4. SIL-Slam am 03.05.2023

Rückblick

08:45 Uhr	Begrüßung	
09:00 Uhr	**Normenrenovierung**	Michael Kindermann
09:20 Uhr	**Normenschlamassel**	Stefan Ditting
09:40 Uhr	**Sicher navigieren auf der Normungsroadmap KI**	Marco Knödler
10:00 Uhr	**Gebrauchsdauer**	Peter Arnold
10:20 Uhr	Pause	
10:30 Uhr	**Täglich grüßt das TRGS 725 – Murmeltier**	Martin Herrmann
10:50 Uhr	**Beschreibt die SRS die Anforderungen genau?**	Christian Demski
11:10 Uhr	**Auszug aus einem Prüfbericht**	Stefan Lauer
11:30 Uhr	**FuSi für Monteure und Techniker - Welches Wissen ist für Arbeiten im Feld relevant**	Jan-Niklas Stender
11:50 Uhr	**Wann muss ein SIS Ventil erneuert werden?**	Udo Menck
12:10 Uhr	Mittagspause	
13:00 Uhr	**Was Sie schon immer über Markovmodelle wissen wollten**	Frank Schiller, Patrick Gehlen, Jürgen Mottok
13:20 Uhr	**Zufällige Fehler in Mechanik - Mythos oder Wirklichkeit?**	Christoph Theilen
13:40 Uhr	**„Betrachten Sie die Funktionale Sicherheit?“ Was steckt hinter dieser Frage?**	Malika Mast
14:00 Uhr	**Der Tropfen, der das Fass zum Überlaufen bringt**	Ingo Rolle
14:20 Uhr	**LDM und HDM - So überflüssig wie ein Kropf?**	Andreas Hildebrandt
14:40 Uhr	Abschlussdiskussion	

Pepperl+Fuchs

Normenrenovierung

Wie geht’s voran in der Normung?

Welche Richtung ist voran?

Na dann los.

Beispiel IEC 61508

About the presenter

Dipl.-Ing. Michael Kindermann

- **Degree in Electrical Engineering (Automation) @ University of Kaiserslautern**
- **10 years R&D @ Pepperl + Fuchs**
- **Design of functionally safe devices since 2001 (EN 954-1 und EN 61508)**
- **3 years of certification in hazardous locations @ UL International**
- **Certified FS-Engineer in HW/SW design**
- **Head of Functional Safety Management @ Pepperl+Fuchs since 2011**
  - **Supervising the work of standard experts** for functional safety
  - **Responsible for processes** linked to functional safety
  - **Functional Safety Manager** for design projects
  - **Committee work** GK 914 (FS – IEC 61508), AK 225.1 (Machines and FS), K132.0.1 (FMEA), K241 (Ex and FS)
  - **Committee Moderator GAK 914.0.3** (FS Software), **AK 914.0.9** (Statistical Evaluation of FS Software) and **AK 914.0.11** (AI and FS)

Wie geht ein Normen-Update?

Source: pixabay

- Jemand kommt auf die Idee dass die derzeitige Norm **nicht das abdeckt** was er / sie braucht.
- Der Vorschlag zur Überarbeitung wird angenommen.
- **Leute kommentieren.**
- Es werden **Lösungen** gesucht um die Norm zu verbessern.
- Die Lösungen werden konsolidiert.
- Die Norm wird **veröffentlicht**.

Wie geht ein Normen-Update bei der 61508?

Schon vor Erscheinen der neuen Norm sind Leute unzufrieden und wollen ein Update.

Da die Norm von so vielen Seiten Interesse erfährt ist mit vielen Kommentaren zu rechnen.

Randbedingung: das Update muss in **begrenzter Zeit** abgeschlossen sein.

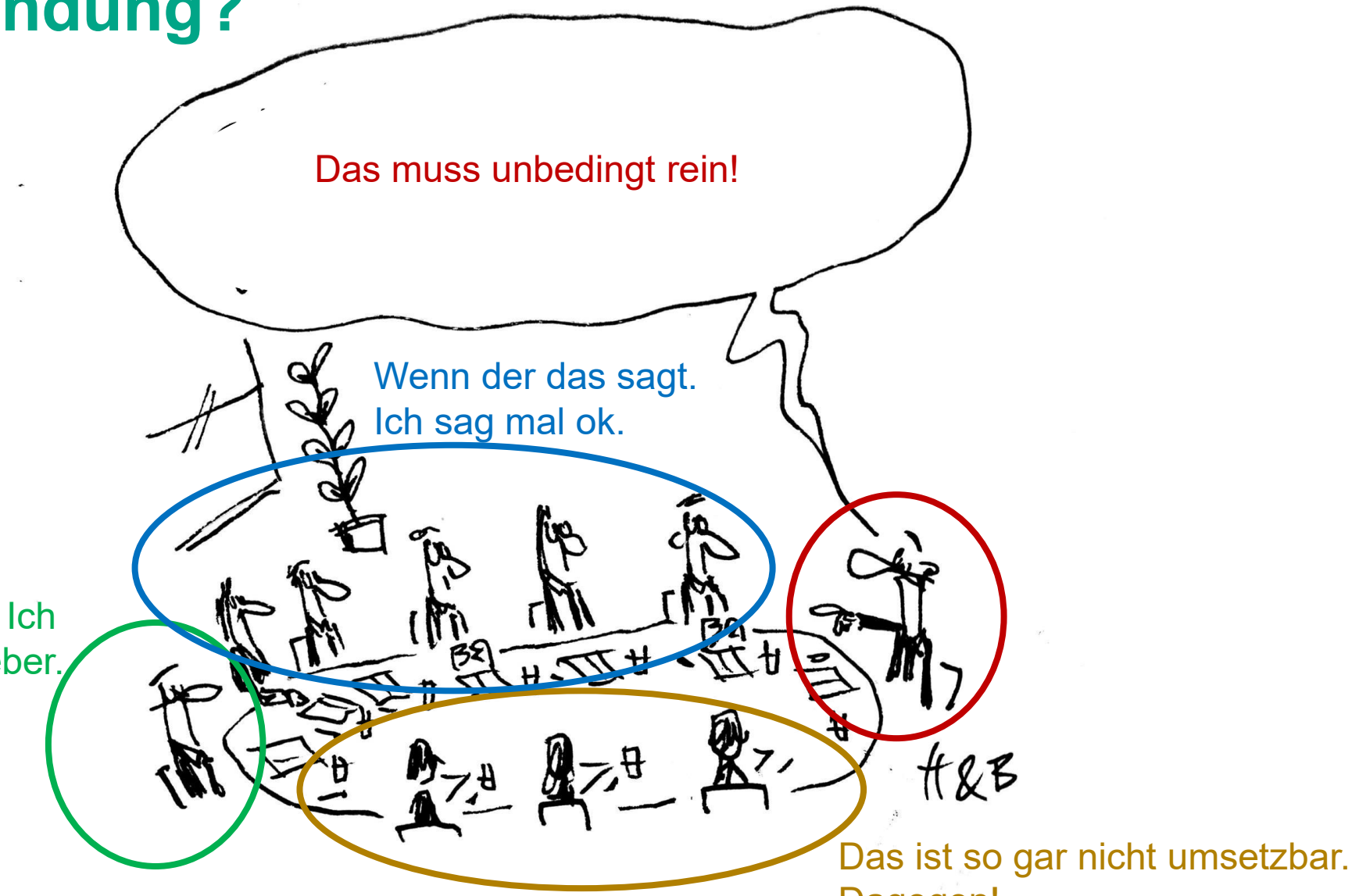
Das Update wird also nicht offiziell gestartet sondern es wird vorsondiert.

Es gibt 500 Kommentare zu 200 Themen.

Man geht schon mal an einzelne Streitthemen.

Source: pixabay

Konsensfindung?



Source: cartoonkaufhaus.de
Postkarte von Hauck & Bauer

Dann ham wer ja mal drüber geredet

Zum Glück lief das Vorsondieren lange.

Los gehts mit der offiziellen Normung.

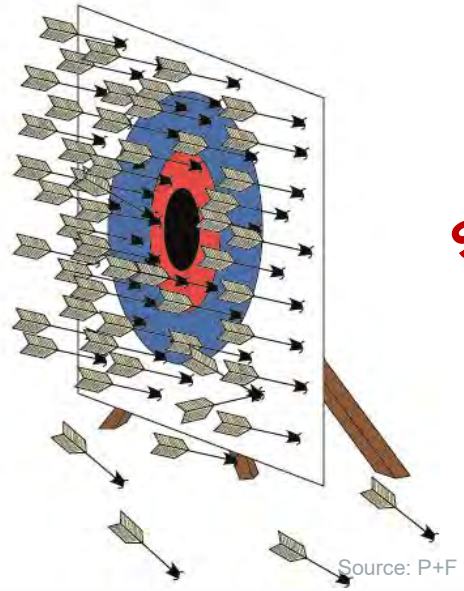
2000 Kommentare

Source: pixabay

So schlimm ist es dann doch nicht…

- **Kommentare sind fast immer komplett ausformuliert**
- **Entscheidungen aus der Vorsondierung werden nicht noch einmal diskutiert.**
- **Viele valide Kommentare kommen aus jedem Land (14x)**

Das Gefühl bleibt….

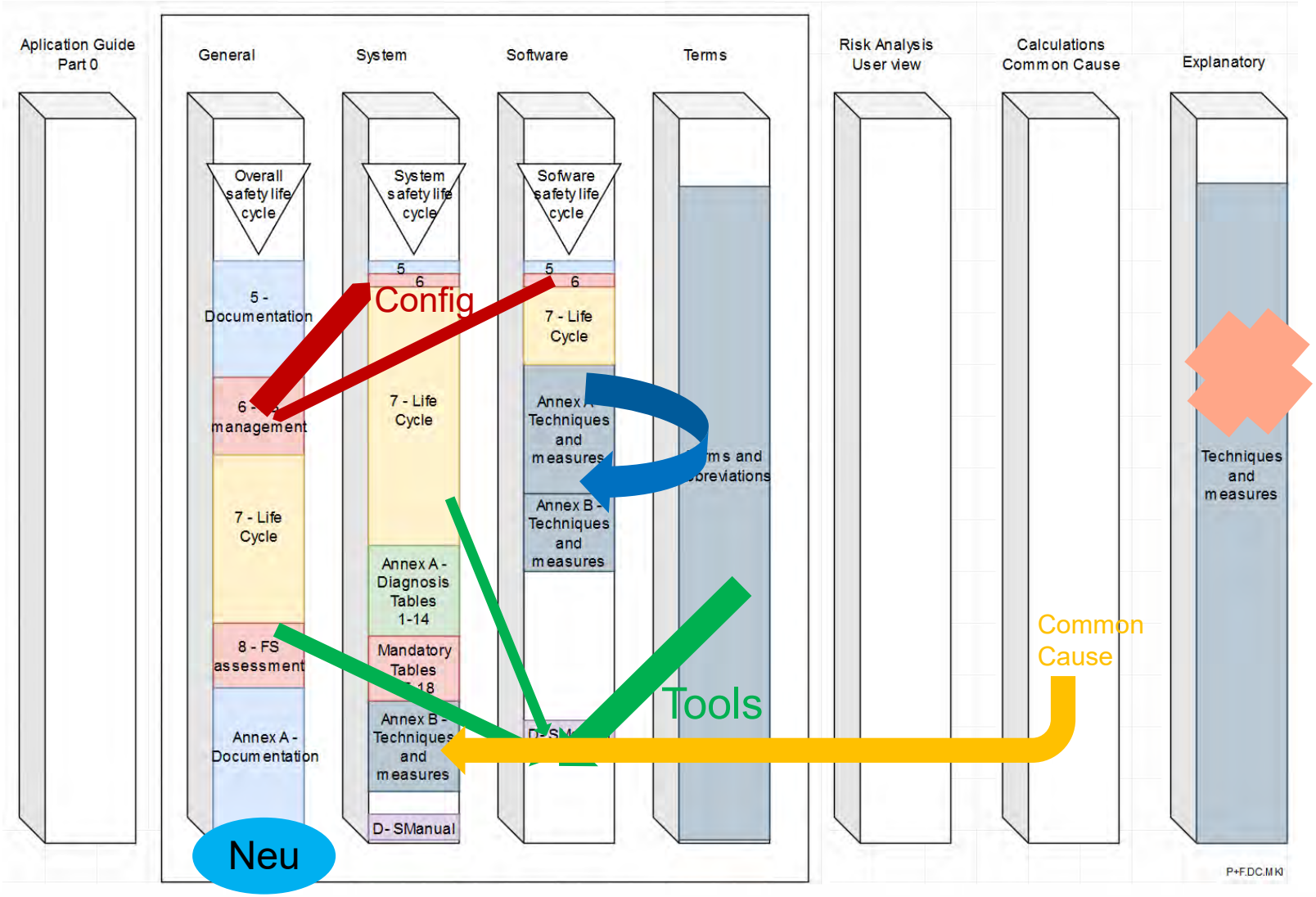


Source: P+F

Schwerpunkte sammeln, konkret aussuchen und bearbeiten?

Dafür schnellere Zykluszeit?

Wie geht ein Normen-Update bei der 61508?



Aber: wir sind nicht allein

Es gibt keine Redline-Version der IEC 62061 wegen der vielen Verschiebungen

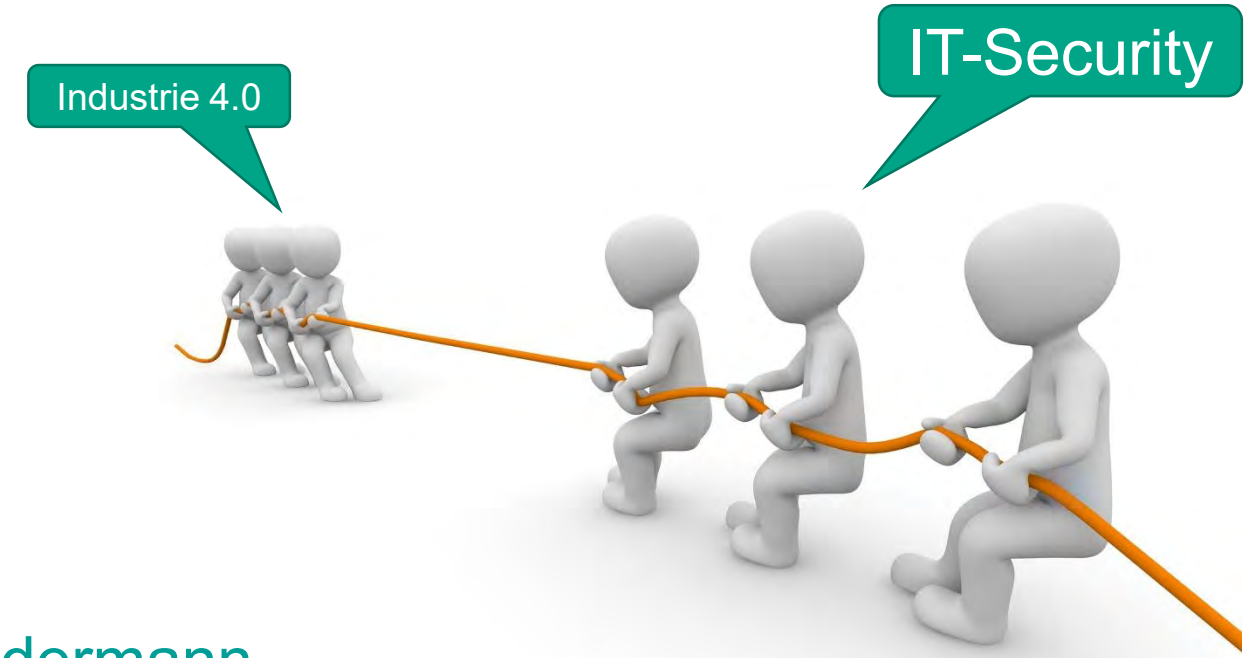
Im Ex-Schutz wurden ganze Zündschutzarten in andere Teile verschoben und umbenannt

Zurück geht aber leider auch nicht mehr…

Source: funny-jokes.com

Source: pixabay

Industrie 4.0 versus IT-Security



Source: Hildebrandt, P+F

Michael Kindermann

Pepperl+Fuchs Group

mkindermann@de.pepperl-fuchs.com

S4S-Normierungsschlamassel.

