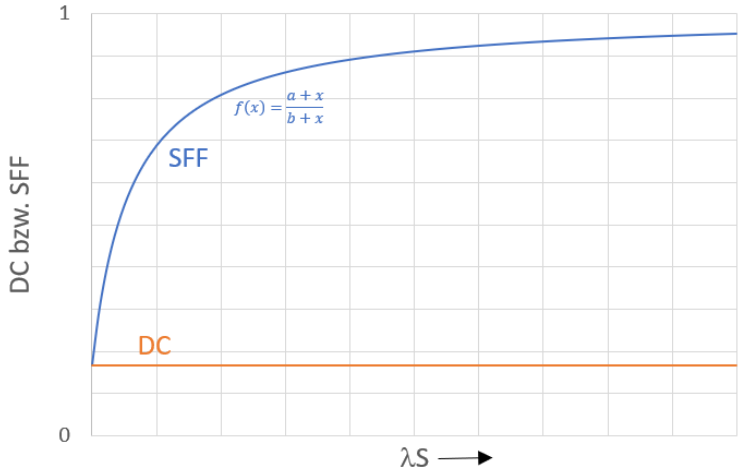
* Unter der Voraussetzung geeigneter MTTF-Werte
** In praktischen Fällen ist SFF immer höher als DC

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

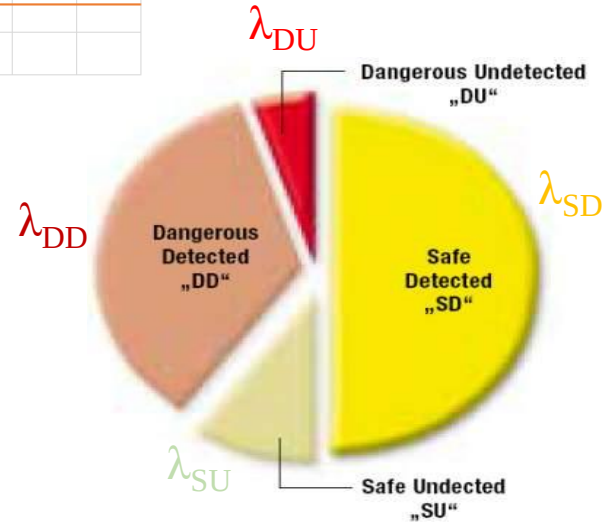
„Vergleich“ DC (Diagnosedeckungsgrad) und SFF (Safe Failure Fraction)

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

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



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



Endress+Hauser

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

- Vergleich FTL81 + FTL825

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

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)	▪ 2 (einkanalig), ▪ 3 (mit SIL 3-fähiger Auswahlschaltung)		
SIL (Software)	3		
Gerätetyp	B		
Betriebsart	Low demand mode		
Sicherheitsfunktionen	MIN	MAX	Bereich
λ_{sd}	52 FIT	367 FIT	419 FIT
λ_{su}	392 FIT	392 FIT	392 FIT
λ_{dd}	367 FIT	52 FIT	0 FIT
λ_{du}	80 FIT	80 FIT	80 FIT
λ_{tot} [1)]	1128 FIT		
$MTBF_{tot}$ [1)]	101 Jahre		
SFF	91,0%		
PFD_{avg} für T_1 = 1 Jahr (einkanalig)[2)]	$3{,}50 \times 10^{-4}$		
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:

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

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

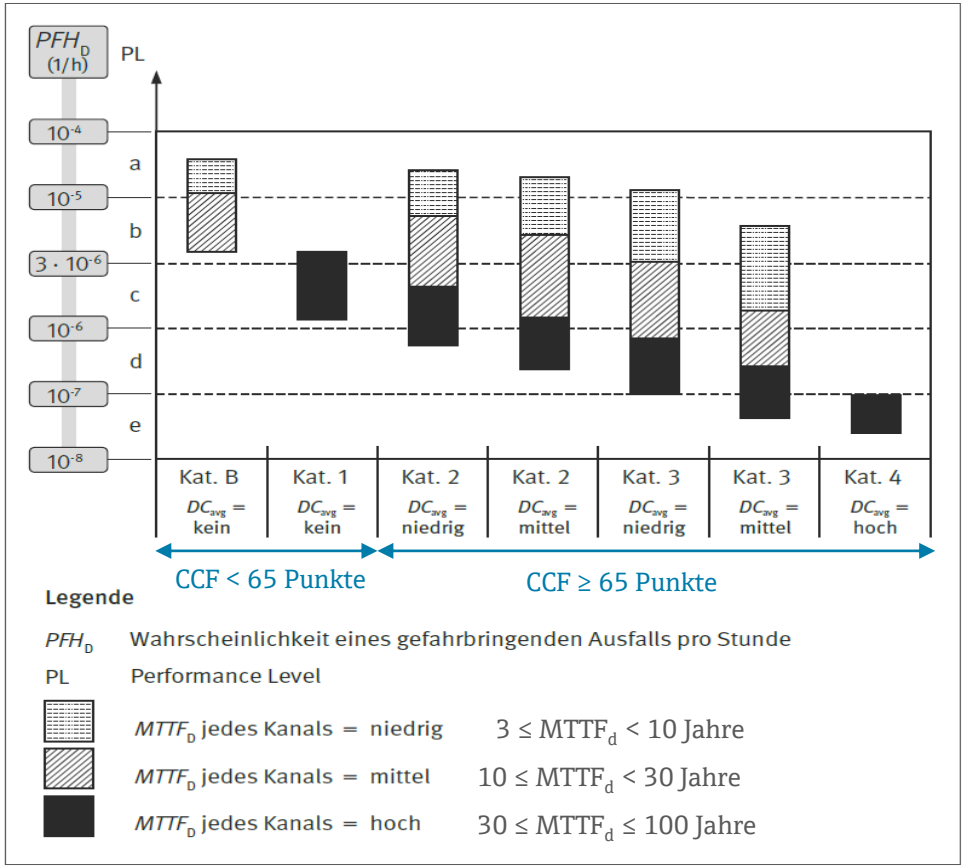
High-Demand Mode - Low-Demand Mode

- 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 ≅ 17 h ausgelöst werden, was im konkreten Anwendungsfall auf Plausibilität zu überprüfen ist. Ansonsten ist der konservative Ansatz zu* wählen ($pfh_D \approx \lambda_{DU} + \lambda_{DD}$).

High-Demand Mode - Low-Demand Mode

Vorgehensweise:

- Beachtung der Architekturanforderungen 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" (≥ 60 %), „mittel" (≥ 90 %) und „hoch" (≥ 99 %) eingeteilt und hängt von den Diagnosemaßnahmen des Systems ab (siehe Tabelle E.1 der DIN EN ISO 13849-1).

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

Endress+Hauser

High-Demand Mode - Low-Demand Mode

Beispiel Cerabar S:

- *Mit λ_{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	$\geq 3*10^{-6}$ bis $< 10^{-5}$	1
c	$\geq 10^{-6}$ bis $< 3*10^{-6}$	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

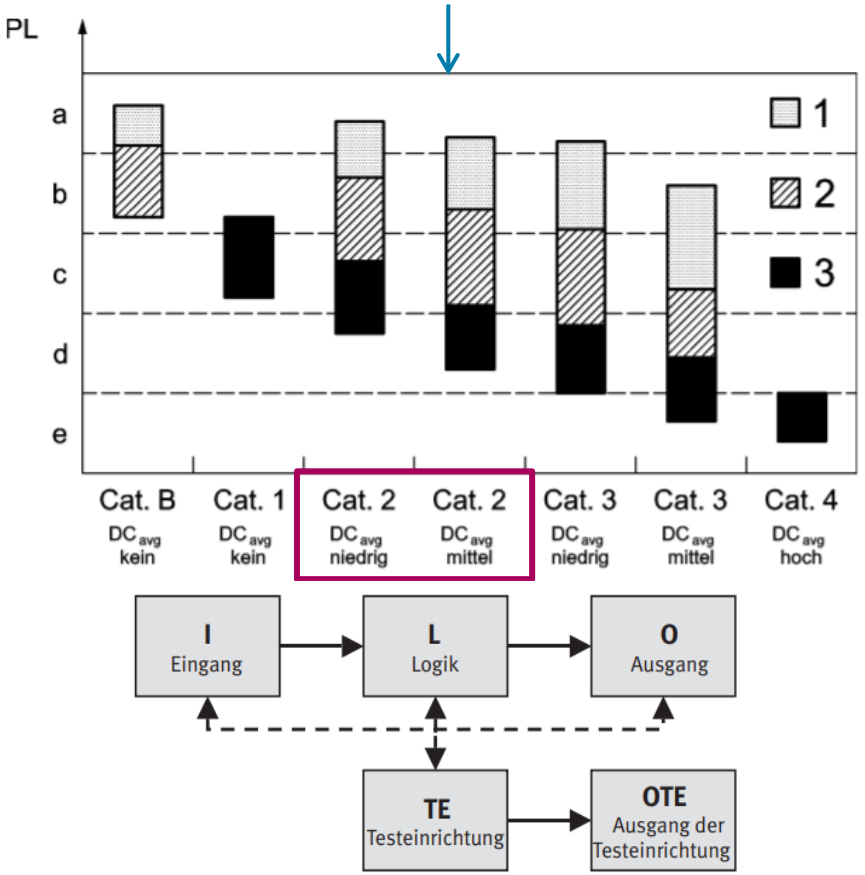
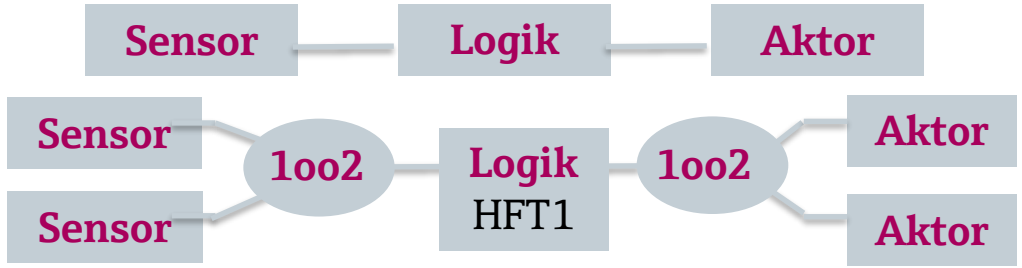


Tabelle 6 der IEC 61511-1

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

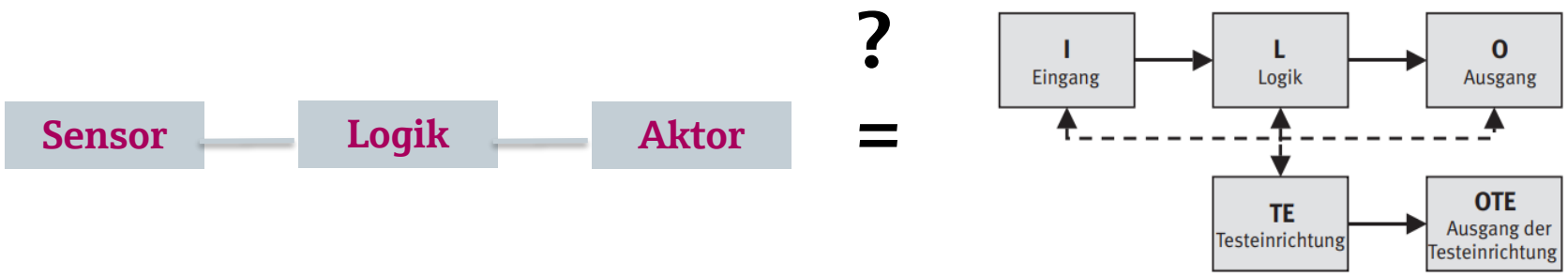


Konkret: SIL 2 und PL d im Vergleich

- 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?

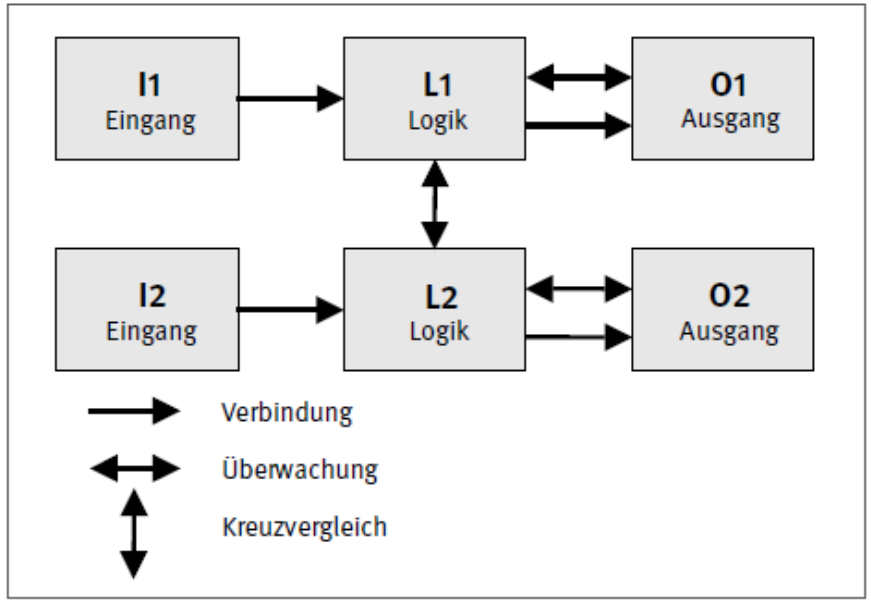
- Der Testkanal muss mindestens 50% der Zuverlässigkeit des getesteten Kanals aufweisen (DIN EN ISO 13849 4.5.4 und 4.5.5), und mindestens eine MTTF von 10 Jahren aufweisen. Es müssen also MTTF-Werte für den Testkanal vorliegen
- Weiterhin darf die Diagnose nicht rein softwarebasiert sein.
- Außerdem muss die Testrate 100x höher sein als die erwartete mittlere Anforderungsrate.

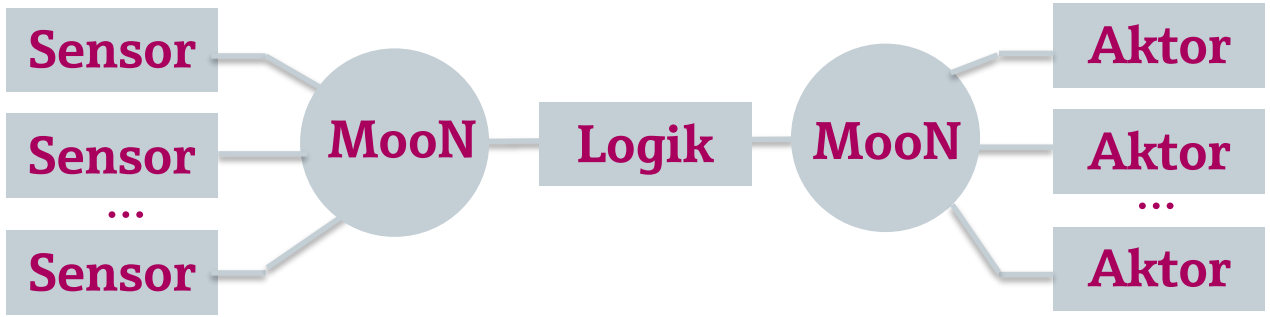


Übersetzung SIL <-> PL – wo geht‘s schief?

- Weiterer Unterschied: Die DIN EN ISO 13849 kennt keine Strukturen mit Kanalzahlen > 2.
- Bei Mehr als 2 Kanälen für den Nachweis die beiden schlechtesten Kanäle nehmen.

Vorgesehene Architektur für Kategorie 4





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 Erfahren zu bringen

Inhalt der VDI-Handlungsempfehlung

- Grundintention der VDI-Handlungsempfehlung:
  Betreiber auf das Thema „Gebrauchsdauer“ aufmerksam machen und es ihnen verständlich nahebringen

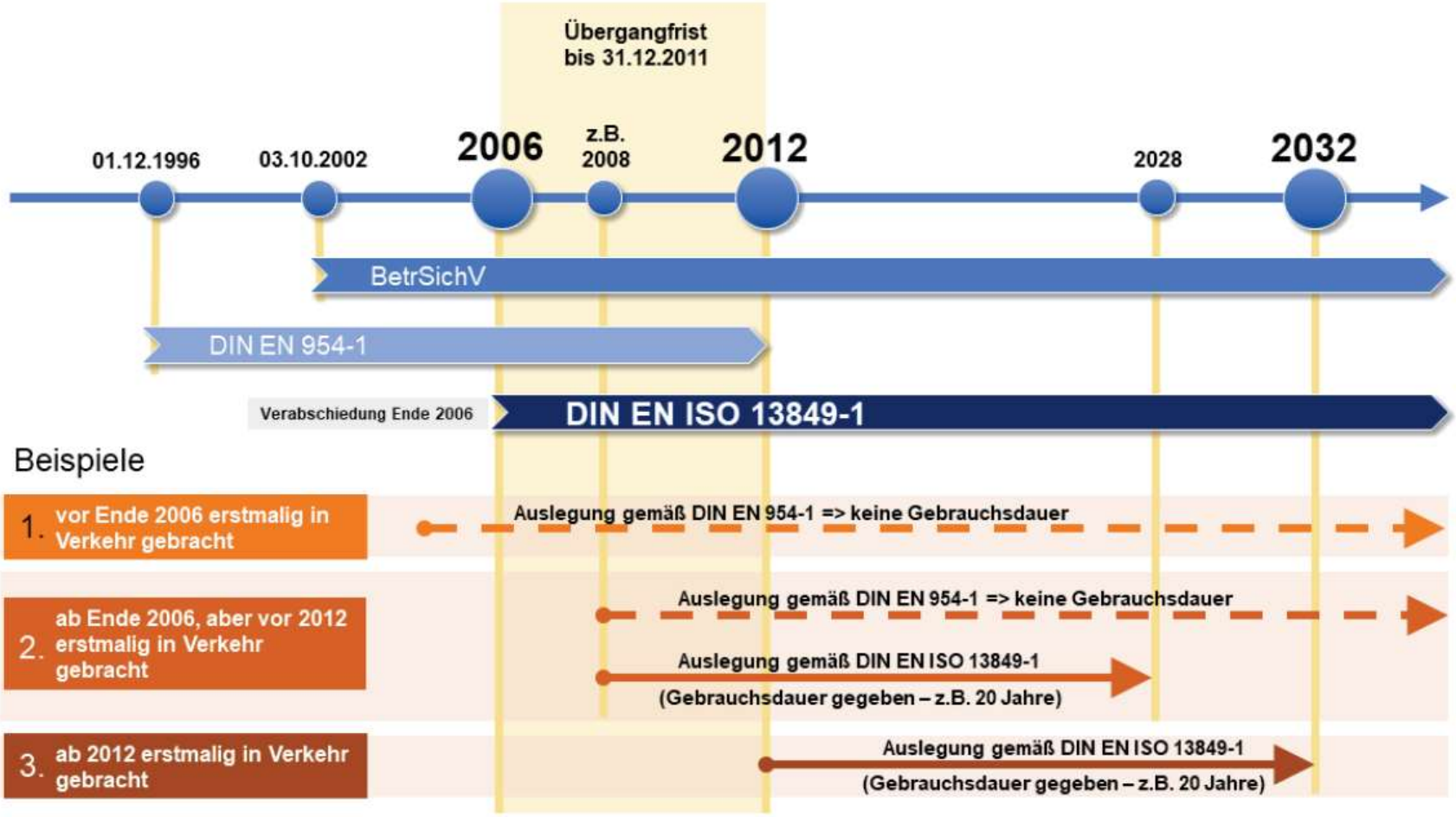
- Das Dokument ist in zwei Kapitel unterteilt

- 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

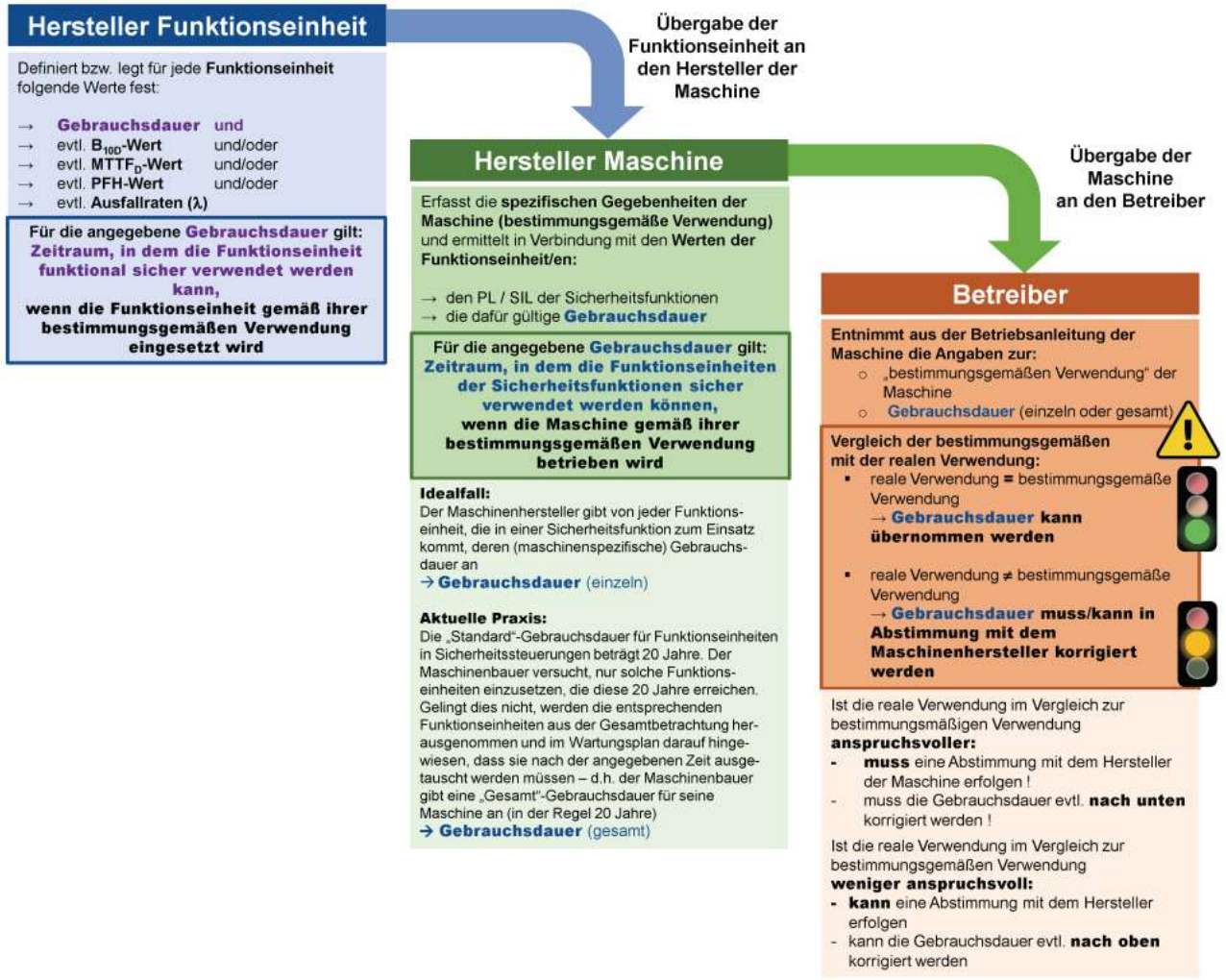

Lichtgitter


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 ?

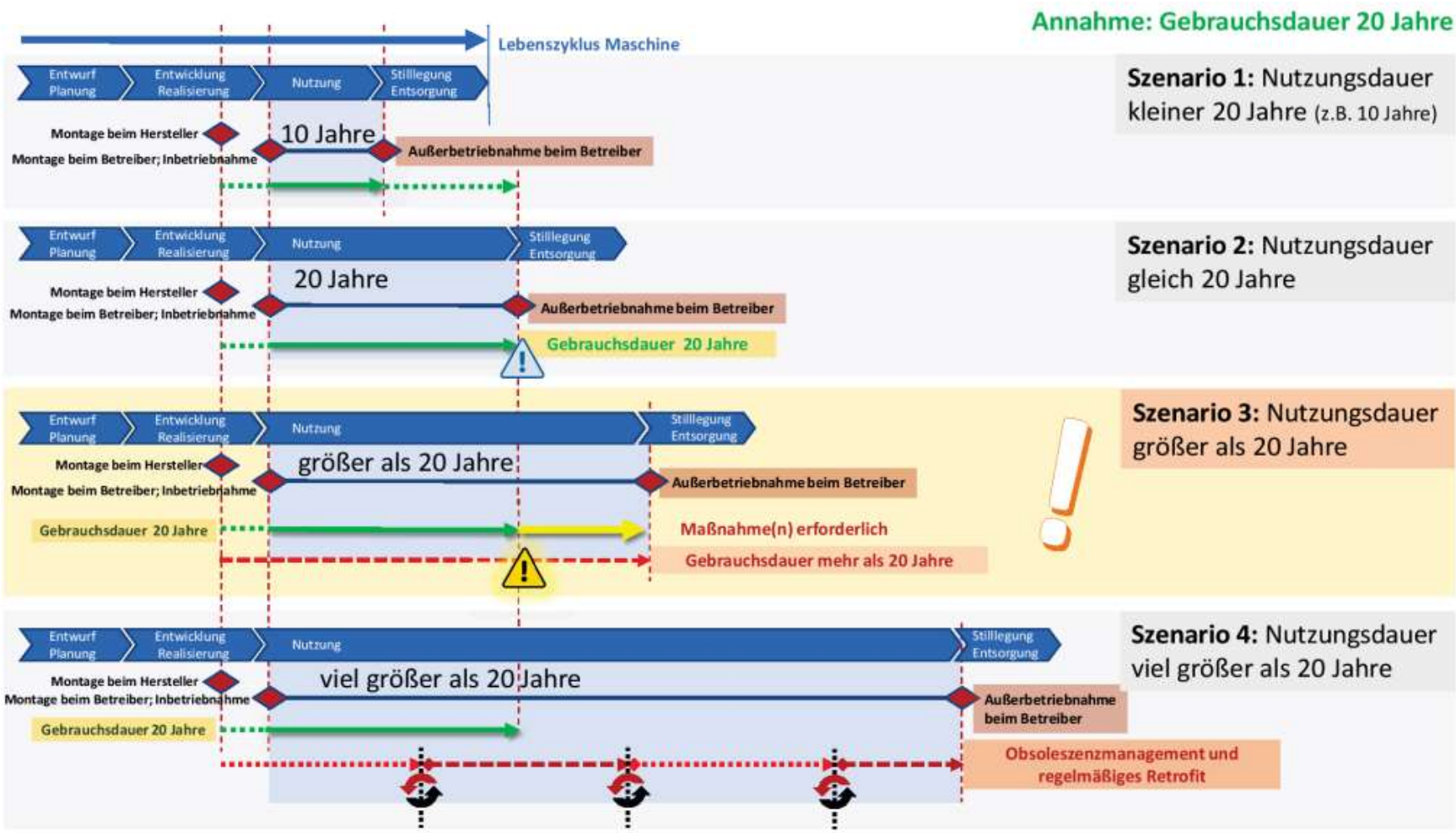
Wann „startet“ die Gebrauchsdauer ?