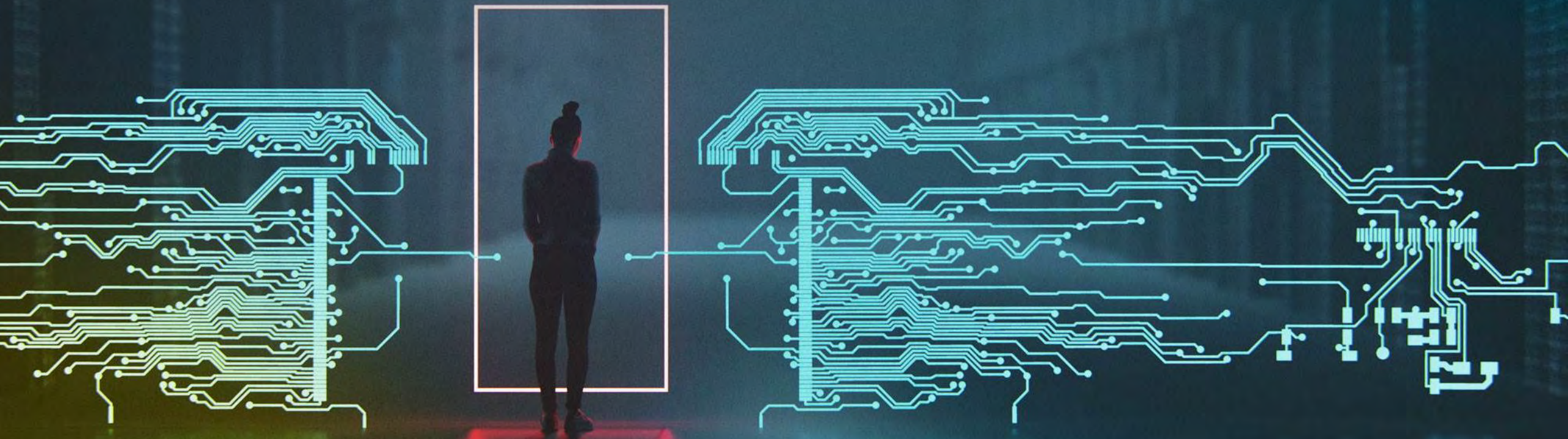
SIL Slam

HIMA EMP SDitting

HIMA

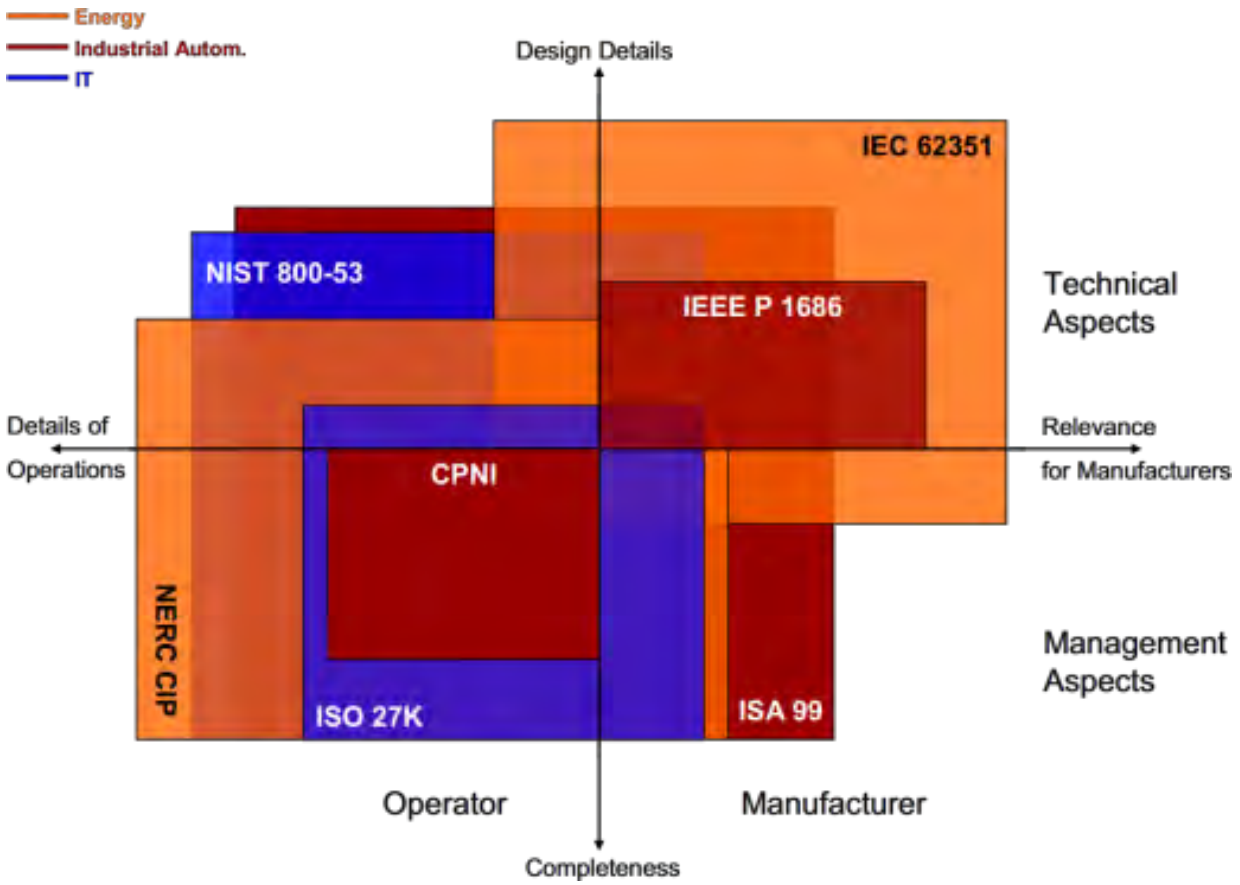
SMART SAFETY.

#safetygoesdigital



Eine frühe Erkenntnis.

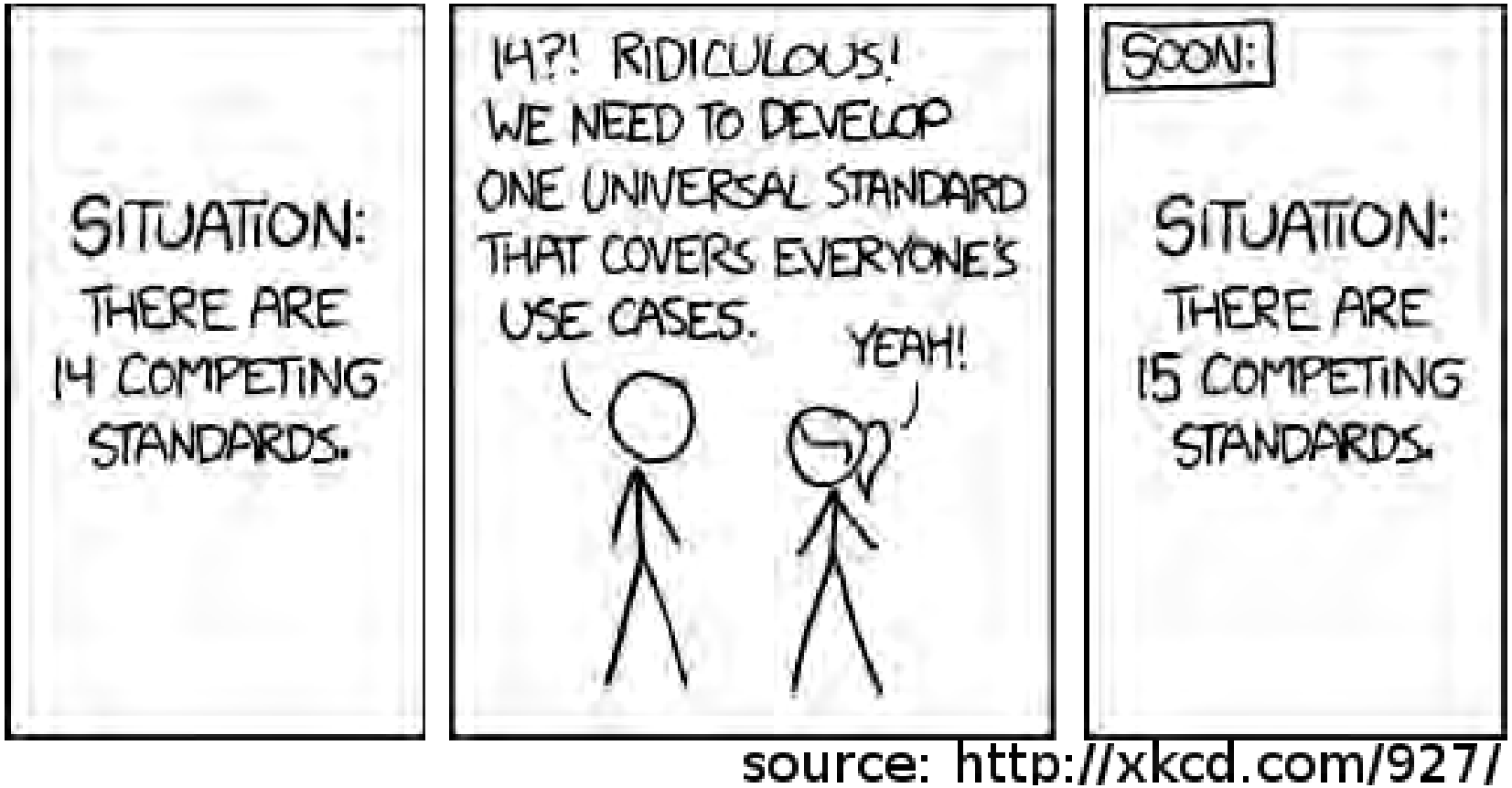
ESCORTS.



- Für Asset-Eigentümer sind 24 von 37 Standards "relevant
- Für Lieferanten sind 14 von 37 Standards „relevant“.

Quelle: http://www.cen.eu/cen/Sectors/Sectors/ISSS/Focus/Pages/FG-ESCORTS.aspx / www.escortsproject.eu
EUROPEAN NETWORK FOR THE SECURITY OF CONTROL AND REAL TIME SYSTEMS
Noch zu finden mit https://web.archive.org/

So isses.

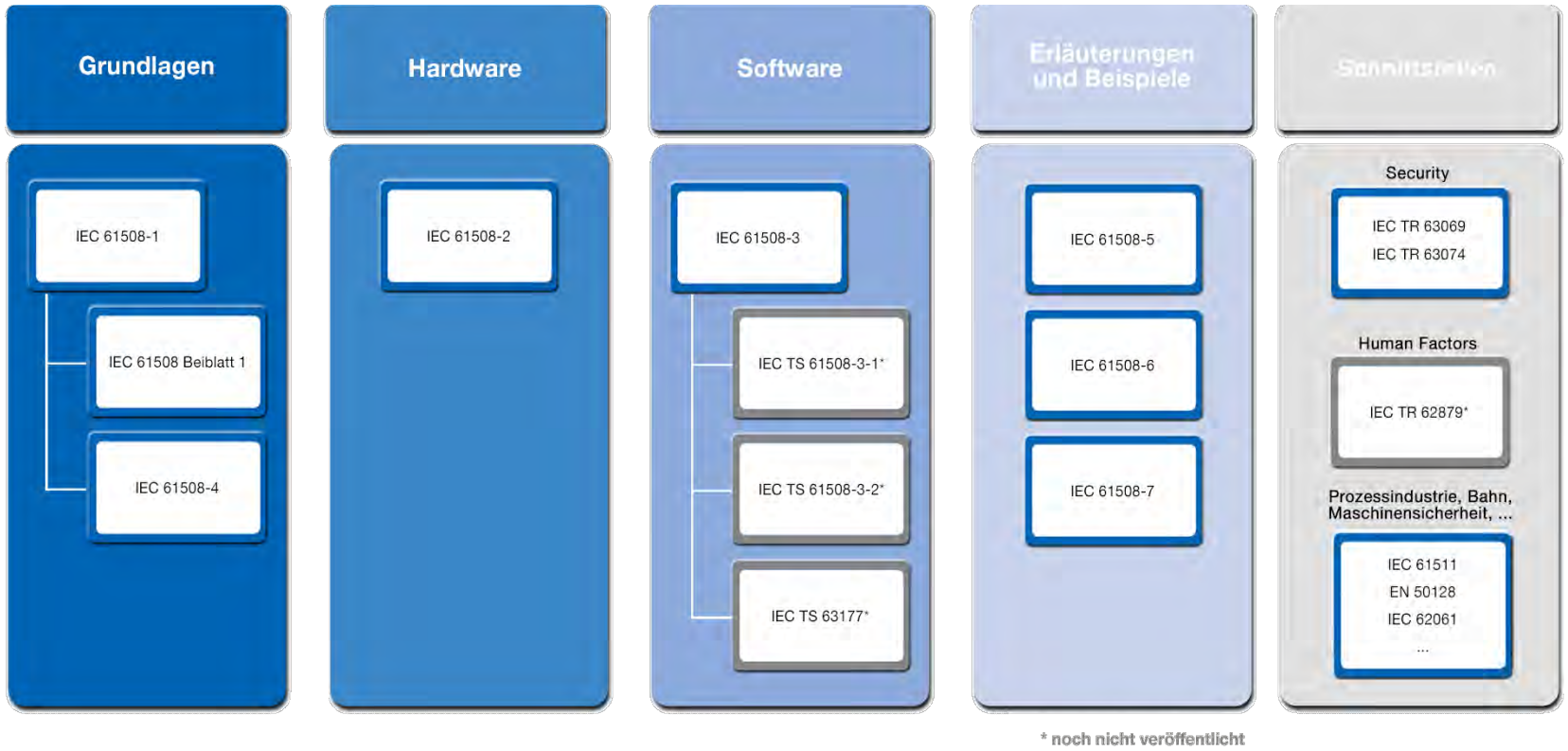


92 Seiten
https://www.vde.com/resource/blob/1805388/cd69053e8991bc23a53c04fa4bd84299/yellow-pages-zum-it-security-navigator-data.pdf

Anzahl Standards 2018: **823**

Aktueller Stand.

Struktur der IEC 61508.



Functional safety of electrical / electronic / programmable electronic safety-related systems.

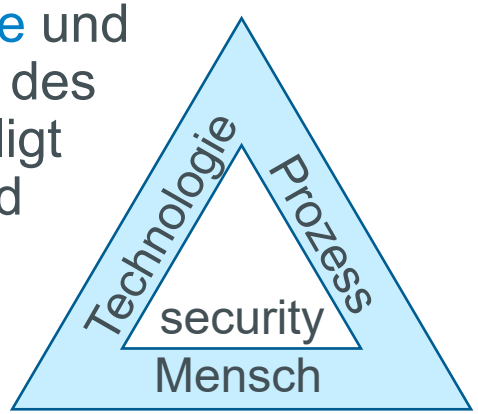
Ist das SIL ausreichend um ein Safety-System zu beschreiben?

https://www.dke.de/de/arbeitsfelder/core-safety/news/vde-dke-tagung-funktionale-sicherheit-2021

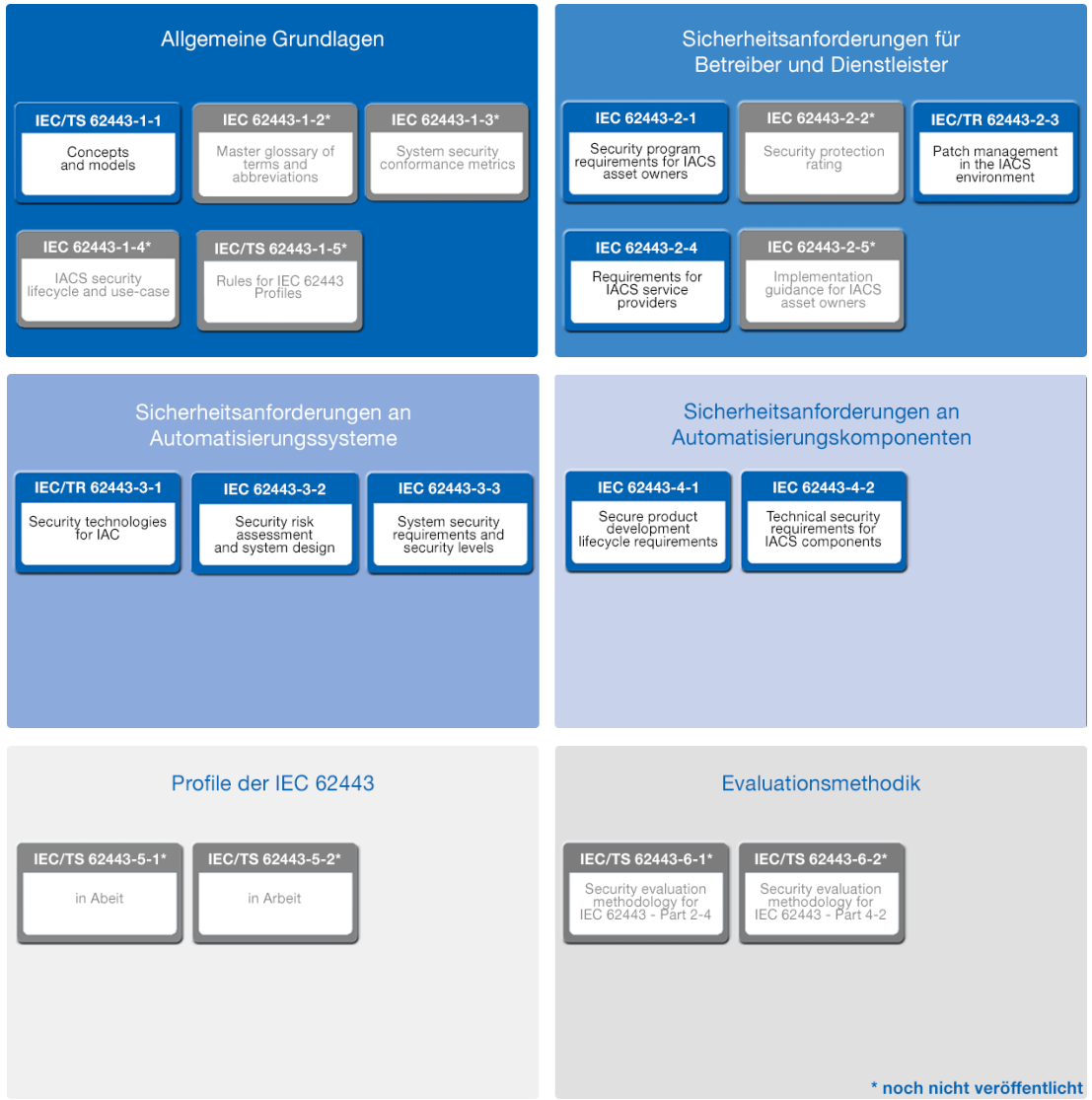
Struktur der IEC 62443.

Security for industrial automation and control systems.

Ein IACS ist definiert als eine Sammlung von Personal, Hardware, Software und Programmen, die am Betrieb des industriellen Prozesses beteiligt sind und dessen sicheren und zuverlässigen Betrieb beeinflussen können.



Ist das SL ausreichend um ein Security-System zu beschreiben?



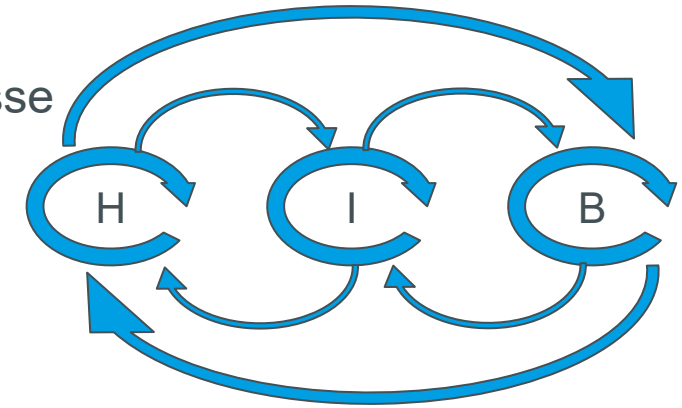
Quelle: https://www.dke.de/de/arbeitsfelder/industry/iec-62443-cybersecurity-industrieautomatisierung

Und was ergibt sich daraus?

Beziehungsstatus: Es ist kompliziert!

	Management		(technische) Eigenschaften		Gesetze	
	Safety	Security	Safety	Security	Safety	Security
Hersteller	61508	62443-4-1	61508	62443-4-2	ProdHaftG ProdSG	CRA
Betreiber	61511	62443-2-1	61511	62443-3-3 (62443-2-4)	BImSchV MaschinenV	NIS2

- Je nach Anwendung
  - 61511 (...) - 13849, 62061
  - TR **63069** (61508/62443)
  - TR 63074
  - TR 50701
- unterschiedliche Prozesse
  - VDI 2182 ->
  - ISO 27k
  - NIST Framework

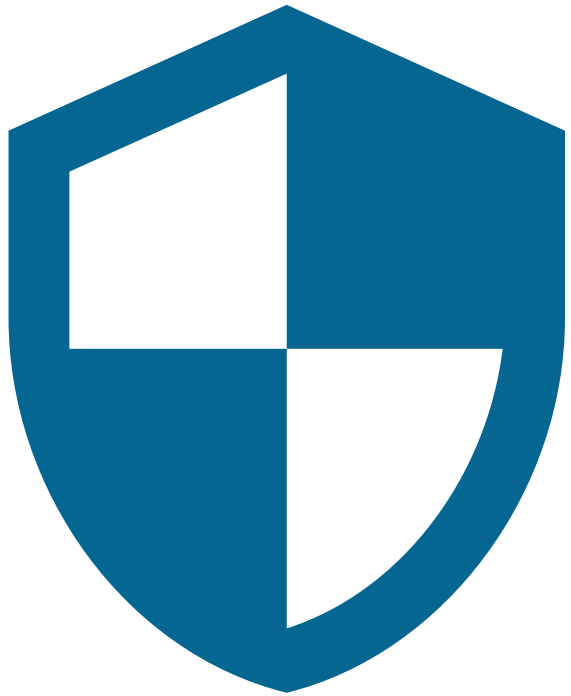


Weitere False Friends

- Risikoanalyse vs. Bedrohungsanalyse
- Lebenszyklusbetrachtung: lang- vs. kurzfristig
- Defense in Depth vs. Layers of Protection
- Trennung von Rollen vs. Zusammenarbeit
- Fail Safe vs Fail Secure
- Technik: public review vs. prooven in use
- Sicherheitslevel: SIL vs. SL

Unglaubliche Erkenntnisse.

- Es gibt nicht DIE Security Norm (nur die Hoffnung, dass sich die IEC 62443 durchsetzt)
- Keine der Normen ist ein Rezeptbuch.
- Das Lesen einer Norm produziert keine Spezialisten.
- Das Erfüllen einer Norm ergibt keine marktgerechten Produkte.
- Secure Produkte ergeben keine(n) Secure Anlagen(betrieb)
- Secure Anlagen werden von Security-Spezialisten entwickelt.
- Safe Anlagen werden von Safety-Spezialisten entwickelt.
- **Beides zusammen machen beide zusammen!**



Und was machen wir daraus?

Erreichen, dass die Synchronisierung zwischen Safety und Security zunächst auf Basis der Grundnormen (IEC 61508 und IEC 62443) beschrieben wird

- IEC 61508 soll ausschließlich safety Anforderungen beschreiben und für security Anforderungen auf IEC 62443 verweisen
- IEC 62443 soll ausschließlich security Anforderungen beschreiben und für safety Anforderungen auf IEC 61508 verweisen
- Es gibt kein führendes Thema, weder Security noch Safety sind “wichtiger“

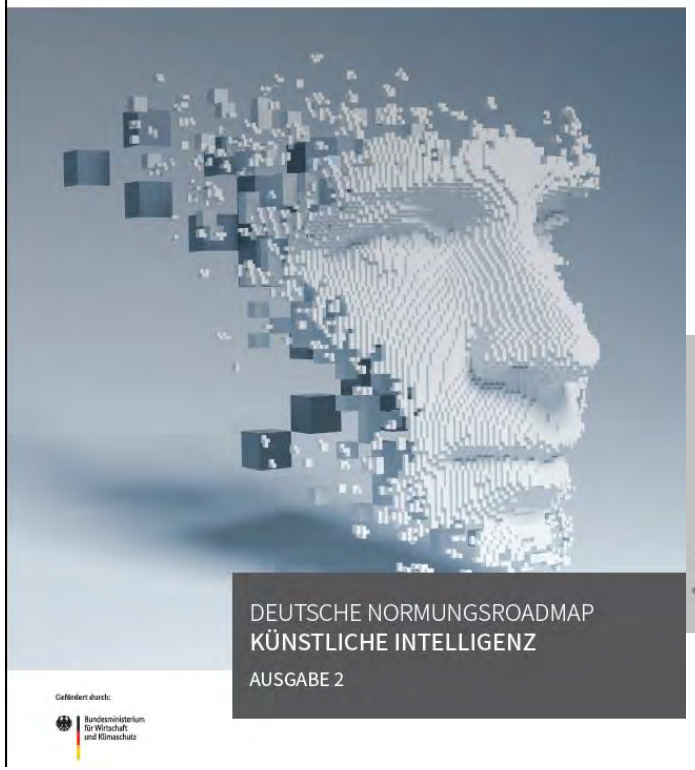
Das führende Element ist das Systeme-Engineering bzw. das übergreifende Risikomanagement!

Kontakt.

Stefan Ditting
Product Manager, Brühl

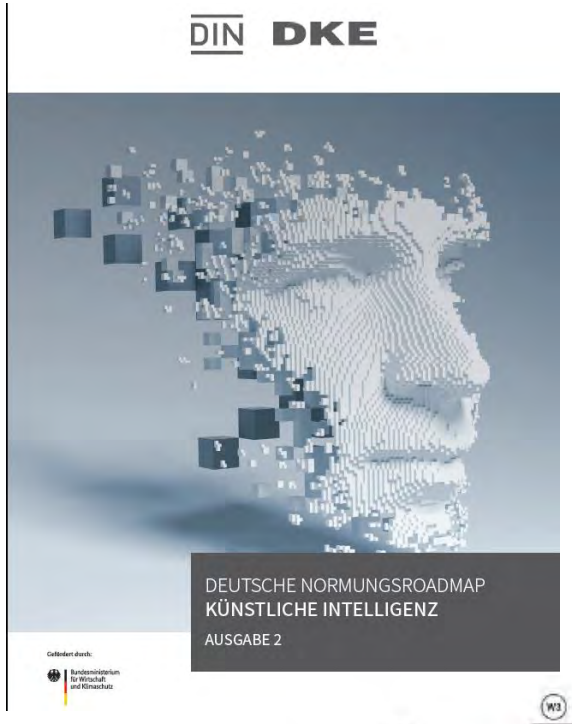
M +49 172 7750583
Email s.ditting@hima.com
www.hima.com

SICHER NAVIGIEREN AUF DER NORMUNGSROADMAP KI

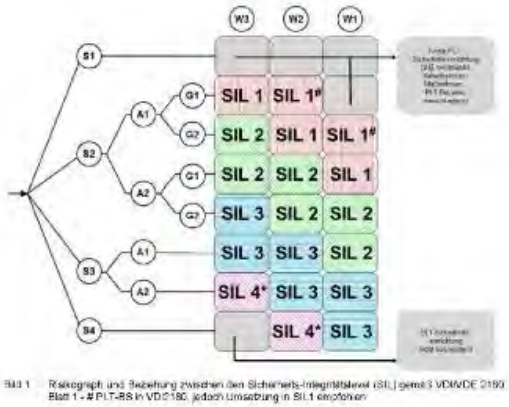


Marco Knödler
– NAMUR WG 4.5 – VDI/VDE-GMA FA 2.18 & 3.22
– DIN NA 003-01-01 AA - CEN/TC 69/WG 1 -
– DKE 914.0.11 & STD_1941.0.8 - SCI 4.0 Expert Panel AI in Industrial Applications
FS Eng (TÜV Rheinland, # 5762/12, SIS - # 5716/12, Machinery)