- **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

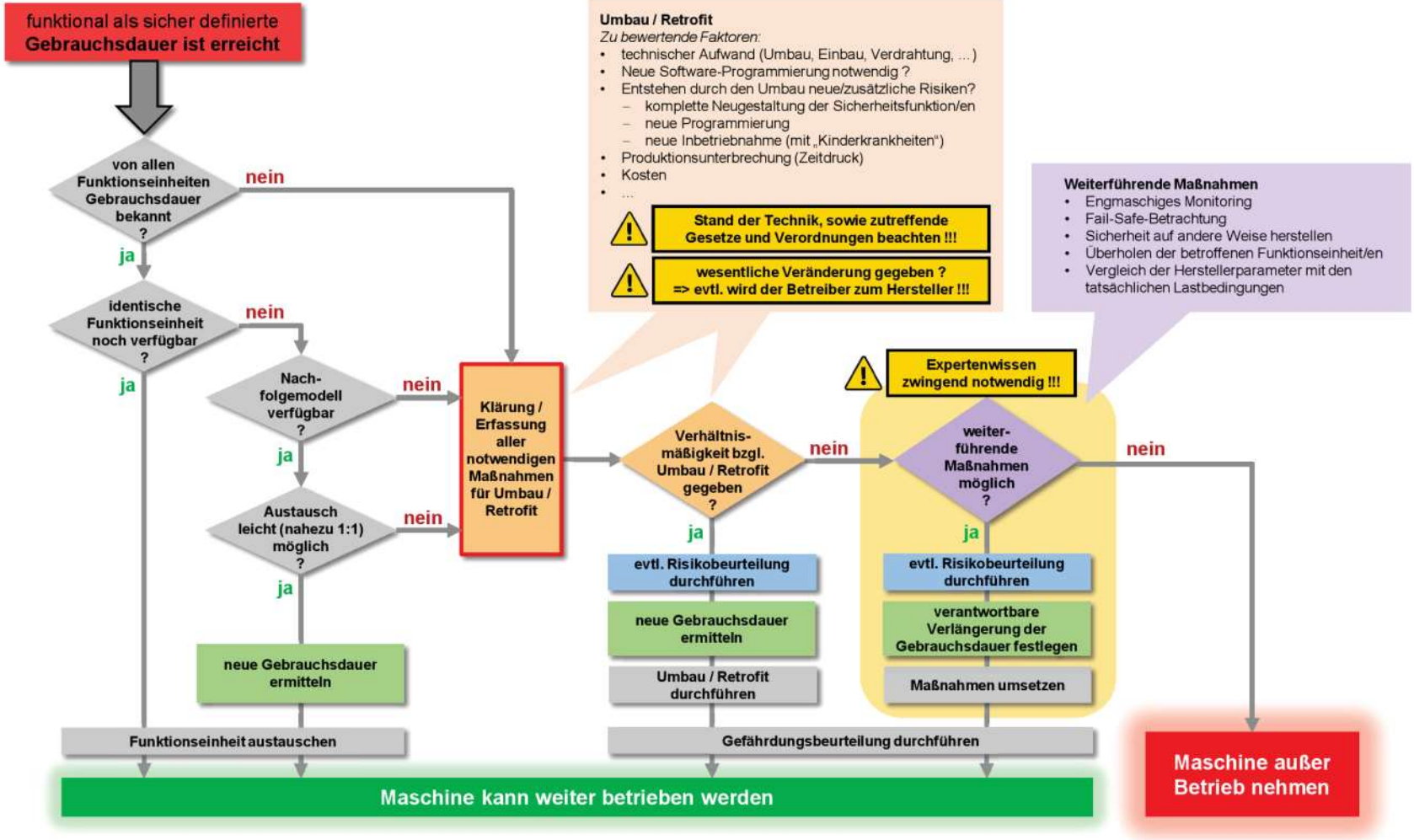
- **Bedeutet für den Betreiber:**
  - beim Kauf einer Maschine:
    erstmalige bestimmungsgemäße Verwendung (Inbetriebnahme) der Maschine
  - beim Kauf einer einzelnen Funktionseinheit (z.B. als Ersatzteil):
    entweder der Zeitpunkt der Anlieferung der Funktionseinheit (und Einlagerung) oder der Zeitpunkt 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



Entscheidungswege für den Betreiber



Hinweis

- Dieses Dokument ist eine Handlungs**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

BECKHOFF

Relationship between Markov Models, PFD and PFH

Frank Schiller[1], Jürgen Mottok[2], Patrick Gehlen[3]

[1]IEC/TC 65/WG 12, Beckhoff Automation GmbH & Co. KG;
[2]Laboratory for Safe and Secure Systems, Ostbayerische Technische Hochschule Regensburg;
[3]IEC/TC 44, Siemens AG

Relationship between Markov Models, PFD and PFH

BECKHOFF

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

Motivation – Demand on a Safety Function

BECKHOFF

- 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.

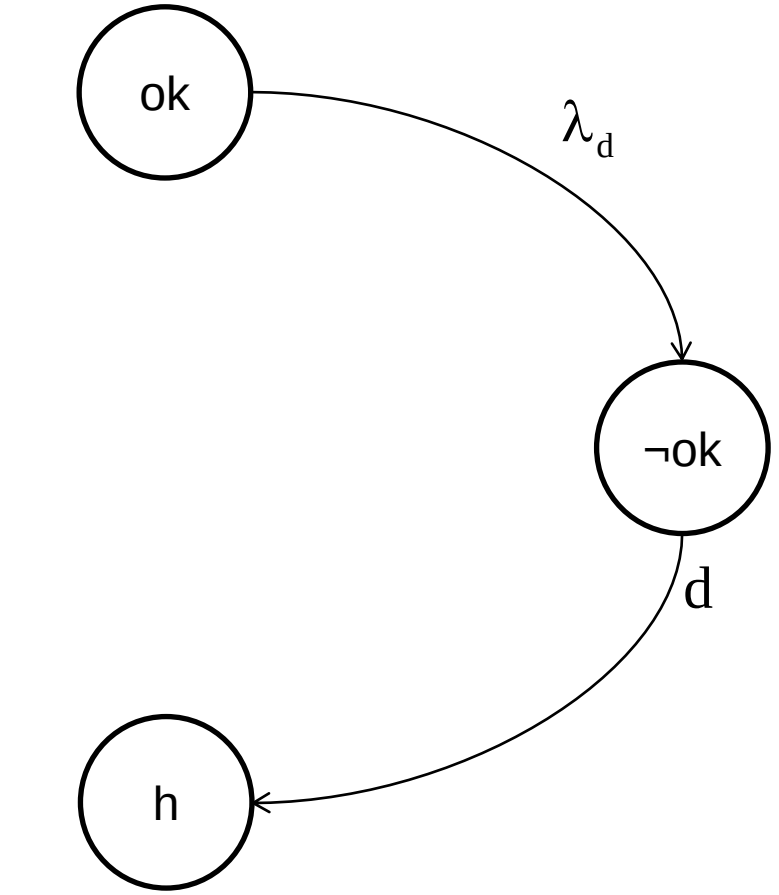
Relationship between Markov Models, PFD and PFH

BECKHOFF

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

Markov Model – Graphical Representation

BECKHOFF

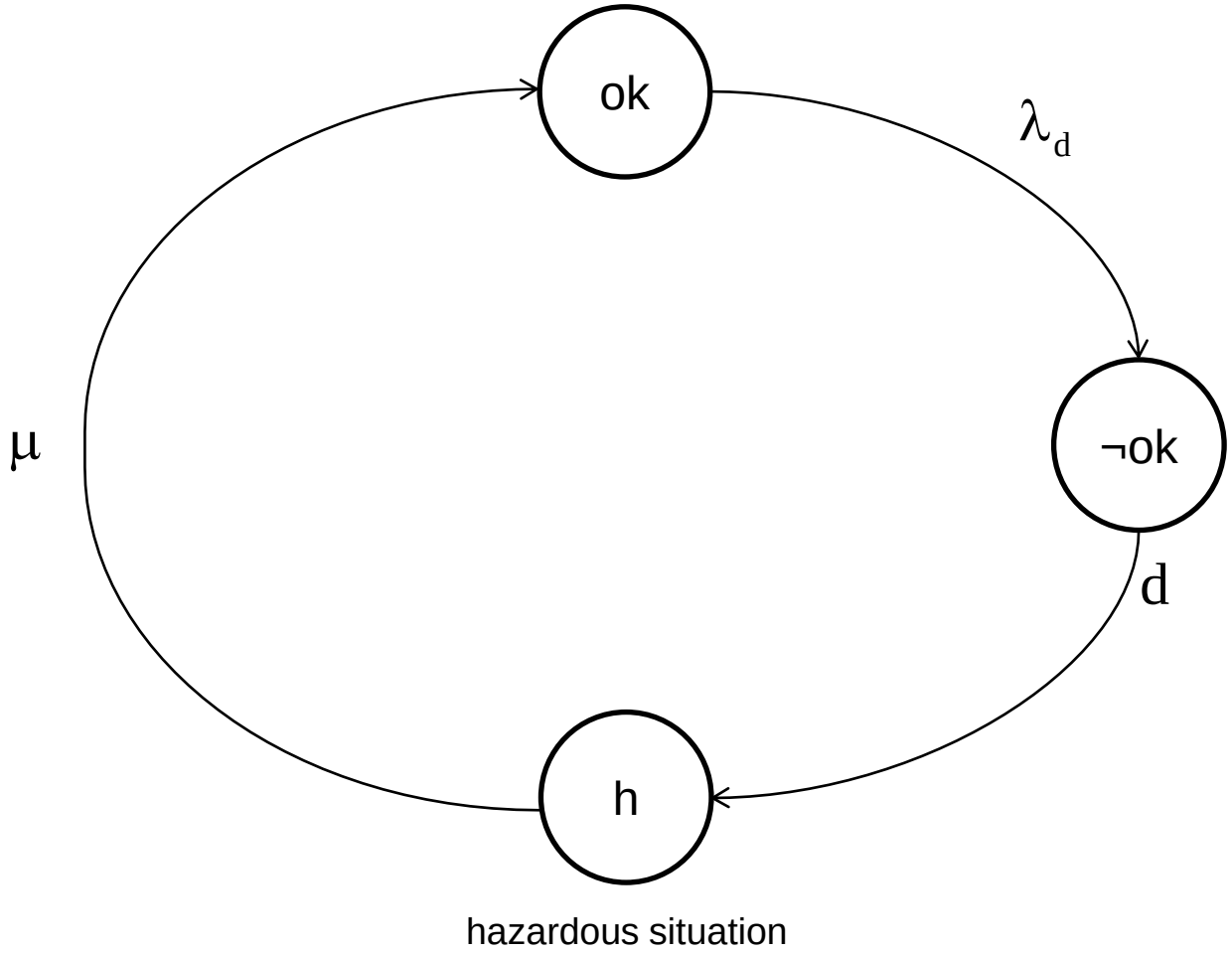


λ_d rate of dangerous errors

d rate of safety demands

At least one dangerous error occurred sometime in the past.

Markov Model – Graphical Representation



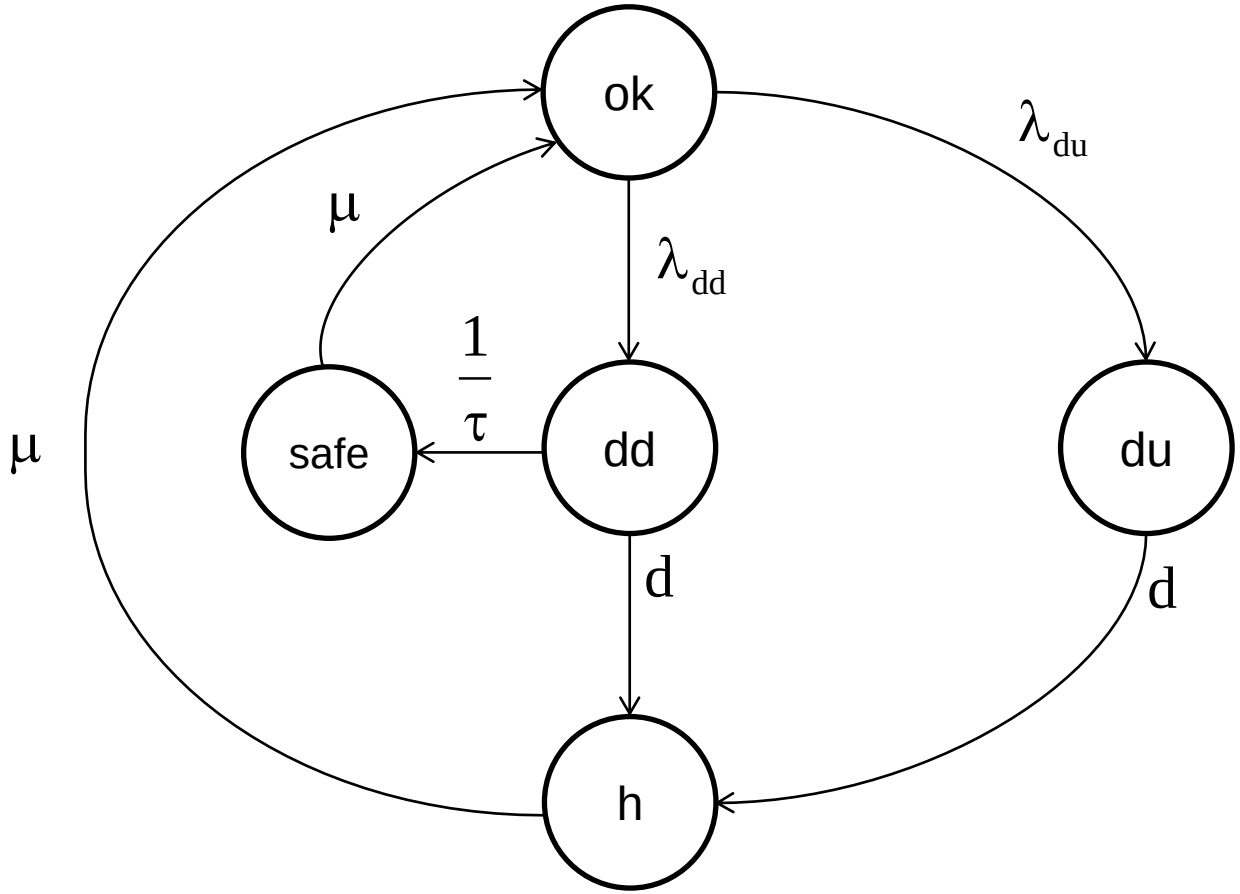
λ_d rate of dangerous errors

d rate of safety demands

μ repair “rate“

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

Markov Model – Graphical Representation



hazardous situation

λ_{du} rate of undetectable dang. errors

λ_{dd} rate of detectable dang. errors

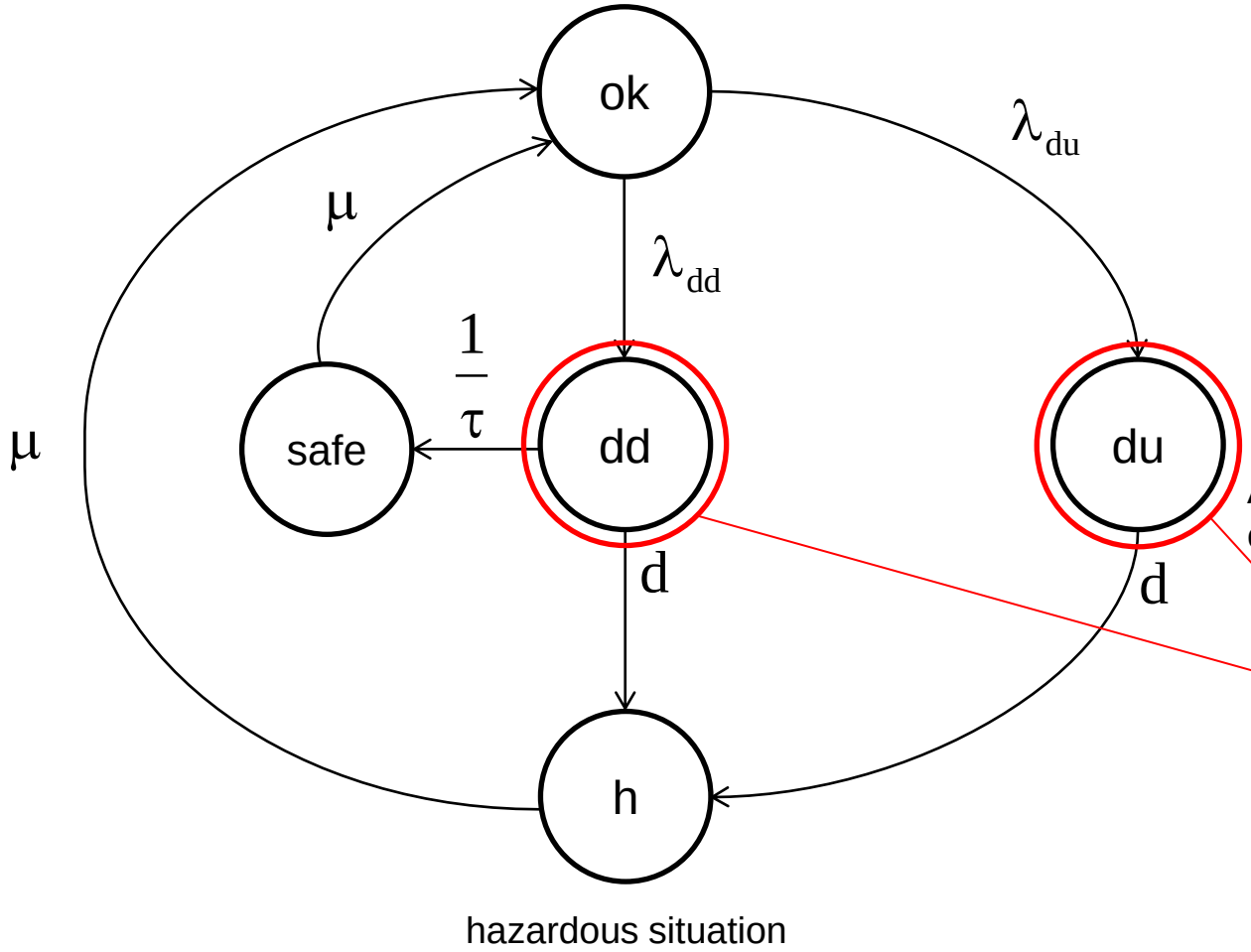
d rate of safety demands

μ repair “rate“

$1/\tau$ rate of error detection algorithm

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

Markov Model – PFD, PFH



λ_{du} rate of undetectable dang. errors

λ_{dd} rate of detectable dang. errors

d rate of safety demands

μ repair “rate“

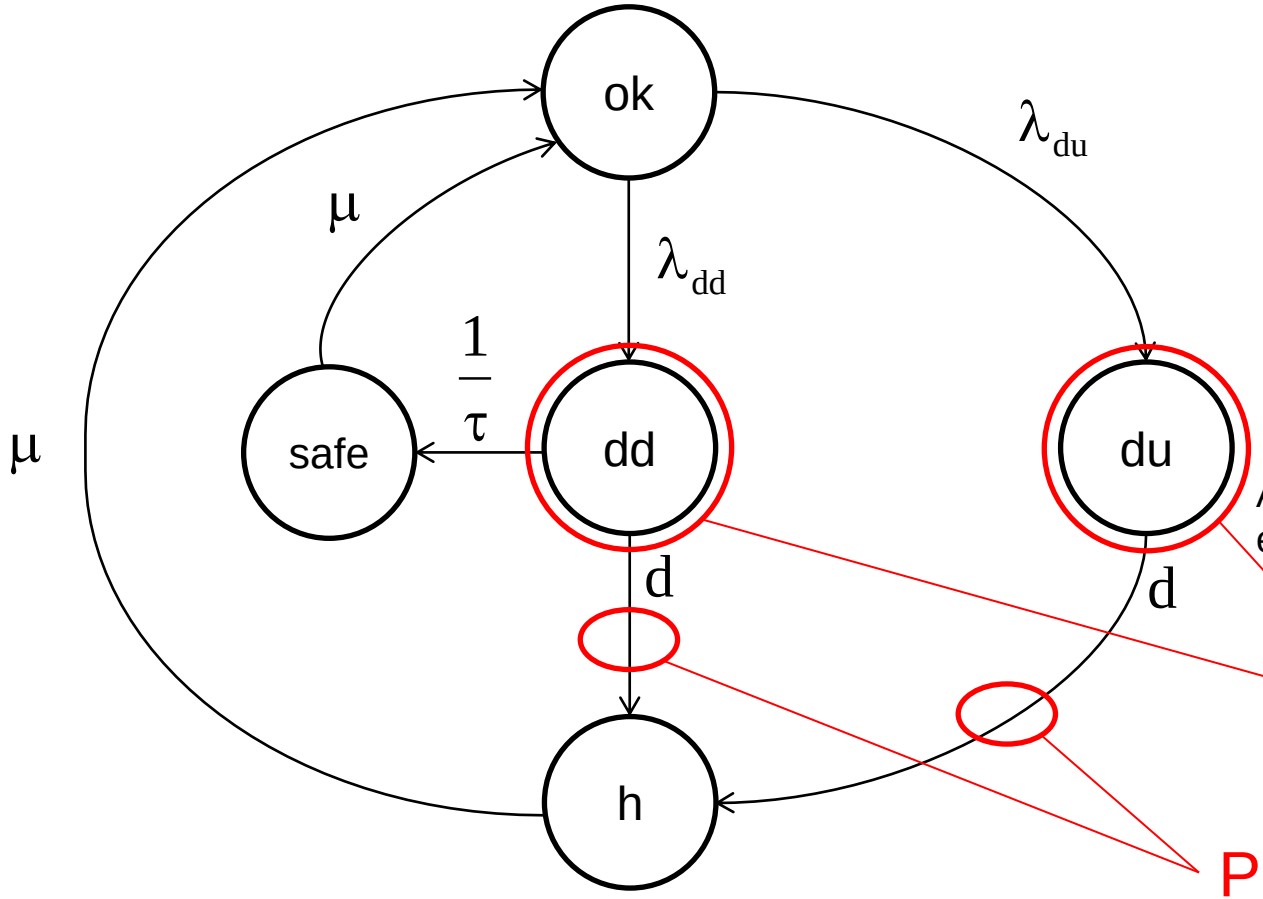
$1/\tau$ rate of error detection algorithm

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

PFD

Probability of dangerous Failure on Demand

Markov Model – PFD, PFH



hazardous situation

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.