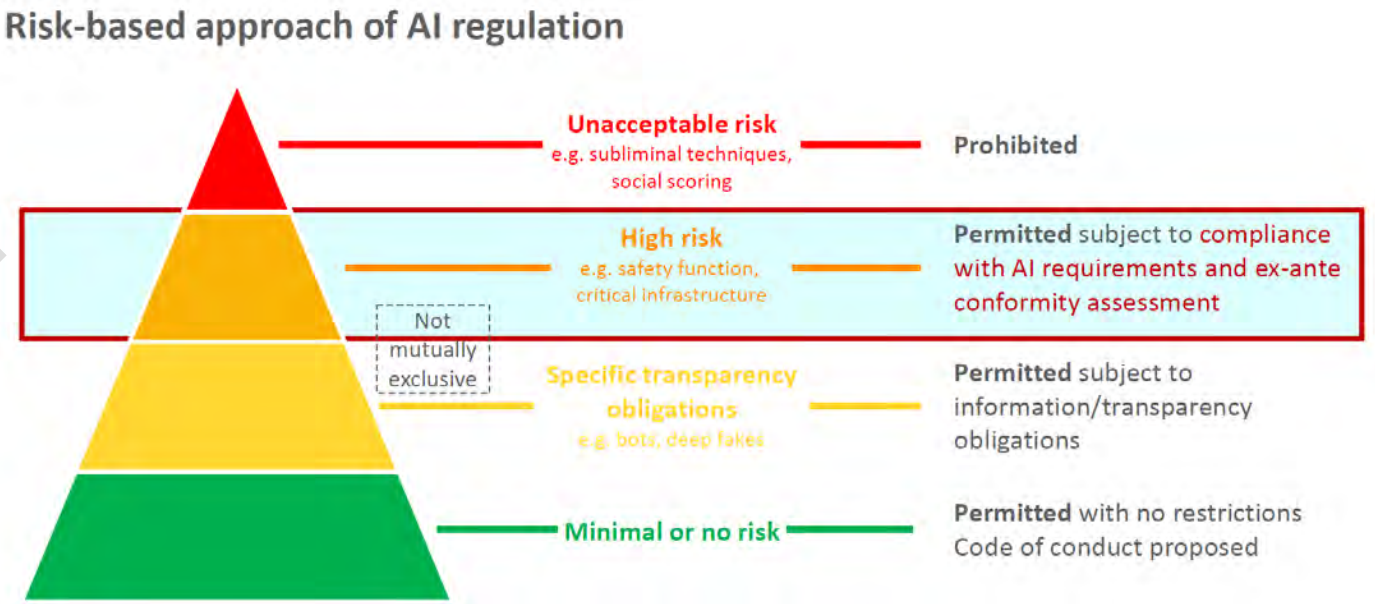
SICHER NAVIGIEREN AUF DER NORMUNGSROADMAP (NRM) KI



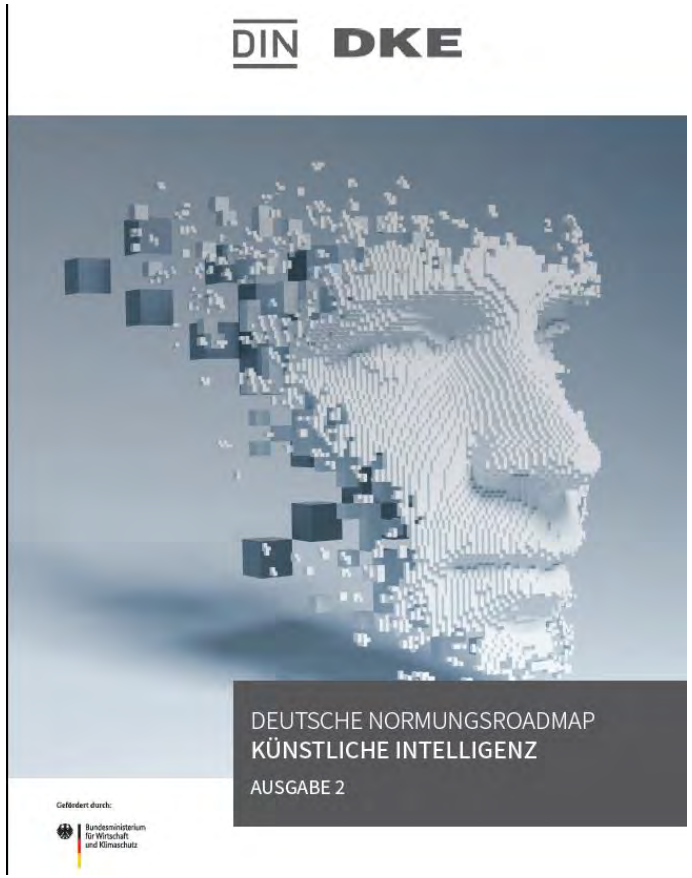
- „Mit der Normungsroadmap wird eine Maßnahme der KI-Strategie der Bundesregierung umgesetzt und damit ein wesentlicher Beitrag zur „**KI – Made in Germany**“ geleistet.
- Die Normung ist Teil der KI-Strategie und ein strategisches Instrument zur Stärkung der Innovations- und Wettbewerbsfähigkeit der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



?



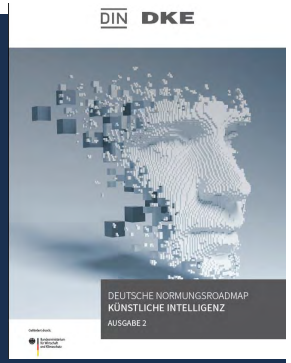
SICHER NAVIGIEREN AUF DER NORMUNGSROADMAP (NRM) KI



- „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.

NRM KI (2.0) – VERTRAUENSWÜRDIGE SAFETY

- **Nennung „Safety“ 238x**
- **Herausforderung:**
  - Safety nimmt eine Sonderstellung unter den Trustworthiness-Aspekten ein



- Vertrauenswürdigkeit (Trustworthiness) = Fähigkeit, Erwartungen nachweislich zu erfüllen.
- Merkmale der Vertrauenswürdigkeit:
  - Zuverlässigkeit
  - Verfügbarkeit
  - Belastbarkeit
  - Sicherheit (im Sinne von Security und Safety),
  - Datenschutz
  - Verantwortlichkeit
  - Transparenz
  - Integrität
  - Authentizität
  - …

Erklärbarkeit (explainability)	Angestrebte Eigenschaft eines KI-Systems, dass Faktoren, die zu einer automatisierten Entscheidung des Systems geführt haben, durch einen Menschen „verstanden“ werden können.
Interpretierbarkeit (interpretability)	Der Grad der Nachvollziehbarkeit der Funktionsweise einer zugrunde liegenden (KI-)Technologie.
Transparenz (transparency)	Verfügbarkeit einer offenen, verständlichen und zugreifbaren Darstellung von Informationen zu funktionalen Aspekten eines KI-Systems. Dies beinhaltet u. a. die Erklärbarkeit das KI-Systems (z. B. neuronale Netze), die Nachvollziehbarkeit des Datenschutzkonzepts sowie Informationen zu Qualitätssicherungsprozessen während der Entwicklung

Erwähnt in ISO/IEC 22989:2022, zentrale Eigenschaft der „sicheren KI“, die jedoch gleich einer Matrjoschka-Schachtelpuppe in sich geschachtelt Eigenschaften birgt.

„ZUVERLÄSSIGE KI“ – EIN FALL FÜR PROBABILISTIK?

Neuronalen Netzen muss eine epistemische Unsicherheit zugeordnet werden

An diesem Beispiel zeigt sich auch, dass Machine Learning als „gefühlt-nicht-deterministisch“ (Dr. Henrik Putzer) bezeichnet werden kann: Nicht immer liefert eine Syste komponente auf Basis von maschinellem Lernen die erwarteten Ergebnisse. Diese Fehlerm öglichkeit kann mit einer Unsicherheit (uncertainty) beschreiben werden. In der Hardware wird dies du ch die Ausfallrate oder das LAMBDA bezeichnet. Im Gegensatz zu dieser aleatorischen Unsicherheit n der Hardware (kann irgendwann zufällig z. B. durch Alterung ausfallen) muss dem Neuronalen N tz eine epistemische Unsicherheit zugeordnet werden (eine Fehlerkennung eines Fußgängerbildes wird immer wieder gleich fehlerhaft ausfallen, ist aber allgemein nicht vorherzusagen). Genau diese Eigenschaft bereitet dem Sicherheitsdenkenden Probleme. Um dies zu handhaben wird n neuer Kennwert, das LAMBDA-AI, vorgeschlagen (Dr. Henrik Putzer). Doch die Methoden zur Erm tlung des LAMBDA-AI sind noch in der Erforschung. Klar ist, dass der Entwicklungsprozess, die Metrik n und ggfs. auch die Analyse des vom Neuronalen Netz gelernten Wissens eine Rolle spielen werden.

Probabilistik?

Erfurter Tage 2019 - Dr. Henrik Putzer | Melanie Kahl / CEF

$$PFD_{1oo1,AI} = PTC_0 \boldsymbol{\lambda_{AI}} \frac{T_0}{2} + (PTC_1 - PTC_0) \boldsymbol{\lambda_{AI}} \frac{T_1}{2} + (1 - PTC_1) \boldsymbol{\lambda_{AI}} \frac{T_2}{2} \; ?$$

besser sein als ein Mensch?

https://www.dke.de/de/news/2019/vde-dke-kongress-funktionale-sicheheit-industrie40-ki

UND WENN ICH MIR „UNSICHER“ BIN?

- **Nennung „Safety“ 238x**
- **Herausforderung:**
  - Safety nimmt eine Sonderstellung unter den Trustworthiness-Aspekten ein
- **Handlungsempfehlung:**
  - Horizontale KI-Basis-Sicherheitsnorm erstellen
- **Normungs- und Standardisierungsbedarf:**
  - Methoden zur Introspektion und zum Nachweis von Safety und Zuverlässigkeit von KI

“VDE-AR-E 2841-61-5:2021 schlägt eine Art Lambda KI vor”

With some AI technologies (e.g. neuronal networks) we see a third type of failure: the *uncertainty-related failure*. This failure cannot be mitigated by good processes and established metrics. It is a characteristics and new kind of failure that is inherent to the technology of neuronal networks and some other machine learning approaches (see [5]). To handle this third kind of failure the *uncertainty confidence indicator* (UCI) is introduced (see Figure 4 and [5]).

type of failure	measures	HW measures	SW measures	AI measures
systematic	qualitative requirements	systematic capability	systematic capability	systematic capability
random	quantitative requirements	λ, SFF, DC, target values	-- / --	-- / --
uncertainty-related	structured approach	-- / --	-- / --	Uncertainty confidence indicator (UCI)

Probabilistik+?

Figure 4: Three Types of Failures plus Mitigating Measures

- [VDE-AR-E 2841-61-5:2021, “Specification and Design of autonomous / cognitive Systems - Part 5: Development at Technology Level”;

PROBABILISTICS UNCERTAINTY VS. CONFIDENCE INDICATOR

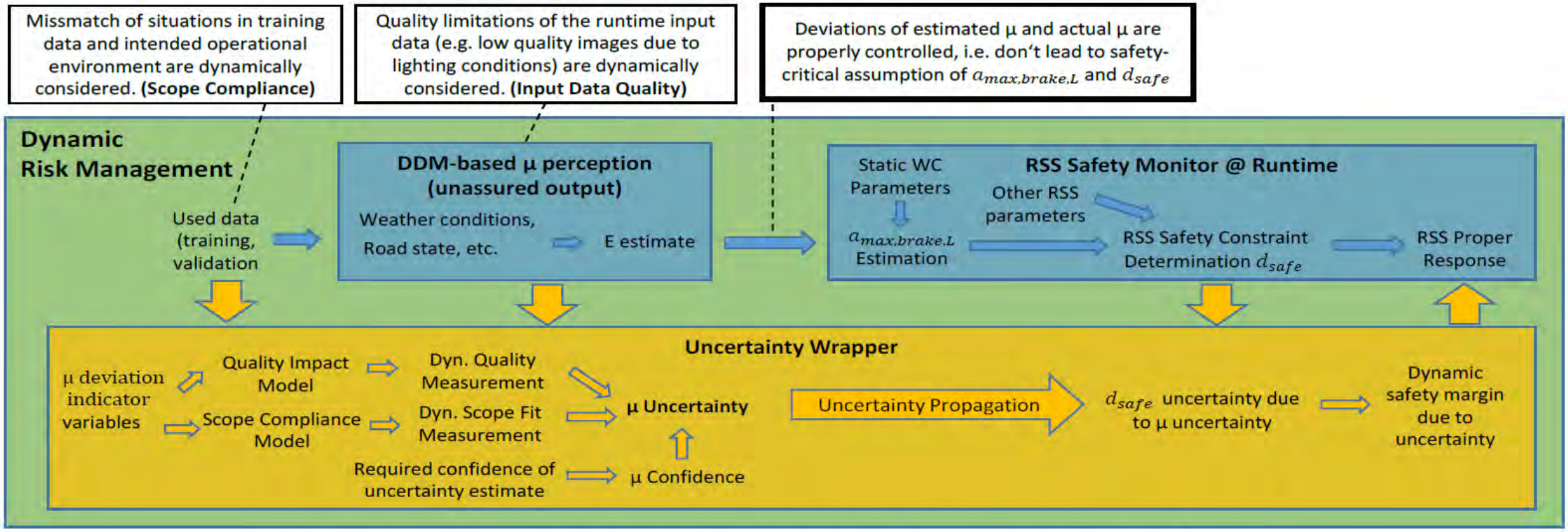


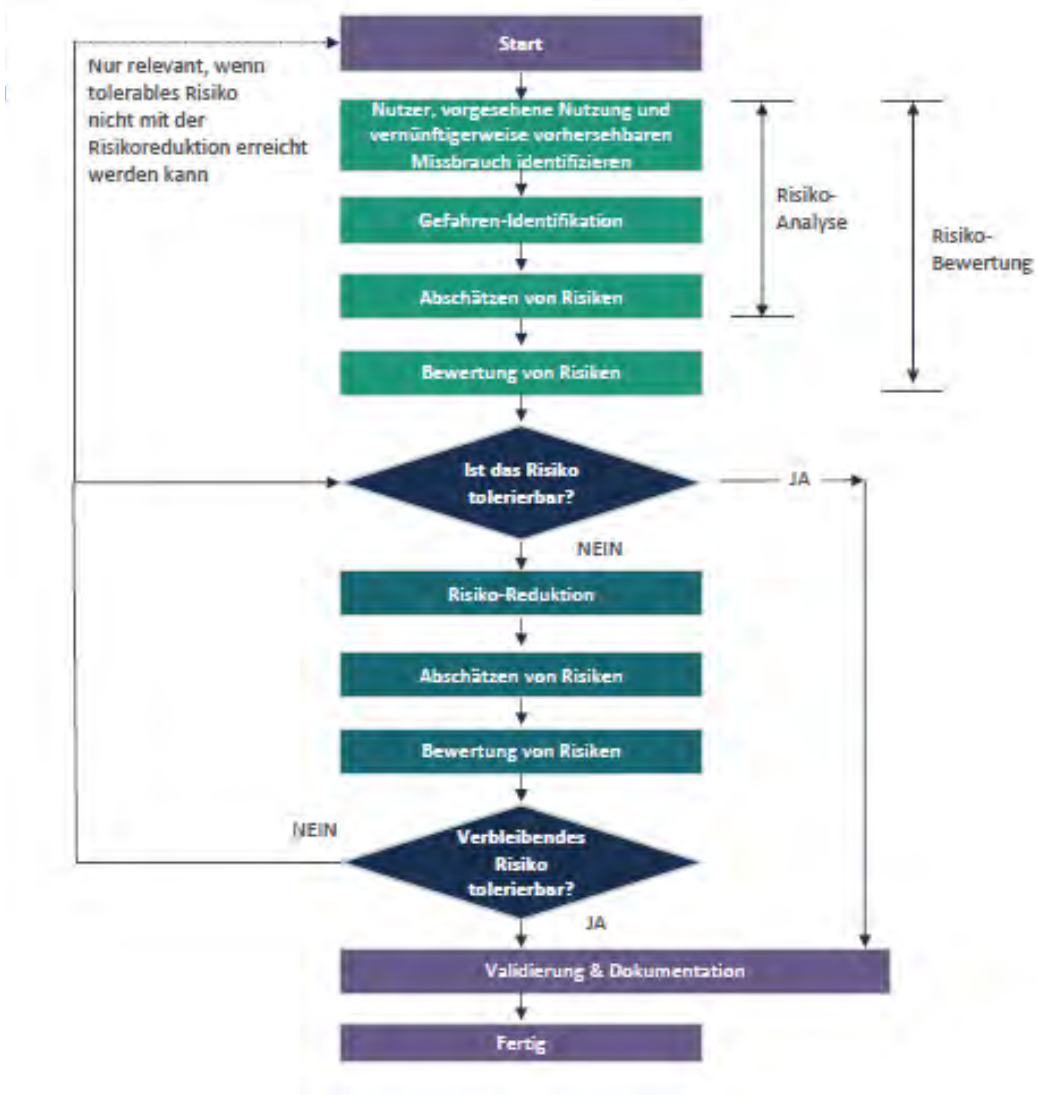
Fig. 3. Uncertainty Wrappers enable using data-driven models for assured dynamic RSS Monitoring

(Responsibility-Sensitive Safety)

https://www.researchgate.net/profile/Ioannis-Sorokos/publication/351659571_Handling_Uncertainties_of_Data-Driven_Models_in_Compliance_with_Safety_Constraints_for_Autonomous_Behaviour/links/60a39746299bf1d21d6ee26f/Handling-Uncertainties-of-Data-Driven-Models-in-Compliance-with-Safety-Constraints-for-Autonomous-Behaviour.pdf

NRM AI (2.0) – WHAT TO EXPECT FOR SAFETY

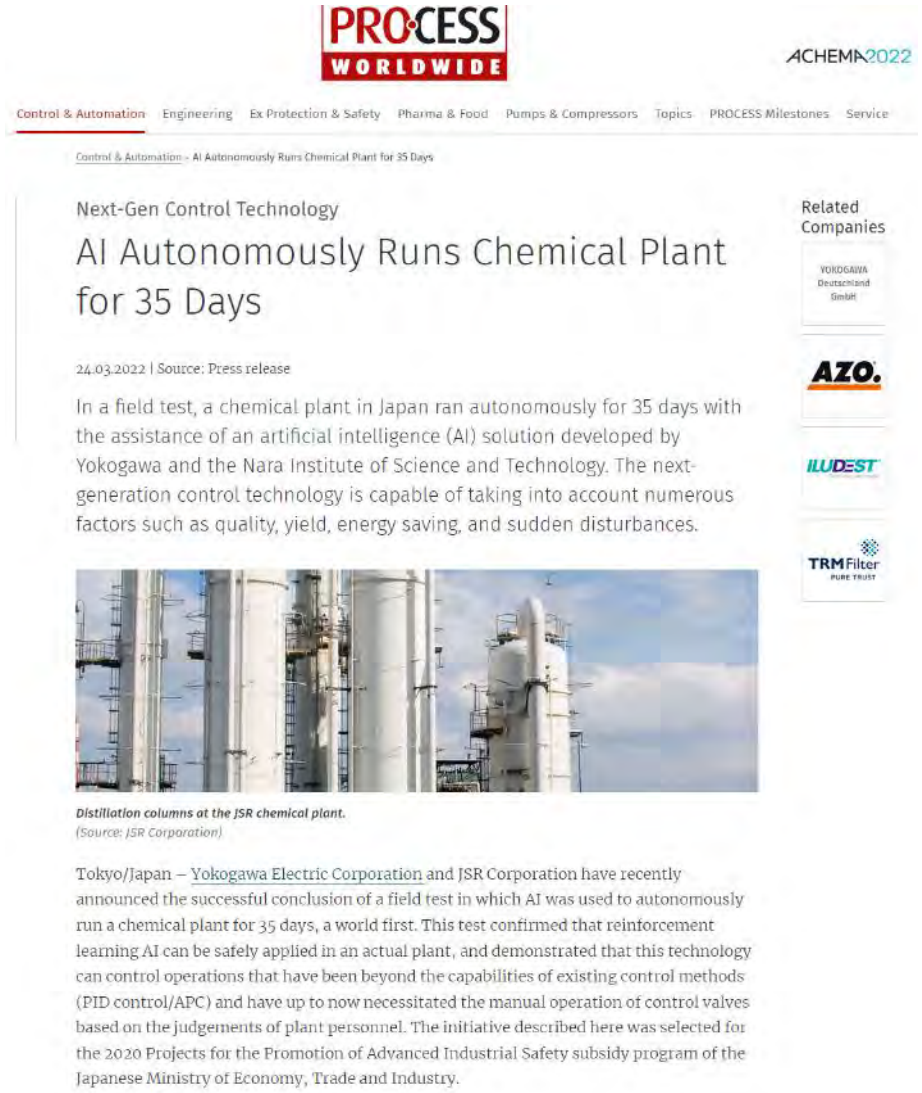
- **Nennung „Safety“ 238x**
- **Herausforderung:**
  - Safety nimmt eine Sonderstellung unter den Trustworthiness-Aspekten ein
- **Handlungsempfehlung:**
  - Horizontale KI-Basis-Sicherheitsnorm erstellen
- **Normungs- und Standardisierungsbedarf:**
  - Methoden zur Introspektion und zum Nachweis von Safety und Zuverlässigkeit von KI
  - anwendungsspezifische Risikoakzeptanzkriterien.
- **<u>„Ein Einsatz von KI im Safety-Kontext muss seinen Platz in iterativer Vorgehensweise der Risikobewertung (in Anlehnung an ISO/IEC Guide 51:2014) finden“</u>**



A WORLD FIRST… WHAT`S NEXT?

- https://www.process-worldwide.com/
- ai-autonomously-runs-chemical-plant-for-35-days
- -a-1105250/?cmp=nl-317&uuid=916df1653133e864a95560eb0a0782fc

- **„[…] This test confirmed that reinforcement learning AI can be safely applied in an actual plant, and demonstrated that this technology can control operations that have been beyond the capabilities of existing control methods (PID control/APC) and have up to now necessitated the manual operation of control valves based on the judgements of plant personnel.”**



PROCESS WORLDWIDE

ACHEMA2022

Control & Automation | Engineering | Ex Protection & Safety | Pharma & Food | Pumps & Compressors | Topics | PROCESS Milestones | Service

Control & Automation » AI Autonomously Runs Chemical Plant for 35 Days

Next-Gen Control Technology

AI Autonomously Runs Chemical Plant for 35 Days

24.03.2022 | Source: Press release

In a field test, a chemical plant in Japan ran autonomously for 35 days with the assistance of an artificial intelligence (AI) solution developed by Yokogawa and the Nara Institute of Science and Technology. The next-generation control technology is capable of taking into account numerous factors such as quality, yield, energy saving, and sudden disturbances.

Related Companies

YOKOGAWA Deutschland GmbH

AZO.

ILUDEST

TRM Filter PURE TRUST

Distillation columns at the JSR chemical plant.
(Source: JSR Corporation)

Tokyo/Japan – Yokogawa Electric Corporation and JSR Corporation have recently announced the successful conclusion of a field test in which AI was used to autonomously run a chemical plant for 35 days, a world first. This test confirmed that reinforcement learning AI can be safely applied in an actual plant, and demonstrated that this technology can control operations that have been beyond the capabilities of existing control methods (PID control/APC) and have up to now necessitated the manual operation of control valves based on the judgements of plant personnel. The initiative described here was selected for the 2020 Projects for the Promotion of Advanced Industrial Safety subsidy program of the Japanese Ministry of Economy, Trade and Industry.

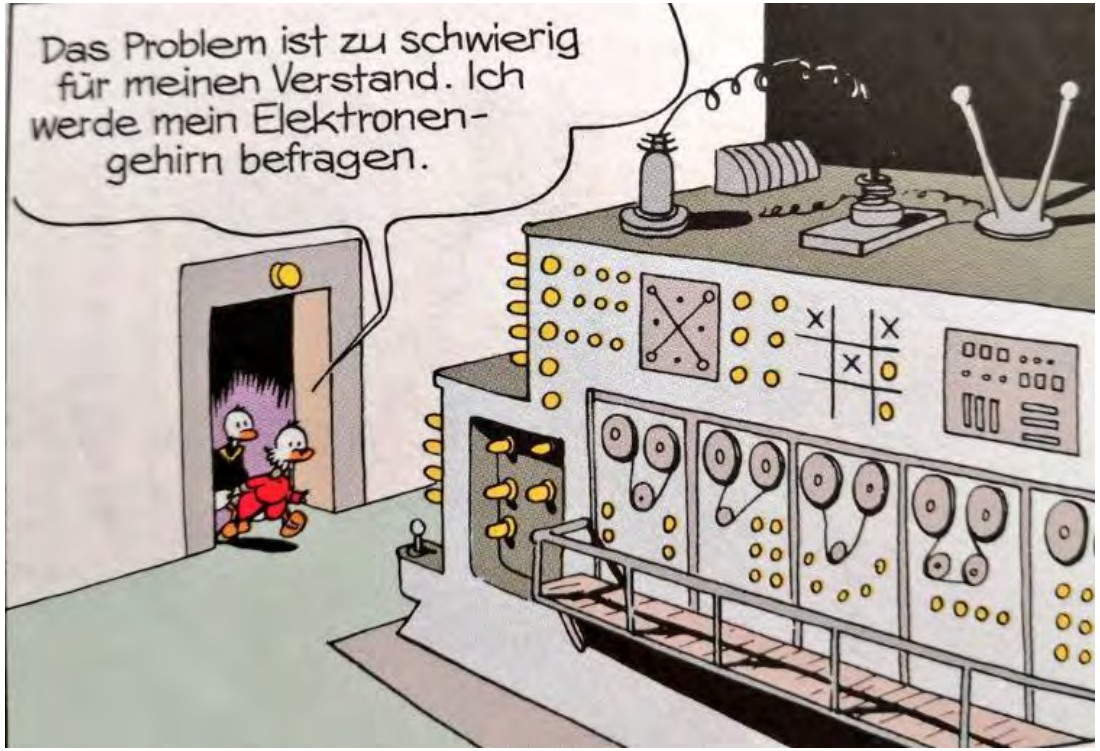
„AUTONOM“… SIND SIE SICHER?

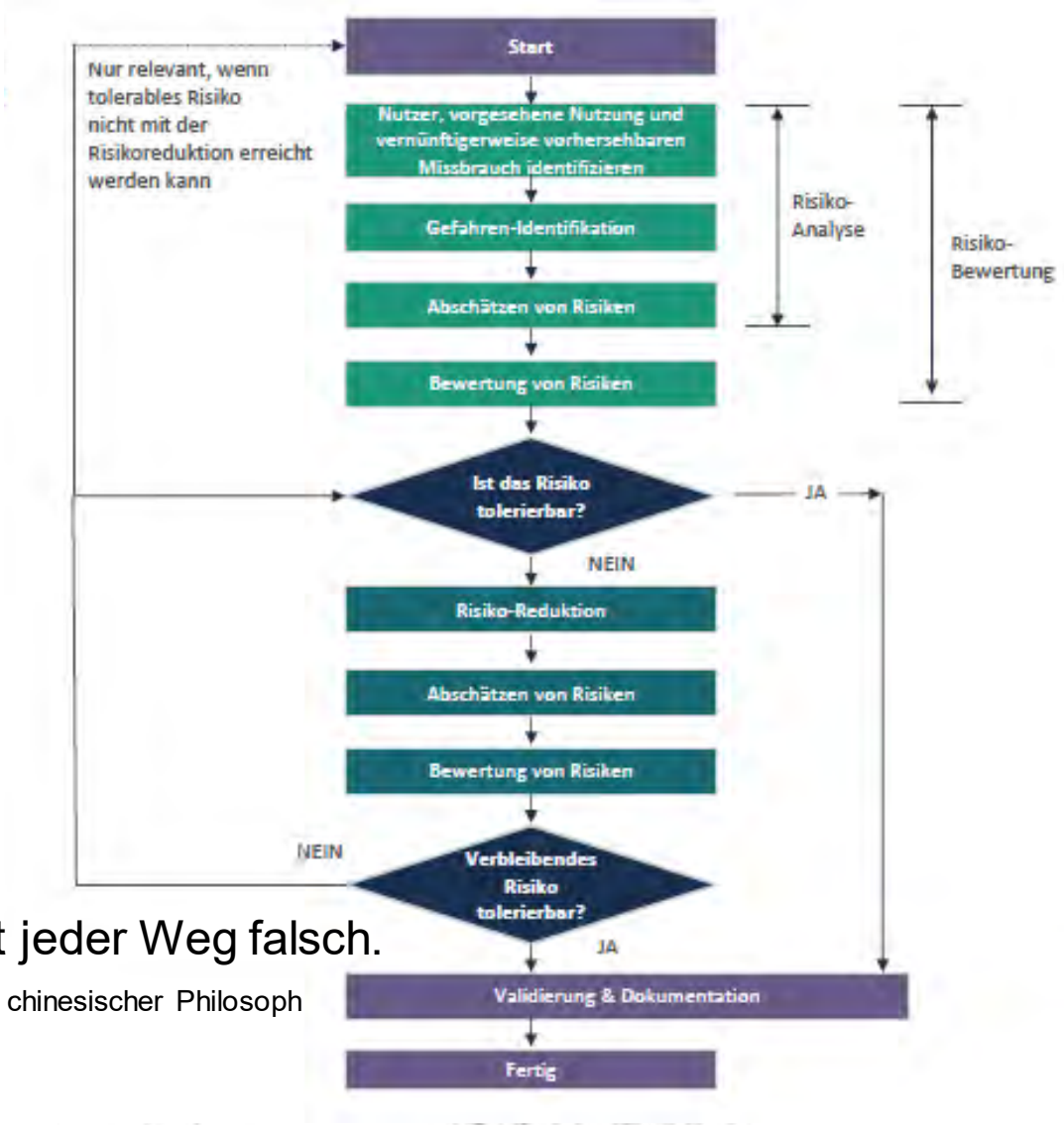
		Level of automation	Comments
Automated system	Autonomous	Autonomy	The system is capable of modifying its operating domain or its goals without external intervention, control or oversight.
	Heteronomous	Full automation	The system is capable of performing its entire mission without external intervention
		High automation	The system performs parts of its mission without external intervention
		Conditional automation	Sustained and specific performance by a system, with an external agent being ready to take over when necessary
		Partial automation	Some sub-functions of the system are fully automated while the system remains under the control of an external agent
		Assistance	The system assists an operator
		No automation	The operator fully controls the system

Japanese Ministry of Economy, Trade and Industry.