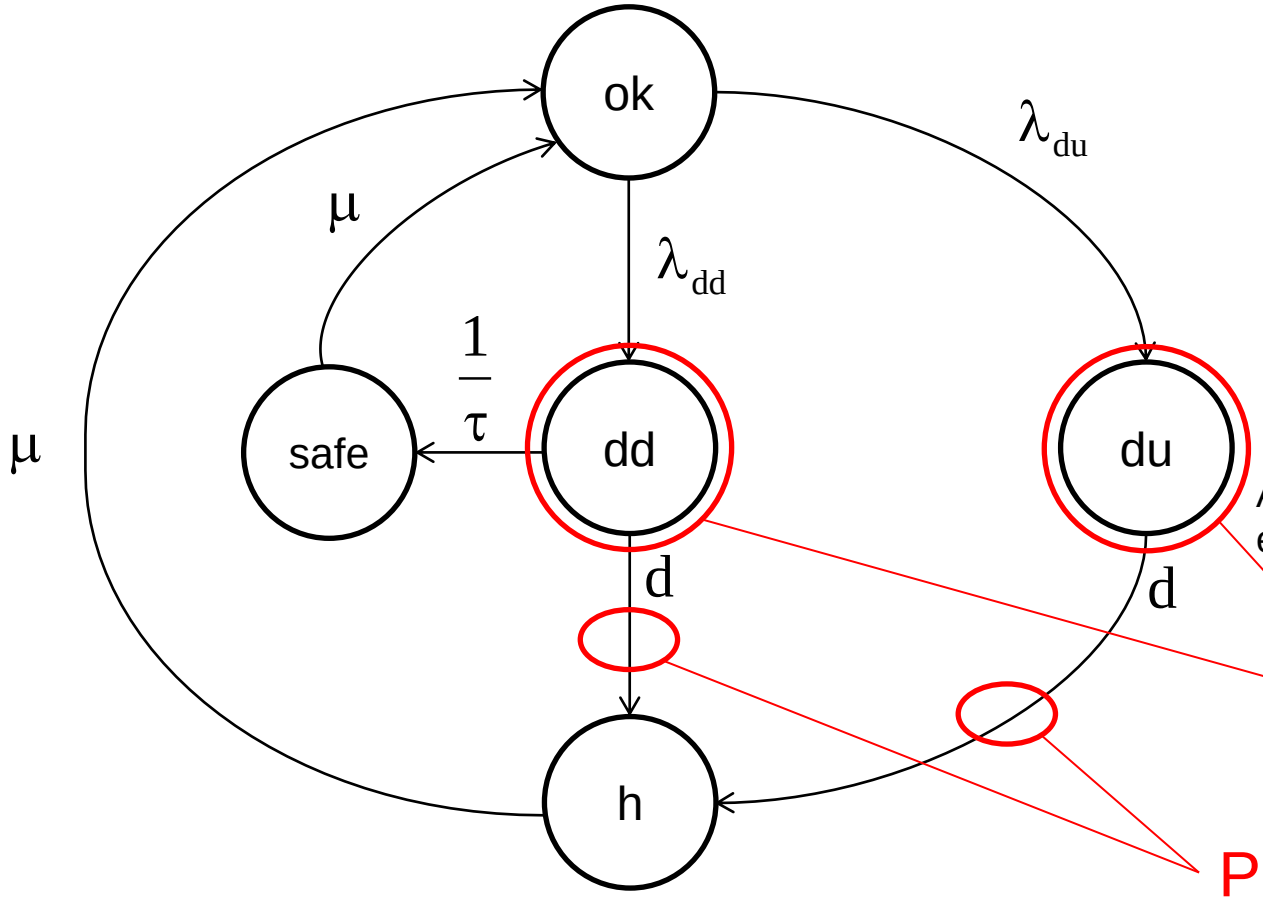
PFD

Probability of dangerous Failure on Demand

PFH

Probability of dangerous Failure per Hour

Markov Model – PFD, PFH



hazardous situation

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}

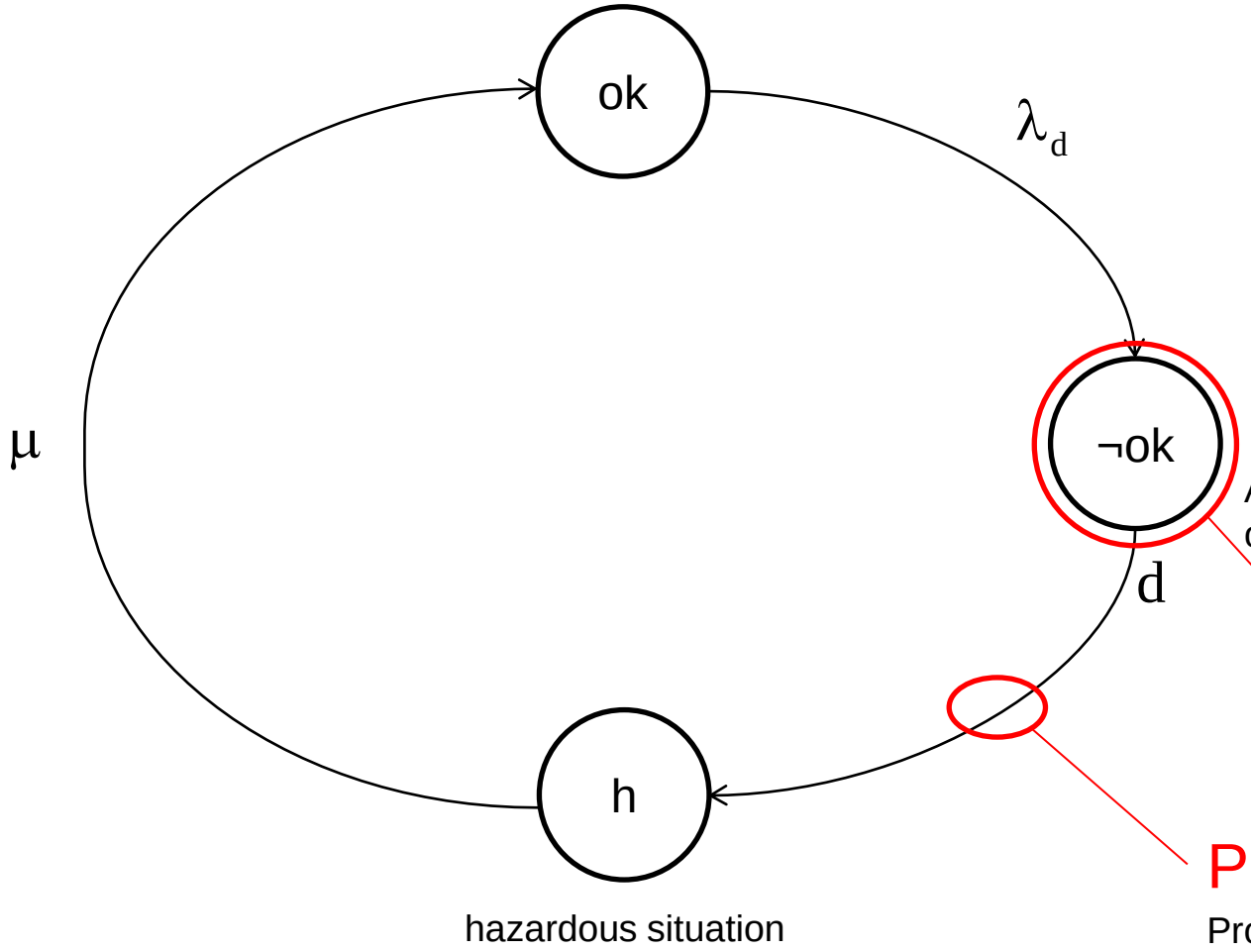
Probability of dangerous Failure per Hour (PFH of 1st edition IEC 61508)

PFH^{Ed2}

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

Markov Model – PFD, PFH

BECKHOFF



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.

PFD

Probability of dangerous Failure on Demand

PFH^{Ed1}

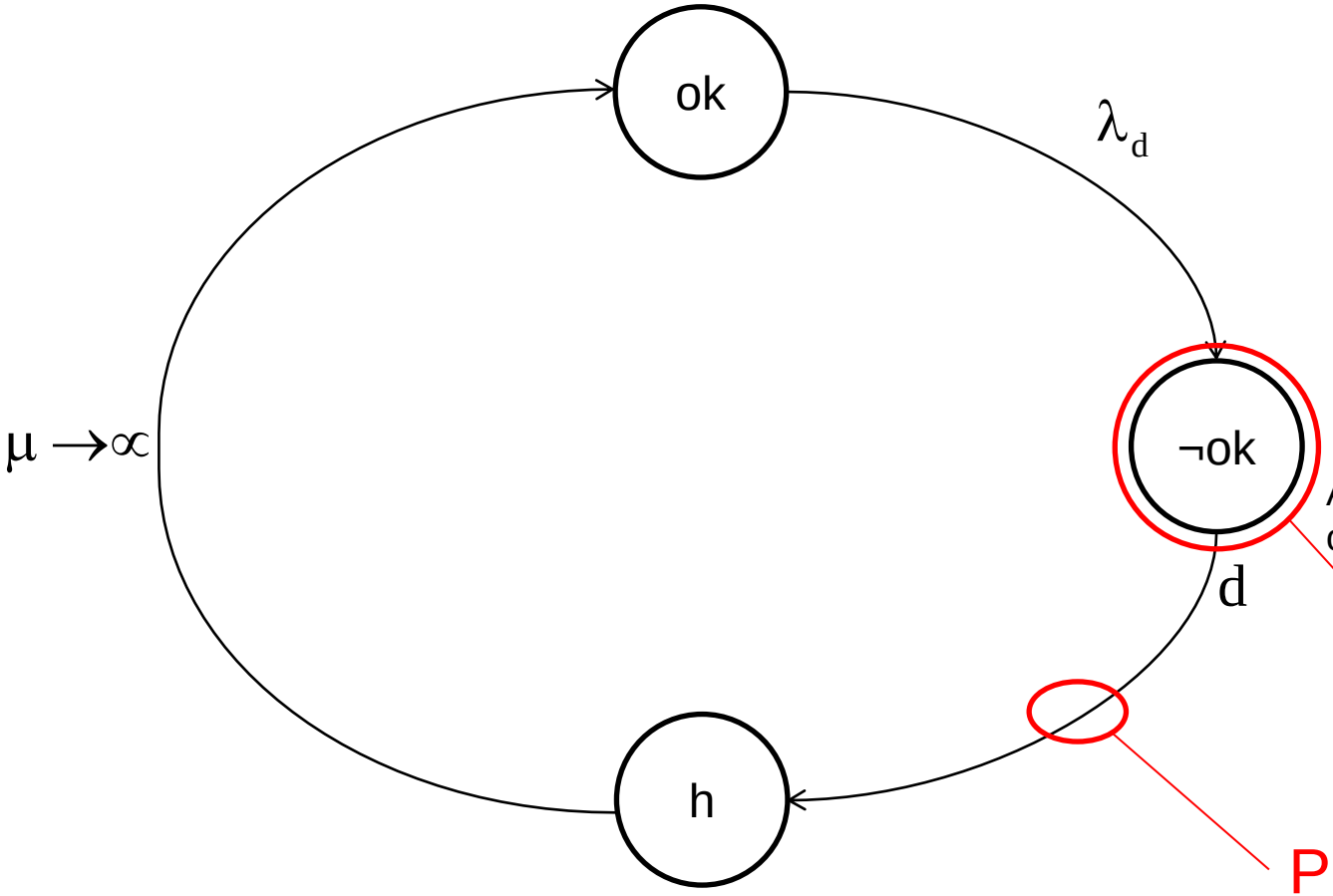
Probability of dangerous Failure per Hour (PFH of 1st edition IEC 61508)

PFH^{Ed2}

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

Markov Model – Worst Case Repair

BECKHOFF



hazardous situation

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.

PFD

Probability of dangerous Failure on Demand

PFH^{Ed1}

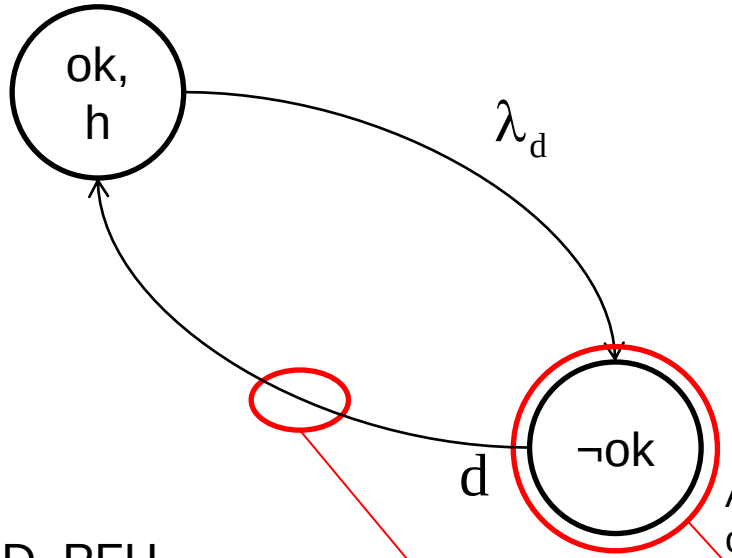
Probability of dangerous Failure per Hour (PFH of 1st edition IEC 61508)

PFH^{Ed2}

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

Markov Model – Worst Case Repair

BECKHOFF



λ_d rate of dangerous errors

d rate of safety demands

$\mu \to \infty$

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}

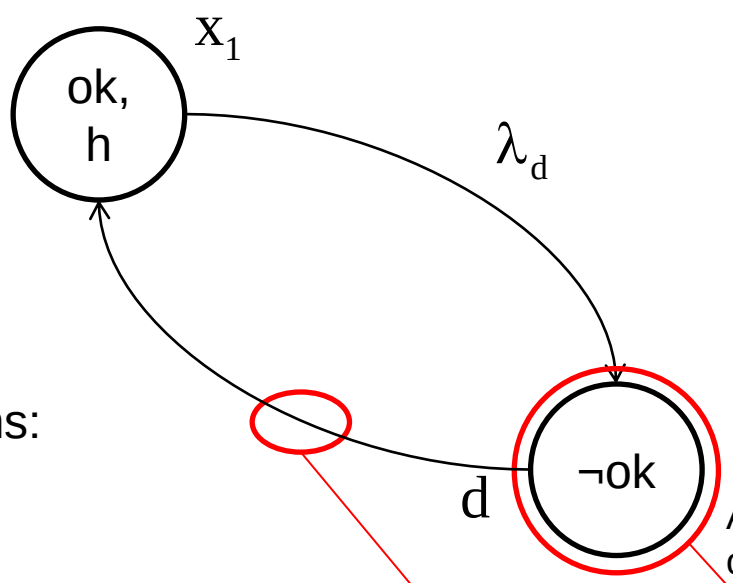
Probability of dangerous Failure per Hour (PFH of 1st edition IEC 61508)

PFH^{Ed2}

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

Markov Model – Mathematical Representation

BECKHOFF



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)

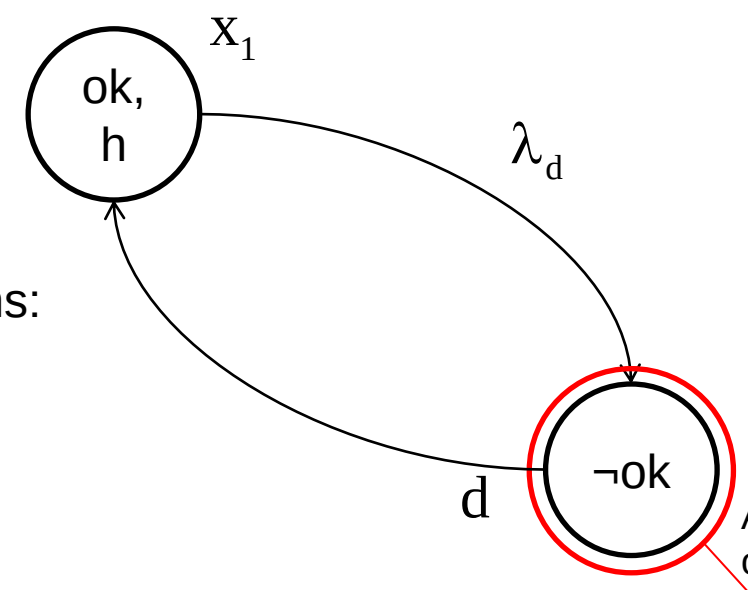
PFH^{Ed2}

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

Relationship between Markov Models, PFD and PFH

BECKHOFF

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



λ_d rate of dangerous errors

d rate of safety demands

Set of differential equations:

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

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

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

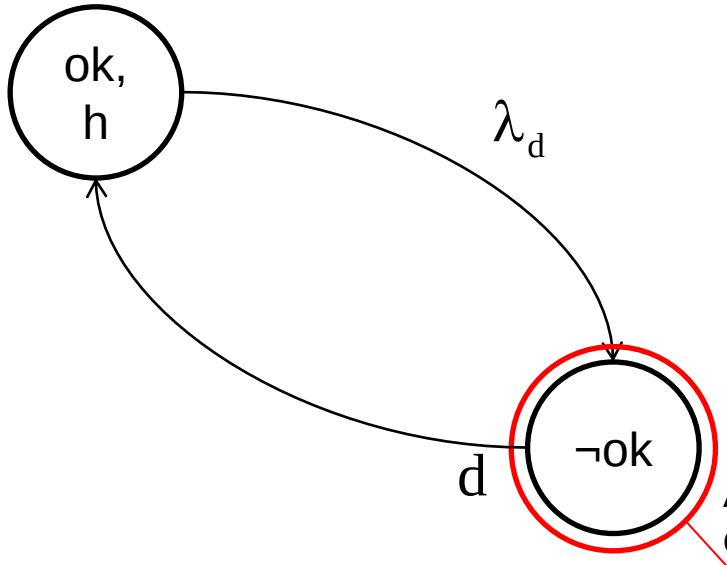
$$x_1 + x_2 = 1$$

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

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

PFD

Probability of dangerous Failure on Demand



λ_d rate of dangerous errors

d rate of safety demands

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

PFD

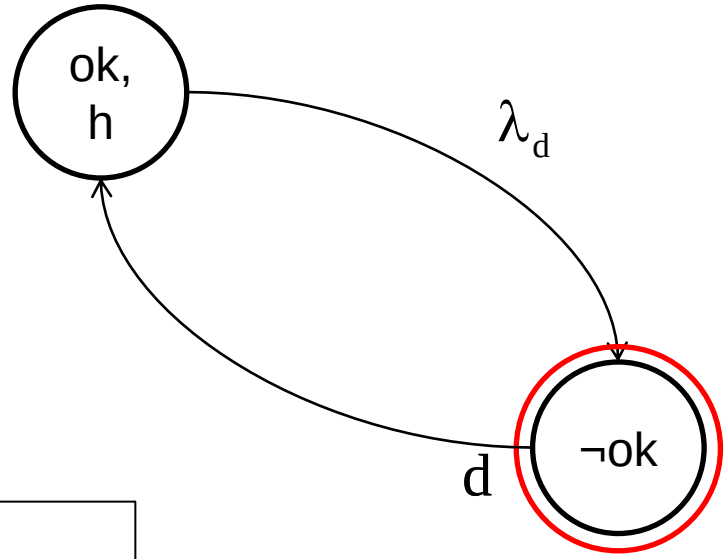
Probability of dangerous Failure on Demand

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

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

Worst case demand?

PFD – Worst Case Demand, d=0



λ_d rate of dangerous errors

d rate of safety demands

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

$$PFD_{avg}(T) \le PFD_{avg}(T, d = 0)$$

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

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

$d = 0$

Disadvantage:

- Greater value for PFD

Advantage:

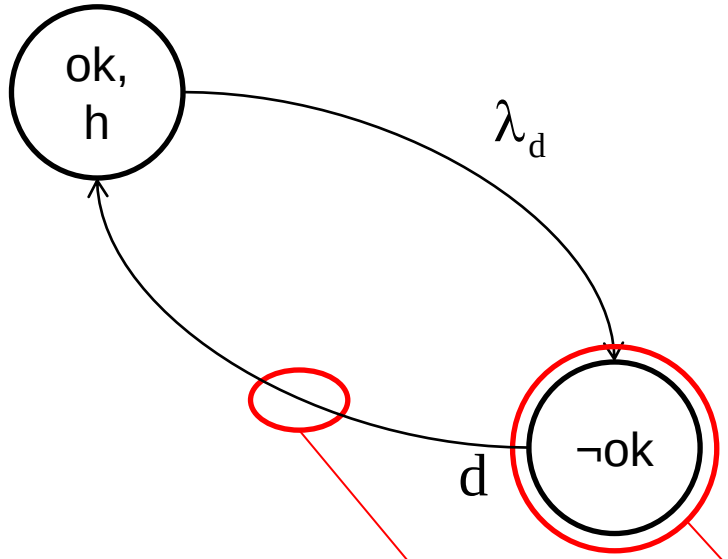
- No assumption about demand necessary, neither its rate nor its characteristic.

Relationship between Markov Models, PFD and PFH

BECKHOFF

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

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



λ_d rate of dangerous errors

d rate of safety demands

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

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

Worst case demand?

PFD

Probability of dangerous Failure on Demand

PFH^{Ed2}

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

PFH^{Ed2} – Worst Case Demand I, $d \rightarrow \infty$

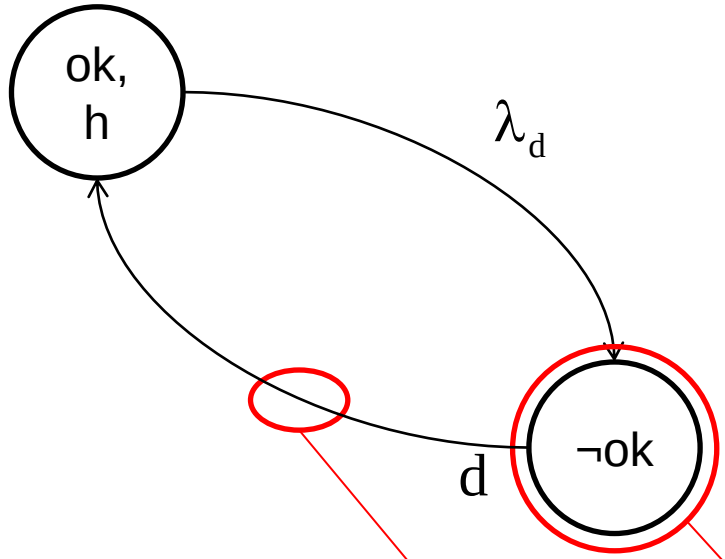
BECKHOFF

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

$$d \rightarrow \infty$$

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

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



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)

Disadvantages:

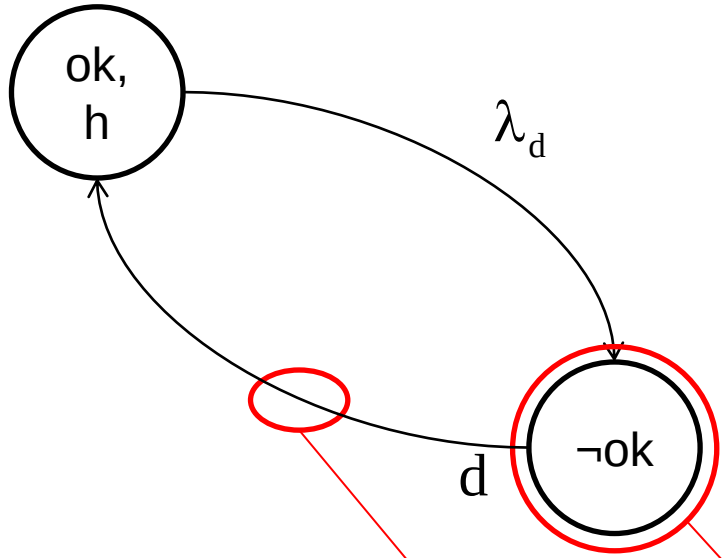
- Greater value for PFH

Advantages:

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

PFH^{Ed2} – Worst Case Demand II, PFD(t) ≤ PFD(t,d=0)

BECKHOFF



λ_d rate of dangerous errors

d rate of safety demands

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

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

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

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

Disadvantage:

- Greater value for PFH

Advantage:

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

PFD

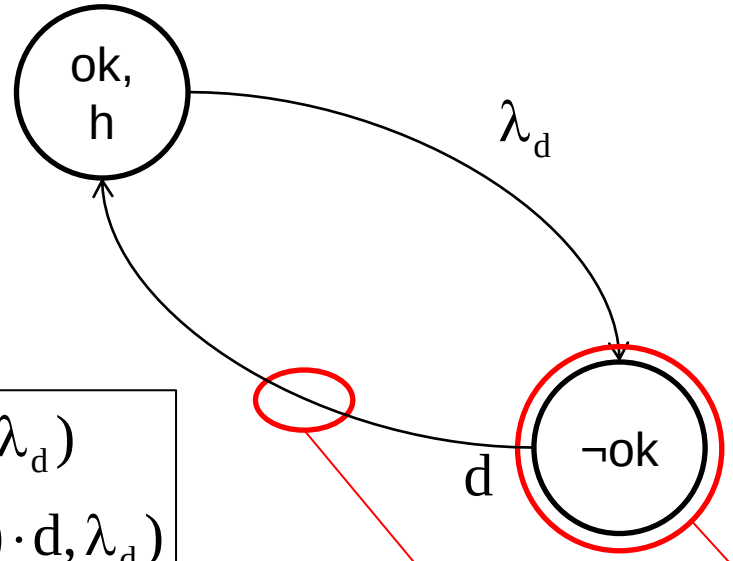
Probability of dangerous Failure on Demand

PFH^{Ed2}

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

PFH^{Ed2} – Worst Case Demand I+II

BECKHOFF



λ_d rate of dangerous errors

d rate of safety demands

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

$$PFH^{Ed2}_{avg}(T) \le \min(PFD_{avg}(T, d=0) \cdot d, \lambda_d)$$

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

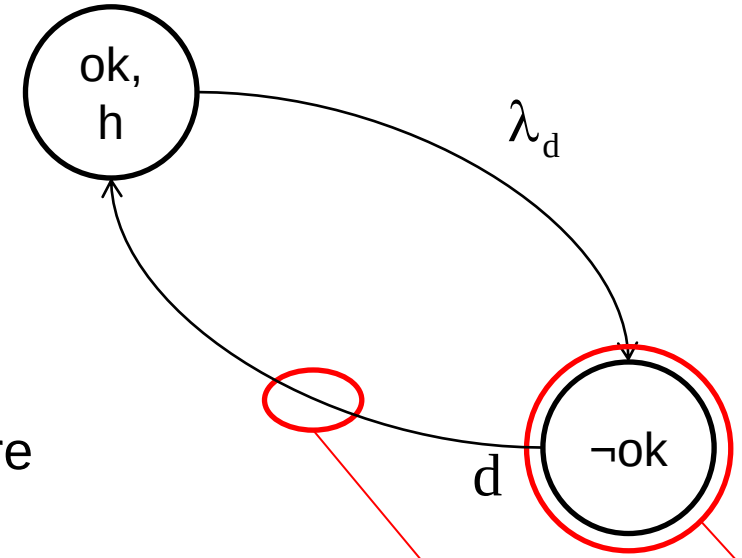
PFH^{Ed2}

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

Relationship between Markov Models, PFD and PFH

BECKHOFF

- 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.

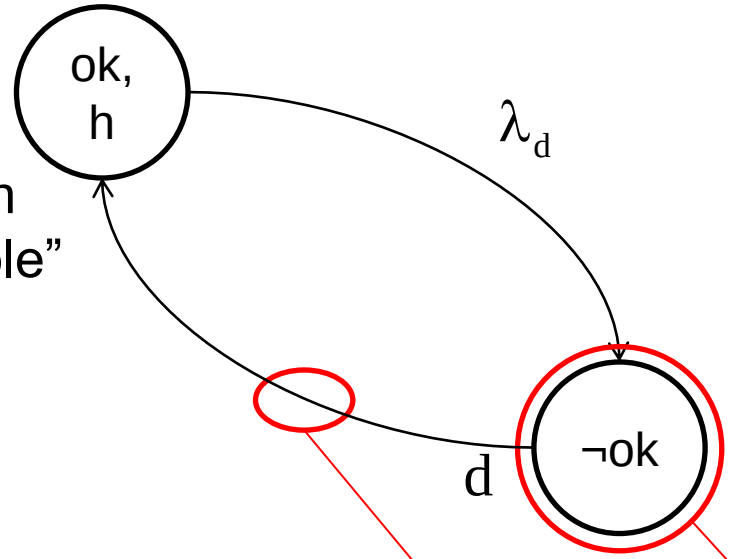
= Probability that a safety system is in state “¬ok” (“dangerous undetectable” and “dangerous detectable”) within one hour and at least one demand occurs within that hour.

PFD

Probability of dangerous Failure on Demand

PFH^{Ed1}

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



λ_d rate of dangerous errors

d rate of safety demands

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.

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

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} – Random Demand

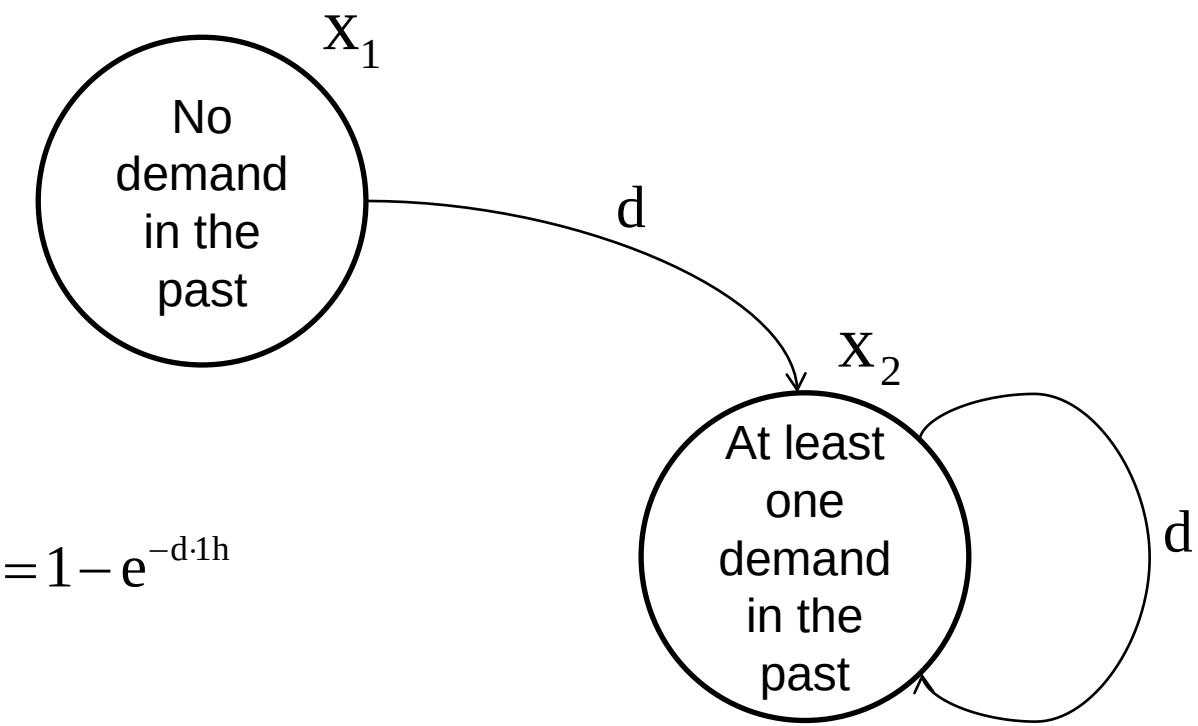
BECKHOFF

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

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

1. Random demand:

$$\dot{x}_1 = -d \cdot x_1$$
$$\dot{x}_2 = d \cdot x_1$$
$$x_1 + x_2 = 0$$
$$x_1(t_0) = 1,\ x_2(t_0) = 0$$



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

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

PFH^{Ed1} – Cyclic Demand

BECKHOFF

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

2. Cyclic demand:

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

Examples:

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

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

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

PFH^{Ed1} – Worst-Case Demand

BECKHOFF

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

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

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.

$$PFH^{Ed1}(t..t+1h) \leq PFD(t+1h, d=0)$$
$$PFH^{Ed1}_{avg}(T..T+1h) \leq PFD_{avg}(T+1h, d=0)$$

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

Relationship between Markov Models, PFD and PFH

BECKHOFF

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

Discussion – PFD vs. PFH^{Ed1}, PFH^{Ed2}

BECKHOFF

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

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

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

$$PFH^{Ed1}(t, t+1h) \le PFD(t+1h, d=0) \cdot \frac{1}{365 \cdot 24h} \cdot 1h$$
$$\le PFD(t+1h, d=0) \cdot 1.1 \cdot 10^{-4}$$

$$PFH^{Ed2}(t) \le PFD(t, d=0) \cdot \frac{1}{365 \cdot 24h}$$
$$\le PFD(t, d=0) \cdot 1.1 \cdot 10^{-4} h^{-1}$$

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

Discussion – PFH^{Ed1} vs. PFH^{Ed2}

BECKHOFF

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

$$\cong$$

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

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

Relationship between Markov Models, PFD and PFH

BECKHOFF

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

Summary

BECKHOFF

- 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.

Summary

BECKHOFF

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

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

$$PFD_{avg}(T) \le PFD_{avg}(T, d = 0)$$

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

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

$$PFH^{Ed2}_{avg}(T) = PFD_{avg}(T) \cdot d$$

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

$$PFH^{Ed2}_{avg}(T) \le \min(PFD_{avg}(T, d = 0) \cdot d, \lambda_d)$$

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

$$PFH^{Ed1}_{avg}(T..T + 1h) \le PFD_{avg}(T + 1h, d = 0) \cdot \min(d \cdot 1h, 1)$$

References

[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…“

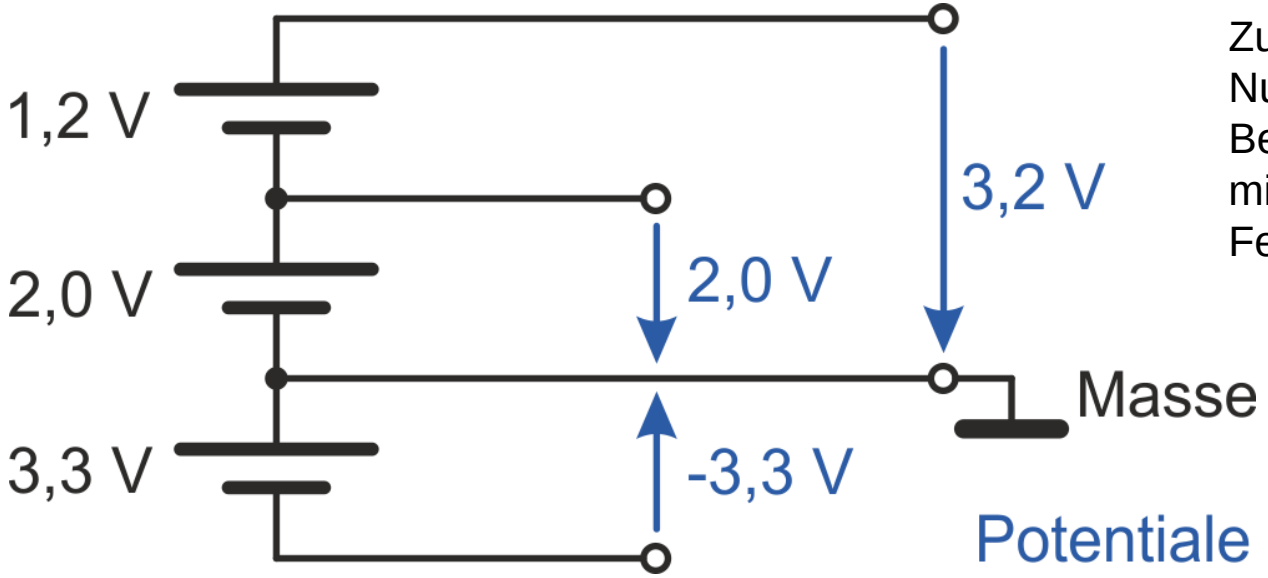
www.yncoris.com

YNCORIS
Industrial Services

SPANNUNG - POTENTIAL – ERDUNG…

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



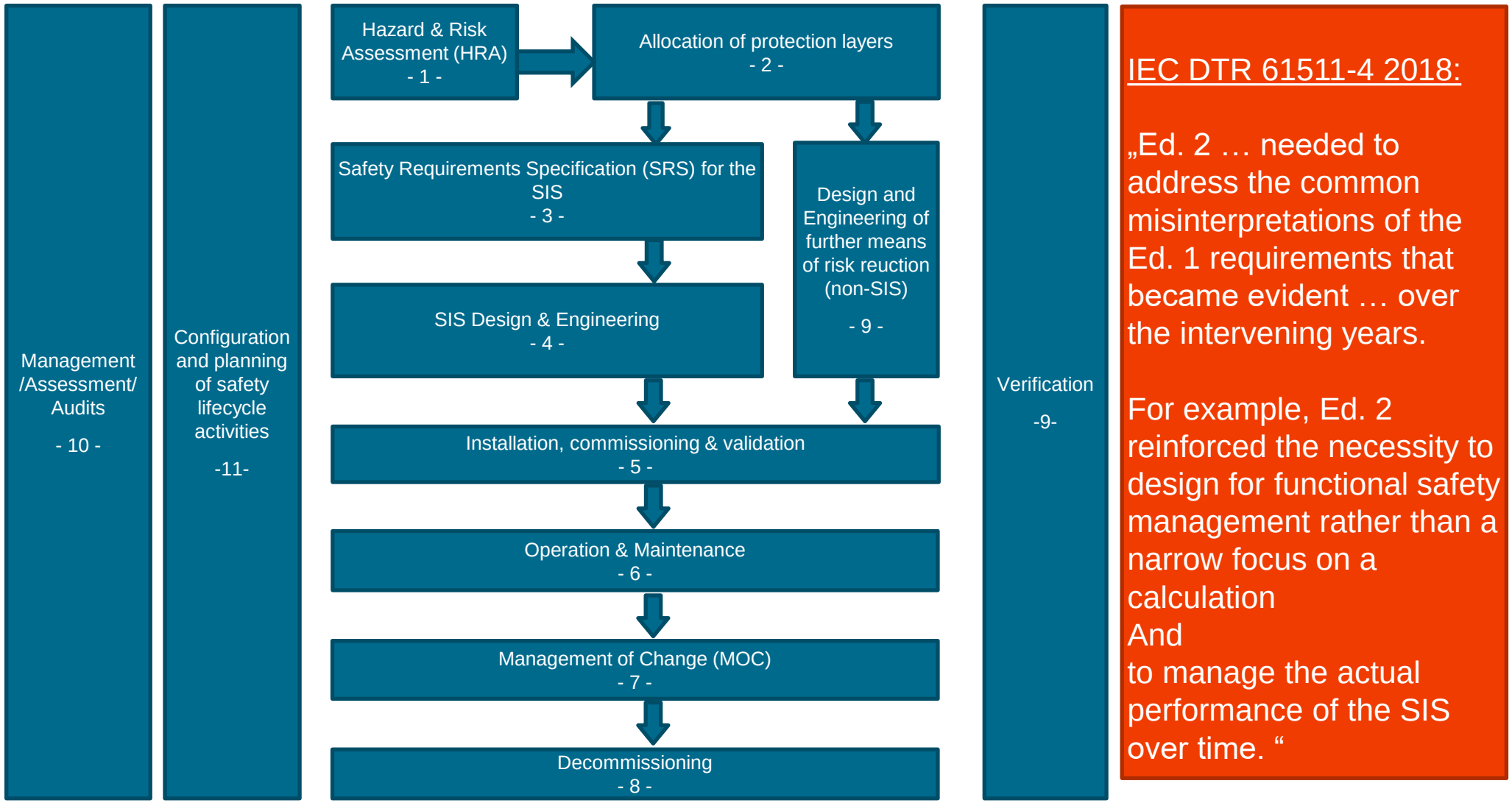
Zur Eindeutigkeit wird ein **Bezugspunkt** P0 festgelegt, der das Nullpotential erhält. […] In der Elektrotechnik wird der Bezugspunkt auf dasjenige Leiterstück gelegt, das mit **„Masse“** bezeichnet wird; **in der Theorie** der elektrischen Felder wird der Bezugspunkt oft **„ins Unendliche“** gelegt.

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

Bild: https://www.homeconstructor.net/de/was-ist-elektrische-spannung

Texte:https://de.wikipedia.org/wiki/Elektrische_Spannung#Elektrisches_Potential

POTENTIAL VON INTELLIGENTER DIGITALISIERUNG: UNTERSTÜTZUNG IM SAFETY LIFE CYCLE (SLC) GEMÄß IEC 61511

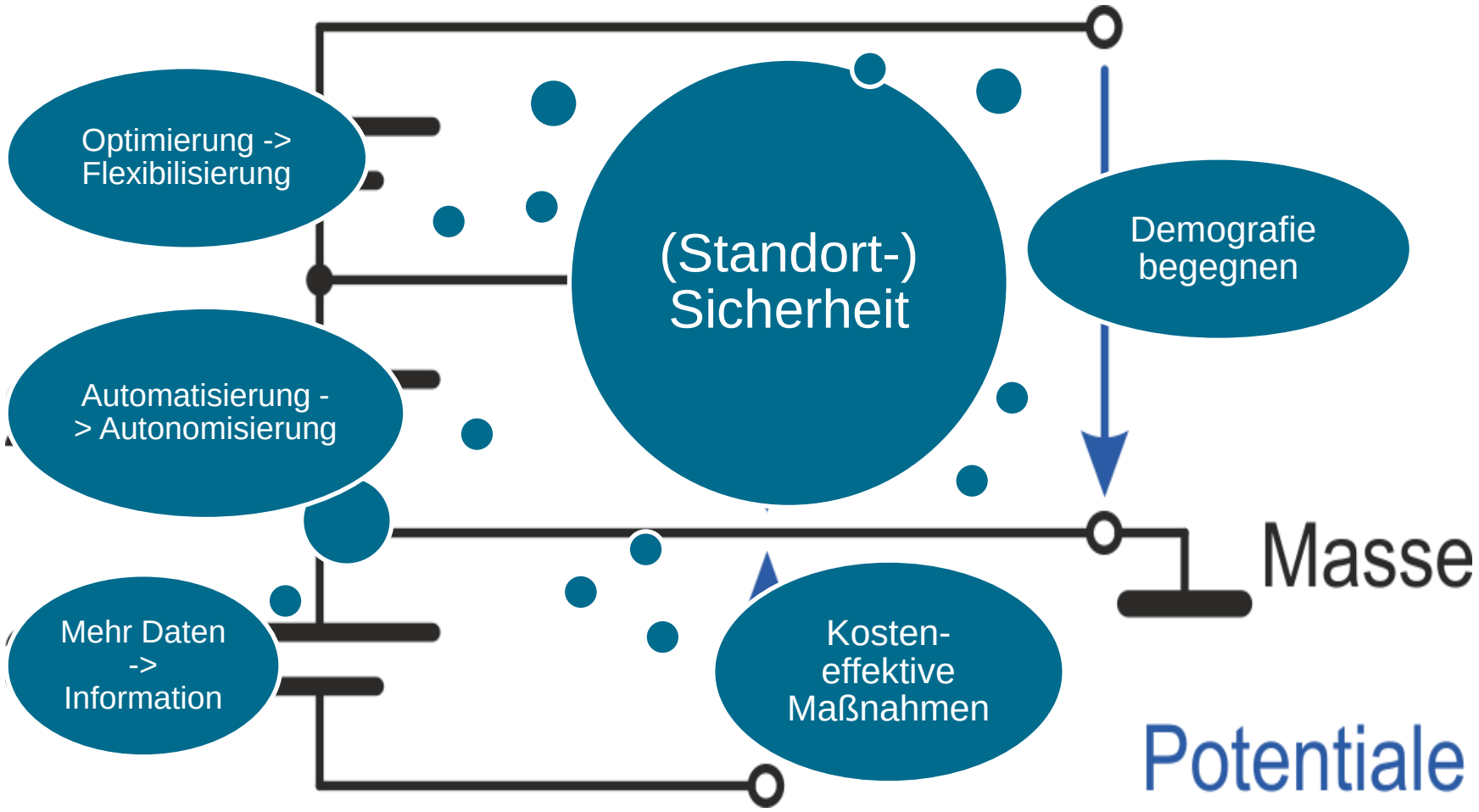


IEC DTR 61511-4 2018:

„Ed. 2 … needed to address the common misinterpretations of the Ed. 1 requirements that became evident … over the intervening years.

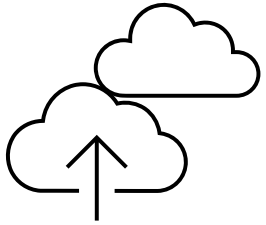
For example, Ed. 2 reinforced the necessity to design for functional safety management rather than a narrow focus on a calculation
And
to manage the actual performance of the SIS over time. “

POTENTIALE VON DIGITALISIERUNG UND KI IM SAFETY LIFECYCLE …

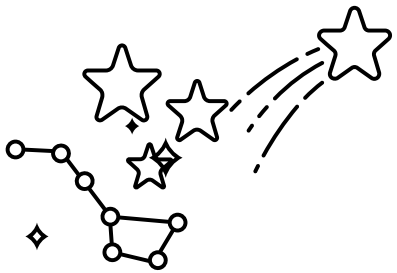


POTENTIAL(BEWERTUNGS)DIFFERENZEN – SPANNUNG VORPROGRAMMIERT?

YNCORIS Industrial Services



Nutzen/ Zukunftsfähigkeit



Wir machen das

manuelle Aufwände reduzieren

Diagnose als Teil flexibler Prüfkonzepte

erhöhte Granulariät -> noch genauere Auswertung möglich -> Optimierung

Störddatenerhebung und Unterstützungsmöglichkeit für Betriebsbewährungsprozesse

Mehr ist nicht besser

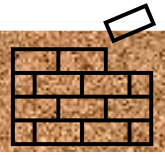
Die Arbeit bleibt doch bei mir hängen

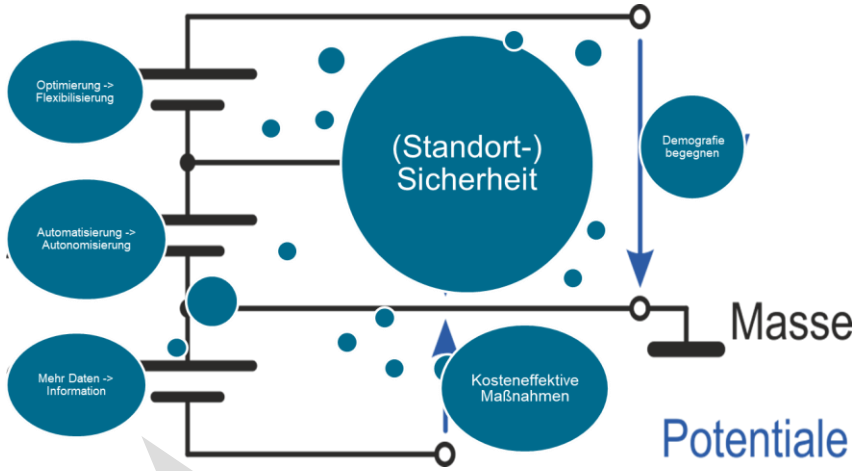
das hat schon mal nicht geklappt

Die Verantwortung kann ich nicht abgeben

Wir lassen das

Kosten/ Risiko

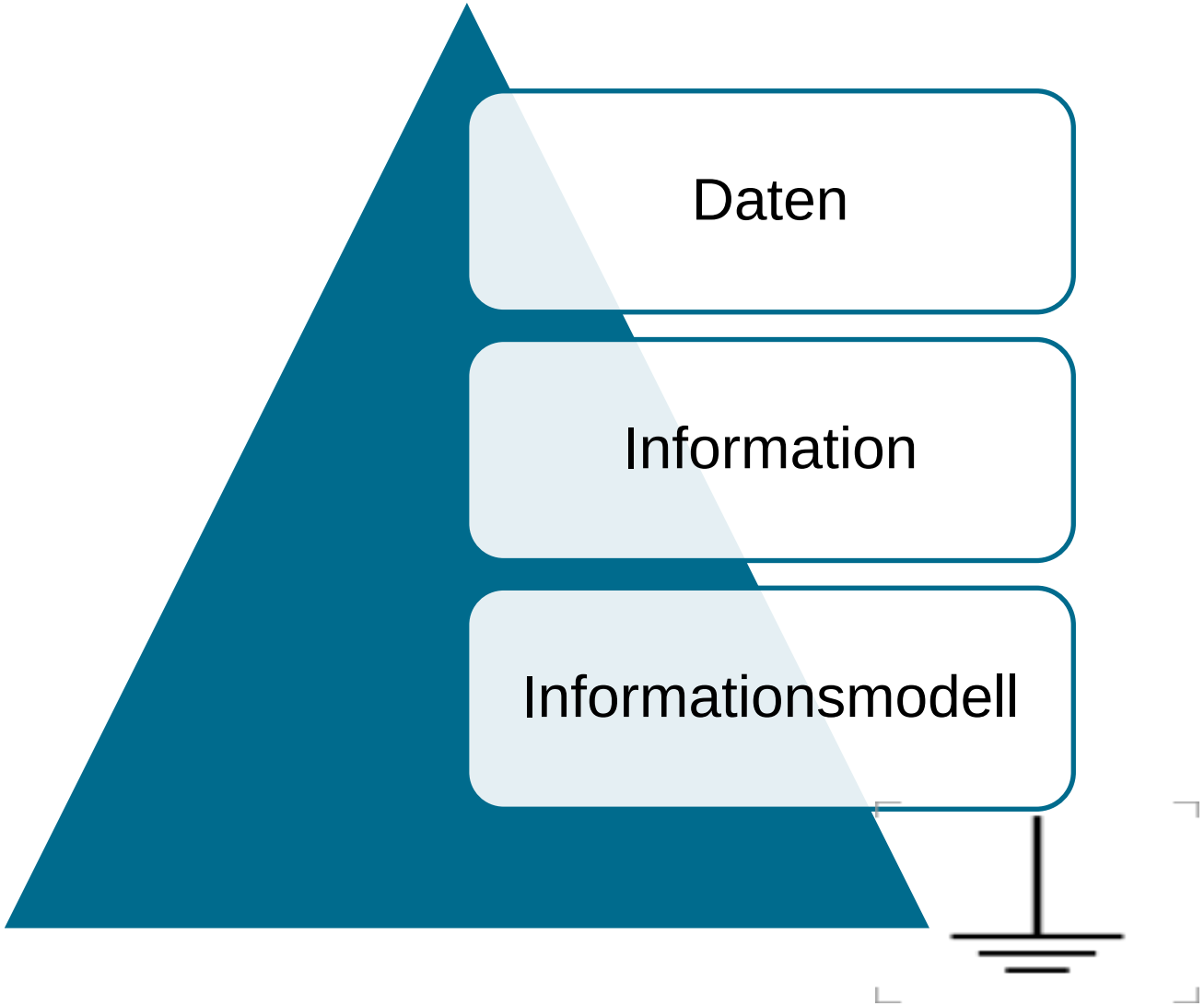




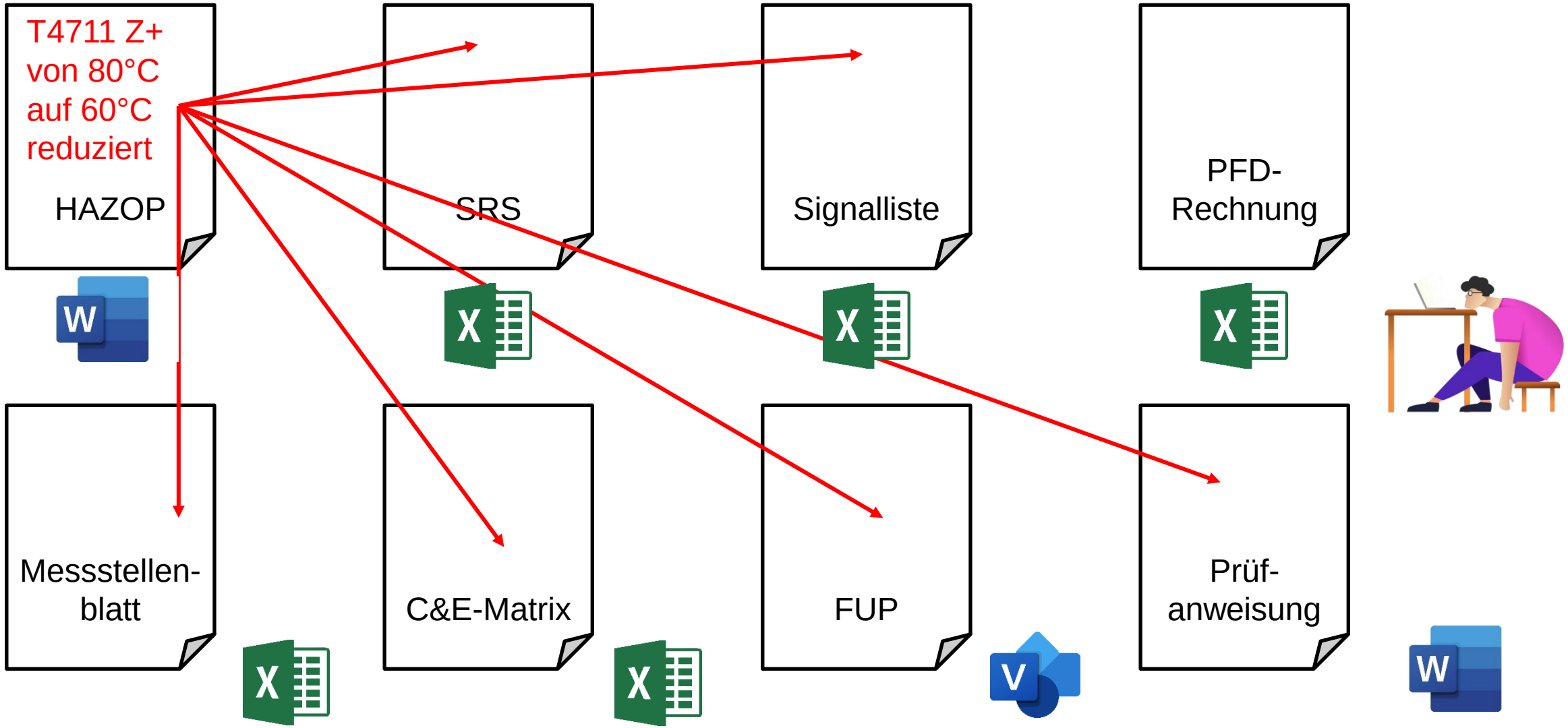
Mehr Daten -> Information

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

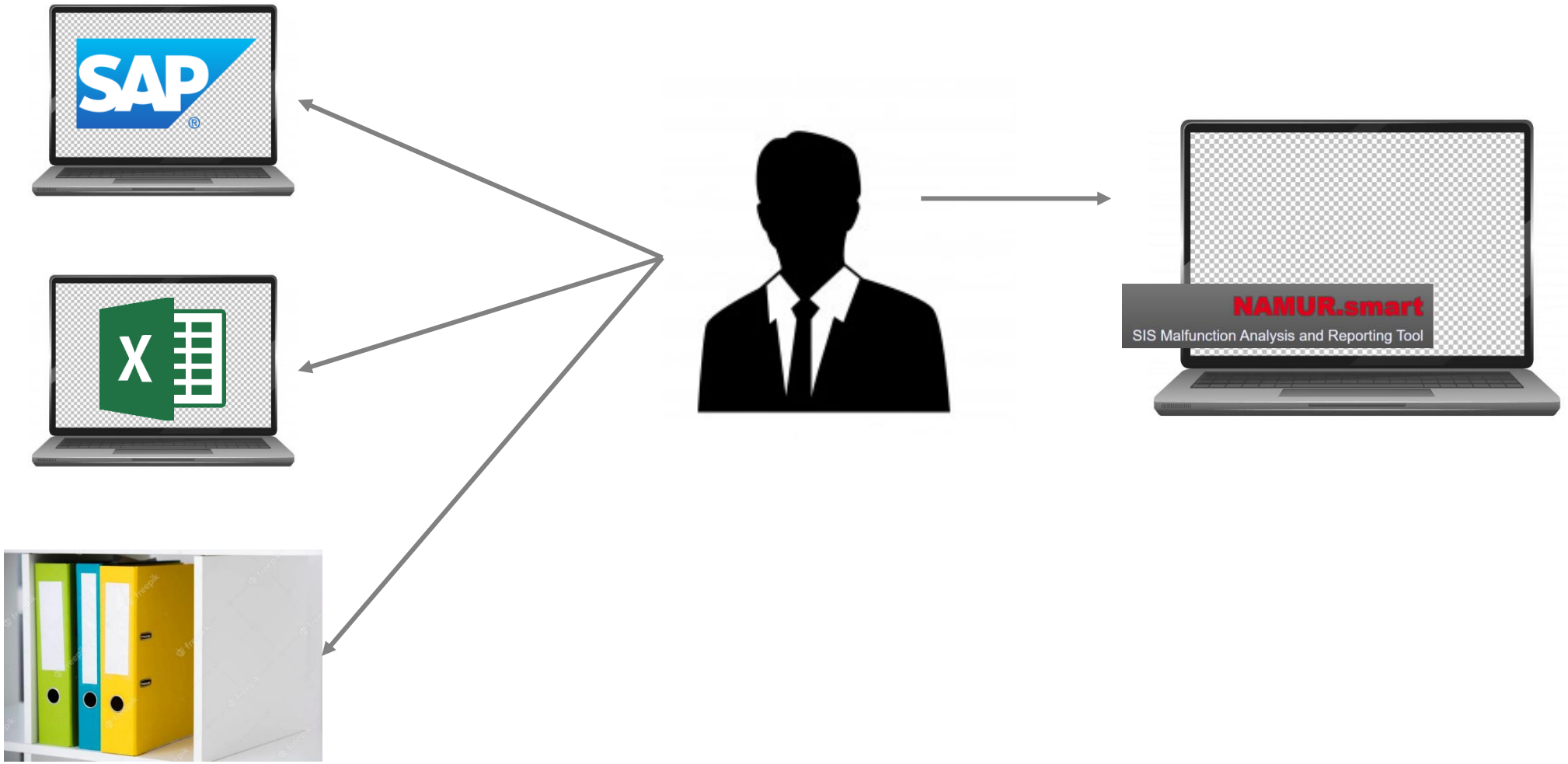
ERDUNG…INFORMATIONSMODELLE ALS DEFINIERTES BEZUGSPOTENTIAL?