Autonomie gemäß ISO/IEC 22989:2022

KONFUZIUS SAGT…





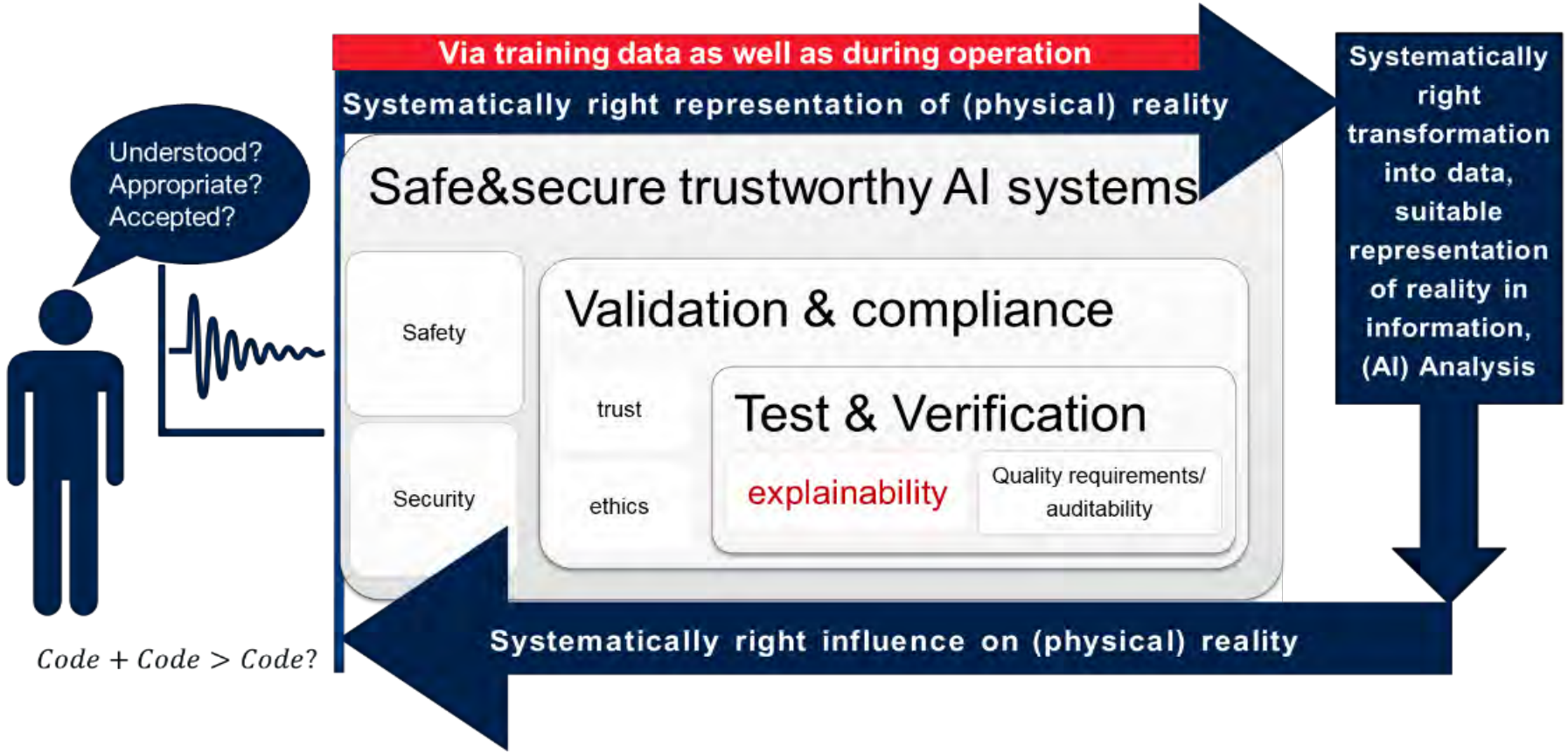
Ohne Ziel ist jeder Weg falsch.

Konfuzius, chinesischer Philosoph

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)



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

VDI-Handlungsleitfaden

„Gebrauchsdauer in der funktionalen Sicherheit“

Ende der Gebrauchsdauer erreicht – was nun ?

„Auslöser“ für den VDI-Handlungsleitfaden

- Auf die Fa. EICHLER GmbH kamen vermehrt Kunden zu mit der Bitte, an ihren SPS-Baugruppen einen Proof-Test durchzuführen

- Nach eingehender Recherche wurde festgestellt, dass nicht nur zum Thema „Proof-Test“, sondern vor allem auch zum Thema „Gebrauchsdauer“ in den Fachkreisen stark unterschiedliche Meinungen gegeben sind

- Problem 1: Kunde (= Betreiber der Maschine / Anlage) hat davon am wenigsten Ahnung
  Problem 2: Kunde muss aktuell nach Ablauf der Gebrauchsdauer die entsprechende/n Funktionseinheit/en austauschen – was nach z.B. 20 Jahren schwierig bis unmöglich ist
  => durch einen Umbau / ein Retrofit könnte er die Maschine / Anlage „am Leben“ erhalten
  => ist dies aber technisch/wirtschaftlich nicht vertretbar, muss er abschalten !!!

- 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

Inhalt

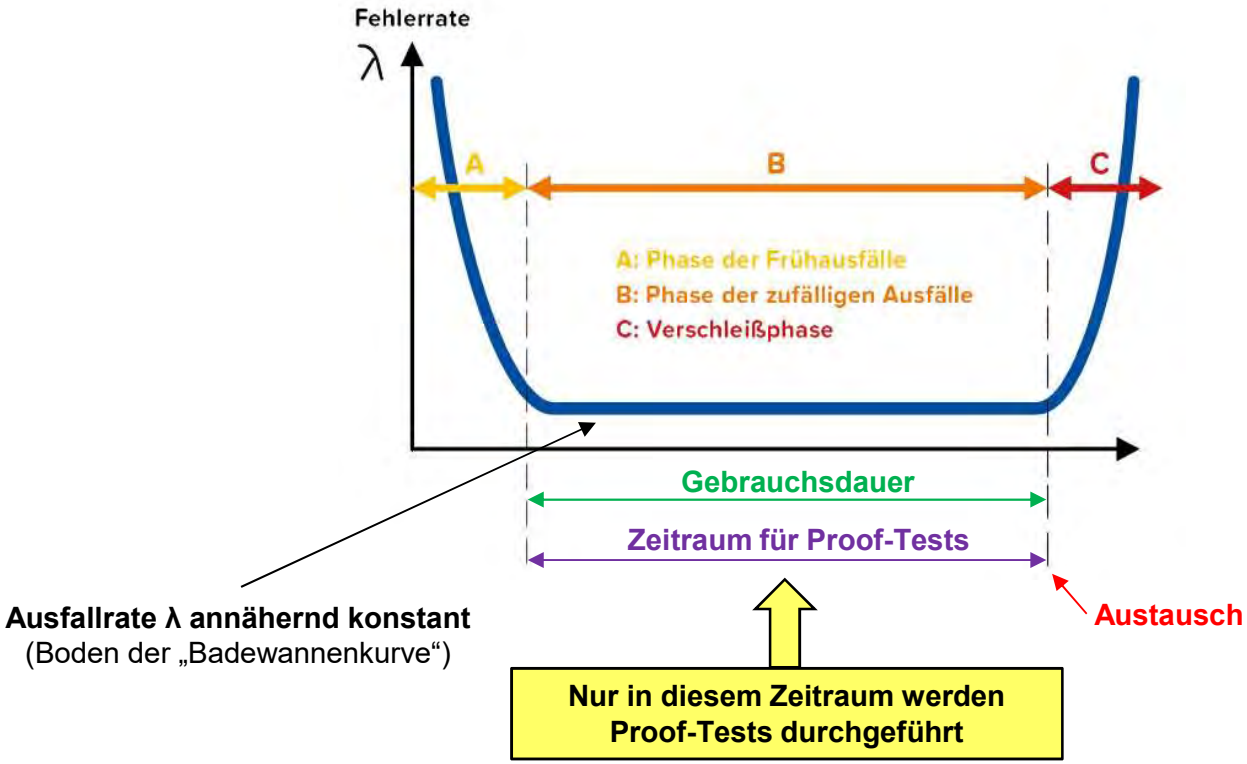
- Das Kapitel 1 ist für den Betreiber bestimmt. Hier wurde speziell darauf geachtet, dass die „fachliche Flughöhe“ niedrig gehalten wurde

- In diesem Kapitel 1 wird erläutert:
    - was ist die Gebrauchsdauer
    - wodurch wird sie beeinflusst
    - wann „startet“ die Gebrauchsdauer
    - Verhalten am Ende der Gebrauchsdauer
    - …

- Das Kapitel 2 ist ausgerichtet für den fachlich Interessierten => beinhaltet weiterführende Informationen und Erläuterungen

- Der Handlungsleitfaden befindet sich aktuell in der letzten Überarbeitungsrunde. Voraussichtlicher Termin der Veröffentlichung wird Ende Sommer / Anfang Herbst 2023 sein

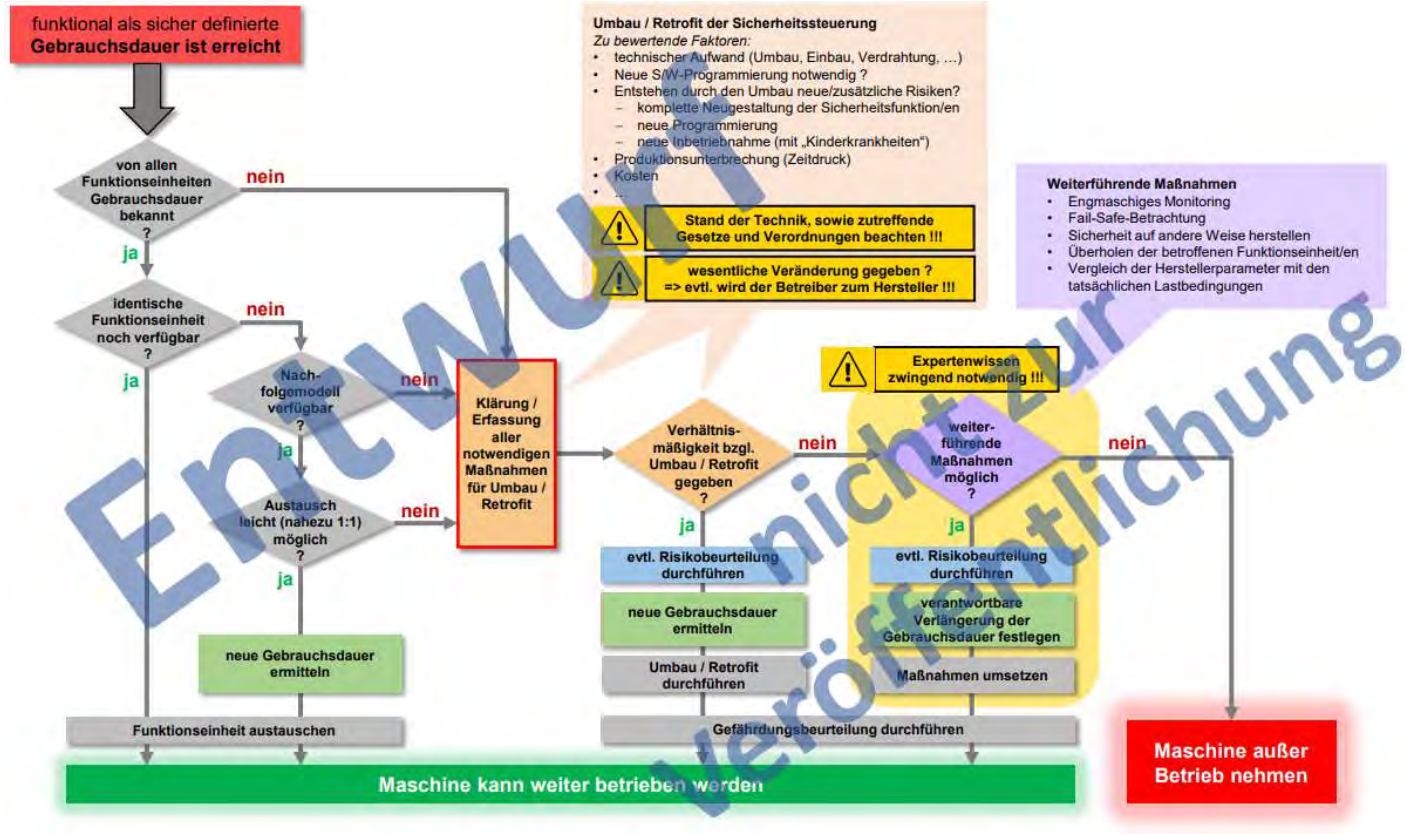
Gebrauchsdauer = Zeitraum für Proof-Tests