Beispiel SIF-Engineering: TS der neuen Pumpe ist geringer

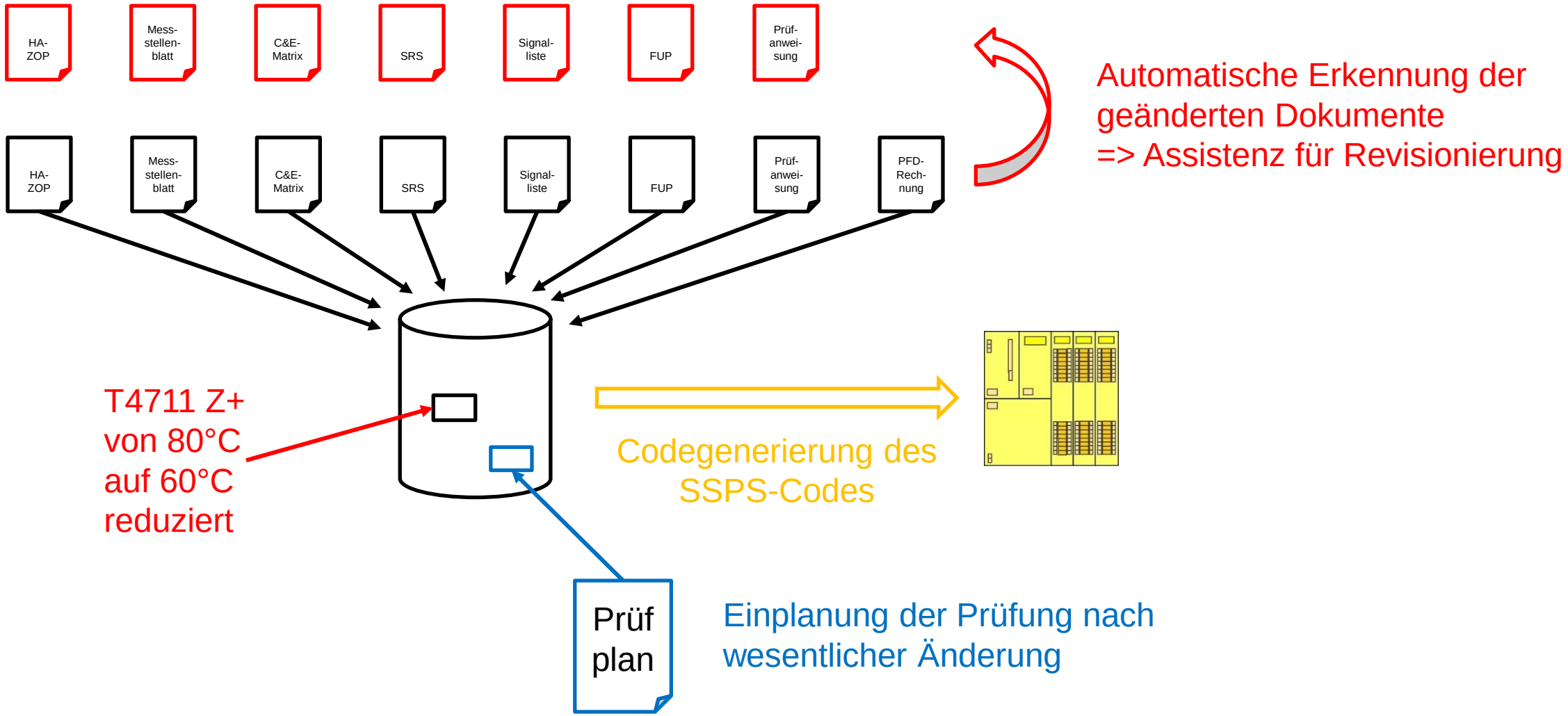


Klassische Ermittlung der Informationen



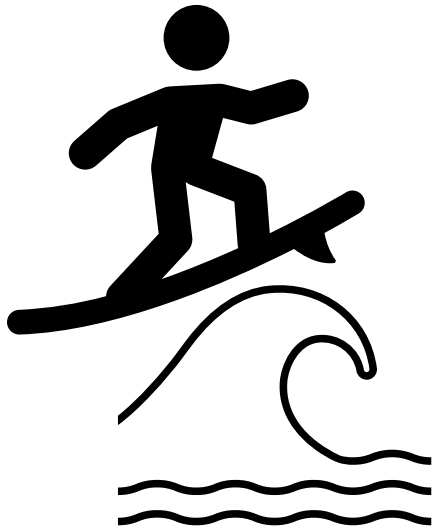
"Bild: Freepik.com". Diese Folie wurde mit Ressourcen von Freepik.com erstellt.

Vision: TS der neuen Pumpe ist geringer

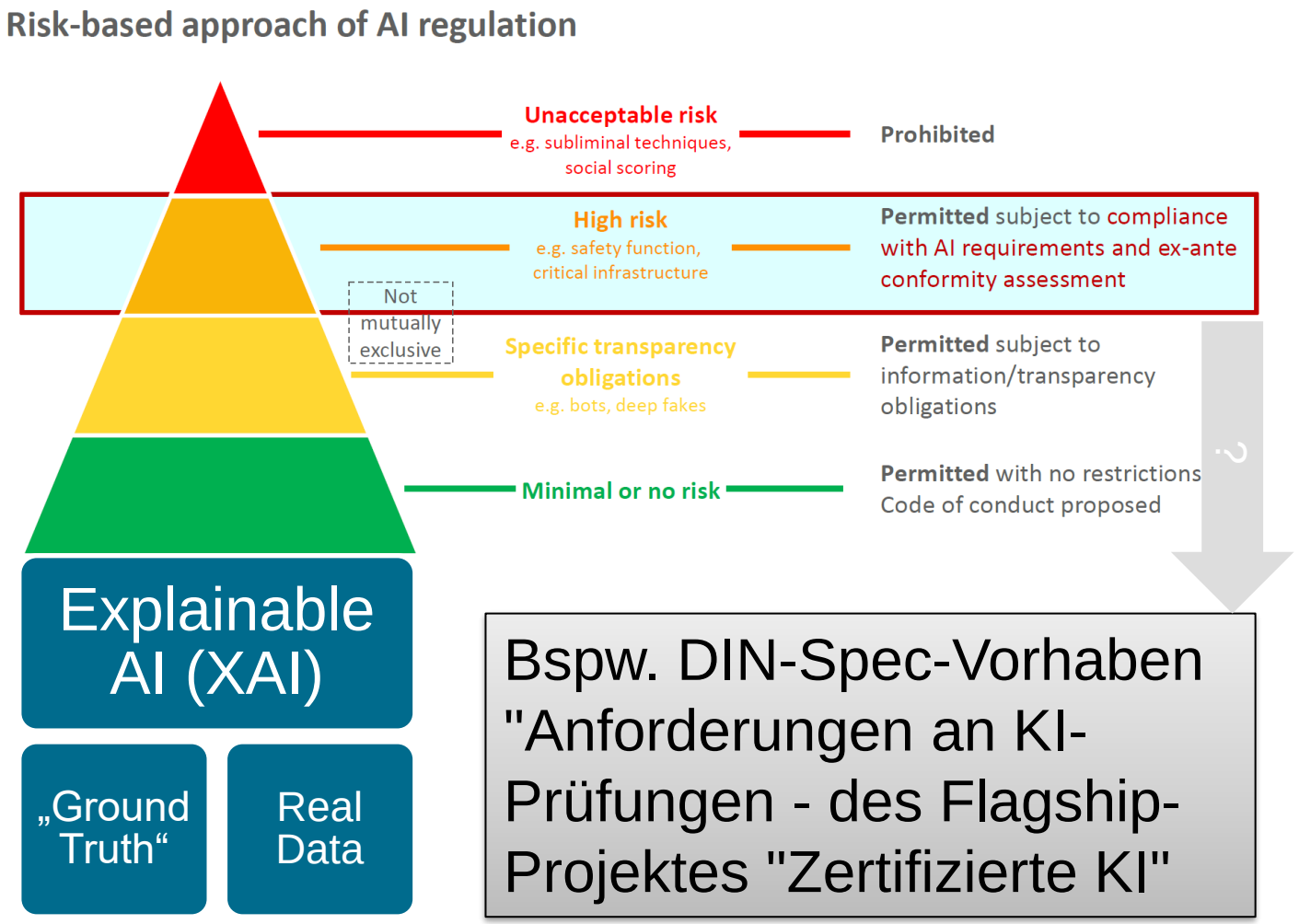


Nutzen von Informationsmodellen für FuSi

- 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 Granulariät -> noch genauere Auswertung möglich
  - Der gute Datenstand kann noch weiter verbessert werden
  - Unterstützungsmöglichkeit für Betriebsbewährungsprozesse

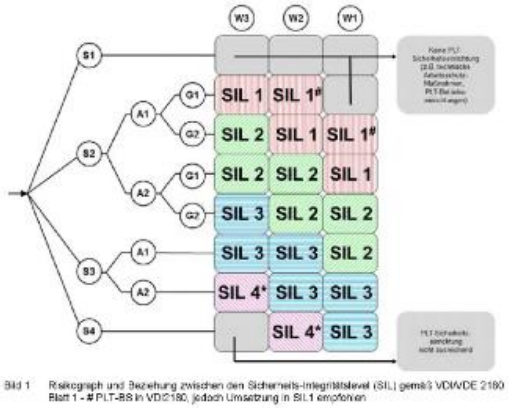


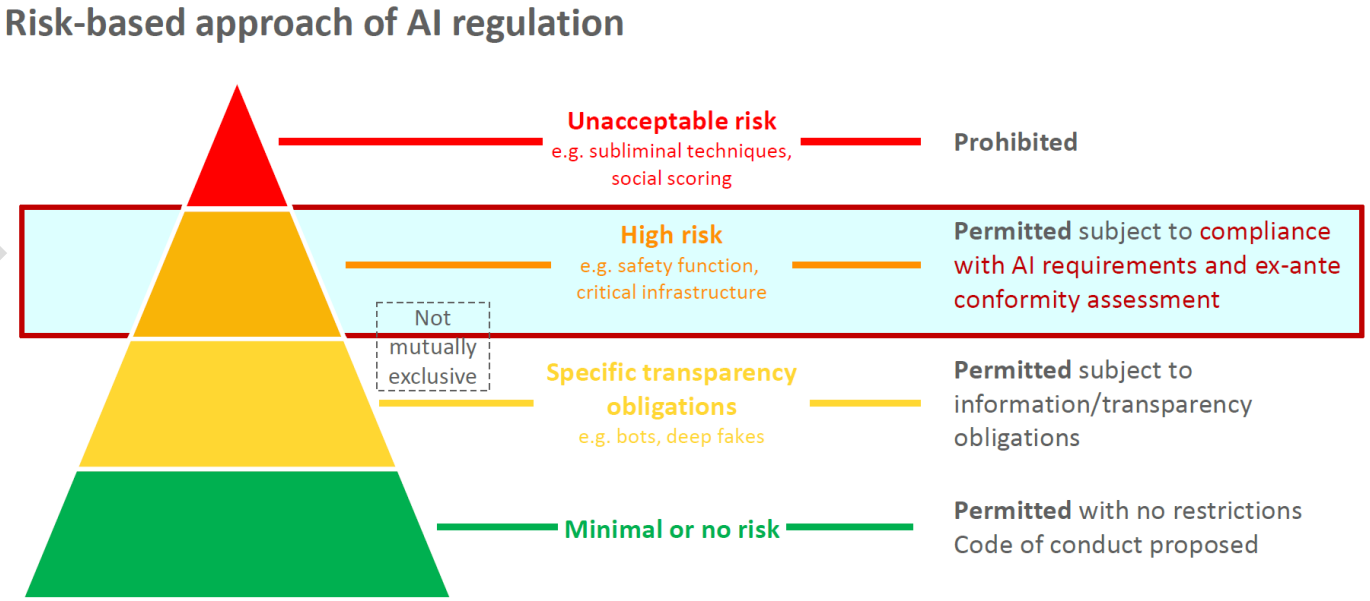
NRM KI (2.0) – PRÜFBARE KI (4 SAFETY)



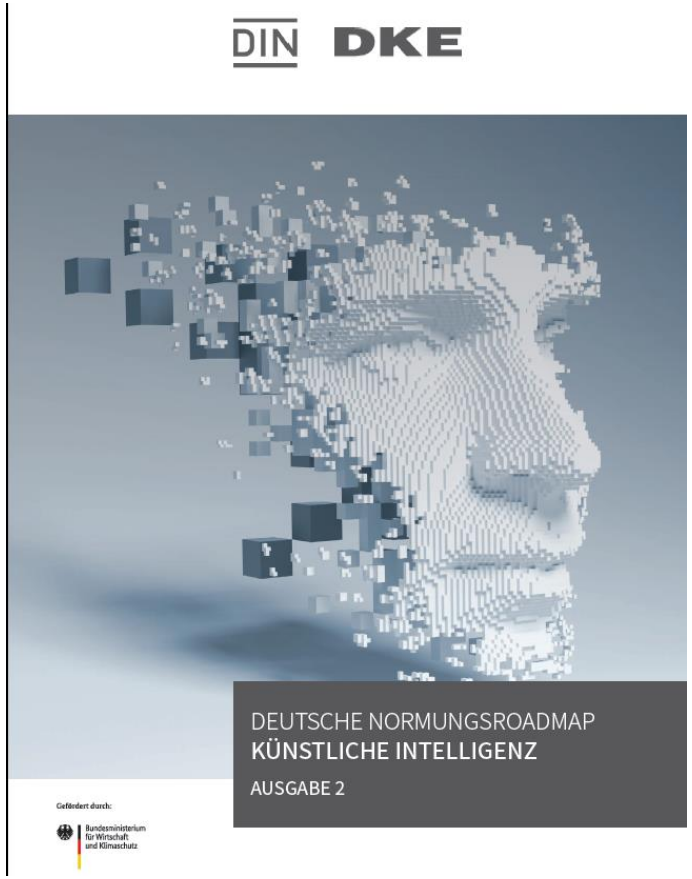
SICHER NAVIGIEREN AUF DER NORMUNGSROADMAP (NRM) KI

- „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. […]





SICHER NAVIGIEREN AUF DER NORMUNGSROADMAP (NRM) KI

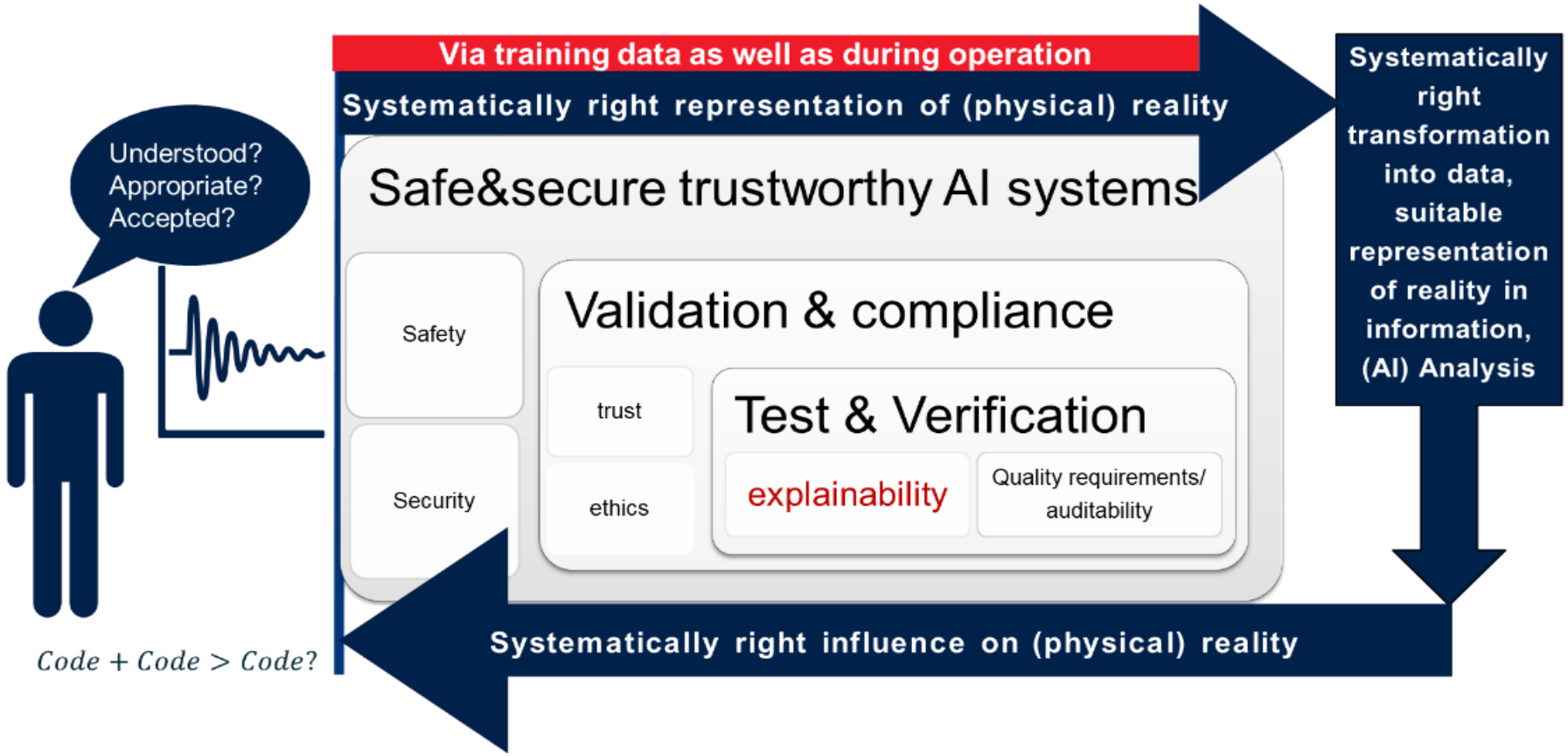


- „Mit der Normungsroadmap wird eine Maßnahme der KI-Strategie der Bundesregierung umgesetzt und damit ein wesentlicher Beitrag zur „**KI – Made in Germany**“ geleistet.
- Die Normung ist Teil der KI-Strategie und ein strategisches Instrument zur Stärkung der Innovations- und Wettbewerbsfähigkeit der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

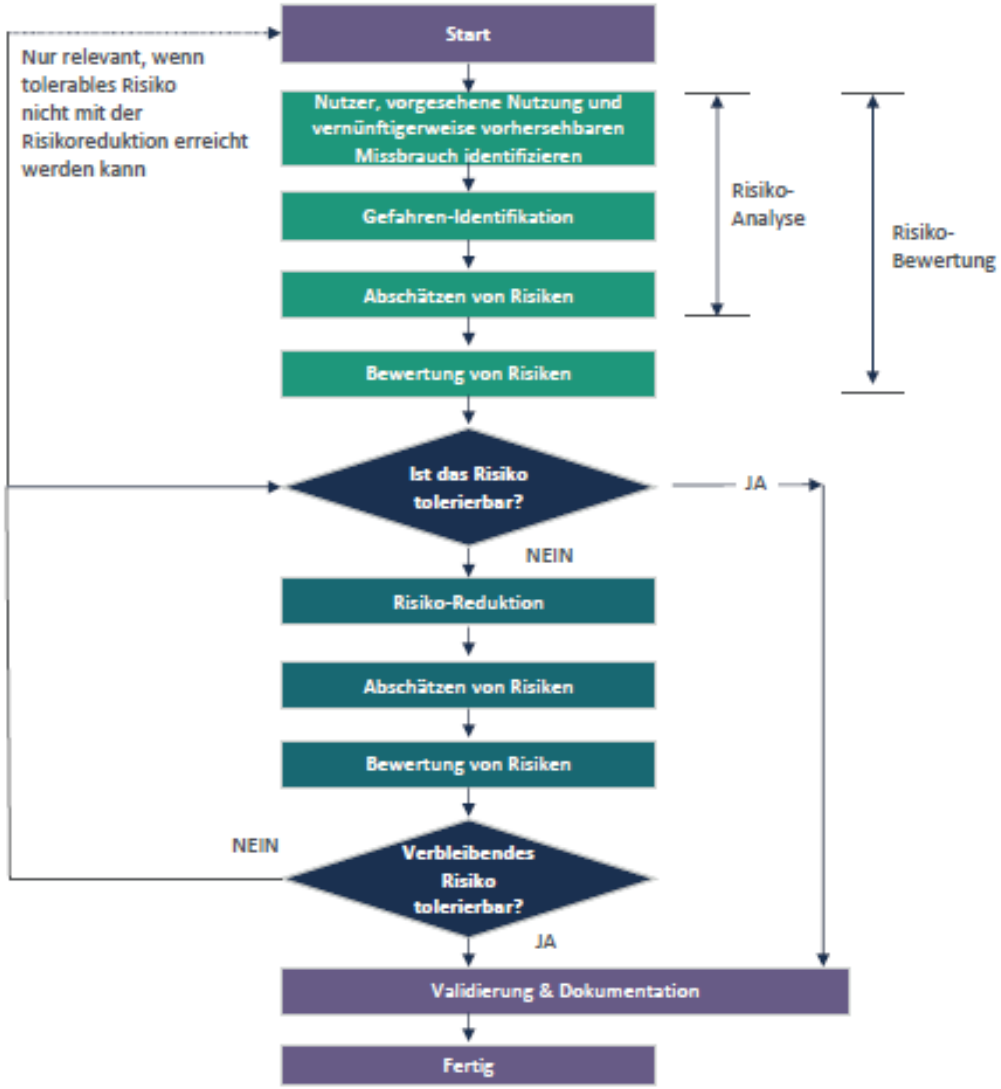
Sie ermöglichen eine zuverlässige und sichere Anwendung von KI-Technologien und tragen zur Erklärbarkeit und Nachvollziehbarkeit bei. Das wiederum macht sie zu Schlüsselfaktoren für die Akzeptanz von KI-Anwendungen.“ (Einleitung, 2. Ausgabe NRM KI)



KONFUZIUS SAGT…

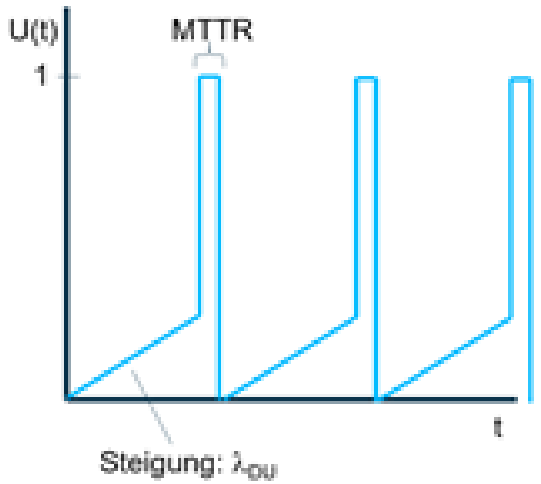
Ohne Ziel ist jeder Weg falsch.

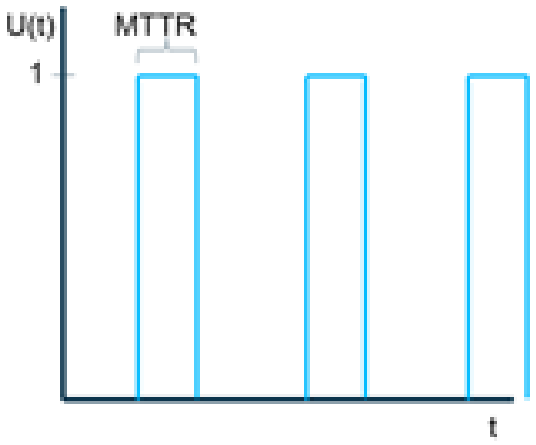
Konfuzius, chinesischer Philosoph



GEDANKENEXPERIMENT:

PERFEKTE DIAGNOSE IM DIGITALISIERTEN SICHERHEITSLEBENSZYKLUS = PERFEKTE SICHERHEIT?





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

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

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

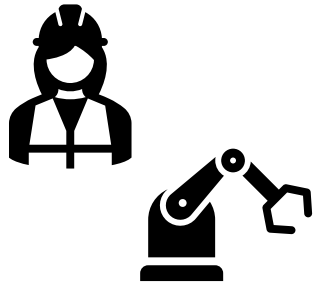
Quelle: NE146

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

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

FELDGLEICHUNG…



actionable information

Daten

Information

Informationsmodell

provided in time/ quality/ structure

Work process

executed in time/ competency/ quality

safety

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

RAMSYS
DAS machen Ingenieure

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 ◆ ATTESTATION ◆ 证明书 ◆ СВИДЕТЕЛЬСТВО ◆ CONSTANCIA ◆ ATTESTAZIONE

TÜV SÜD Industrie Service

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 Inbetriebnahmeunterstüzung

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

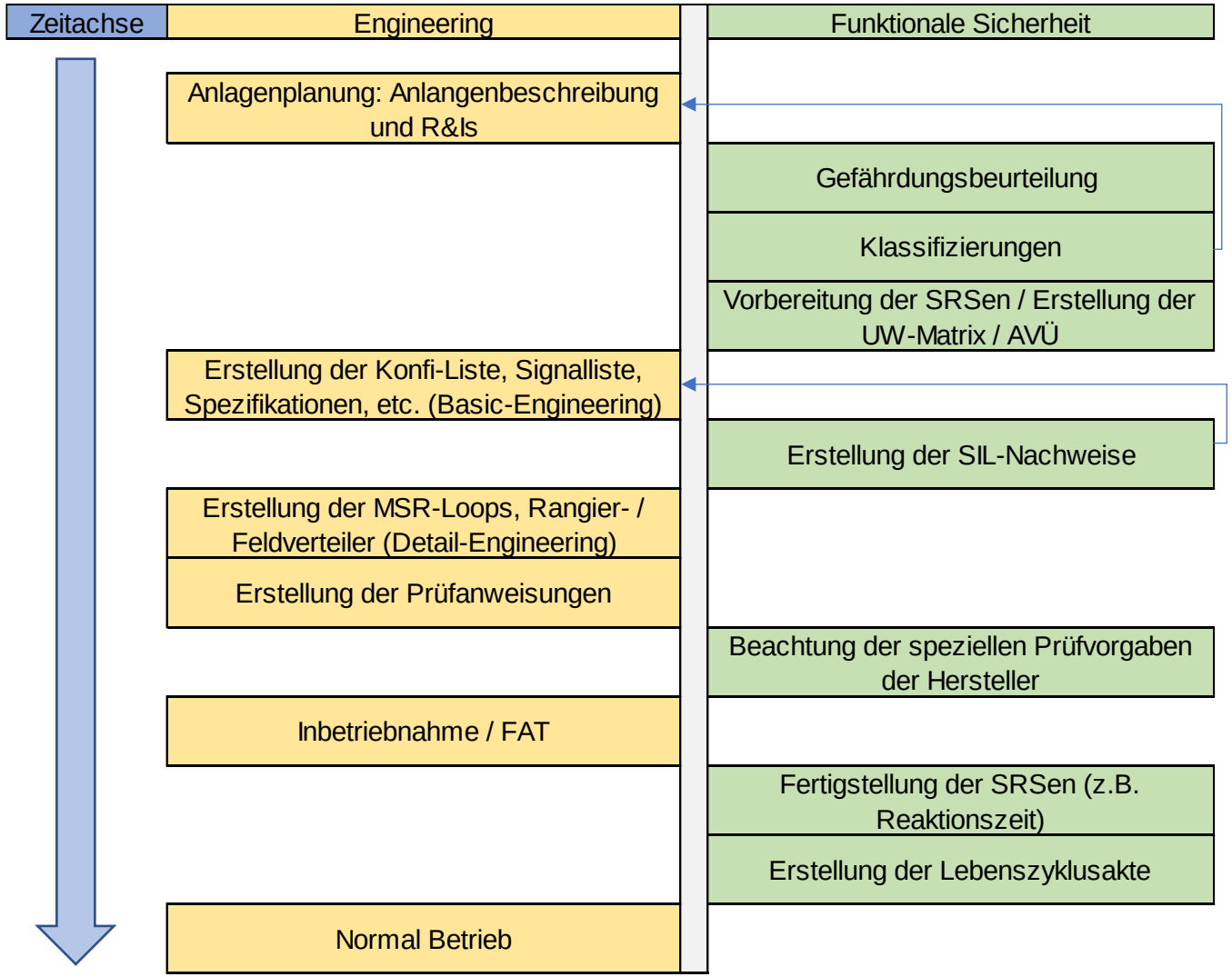
Christian Eberle

TÜV®

(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

RAMSYS
DAS machen Ingenieure

II. In der Praxis

(1) Kommunikation Projektteams / Betrieb

(2) SIL? Und jetzt?

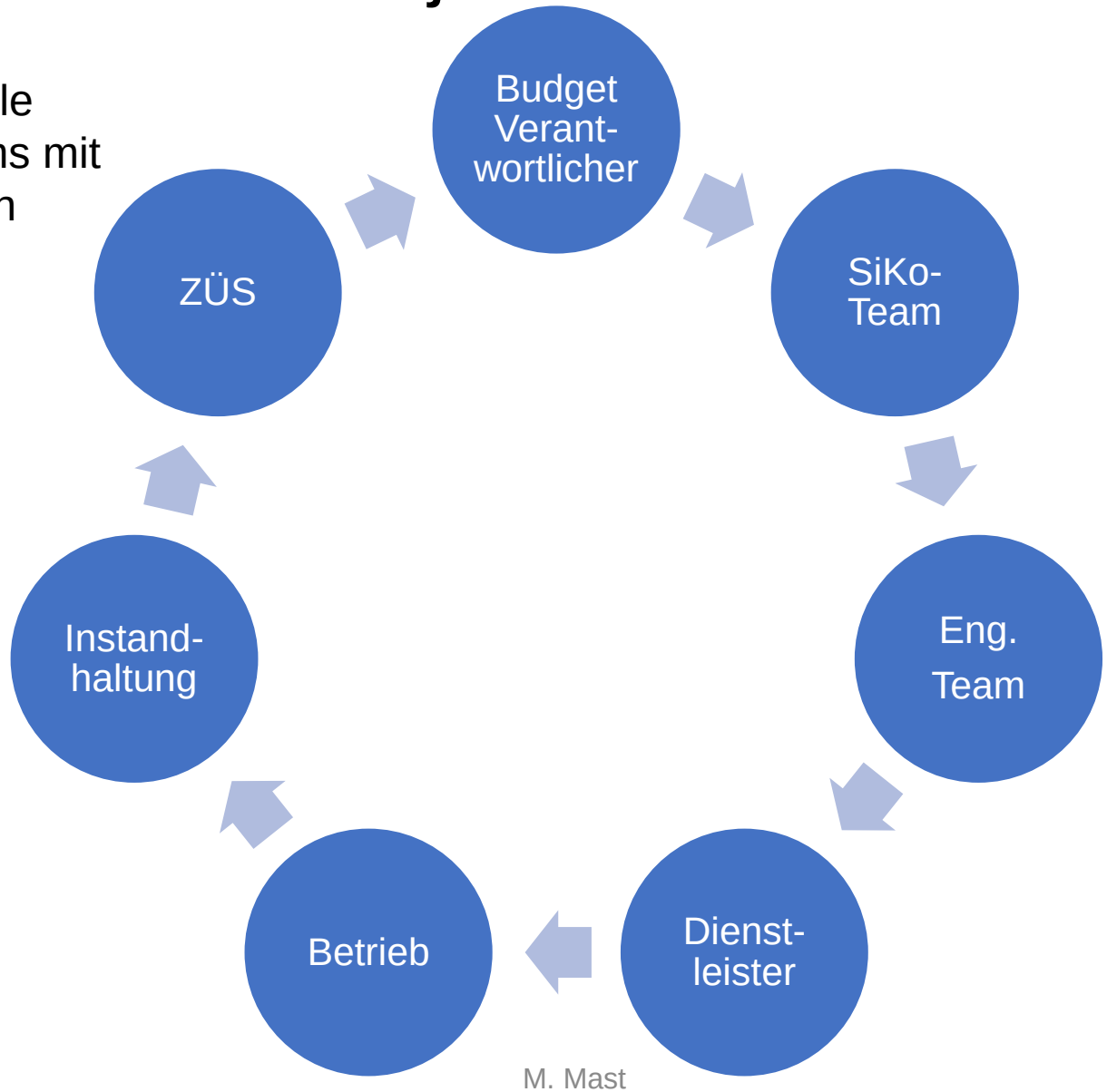
(3) Projektablauf inklusive FuSi

(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?

RAMSYS
DAS machen Ingenieure

- Man spricht gerne bei der Realisierung von Maßnahmen und Anforderungen davon, diese nach aktuellem Stand der Technik umzusetzen

Klingt doch sehr gut und sehr einfach, oder nicht?

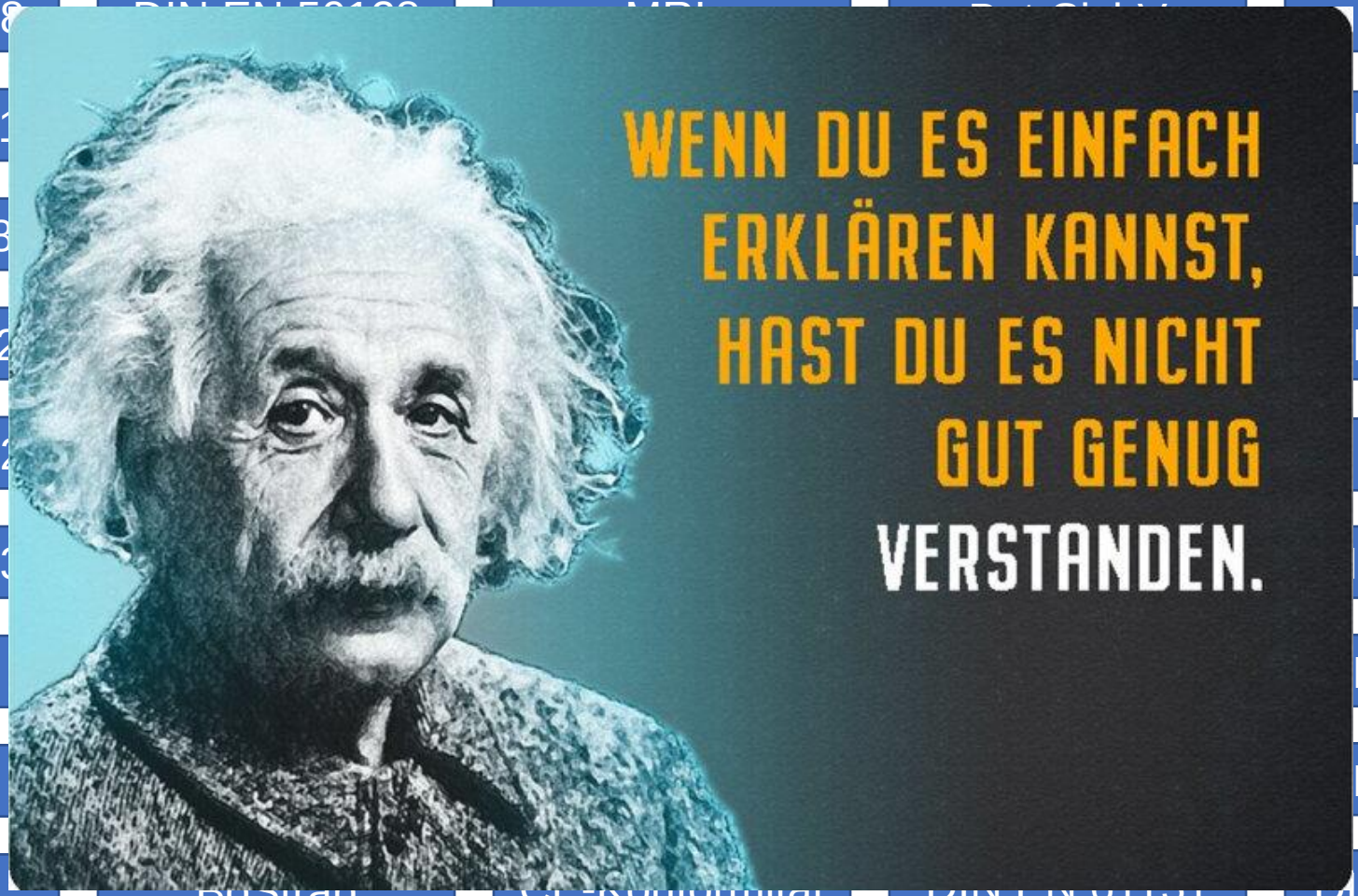
- „Der Stan… ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen od…isen, der die praktische Eignung einer Maßnahme zum Schutz der Gesundheit u…heit der Beschäftigten gesichert erscheinen lässt

- Der Stand der Technik wird in anerkannten Regelw…ieben, z.B.
  - Normen
  - Richtlinien
  - Technische Regeln
  - Verordnungen

(2) SIL? Und jetzt?

RAMSYS
DAS machen Ingenieure

Prozessindustrie	Transportmittel	Maschinen	Verordnungen	Sonstiges
DIN EN 61508				DGRL
DIN EN 6151				IN EN 60601
VDI / VDE 218				IN EN 62304
DIN EN 746-2				IN EN 61513
DIN EN 12952				N ISO 15998
DIN EN 12953				N ISO 25119
NE 130				IN EN 16590
NE 93				IN EN 12999
NA 106	BoStrab	CE-Konformität	DIN EN 61131	DIN IEC 60880



(3) Projektablauf inklusive FuSI: Praxis / Theorie

RAMSYS
DAS machen Ingenieure

Praxis

1. SIL-Ermittlung
2. Engineering Prozess
3. Prüfkonzept Ermittlung
4.1 Detailplanung
4.2 Programmierung
5. Montage
6. FAT + Abnahme
7. SIL-Berechnung und Plausibilitätsprüfung

Theorie

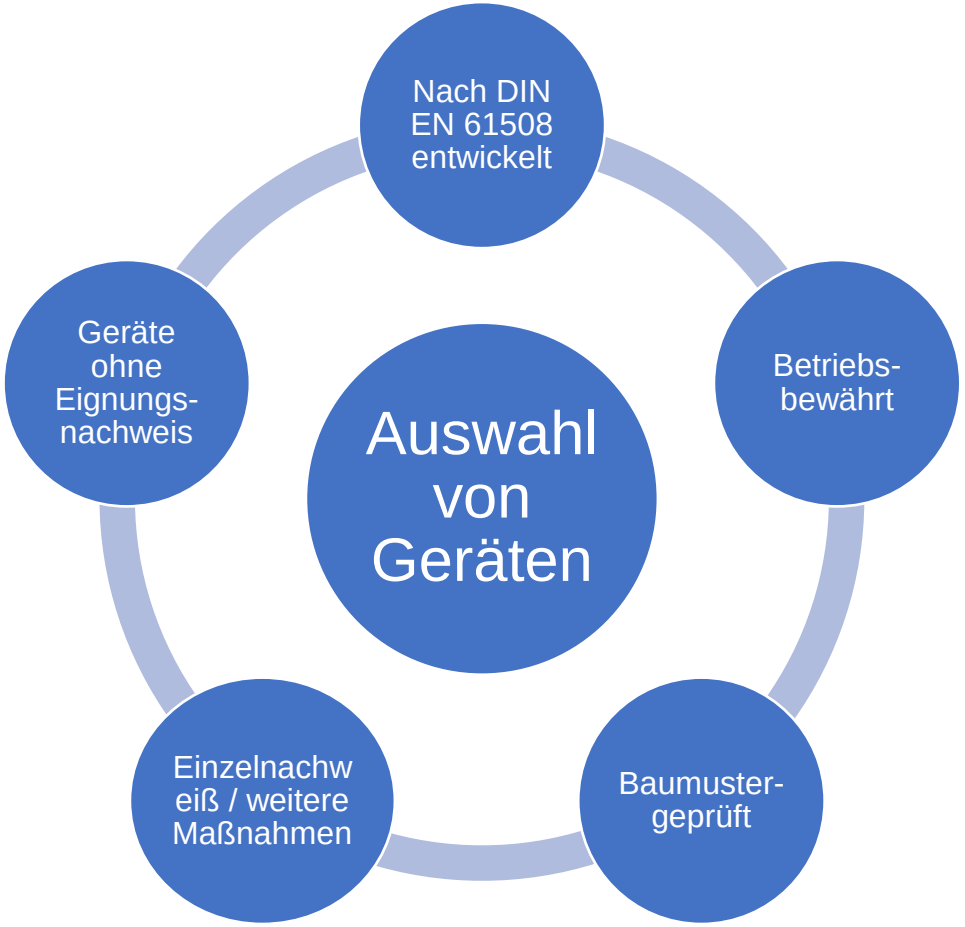
1. SIL-Ermittlung
2. Engineering Prozess
3. Prüfkonzept Ermittlung
4. SIL-Berechnung und Plausibilitätsprüfung
5.1 Detailplanung + Montage
5.2 Programmierung
6. Validierung
7. FAT + Abnahme

(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) 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?

RAMSYS
DAS machen Ingenieure

III. Dokumentation

(1) FuSi - Dokumentation

(2) Ablagemanagement

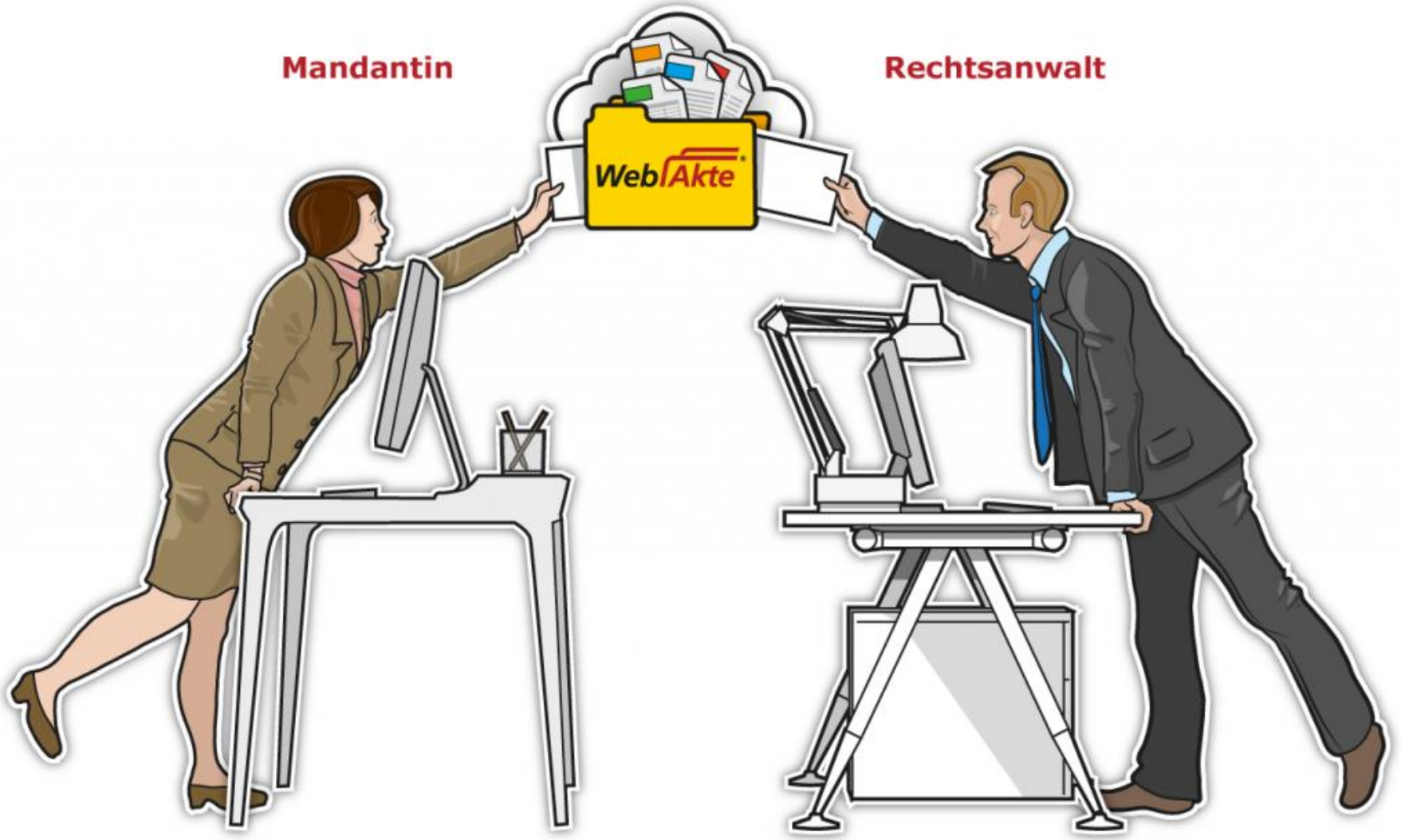
(1) FuSi-Dokumentation

RAMSYS
DAS machen Ingenieure

- 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

PEPPERL+FUCHS

Your automation, our passion.

SIL-Sprechstunde 2023

Fragen und Antworten (Tag 2)

14. SIL-Sprechstunde 2023

1. Wenn ein Gerät nach IEC 61508 vom Hersteller bewertet wurde und für den Einsatz im Low- und High demand mode bei einem HFT = 0 bis SIL 2 geeignet ist, darf es dann auch 1-kanalig nach der DIN EN ISO 13849 bis PL = d eingesetzt werden? Im High Demand Mode entspricht SIL 2 einem PL = d. Es handelt sich um ein Typ A Gerät mit einem SFF von 62%. Laut DIN EN 61508-2 Tabelle 2 "… Zulässige Sicherheitsintegritätslevel Typ A Elemente…" ist ein HFT 0 für SIL 2 ausreichend und somit für PL = d? Ist das ein Wiederspruch zur DIN EN ISO 13849 in der zur Erreichung eins PL = d ein zweikanaliges System (Kategorie 3) vorgesehen/gefordert wird (mit Ausnahme eines einkanaligen Systems mit Testung (Kategorie 2))?

Experte: Rein formal gesehen geht das nicht, da der PL eine Architektur wie z.B. Kategorie 2 benötigt, und für Kategorie 2 ist ein Testkanal / Diagnose vorgesehen. Daher ist ein einkanaliges System nicht ausreichend.

Zweiter Experte: Eine Testung muss ja nicht im Gerät oder Sensor erfolgen. Wenn das Gerät / Sensor eine Bus-Schnittstelle wie z.B. HART oder CAN-open hat, kann man die Diagnose auch darüber verwirklichen und Kategorie 2 und PL d erreichen. Dazu muss aber zumindest der Logikteil der Sicherheitsfunktion geprüft werden.

Weiterer Experte: Die Testung ist in so einem Fall aber nicht vom Hersteller vorgegeben. Bei der Testung nach der 13849 ist zu beachten, dass diese 100x öfter erfolgen soll, als die Anforderung der Sicherheitsfunktion. Daher ist es schwierig, mit einer manuellen äußeren Testung diese Häufigkeit zu erreichen, wenn diese nicht im Gerät implementiert ist.

Zweiter Experte ergänzt: Richtig, aber bei einem Bus-Protokoll kann man die Testung bei z.B. bei jedem Telegramm verwirklichen und erhält somit eine sehr große Häufigkeit. Natürlich muss man das im Auge behalten, das Prüfintervall sollte natürlich passen, aber darüber sollte es doch sehr häufig umsetzbar sein. Es empfiehlt sich aber, ein zertifiziertes SIL2 Gerät zu benutzen.

Teilnehmer: Für jemanden der die Nachweisrechnung erstellt ist es aber dennoch schwierig. Es mag zwar von den Werten (rechnerisch) richtig sein, dennoch gibt es andere Punkte zu beachten, die dann häufig vergessen werden.

Experte dazu: Es kann zu Problemen mit dem formalen Nachweis kommen. Im Beispiel geht es um ein Typ A Gerät mit einer SFF von 62%, einkanalig verwendet, daher werden die Bedingungen für PL d nicht erfüllt.
Generell gesagt muss man bei Komponenten die nach 61508 entwickelt wurden, die in Sicherheitseinrichtungen nach 13849 eingesetzt werden, sich den Einzelfall anschauen. Es kann funktionieren, aber es gibt mehr als die reine Berechnung zu beachten. Das gilt auch wenn etwas nach 13849 entwickelt wurde und nach 61508 eingesetzt werden soll.

Weiterer Experte: Im Maschinenbau ist die Situation bei Positionsschaltern so, dass diese zu 80% in die sichere Richtung ausfallen, und diese 80% die Rechnung sehr positiv beeinflussen

würden bai Ausführung in SIL2. Daher gibt es ein Papier (Veröffentlichung) das einen einzelnen Kanal als Grundlage nicht als geeignet darstellt. Die Industrie möchte 2 kanalige Systeme für PL d sehen.

Weitere Anmerkung: Wieso gibt es dann die 13849? Die 61508 ist die Grundnorm. Aber wenn ein PL d gefordert ist dann ist das nicht gleich SIL2.
Mit SISTEMA hat man die Möglichkeit, einzelne Komponenten mit SIL-Qualifizierung in einem Sicherheitskreis integrieren zu können um einen Performance Level zu erreichen.

Experte: Man kann natürlich SIL-Komponenten benutzen. Auch in SISTEMA. Aber die Berechnung alleine genügt nicht. Wenn man zwei Kanäle benötigt dann müssen diese SIL-Komponenten redundant sein.

Fazit: Die Architekturanforderungen müssen erfüllt werden. Nach dem Säulendiagramm ist einkanalig PL d zu erreichen, für Kat. 2 muss aber ein Testkanal mit separater Abfragemöglichkeit vorhanden sein. Beispiel: ein Trennschaltverstärker der ein Signal entkoppelt aber keine Testmöglichkeit hat muss zweikanalig aufgebaut werden. Evtl. ist es alternativ möglich mit Fehlerausschluss (ISO 13849-2) arbeiten.