Definition „Funktionseinheit“

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

Entscheidungswege für den Betreiber



EICHLER GmbH

Elektronik-Service-Center
und Schulungszentrum

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

Peter Arnold

Entwicklung
CE-Koordinator

Tel.: +49 8196 9000-786
peter.arnold@eichler-service.de

Überarbeitung der TRGS 725

Funktionale Sicherheit im Explosionsschutz

SIL-Slam 2023

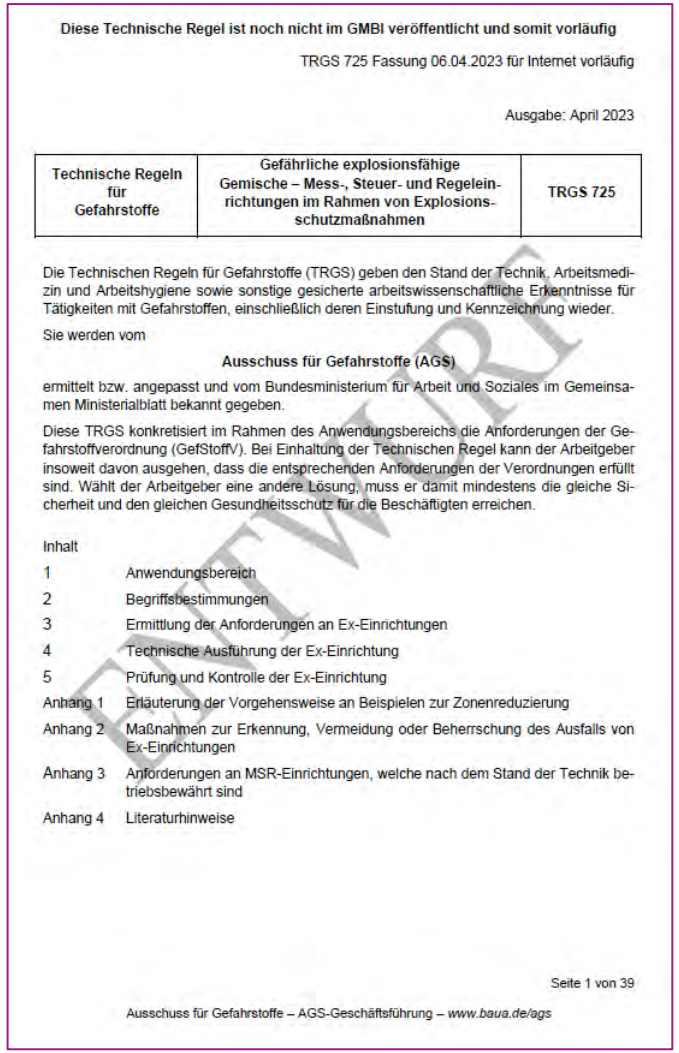
Marl, 03. Mai 2023 | Martin Herrmann Evonik Operations GmbH

EVONIK
Leading Beyond Chemistry

Explosionsschutz und Funktionale Sicherheit

Welche **Sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen** fallen unter den Anwendungsbereich der TRGS 725?

Überarbeitung der TRGS 725



Diese Technische Regel ist noch nicht im GMBl veröffentlicht und somit vorläufig

TRGS 725 Fassung 06.04.2023 für Internet vorläufig

Ausgabe: April 2023

Technische Regeln für Gefahrstoffe	Gefährliche explosionsfähige Gemische – Mess-, Steuer- und Regeleinrichtungen im Rahmen von Explosionsschutzmaßnahmen	TRGS 725

Die Technischen Regeln für Gefahrstoffe (TRGS) geben den Stand der Technik, Arbeitsmedizin und Arbeitshygiene sowie sonstige gesicherte arbeitswissenschaftliche Erkenntnisse für Tätigkeiten mit Gefahrstoffen, einschließlich deren Einstufung und Kennzeichnung wieder.

Sie werden vom

Ausschuss für Gefahrstoffe (AGS)

ermittelt bzw. angepasst und vom Bundesministerium für Arbeit und Soziales im Gemeinsamen Ministerialblatt bekannt gegeben.

Diese TRGS konkretisiert im Rahmen des Anwendungsbereichs die Anforderungen der Gefahrstoffverordnung (GefStoffV). Bei Einhaltung der Technischen Regel kann der Arbeitgeber insoweit davon ausgehen, dass die entsprechenden Anforderungen der Verordnungen erfüllt sind. Wählt der Arbeitgeber eine andere Lösung, muss er damit mindestens die gleiche Sicherheit und den gleichen Gesundheitsschutz für die Beschäftigten erreichen.

Inhalt

Ausschuss für Gefahrstoffe – AGS-Geschäftsführung – *www.baua.de/ags*

Überarbeitung der TRGS 725

Diese Technische Regel ist noch nicht im GMBl veröffentlicht und somit vorläufig

TRGS 725 Fassung 06.04.2023 für Internet vorläufig

Ausgabe: April 2023

Technische Regeln für Gefahrstoffe	**Gefährliche explosionsfähige Gemische – Mess-, Steuer- und Regeleinrichtungen im Rahmen von Explosionsschutzmaßnahmen**	**TRGS 725**

Die Technischen Regeln für Gefahrstoffe (TRGS) geben den Stand der Technik, Arbeitsmedizin und Arbeitshygiene sowie sonstige gesicherte arbeitswissenschaftliche Erkenntnisse für Tätigkeiten mit Gefahrstoffen, einschließlich deren Einstufung und Kennzeichnung wieder.

Sie werden vom

Ausschuss für Gefahrstoffe (AGS)

Überarbeitung der TRGS 725

Wesentliche Inhalte der neuen TRGS 725:

- Überarbeitung der Begriffe => ~~Ex-Vorrichtung = Ex-Einrichtung + Überwachung~~
- **Neu:** MSR Einrichtung für den Explosionsschutz **=> Ex-Einrichtung**
- Wegfall der Reduzierungsstufen
- Ersatz von “Ausfallverhalten” durch “Zuverlässigkeit”
- Neue Begriffe:
  - ✓ **Verfügbarkeit** der Explosionsschutzmaßnahmen (ausreichend, hoch oder sehr hoch)
  - ✓ **Zuverlässigkeit** der Ex-Einrichtung (K1, K2 oder K3)
- Ermittlung der Anforderungen an Ex-Einrichtung erfolgt nach Festlegung der Ex-Maßnahmen nach TRGS 722-724

Überarbeitung der TRGS 725

NACH WIE VOR GILT:

TRGS 725 Nummer 3.2 Gefährdungsbeurteilung:

(1).....

(7) Die …. dargestellten Anforderungen an die Verfügbarkeit der Explosionsschutzmaßnahmen sind **nur anwendbar**, **wenn das Auftreten gefährlicher explosionsfähiger Atmosphären und das Wirksamwerden von Zündquellen voneinander unabhängig sind**.

(8) Die Fälle, in denen keine Unabhängigkeit zwischen dem Auftreten der gefährlichen explosionsfähigen Atmosphäre und der Zündquelle gegeben ist, **erfordern eine gesonderte Betrachtung in der Gefährdungsbeurteilung.**

Überarbeitung der TRGS 725

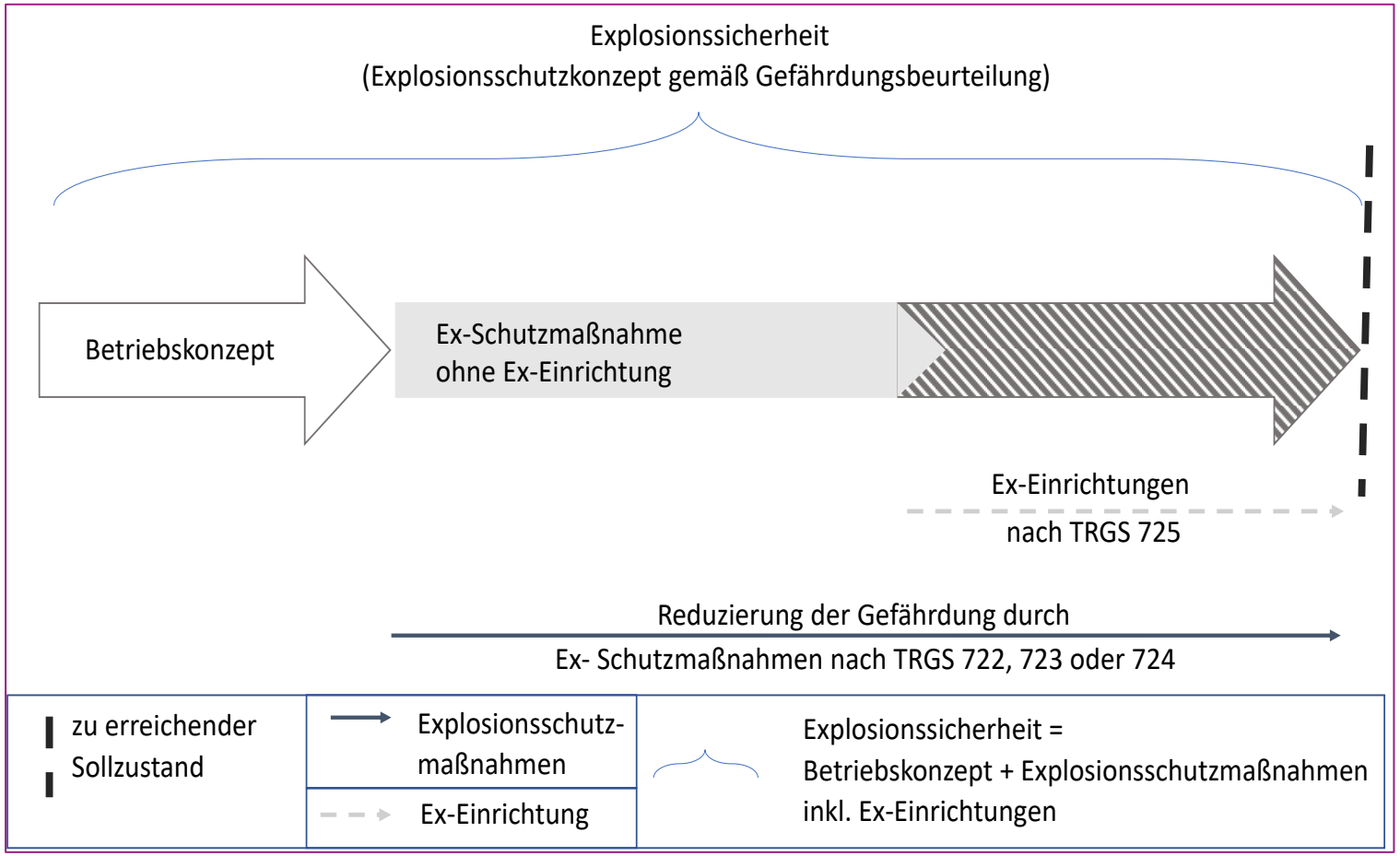


Abbildung 1: Explosionsschutzmaßnahmen und Ex-Einrichtungen

Überarbeitung der TRGS 725

Ausgangssituation unter Berücksichtigung des Betriebskonzeptes	**Explosionsschutzmaßnahme** (Verfügbarkeit)	Zielzone
	Ex-Einrichtung (Zuverlässigkeit)	

Zone 0/20	Sehr hoch	keine Zone
	hoch — K1	
	ausreichend — K2	
	K3	

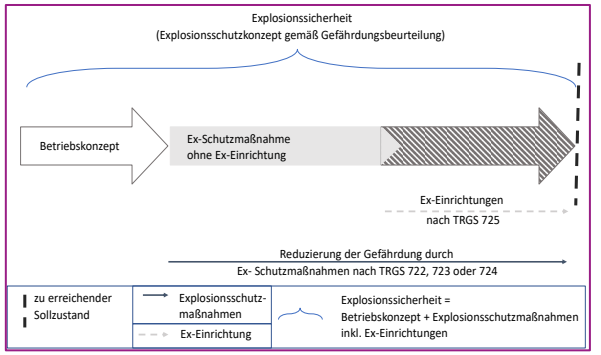


Abbildung 3: Bestimmung der erforderlichen Klassifizierungsstufe in Abhängigkeit von der Ausgangssituation

Überarbeitung der TRGS 725

Ausgangssituation unter Berücksichtigung des Betriebskonzeptes	**Explosionsschutzmaßnahme** (Verfügbarkeit) **Ex-Einrichtung** (Zuverlässigkeit)	**Zielzone**
Zone 0/20	Sehr hoch hoch – K1 ausreichend – K2 K3	keine Zone
	hoch ausreichend – K1 K2	Zone 2/22
	ausreichend K1	Zone 1/21

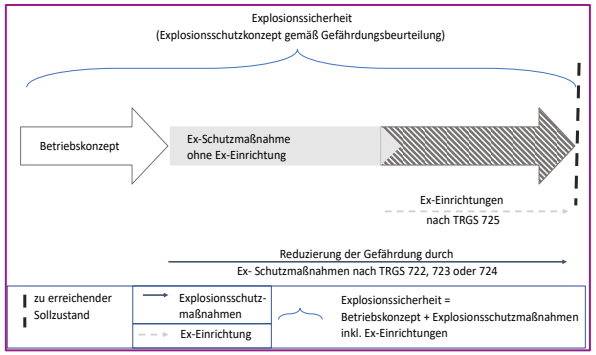


Abbildung 3: Bestimmung der erforderlichen Klassifizierungsstufe in Abhängigkeit von der Ausgangssituation

Überarbeitung der TRGS 725

Fortsetzung: Wesentliche Inhalte der neuen TRGS 725:

- Klarstellung zur Umsetzung nach etablierten Methoden der funktionalen Sicherheit:
  Ausstieg aus der weiteren Bearbeitung nach TRGS 725
- Die Klassifizierungsstufe beschreibt den Grad der erforderlichen **Zuverlässigkeit** einer Ex-Einrichtung oder Funktionseinheit
- **Fokus** im Hauptteil auf Ex-Einrichtungen mit **ausreichender Zuverlässigkeit (K1)** bzw. einfache Kombinationen
- Aufnahme von Beispielen im Anhang 1