2. Niedrige PL Funktionen werden auch auf Standard-Baugruppen / Steuerung implementiert (ähnlich auch den BPCS Risikominderungen mit Faktor 10). Ferner gibt es auch Sensorik, mit eingebauter Firmware, die nur im Verbund (Redundanz) sicherheitsgerichtet verwendet wird. Wie kann mit solchen Funktionen und Software umgegangen werden, wenn künftig jegliche Safety-Auswirkungen durch Sabotage (z.B. Schutz gegen Korrumpierung - Maschinenverordnung) einer besonderen Betrachtung unterliegen?

Ergänzung des Fragestellers: Die Frage bezieht sich auf die Maschinenverordnung. Durch diese ergeben sich neue Anforderungen für Steuerungen insgesamt (Maschinen- und Prozessindustrie).

Wenn z.B. eine sicherheitsgerichtete Steuerung vorhanden ist, die Sensorik oder Aktorik aber nicht qualifiziert ist (z.B. bei redundanten Systemen), dann sind die Produkte zwar nicht zertifiziert, mit diesen zusätzlichen Sensoren ist die Implementierung einer Sicherheitsfunktion aber möglich. Wenn SW enthalten ist darf man nicht einfach nur auf die Sicherheitsfunktion schauen. Hier strahlt die Anforderung des Sabotageschutzes auch auf Nicht-Safety-Produkte aus. Wie kann man hier den Security-Fall abdecken? Wie kann man hier den Bereich der Zulieferer dieser Produkte, als auch andere Faktoren im Steuerungssystem (Risikominderung Faktor 10) oder auch normale Steuerungsfunktionen abdecken? Wie geht man damit um?

Experte: Die Feststellung ist korrekt. Auch, dass die Anforderungen auch in Anwendungsfällen gelten für die sie per se nicht gedacht waren. Leider gibt es noch keine Norm für Cybersecurity die absehbar unter der Maschinenverordnung gelistet wird. Die weit verbreitete Grundlage ist die 62443-Reihe Security im Bereich der operativen Steuerungssysteme. Es soll eine Norm nach der Vorlage der 62443 für den Maschinenbereich erstellt und harmonisiert werden. Deshalb erscheint es derzeit eine gute Idee, Anforderungen der 62443 umzusetzen.

Fragesteller: Das Problem momentan ist aber, dass der, der den Sensor verkauft und der Einkäufer für die Maschine nicht wissen, dass sie unter diese Maschinenverordnung fallen. Aber in der Applikation muss ich als Betreiber dann die Zulieferer unterrichten, dass sie diese Anforderungen umsetzen sollen, weil ich sonst solche Sensoren nicht sicherheitsgerichtet einsetzten kann. Wie unterrichtet man die Beteiligten, dass sie das zu beachten haben.

Experte: Für Security ist nicht nur die Komponentenebene relevant, das Gesamtsystem unterliegt den Anforderungen. Im Beispiel mit 2 Standard-Sensoren, würde man die Anforderungen über Zugriffsschutz in / über der Steuerung realisieren. Wenn diese Steuerung die Anforderungen an den Korrumpionsschutz erfüllt, und den PL erfüllt, dann sollte das System geeignet sein.

Fragesteller: Ok, dann ein Beispiel mit 2 Sensoren. Diese Sensoren haben SW enthalten, über die man diese Konfigurieren kann (z.B. eine Skalierung der Messwerte vornehmen kann). Der Saboteur hackt sich in beide Sensoren, und ändert die Einstellung von beiden Sensoren gleich, und das kann dann zu einer falschen Aussage führen. Das ist keine Frage der Funktionalen Sicherheit, sondern die, dass die allgemeine Einstellung (Meinung) ist, dass wenn man ein Sicherheitssystem (Sicherheitssteuerung) gegen Sabotage schützt, dass man dann kein Problem hätte. Dem ist aber nicht so, da man ja über andere Produkte gehen kann, die auch sabotiert werden können.

Weiterer Experte: Aus dem Bereich der Security unterscheidet die 62443 im Lebenszyklus 3 Akteure. Zum einen den Hersteller der Komponente, den Integrator der im Auftrag des Betreibers handelt und die Maschine zusammenbaut und in Verkehr bringt, und den Betreiber. In der Security geht es nicht wie in der FS um eine Funktion und Anforderungen dafür sondern um das Erreichen eines Schutzzieles für die Funktion was der Betreiber mit dem Security Level vorgibt. Gegen Akteure mit sehr guten Fähigkeiten benötigt er ein hohes Security Level. Das bedeutet, dass der Hersteller eine Komponente zur Verfügung stellen muss, die dieses Security Level erfüllen kann. Man nennt das Security Level Target (benötigter Security Level). Der Hersteller müsste jetzt eine Komponente auf dem Markt bereitstellen, die dieses Security Level erfüllt. Anforderungen stehen in der 62443-3-3, von Passwortschutz über verschiedene andere nötige Maßnahmen gibt es 58 Punkte, die verschiedene Möglichkeiten beschreiben. Eine pauschale Lösungsvorgabe gibt es aber nicht.

Fragesteller: Theorie ist klar. Aber: Ist den Beteiligten klar, dass die beschriebene Situation eintreten kann? Ist den Beteiligten klar, dass es nicht ausreicht die „gelbe Box“ gesondert zu behandeln? Ist klar, dass unter Umständen weitere Anforderungen gelten als bisher? Unter Umständen ist ein Zulieferer überrascht, dass er Dinge machen muss, obwohl er von der Maschinenverordnung eigentlich nicht betroffen ist. Es ist also eher die Frage, ob dies kommuniziert wird. Findet hier ein Austausch unter den Beteiligten statt?

Anderer Teilnehmer: Den Akteuren ist es vermutlich nicht bewusst aber dieses Bewusstsein wird recht schnell wachsen. Wichtig: Security kennt auch andere Schutzkonzepte als die sichere Komponente, z.B. die Einteilung in unterschiedliche Zonen mit unterschiedlichen Barrieren.

Weiterer Teilnehmer: An SSPS werden viele intelligente Feldgeräte angebunden die digital kommunizieren können – der Klassiker ist HART. Darüber werden Daten übertragen aber es

ist auch möglich zu parametrieren. Erfahrung zeigt, dass auch großen globalen Konzernen der Rahmen der Security nicht bewusst ist. Diskussionen zur Lösung laufen, speziell wenn die Gerätehersteller Geräte liefern die den Security Level nicht ermöglichen. In dem Fall muss die Umgebung geeignet gestaltet werden um den Security Level zu erreichen. Das muss nicht unbedingt eine Geräteeigenschaft sein. Wenn also kein Passwortschutz oder keinen Schutz gegen unberechtigten Zugriff im Gerät vorhanden ist, muss eine Umgebung geschaffen werden, die Zugriffsbegrenzung sicherstellt.

Nächster Teilnehmer: Bei Niederspannungs-Leistungsschaltern wurde früher die Einstellung per Hand vorgenommen, heute gibt es Schalter, die nach bestimmten Kennlinien abschalten müssen. Diese sind natürlich SW-gesteuert. Für diese Geräte wird teilweise geworben, dass diese bequem von einer App mit dem Smartphone aus programmiert (eingestellt) werden können. Da scheinen die Hersteller noch nicht über Security nachgedacht zu haben. Die Entwicklung geht aber weiter. Die Anwender haben mittlerweile einen Report für die Security geschrieben und dargestellt, wie in solchen Fällen Security beachtet werden soll.

Prüfstelle: Es gibt seit März für die Prozessindustrie die TRBS 1115-1 – Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen – aber auch für die Maschine entwickeln Hersteller nach 62443 auch wenn es dem Vertrieb vor Ort eventuell noch nicht bewusst ist. Die Überprüfung ist aber schwierig mangels Prüfvorschrift. Außerdem sind die Anlagen teilweise seit 20 -30 Jahren in Betrieb und die Anforderungen sin nicht erfüllbar.

Weiterer Teilnehmer: Es geht um eine Implementierung in ein System das nicht dafür ausgelegt wurde. Wenn ein Security-Level vorgeschrieben wird ändert sich der Umgang mit dem ganzen System im täglichen Alltag, der ganze Arbeitsablauf ist beeinflusst. Es wird schwieriger, im Sinne der Safety schnell zu agieren.

3. Frage in die Runde: Gibt es derzeit schon sicherheitsgerichtet Funktionen im Feld (also für PL / SIL eingestufte), welche mit sog. neuen Technologien (e.g. ML – Maschine learning, etc.) arbeiten?

   Offene Frage, ob es schon Maschine-learning Funktionen in SIF gibt? Man möchte das wissen, da man natürlich nach Beispielen sucht.

   Aus einer anderen Konferenz, einen Hersteller von Sicherheitsmaschinen zitiert: Es wird gerade geforscht und momentan ist noch keine Sicherheitsfunktion im Einsatz. Nur zur Forschung, in gekapselten, abgeschlossenen Systemen. Die Prüfung dieser Systeme ist noch nicht definiert. Es gibt eine Anlage die zur Abwehr von Materialschäden KI schon einsetzt mit Risikoreduktion einer Sicherheitsfunktion.

   Wenn man den AI-Act der EU eng liest und eng auslegt, dann sind selbst Steuerungen von Garagentoren KI. Der ZVEI hat das auch kommentiert - auch Heizungssteuerungen wären KI.

4. SIL-Nachweis: Eine SIF löst nur in einem bestimmten Betriebszustand aus, der durch eine zusätzliche Messung erfasst wird, die in der Logik die "Hauptmessung" überbrückt. M.E. muss bei der Rechnung auch diese zusätzliche Messung berücksichtigt werden. Ist das richtig? Ein Betreiber wollte das "wegdiskutieren".

Es gibt eine normale Messung (Hauptmessung) einer Größe und es gibt einen zweiten Sensor der die gleiche Größe misst, der die Hauptmessung überbrückt (mutet).

Im Prozess ist das wie an der Maschine als Muting zu verstehen (z.B. Anfahrprozesse). Die Messung wird für eine bestimmte Zeit (Phase) außer Kraft gesetzt. Das ist ein wichtiger Bestandteil der SIF der berücksichtigt werden und in die Auslegung und Berechnung (rechnerische Nachweise) mit aufgenommen werden muss da die Messung ignoriert wird wenn das Muting durch einen Fehler dauerhaft signalisiert wird.

Teilnehmer: Mögliche Ausnahme wäre z.B. eine Anfahrüberbrückung einer Pumpe die über eine Zeit gesichert ist, d.h. über einen zusätzlichen Kontakt die Rückmeldung erfolgt, dass die Pumpe angelaufen ist und über die eingestellte Zeit nichts passieren kann. Dort gibt es keinen zusätzlichen Sensor, es werden die Kontakte vom Schütz genutzt. Das Ein- und Ausschalten Bestandteil des Programms und damit berücksichtigt.

Überwachungsstelle: Das Signal das das Muting an der Pumpe auslöst muss sicher erkannt werden und ist Teil der Prüfung. Es gibt Fälle, in denen das Signal für die Triggerung des Muting dem PLS entnommen wird. Die Zeitverzögerung bringt hier nichts, es muss z.B. ein sicherer Ausgang des Frequenzumrichters genutzt werden, oder ein anderes verwertbares sicheres Signal hat.

5. Können SIL-zertifizierte Bauteile auch in Anlagen verbaut werden die nach DIN EN ISO 13849 installiert werden (Performance Level)?
   a. Wenn ja, welche Werte sind dann heranzuziehen?

   Die Frage ist schon ähnlich beantwortet, wobei die Frage eher von 13849 nach Prozessumfeld verlief. Prinzipiell kann man auch das mit „ja“ beantworten, aber die SIF ist entsprechend zu bewerten (Demand Mode berücksichtigen).

6. Wie werden Low und High Demand definiert.
   a. Beispiel Druckschalter soll die Anlage während des Betriebs abschalten, wenn der Druck unter einen Wert fällt. → Sicherheitsfunktion.
   b. Der Schaltpunkt wird aber öfters erreicht, bei Abschalten der Maschinen.
   c. Unter welche Anforderung fällt diese Anwendung?

   Teilnehmer: Die Frage ist gerechtfertigt da das Signal bei Abschalten der Maschine keinen Demand darstellt. Die Normen sind hier etwas ambivalent, es könnte als Low Demand gelten aber das öftere Erreichen des Schaltpunkts spricht für High Demand – falls das Erreichen des Schaltpunktes tatsächlich einen Demand darstellt. Laut IEC 62061 sollte ab und zu geschaltet werden falls zu wenige Anforderungen kommen was eigentlich keinen Demand darstellt.

   Anderer Teilnehmer: Beim Lichtgitter könnte man jedes Betätigen / Hineingreifen als Demand zählen - dann wird die Anlage gestoppt (ausgeschalten). Die SIF wird aber nicht bis zum Ende durchlaufen da die Anlage energiefrei ist – daher ist das kein Betätigen der SIF.

   Anderer Teilnehmer: In der 62061 ist kein Low Demand definiert und man kennt Probleme nicht wie die Frage, ob der Schalter überhaupt noch funktioniert. Deshalb behilft man sich mit

der Testschaltung und behandelt es dann wie High Demand. Aber eigentlich ist es Low Demand bei dem trotzdem der Verschleiß zu berücksichtigen ist.

Überwachungsstelle: Die Antwort kommt wohl aus der Prozessindustrie. Eine 1oo2 Anwendung darf so nicht bewertet werden – das wird in der Gefährdungsbeurteilung bewertet. Es ist nicht einfach geeignet wegen Mitbenutzung.

7. Kann man "high-demand"-Werte (PFH) in "low-demand"-Werte (PFD) oder in MTTF- Werte umwandeln?
   a. Gibt es hier geeignete Programme?

   Teilnehmer: Am Fuße der Badewannenkufe macht man die Annahme dass sich die Wahrscheinlichkeiten auf-akkumulieren, sich die PFH, dann die PFD ergibt, und dann hat man die Formel
   PFD = PFH * <Abstand zwischen 2 Prüfungen> / 2.

   Weiterer Teilnehmer: Viele Geräte sollen regelmäßig betätigt werden (Stichwort Rost). Deshalb wären zusätzliche Messzyklen einzubauen. Dies kann aber nicht pauschalisiert werden.

   Weiterer Teilnehmer: Kann man den Tankinhalt eines Autos in km umrechnen? Verschiede Einheiten, daher geht die Umrechnung nicht. Wenn ich zusätzliche Informationen habe, dann kann ich den Tankinhalt umrechnen. Vielen ist auch nicht klar, dass PFD eine Wahrscheinlichkeit ist, und PFH eine Häufigkeit (eine Rate). Also unterschiedliche Dinge. Daher ist auch bei PFH und PFD die Umrechnung nur mit zusätzlichen Angaben möglich. Man muss ebenfalls unterscheiden zwischen PFD und PFH bzw. LD bzw. HD. Das kann man nicht synonym verwenden. Das eine ist die Berechnung, das andere die Anwendung.

   Weiterer Teilnehmer: Geht der Rostprozess innerhalb eines Jahres voran? Das ist ein systemantischer Fehler.

   Statt Berechnung wird die Systematik relevant. Ist die Komponente überhaupt geeignet? Auch PL in SIL umrechnen geht grundsätzlich, Frage ist dann ob die Armatur überhaupt geeignet ist. Verschleiß ist zu beachten. Diese Erkenntnis ist wichtiger als die Rechenwerte.

8. Kann man Hydraulische Ventile mit SIL3-Zulassung, die sicherheitsrelevant abschalten müssen und über pneumatische Ventile angesteuert werden, in eine PL-Berechnung einbauen?
   a. Und wenn ja, was ist dabei zu beachten

   Hinterfragen wie das Ventil aufgebaut ist (siehe Frage 10), damit es SIL 3 erreicht. SIL3 bedeutet nach 61511 dass HFT=1. Es muss also ein redundantes Ventil sein was es nicht gibt. Also gilt es zu hinterfragen, welche Qualität hinter der Einstufung steht. Vermutlich ist hier die SC3 gemeint, denn SIL3 erscheint nicht glaubwürdig.

   Der Fragesteller: Ich habe eine Maschine im PL zu berechnen, mit 2 hydraulischen Ventilen, redundant in die Leitung eingebaut (in Reihe um die Leitung zu kappen). Die Ventile haben unter Berücksichtigung der Architektur und weiterer Voraussetzungen eine SIL3 Zulassung, sind

also für SIL3 geeignet. Wir benötigen aber PLd. Wie betrachte ich das jetzt? Die Ventile werden von einer Sicherheits-SPS in redundanter Ausführung angesteuert. Daher die Frage, ob das möglich ist.

Experte: Im geschilderten Fall ja, da die Architekturanforderungen an PLd erfüllt werden. Aber es gilt vermutlich eine hohe Anforderungsrate.

Wie wirken sich Einflüsse wie, Einbau, Prozess, Stoffeinflüsse auf das Ventil aus, wenn ich es häufiger bewege (Verschleiß). Muss man sich ein komplett anderes Instandhaltungs- und Austauschkonzept überlegen?

Die Systematik betrachten, Sachverstand und gesunden Menschenverstand einsetzen, dann ist das möglich.

9. Viele Geräte haben nur Angaben für SIL oder PL, nicht beides. Gibt es eine Möglichkeit solche Bauteile in einer Sicherheitskette zu verbauen, ohne Umrechnen zu müssen?
   a. Geräte, die man nicht kennt zu berechnen, birgt immer die Gefahr, falsche Werte heranzuziehen.

   2te Annahme stimmt. Die Antwort ist schon beantwortet.

10. Wie kann man redundant-schaltenden Ventil in SIL oder Performance Level berechnen

    1oo2, 2oo2 Die Formeln sind bekannt. Man muss schauen ob die Ventile in Reihe oder parallel sind. Dann können die bekannten Formeln angewendet werden.

    Fragesteller: Die Werte für die redundanten Ventile sind gegeben - Diagnosedeckungsgrad vorhanden. Was muss bei Redundanz anders gerechnet werden, was bleibt gleich?

    Experte: Die Formeln für die 1oo2 Architektur aus IEC 61508-6 verwenden. Bei Ventilen die systematischen Fehler anschauen, die Werte der Ventile sind gar nicht so relevant. Die Prüfung und das Prüfungsintervall sind entscheidend.

    Anderer Teilnehmer: Sie sagten die Diagnose erhöht sich. Wie ist das gemeint?

    Fragesteller: Verhalten bekannt von Schützen. Für ein Schütz sind 73% DC gegeben. Wie ist das mit 2 Schützen in Redundanz? Erhöht sich dann die DC oder bleibt die gleich?

    Antwort: Wert für einzelnes Schütz gleich, bei 1oo2 fällt ein Ausfall durch Redundanzprüfungen auf. Aber das einzelne Gerät hat nicht mehr Diagnose. Bei Sensoren ist das so wenn man beide kontinuierlich miteinander vergleichen kann. Natürlich hat jeder Sensor sichere und gefährlichen Ausfälle, die Diagnose hat aber nichts mit den Werten für das einzelne Gerät zu tun. Für Sensoren i.O, aber für „final Elements“ fraglich, wenn diese nicht schalten oder schalten, wenn sie es nicht sollen….

    Anderer Teilnehmer: Passende Frage: wieviel Diagnose kommt zwischen den beiden Ventilen oder Schützen? Solange die beiden Schütze immer gleich agieren ist alles gut, aber wenn ein Schütz nicht schaltet nicht. Beim Beispiel dass der Hilfskontakt im Rückführkreis überwacht ob beide geschalten haben gilt: mit extra Diagnose ist mehr Wissen vorhanden, höhere DC.

    Fragesteller: Auf welchen Wert komme ich wenn jedes Schütz für sich 73% hat?

Antwort: Könnte man eventuell einer Tabelle der 61508 oder 13849 entnehmen. Dort noch mal nachschauen, ob da was gegeben ist. In der 13849 ist eine Tabelle mit Punktesystem. Wenn Sie die nötigen Punkte zusammenbekommen, dann erreichen Sie einen gegebenen DC.

Weiterer Teilnehmer: Eine Diagnose erhalte ich bei einem Relais nur wenn ich schalte. Damit kann ich auch nur in dem Intervall Informationen daraus ziehen - die Anforderung von 100x schnellere Diagnose nach ISO 13849 kann damit nicht erreicht werden. Daher sollte man erst überlegen ob es um einen Teil- oder Volltest geht statt einer Diagnose die Lambda-du nach -dd verschiebt.

Nächster Teilnehmer: Was ist das Ziel? Wenn sie was sicherheitsgerichtet abschalten wollen und sie erkennen dass ein Schütz nicht schaltet, dann ist das sicherlich eine Diagnose die das Gesamtsystem sicherer macht. Voraussetzung: defektes Element wird erkannt und ausgetauscht.

Weiterer Teilnehmer: Es sei denn die Anforderungen sind sehr selten (alle 4 Jahre) dann ist Common cause failure (CCF) zu berücksichtigen. Es kostet alles Geld - Sie müssen sich fragen, was ist das Ziel ist. Die Diagnose muss „Rechtzeitig“ abschalten - beachten.

11. Wie kann man bei analogen Sensoren 4-20mA, in SIL 2-Ausführung (100 Mio. Lastzyklen), die PFD, PFH und MTTF-Werte ermitteln?

    Ein Drucksensor hatte diese Angabe im Datenblatt. Aber es steht nicht darin für was. Was ist bei einem Drucksensor ein Lastzyklus?
    Wir haben beim Hersteller angefragt was das zu bedeuten hat, und haben als Antwort bekommen, die Sensoren hätten eine Lebenserwartung von 200 Jahren.

    Das Problem scheint hier der Begriff MTTF zu sein. Die Begriffe MTTF und MTBF sind mit Bedacht zu verwenden. Die Maschinenbauer verstehen darunter in der Regel die „mittlere Lebensdauer“, was auch korrekt ist denn so ist der Begriff definiert. Die Elektrotechniker verstehen unter der MTTF „den Kehrwert der Ausfallrate Lambda“ im flachen Teil der Badewannenkurve.

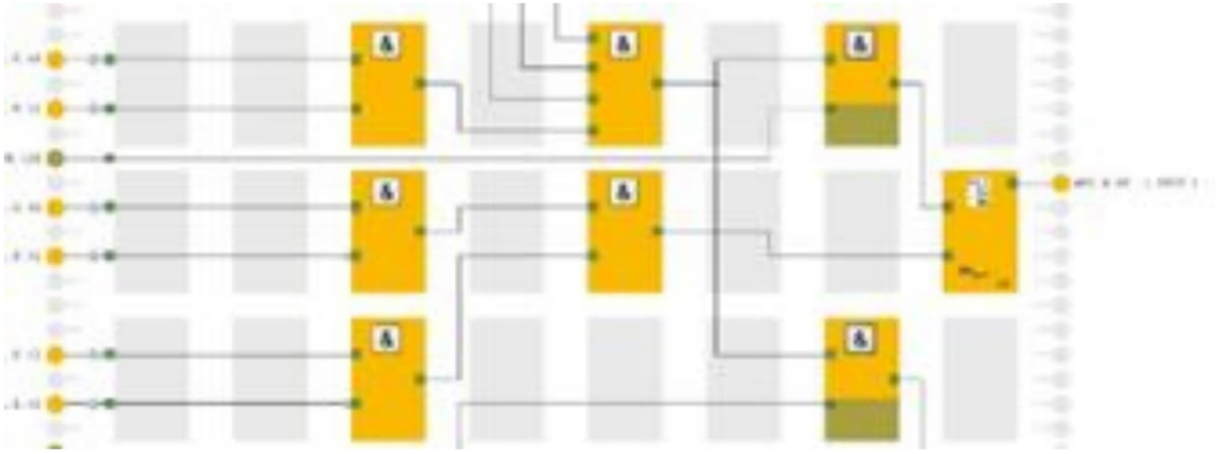
    Fazit: Das Gerät nicht verwenden. Wenn die Daten nicht zur Verfügung stehen, dann kann das Gerät nicht verwendet werden.

12. Zwei redundante Leistungsschütze schalten bei Not-Aus sicherheitstechnisch im „low-demand“, die Maschine aus. Das passiert 1x im Jahr bestenfalls zu Testzwecken. Da die Maschine aber täglich Ein-, und ausgeschaltet wird haben die Schütze viel mehr Schaltspiele. Können die Schütze dann noch im „low-demand“ betrachtet werden?

    Ist Low Demand, wobei aber die Physik beachtet werden muss (Thema Verschleiß bei häufigem Schalten). Evtl. B10 oder B10D-Wert für die Lambda-d Ermittlung um einen PFD zu berechnen.

13. Anwendungsbeispiel 1

Ein Ventil wird im „low demand“ sicherheitstechnisch betrachtet. In der Regel sind die sicheren Eingänge immer „on“. Über die Software soll es aber mehrmals täglich (stündlich) geschaltet werden. Als Überwachung dient die Stellungsabfrage.
Kann das Ventil dann noch im „low demand“ betrachtet werden, oder ist das „high demand“?
Ich gehe davon aus, dass ein Softwareeingang, der virtuell von der Prozess-SPS übergeben wird, sicherheitstechnisch nicht betrachtet wird.



Der Fragesteller: Fall von Ventilen siehe Frage zuvor. Es sind 2 redundante pneumatische Ventile die hydraulische Ventile schalten. Diese wurden im Low Demand betrachtet, Frage besteht zur Ansteuerung durch SW. Es darf immer nur ein Kreis aktiv sein. Jeder Kreis muss redundant abgeschaltet sein. Kann das als LD gesehen werden oder ist das HD.

Sicherheitsfunktion ist dass abgeschaltet wird wenn Flüssigkeit austritt. Dies kommt in der Regel nicht vor.

Auf der DKE-Seite sind FAQ‘s zu finden. Lösung ist dass die SIF Low Demand ist und die Betriebsfunktion High Demand.

Rückfrage: Was ist mit dem SW-Eingang gemeint?

Die Ventile machen im Prinzip die SIF, werden aber vom Prozess mit benötigt.

Teilnehmer: Das hängt davon ab, wie die Ventile angesteuert werden. Betrieblich darf die SIF nicht überfahren werden.

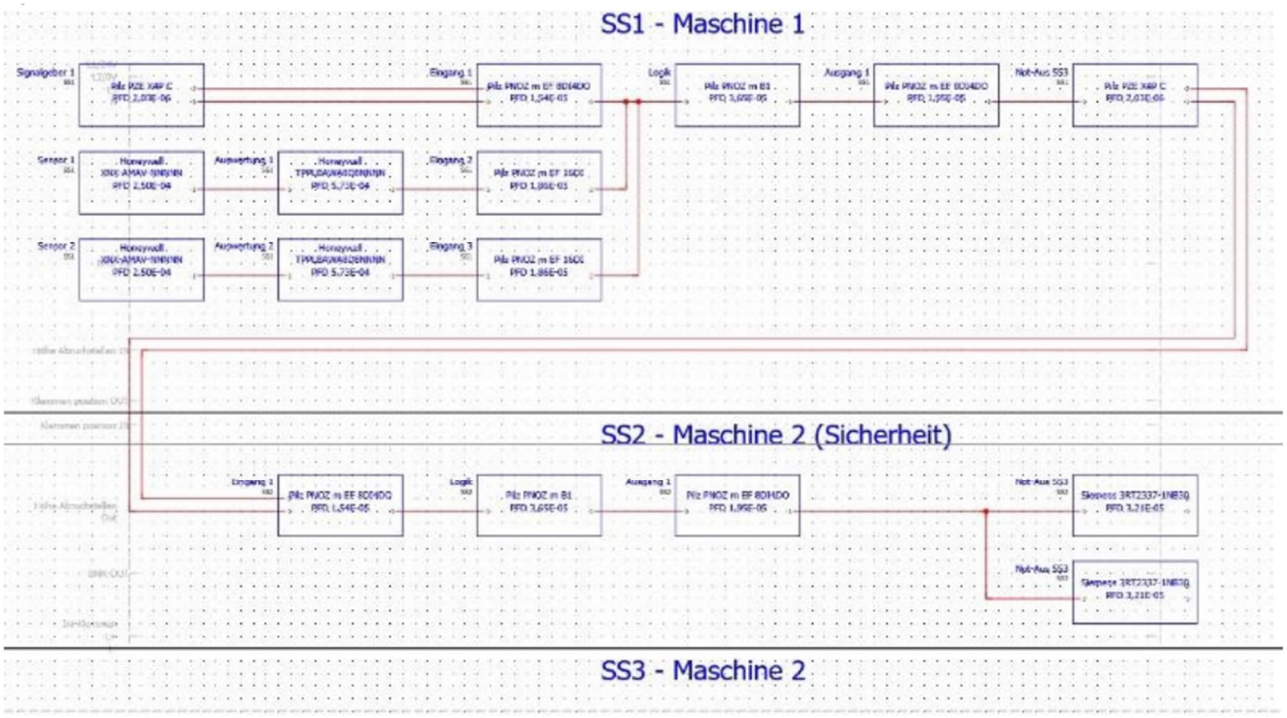
Fragesteller: Nein, die SIF muss ausgeführt werden bevor der SW-Eingang schalten kann. Nur wenn alle sicherheitstechnischen Gegebenheiten erfüllt sind, kann die SW betrieblich schalten. Die Kreise sind gegenseitig verriegelt.

14. Anwendungsbeispiel 2

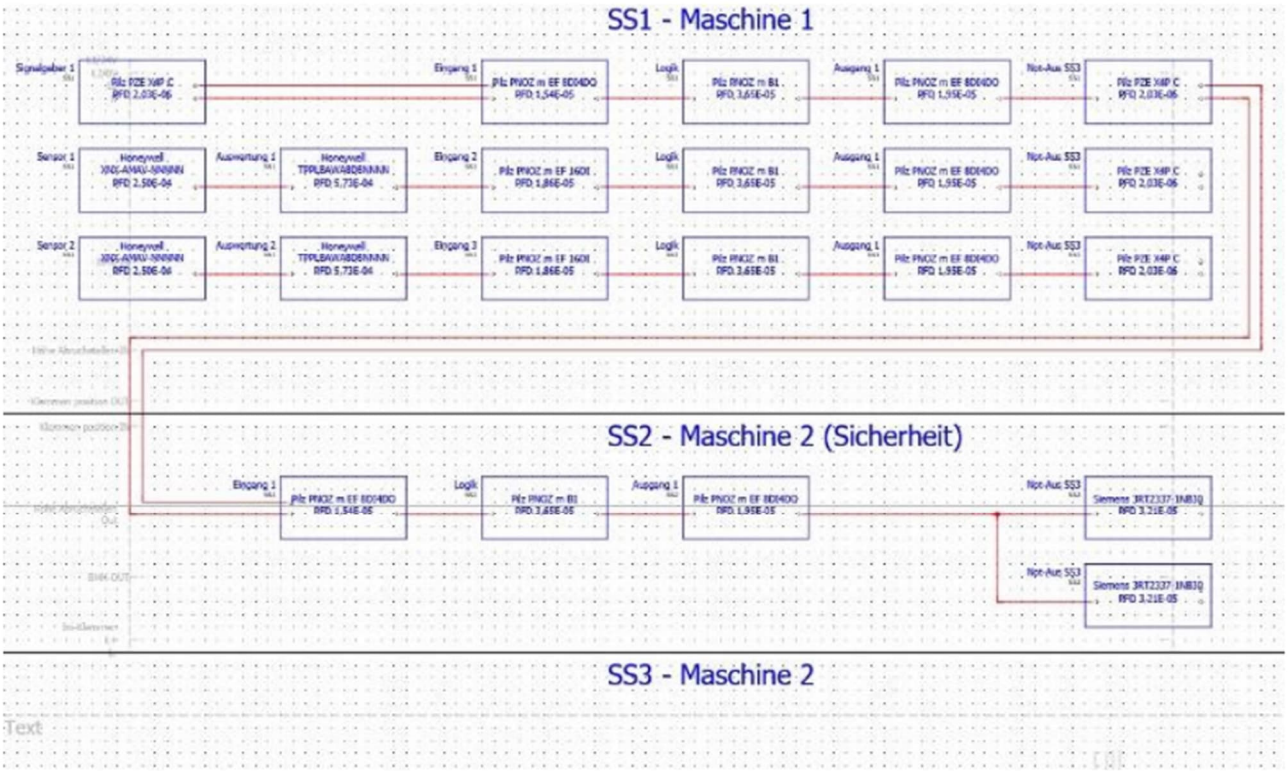
Drei Sensoren gehen auf eine Sicherheits-SPS und regeln einen Ausgang.
Muss man bei der Berechnung der PFD-Werte, die Werte für die Logik, für den Ausgang und für die Kontakterweiterung nur einmal rechnen, oder muss das bei jedem Strang mit einbezogen werden?

Können die Sicherheitsketten für jede Maschine berechnet werden, oder muss die SIL-Berechnung übergreifend für 2 Maschinen erfolgen? Umrechnung SIL in PL.

Fall 1



Fall 2



Fragesteller: Zwei Sicherheitsfunktionen, eine in SIL, die andere in PL zertifiziert (ein Gebäude und eine Maschine). Im Gebäude ist Gas-Sensorik an einer SSPS verwendet. Die Maschine

wird von ihrer eigenen SSPS 2-kanalig angesteuert. Frage: Genügt es wenn die Gebäude-SSPS Sensordaten für die Berechnung zusammenfasst oder müssen beide SSPSsen das Sensorsignakl bewerten?

Eingangsseitig 3 Sensoren, ein Notfalltaster, 2 Gassensoren mit gemeinsamer Bewertung in der Gebäude-SSPS.

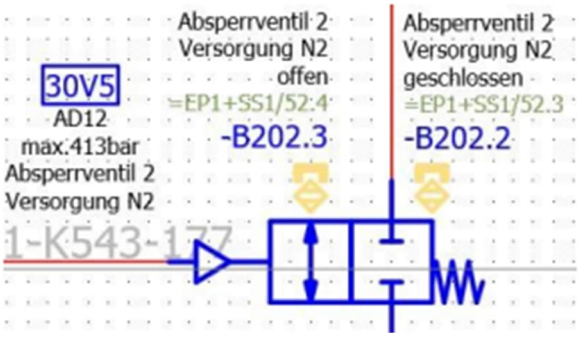
Ein Teilnehmer: Egal wie die Verschaltung ist – was ist die SIF? 1x Notaus, 1x Gasüberwachung, also eigentlich 2 Funktionen. Eine Zuverlässigkeitsbetrachtung ist immer für die Funktion und nicht für die Hardware, für jede Funktion muss PFD oder PFH berechnet werden - einmal Notaus, einmal Gasüberwachung.

Ein Blockdiagramm vereinfacht die Beurteilung. Bitte immer ein Zuverlässigkeitsblockdiagramm zeichnen - dadurch wird die Funktion klarer und die Fragen erledigen sich. Dafür muss man die SIF kennen.

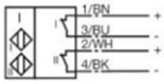
Wenn es eine Gefährdungsbeurteilung gibt muss genau das als Ergebnis herauskommen. Hier können es sogar 3 SIF sein.

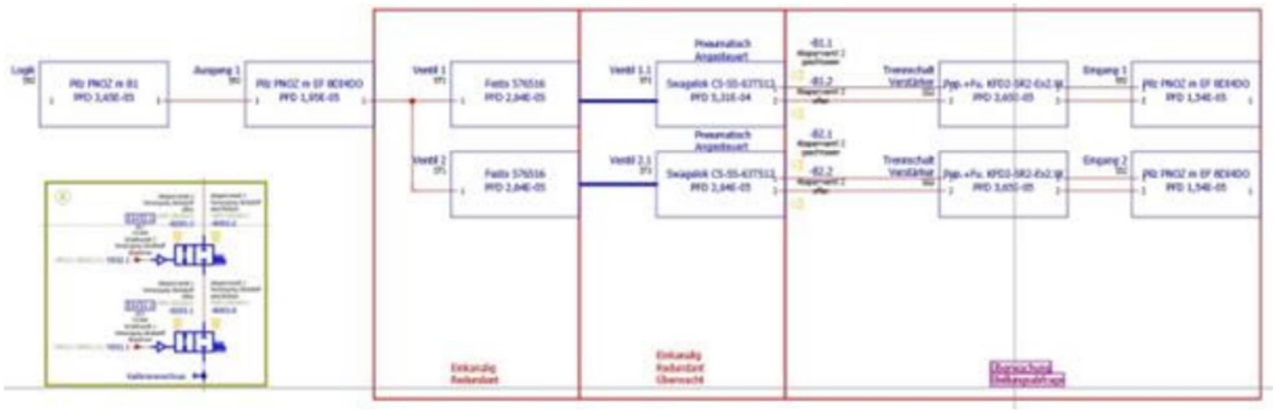
15. Anwendungsbeispiel 3

Ein hydraulisches Ventil ist Stellungsüberwacht.



Die Stellungsüberwachung wird über einen Schalter mit 2 Schaltkontakten realisiert.





Kann man die Überwachung auch auf die elektrisch angesteuerten Ventile anwenden?
Wie ändern sich die Betrachtungen von HFT, PFD/H, und SFF bei Redundanz?

Ebenso die Betrachtung von Schützen einzeln (mit Überwachung) und redundant (mit Überwachung). Jedes einzelne hat angegebene Werte (Ant. Gefahrbringender Ausfälle 73%, B10 1369863, 100 FIT, T1 20y, PFD-3,21E-05). Was muss man bei redundanter Ausführung beachten und welche Werte ändern sich? Wie bekommt man aus diesen Werten den MTTFd-Wert für redundante Ausführung?

Geklärt durch Aufschlüsselung in Zuverlässigkeitsblockdiagramm.

16. Anwendungsbeispiel 4

Inertisieren einer Thermokammer:
Die Thermokammer wird vor dem Start der Prüfungen mit Stickstoff durchgespült, um eine inerte Atmosphäre zu schaffen. Um sicherzustellen das ausreichend Volumen in die Kammer gespült wurde, verwenden wir hierfür einen Schwebekörper-Durchflusssensor mit SIL-Zertifikat.
Der Schaltpunkt zum Start von Prüfungen wird bei jedem Prüfbeginn erreicht. Die Sicherheitsabschaltung wird vermutlich <1 Mal im Jahr erreicht.
Welche Werte kann man hier annehmen? Welche Anforderung ist das (low oder high demand?)

Type A device | Hardware Fault Tolerance HFT=0 | Low demand mode

H250/M40/K*-SK with 1 or 2 fail-safe limit switches (MIN/MAX) and welded process connections

	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	DC_D	MTBF	SIL Level
Stress profile 2 (low stress)	0 FIT	50 FIT	10 FIT	38 FIT	61 %	20 %	487 years	SIL2
Stress profile 4 (high stress)	0 FIT	50 FIT	10 FIT	73 FIT	45 %	12 %	356 years	SIL1

T[Proof]	1 year	2 years	5 years
$PFD_{AVG\ (Profile\ 2)}$	1.82E-04	3.46E-04	8.41E-04

H250/M40/K*-SK with 1 or 2 standard limit switches (MIN/MAX) and welded process connections

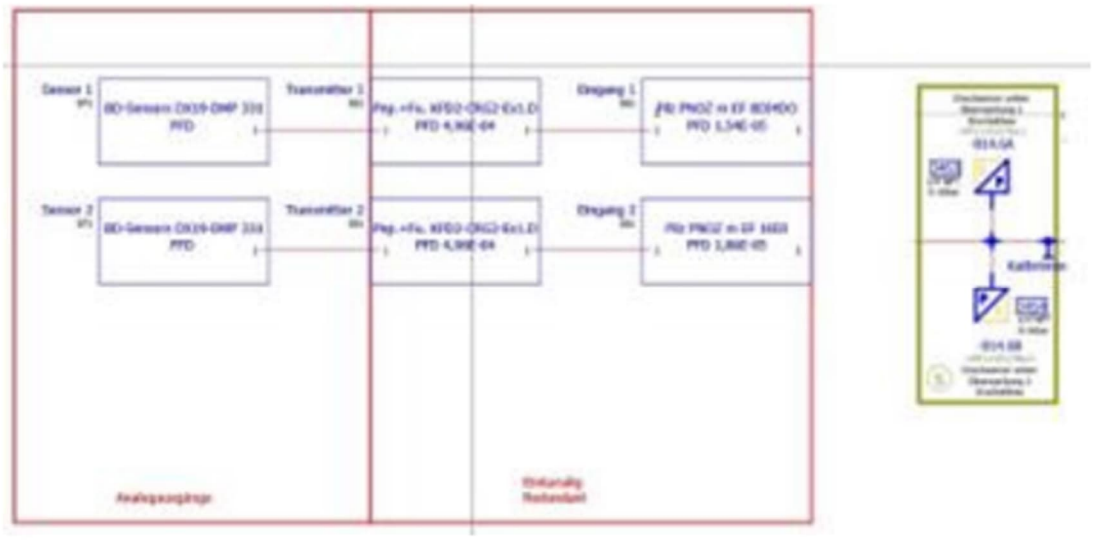
	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	DC_D	MTBF	SIL Level
Stress profile 2 (low stress)	0 FIT	81 FIT	10 FIT	77 FIT	54 %	11 %	376 years	SIL1
Stress profile 4 (high stress)	0 FIT	81 FIT	10 FIT	112 FIT	44 %	8 %	293 years	SIL1

T[Proof]	1 year	2 years	5 years
$PFD_{AVG\ (Profile\ 2)}$	3.68E-04	7.02E-04	1.70E-03

Nach Beschreibung Low Demand, mit Zuverlässigkeitsblockdiagramm lösbar.

17. Anwendungsbeispiel 5

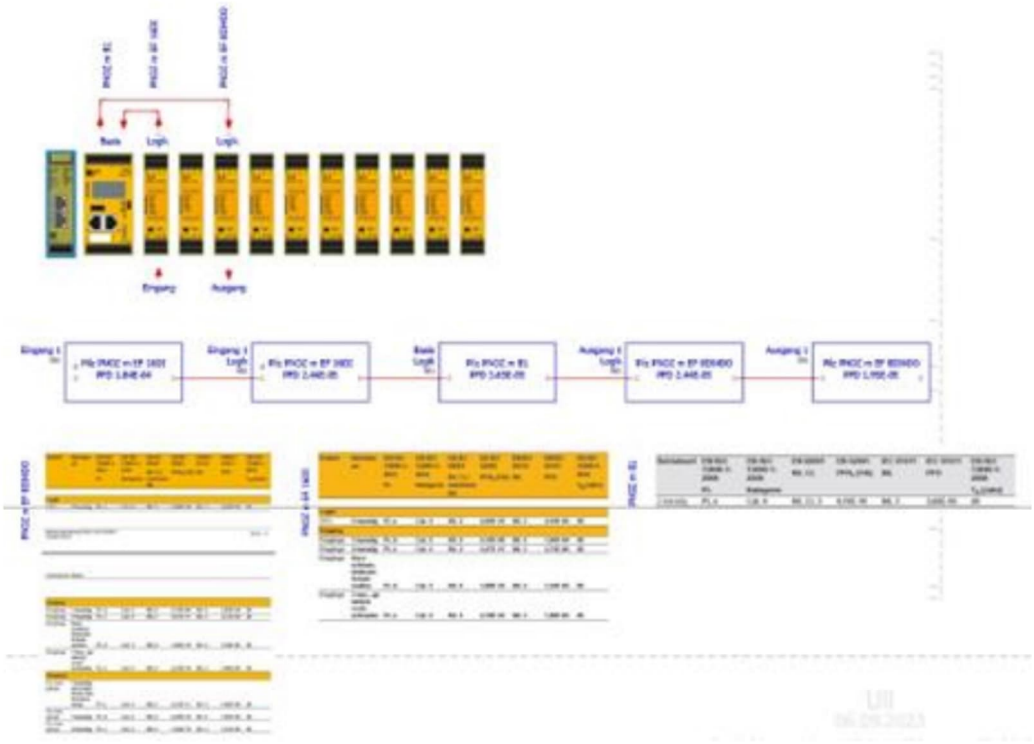
Wie betrachtet man eine Anwendung mit 2 redundanten Drucksensoren (analog), die nur eine schriftliche Erklärung des Herstellers haben, dass die Geräte „einen MTTF-Wert von größer als 200 Jahren haben“?



Geklärt – der MTTF Wert darf laut ISO 13849 verdoppelt werden um den $MTTF_D$-Wert zu bekommen – damit kann SISTEMA als Tool arbeiten.

18. Anwendungsbeispiel 6

Eine Sicherheits-SPS ist ein Zusammenschluss vieler einzelner Bauteile. Es gibt ein Basismodul mit Logik und E/A-Module, die auch jedes für sich, Logikbausteine haben.
Muss in der PFD-Berechnung jede einzelne Logik angeführt werden?



Das sind Auszüge aus den voran gegangen Fragen.

Das Vorgehen ist wie vorher. Jede einzelne Funktion betrachten um Berechnungen zuzulassen. Common Cause für gemeinsam benutzte Bausteine abschätzen bzw. je nach Risiko entscheiden ob separate Hardware vorzusehen ist - es könnten auch die Logiken einen Fehler haben.

19. Wie ist im Rahmen der SIL Nachweisführung mit dem Thema Betriebsbewährung hinsichtlich Konformität umzugehen. Folgendes Szenario: es liegen weder SIL Zeritifizierte/SIL Kenndaten noch Nachweise gemäß NE93, NE130 für eine Betriebsbewährung des Gerätes vor. Es besteht für den sicherheitsgerichteten Kreis eine SIL2 Anforderung. Als Rechtfertigung zieht der Betreiber hinsichtlich "betriebsbewährte Geräte" seine regelmäßigen stattgefundenen Instandhaltungs- und Wiederholungsprüfungen (letzten 10 Jahre) an, welche keine Beanstandung aufweisen.
    1. Frage: Ist dies für eine Einstufung als betriebsbewährtes Gerät akzeptabel und kann dieses Gerätes in einem SIL Loop eingesetzt werden?
    2. Frage: Wie ist mit dem Sachverhalt in der SIL Nachweisführung damit umzugehen (Betriebsbewährung über regelmäßige Instandhaltungsnachweise, aber nicht nach NE130)?

    Ausgangspunkt ist ein Gerät das über 10 Jahre alt ist. Daten zur Betriebsbewährung liegen vor, falls diese nicht genügen kann man sich mit anderen Betreibern zusammentun oder verwendet ein zertifiziertes Gerät für das damit zusätzliche Daten vorliegen. Weitere Lösungen sind eher schwierig.

    Fragesteller: Der Betreiber wurde auf einen systematischen Fehler hingewiesen, aber die Prüfstelle ist der Betrachtung mit Betriebsbewährtheit, 10 Jahren Instandhaltungsprotokollen und Wiederholungsprüfung ohne Beanstandungen mitgegangen.

    Zwischenfrage: Betriebsbewährung ist eher für eine Population und nicht für ein einzelnes Gerät möglich, möglich nur wenn gut dokumentiert. Zu bedenken: das Gerät ist dann schon 10 Jahre im Betrieb, wie lange soll es insgesamt halten? Betriebsstunden sind für die Betriebsbewährung die Grundlage, zu beachten sind dabei nach Norm die „vergleichbaren Einsatzbedingungen“. Basis sind zwischen 100.000 und 1.000.000 Betriebsstunden. Für einen Einzelanwender selten zu erreichen.

    Unterschied zwischen Betriebsbewährung seitens Hersteller („proven in use“) oder Anwender („prior use“). Woher kommen die Daten. Oft ist nichts protokolliert. Betriebsbewährung nur wenn eine hohe Zahl fehlerfreier Betriebsstunden nachgewiesen werden kann. Die Doku ist entscheidend. Nachweisplicht gegeben.

    Weiterer Teilnehmer: Betriebsbewährung ist entstanden weil es damals noch keine zertifizierten Geräte gab, heute sollte man wegen der Komplexität der neuen Geräte von reiner Aussage auf Betriebsbewährung Abstand nehmen. Als Anwender ist es nicht möglich die wirkliche Komplexität (Anzahl der Zeilen an Code in Software, usw.) zu beurteilen. Reine Betriebsbewährung nur in Ausnahmefällen zulassen oder anwenden.

Grundsatzfrage: Gibt es eine Risikoabschätzung für jede Anwendung die für die Betriebsbewährung benutzt wird? Bitte ganz vorne anfangen. Wenn die Grundlagen geklärt sind, dann rechnen.

Führen wir für mechanische Komponenten den SIL Nachweis? Hat so ein Gerät auch zufällige Fehler oder nur systematische, sprich Sicherheitsnachweis ja oder nein?

SIL-Nachweis ja, es bleibt die Frage ob einzurechnen. Die systematischen Fehler müssen auf jeden Fall betrachtet werden (SIL-Nachweis), und man muss sich die ganze Kette anschauen die mit in den Kreis geht und Teile davon auch berechnen.

Achtung: Berechnung ist nicht gleich SIL-Nachweis. Es gibt die zufälligen Fehler, die systematischen Fehler und die HFT. Alle drei Punkte gehören in den SIL-Nachweis. Der Ventilkörper muss also nicht (unbedingt) berechnet werden. Auslegung und Systematik sind entscheidend.

20. In der chemischen Industrie wird häufig die DIN EN 61511 für typische Gefährdungen der Maschinensicherheit (z.B. Eingreifen mit der Hand in laufendes Reaktor-Rührwerk) angewendet und nicht die DIN EN 13849. Ist das formal zulässig und worin besteht der Nachteil dieser Vorgehensweise.

    Teilnehmer: Eingreifschutz beginnt nicht mit einer Sicherheitsfunktion. So konstruieren, dass die Gefahrenstelle nicht direkt erreichbar ist. Ist es dann noch eine Maschine oder eine Prozessanlage? Wenn es eine Maschine ist, ist es eine vollständige oder unvollständige Maschine. Wenn eine Gefährdung möglich ist und dies eine Sicherheitsfunktion erfordert muss eine Prüfung auf Änderung der Maschine erfolgen. Danach erst die Prozesssicherheit realisieren.

    Anderer Teilnehmer: Die Einordnung ob es ein Prozess oder eine Maschine ist egal, die Anwendung muss sicher sein. Werkzeuge nach der Maschinenrichtlinie sind bewährt, kein Problem das als Maschine zu sehen.

    Überwachungsstelle: Ja aber, bei einer Druckgeräteanlage nach der Druckgeräterichtlinie, lande ich in der Betrachtung wieder bei der 61511.

    Nächster Einwand: Es gilt Herstellerverantwortung, d.h. der Hersteller muss sein Produkt positionieren. Er muss eine Risikoanalyse erstellen und daraus ergeben sich die anzuwendenden Normen.

    Weiterer Teilnehmer: Hängt das Ergebnis vom Verfahren ab? Welche Ansprüche ergeben sich? Kann es sein, dass durch Betrachtung nach der Prozess-Norm andere Ansprüche an die SIF gestellt werden als nach der Maschinen-Norm? Im Prozess können es andere Dimensionen sein. Nicht unbedingt „nur“ der Verlust eines Fingers. Daher muss die Risikoanalyse passend zur Problemstellung (Gefährdung) erfolgen, und nicht passend zum Gerät (Maschine).

    Frage eines Teilnehmers: Ein Eingreifschutz in ein Reaktorrührwerk ist eine Fragestellung für die Maschinenrichtlinie. Erst Prüfung auf sichere Funktion nach Maschinenrichtline, dann die Prüfung für Prozess und oder Druckgeräterichtlinie.

Nächster Teilnehmer: Reihenfolge richtig, es könnten von der Maschine ja auch Gefahren für den Prozess ausgehen.

Der Hersteller muss sich auch Gedanken über die Verwendung machen. Die Maschine wird ja in einem Prozess verwendet. Sonst hat der Verwender ja das Problem, dass er die Maschine evtl. nicht bestimmungsgemäß verwendet.

Wenn ein prozesstechnisches Risiko gemindert werden muss dann sind die Normen der Prozesswelt zu verwenden und umgekehrt. Wenn die Gefahr von der bestimmungsgemäßen Verwendung ausgeht dann ist es ein maschinentechnisches Problem, wenn die Gefahr von einem gestörten Betrieb ausgeht, ist es ein protzesstechnisches Risiko. Daraus ergibt sich die Zuständigkeit der Richtlinie / Norm.

Harmonisierte Normen lösen Vermutungswirkung aus - Artikel 7 Absatz 2 in der Maschinenrichtlinie. In den Normen selbst steht drin, welche Anforderungen aus dem Anhang 1 sie adressieren - siehe Anhang ZA. Nur für diese Punkte gilt die Vermutungswirkung. Eine B-Norm listet wesentlich weniger Punkte als eine C-Norm. Daher können Produkte nicht nach einer Typ-B-Norm gebaut werden, also auch keine Vermutungswirkung für das Gerät davon ausgehen. Die Vermutungswirkung geht von den gelisteten Normen aus.

Nächster Termin für die SIL-Sprechstunde ist der 18+19.9.2024

Grafiken der Beispiele stammen von der Firma Sinplas. Ist es möglich, bessere Auflösung zu bekommen?