Überarbeitung der TRGS 725

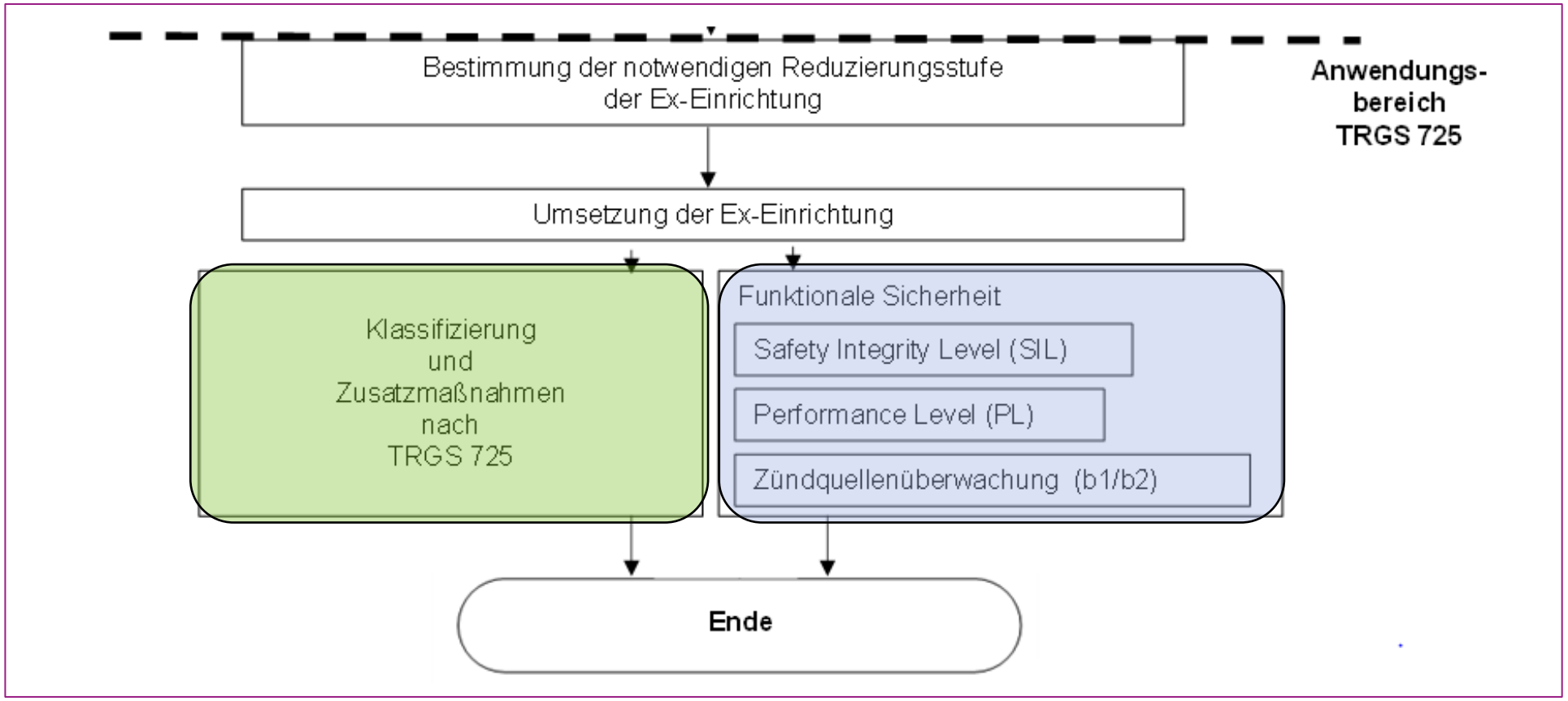


Abbildung 2: Vorgehensweise bei der Gefährdungsbeurteilung im Anwendungsbereich der TRGS 725

Überarbeitung der TRGS 725

Zugrunde liegende Norm	Anforderung für Klassifizierungsstufe		
	K3	K2	K1
DIN EN 61511	SIL[1] 3	SIL[1] 2	PLT-Betriebs-einrichtung als Schutzebene oder SIL[1] 1
DIN EN 62061	SIL[1] 3	SIL[1] 2	SIL[1] 1
DIN ISO 13849-1	PL[2] e	PL[2] d	PL[2] c, b[3]
DIN ISO 80079-37[4]	-	b2	b1
VDI/VDE 2180	SIL[1] 3	SIL[1] 2	PLT BS[5] oder SIL[1] 1

1 SIL, Safety Integrity Level

2 PL, Performance Level
Der Performance Level beschreibt die Anforderungen an die funktionale Sicherheit der sicherheitstechnischen Funktionen, w obei der Performance Level e den höchsten Grad der Sicherheitsintegrität, der Performance Level b den niedrigsten darstellt.

3 nach DIN EN ISO 13849-1: Kategorie B oder 1, MTTF mittel

4 Zündquellenüberwachung

5 Betriebseinrichtung mit Sicherheitsfunktion

Tabelle 3: Anforderungen an die funktionale Sicherheit in Abhängigkeit von der Klassifizierungsstufe.

TRGS 725

vs.

Funktionale Sicherheit

- VDI/VDE 2180
- TRBS 1115

Explosionsschutz und Funktionale Sicherheit

Eine **PLT-BS** oder eine **SIL 1** Einrichtung (i. S. der VDI/VDE 2180) können zur Realisierung einer **Klassifizierungsstufe 1** nach TRGS 725 verwendet werden!


EVONIK
Leading Beyond Chemistry

Auszug aus einem Prüfbericht

SIL Slam 03.05.2023

Auszug aus einem Prüfbericht

Folgendes (reales) Szenario:

- Anlagenteil, Prüfung vor Inbetriebnahme mit Prüfstelle
- Prüfung u.a. auch von Sicherheitskreisen nach TRGS725 mit SIL (z.B. Trockenlaufschutz Rührer)
- Bewertungskriterien: BetrSichV, TRGS725, DIN EN 61511

→ Prüfung ergab Mängel

- Geringfügige Mängel
- Erhebliche Mängel (Unverzüglich abzustellen)
- Gefährliche Mängel (Vor IBN abzustellen)

Auszug aus einem Prüfbericht

Prüfbericht:

- **Gefährliche Mängel (Vor IBN abzustellen)**
  - Teil einer Sicherheitseinrichtung fehlte (noch nicht fertiggestellt)
- **Erhebliche Mängel (Unverzüglich abzustellen)**
  - Verschraubung defekt
  - Fehlende SIL-Berechnungen
- **Geringfügige Mängel**
  - Prüfkonzept, Prüfprotokolle, Prüfanweisungen großteils unvollständig
  - Sicherheitshandbücher und Betriebsanleitungen, Zertifikate fehlen zum Teil
  - “Management der funktionalen Sicherheit fehlt”

Bildquelle: Pixabay

Auszug aus einem Prüfbericht

Prüfbericht:

- **Gefährliche Mängel (Vor IBN abzustellen)**
  - Teil einer Sicherheitseinrichtung fehlte (noch nicht fertiggestellt)
- **Erhebliche Mängel (Unverzüglich abzustellen)**
  - Verschraubung defekt
  - Fehlende SIL-Berechnungen
- **Geringfügige Mängel**
  - Prüfkonzept, Prüfprotokolle, Prüfanweisungen großteils unvollständig
  - Sicherheitshandbücher und Betriebsanleitungen, Zertifikate fehlen zum Teil
  - “Management der funktionalen Sicherheit fehlt”

Management der funktionalen Sicherheit fehlt…

Bildquelle: Pixabay

Auszug aus einem Prüfbericht

Interessantes und Bemerkenswertes - evtl. auch etwas, zum an die eigene Nase fassen…

- Durch ein Management der funktionalen Sicherheit wären vermutlich die meisten Fehler verhindert worden…

Gefährliche Mängel (Vor IBN abzustellen)

Teil einer Sicherheitseinrichtung fehlte (noch nicht fertiggestellt)

Erhebliche Mängel (Unverzüglich abzustellen)

Verschraubung defekt

Fehlende SIL-Berechnungen

Geringfügige Mängel

Prüfkonzept, Prüfprotokolle, Prüfanweisungen großteils unvollständig

Sicherheitshandbücher und Betriebsanleitungen, Zertifikate fehlen zum Teil

“Management der funktionalen Sicherheit fehlt”

Auszug aus einem Prüfbericht

Interessantes und Bemerkenswertes - evtl. auch etwas, zum an die eigene Nase fassen...

- Durch ein Management der funktionalen Sicherheit wären vermutlich die meisten Fehler verhindert worden...

Gefährliche Mängel (Vor IBN abzustellen)

Teil einer Sicherheitseinrichtung fehlte (noch nicht fertiggestellt)

Erhebliche Mängel (Unverzüglich abzustellen)

Verschraubung defekt

Fehlende SIL-Berechnungen

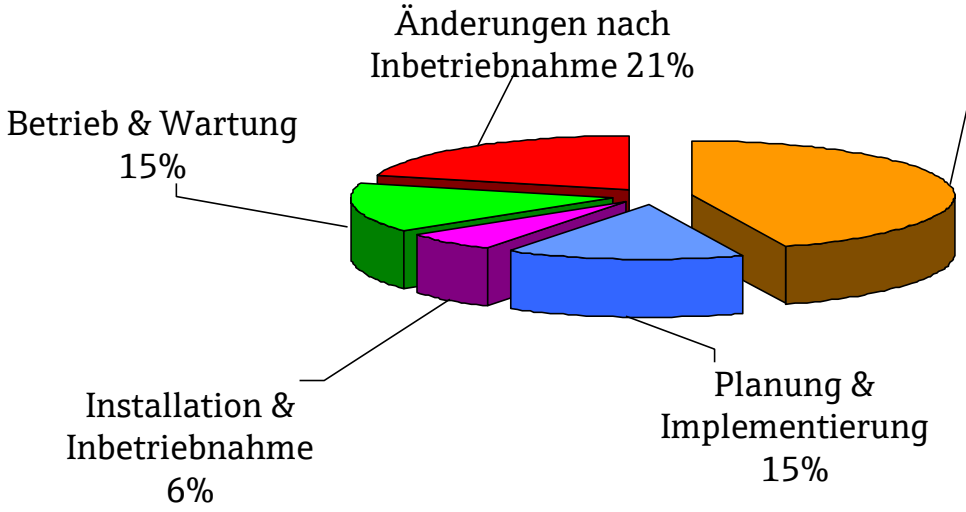
Geringfügige Mängel

Prüfkonzept, Prüfprotokolle, Prüfanweisungen großteils unvollständig

Sicherheitshandbücher und Betriebsanleitungen, Zertifikate fehlen zum Teil

Ziel eines Functional Safety Management Systems

Vermeidung systematischer Fehler...



...und diese überwiegen in der Praxis!

Ca. 60% aller Fehler, die zu Unfällen führten, sind bereits vor der Inbetriebnahme des Systems eingebaut (Quelle: Studie Health and Safety Executive, HSG 238 „out of control“, 2003). Hauptquelle für systematische Fehler ist in der Regel der Mensch.

Eine der Grundsäulen eines FSM: Prozessdefinition

Prozesse für Tätigkeiten im Sicherheitslebenszyklus mit Zuordnung der Verantwortlichkeiten

- Prozessabläufe, welche Tätigkeiten werden durchgeführt, wer macht was mit welcher Qualifikation, welche Prüfungen werden durchgeführt, Checklisten, welche Informationen werden benötigt, sind auszutauschen,…
- Schriftlich festgehalten und kommuniziert (z.B. in Prozessdokumentation) + regelmäßige Audits
- Prozessdefinition und Verfahren für mindestens die folgende Punkte:
- Gefährdungs- und Risikoanalyse, **Tätigkeiten zur Beurteilung der funktionalen Sicherheit**, **Verifikations- und Validierungstätigkeiten**, Konfigurationsmanagement, Bericht und Analyse von Zwischenfällen, Tätigkeiten nach Ereignissen und Unfällen, Verfahren für Audits, Vorgehensweisen bei Modifikationen, Konfigurationsmanagement der sicherheitsbezogenen Systeme
  (DIN EN 61508-1 6.2.5 bzw. DIN EN 61511-1 5.2.5.1)

Eine weitere Säule des Functional Safety Management Systems

Verifikationstätigkeiten

- Kontrolle (Überprüfung, Analyse, Tests), ob die getroffenen Massnahmen und durchgeführten Tätigkeiten zur Erreichung der funktionalen Sicherheit ausreichend und passend sind -> **Rückkopplung!**
- Verifikation mit Prüfungen nach dem 4-Augen-Prinzip für alle relevanten Punkte aus dem Sicherheitslebenszyklus
- Tests und Prüfungen nach Abschluss von Tätigkeiten, evtl. anhand von Checklisten
- Schriftlich dokumentiert (Ersteller/Prüfer)
- **Müssen geplant erfolgen -> Im Vorfeld Planen, wie Beurteilung erfolgt, Verifikationsplan**
- Validierung: Verifikation an der installierten Hardware
- **Beispiel: SIL-Nachweis -> Entspricht die entworfene SIS den Anforderungen?**

Auszug aus einem Prüfbericht

Interessantes und Bemerkenswertes - evtl. auch etwas, zum an die eigene Nase fassen…

- Durch ein Management der funktionalen Sicherheit wären vermutlich die meisten Fehler verhindert worden…

Gefährliche Mängel (Vor IBN abzustellen)

Teil einer Sicherheitseinrichtung fehlte (noch nicht fertiggestellt)

Erhebliche Mängel (Unverzüglich abzustellen)

Verschraubung defekt

Fehlende SIL-Berechnungen

Geringfügige Mängel

Prüfkonzept, Prüfprotokolle, Prüfanweisungen großteils unvollständig

Sicherheitshandbücher und Betriebsanleitungen, Zertifikate fehlen zum Teil

Auszug aus einem Prüfbericht

Zurück zum Prüfbericht…

- Prüfbericht weist fehlendes Management der funktionalen Sicherheit als geringfügigen Mangel aus.
- Mangel ist ggf. so schnell nicht behebbar
- Inbetriebnahme der Anlage deswegen stoppen?
- Wirklich geringfügiger Mangel?
- Meinungen, Erfahrungen aus dem Auditorium?

Bildquelle: Pixabay

Auszug aus einem Prüfbericht

Weiteres Fazit:

- Mit der Anwendung der TRGS725 mit SIL handelt man sich ggf. einen Rucksack ein…
- Wer nicht schon zuvor Sicherheitsfunktionen nach SIL umgesetzt hat, tut sich gegebenenfalls schwer.

Auszug aus einem Prüfbericht

Herzlichen Dank für Ihre Aufmerksamkeit!

Endress+Hauser

Funktionale Sicherheit für Monteure und Techniker

Welches Wissen ist für Arbeiten im Feld relevant.

Warum der Vortrag?

Ingenieursausbildung:

- Viel Theorie und Wissensaneignung im Studium
- Wenig „fassbare“ Praxis mit Industrie Bezug
- Ausnahmen

Aus- und Weiterbildung der eigenen Techniker:

- Wenig Zeit für Weiterbildung
- Kaum Ressourcen für digitale Wissensaneignung
- Wenig Bezug zum Planungsprozess

Was passiert, wenn nicht gewissenhaft gearbeitet wird?

Planer	Ausführender	Problem
Plant richtig	Führt Planung richtig aus	nein
Plant richtig	Führt Planung falsch aus	ja
Plant falsch	Führt Planung richtig aus	ja
Plant falsch	Führt Planung falsch aus	ja
Plant falsch	Erkennt Planungsfehler	nein

Jeder muss sich seiner Verantwortung bewusst sein!

Problem = Risiko!

Definition Risiko:

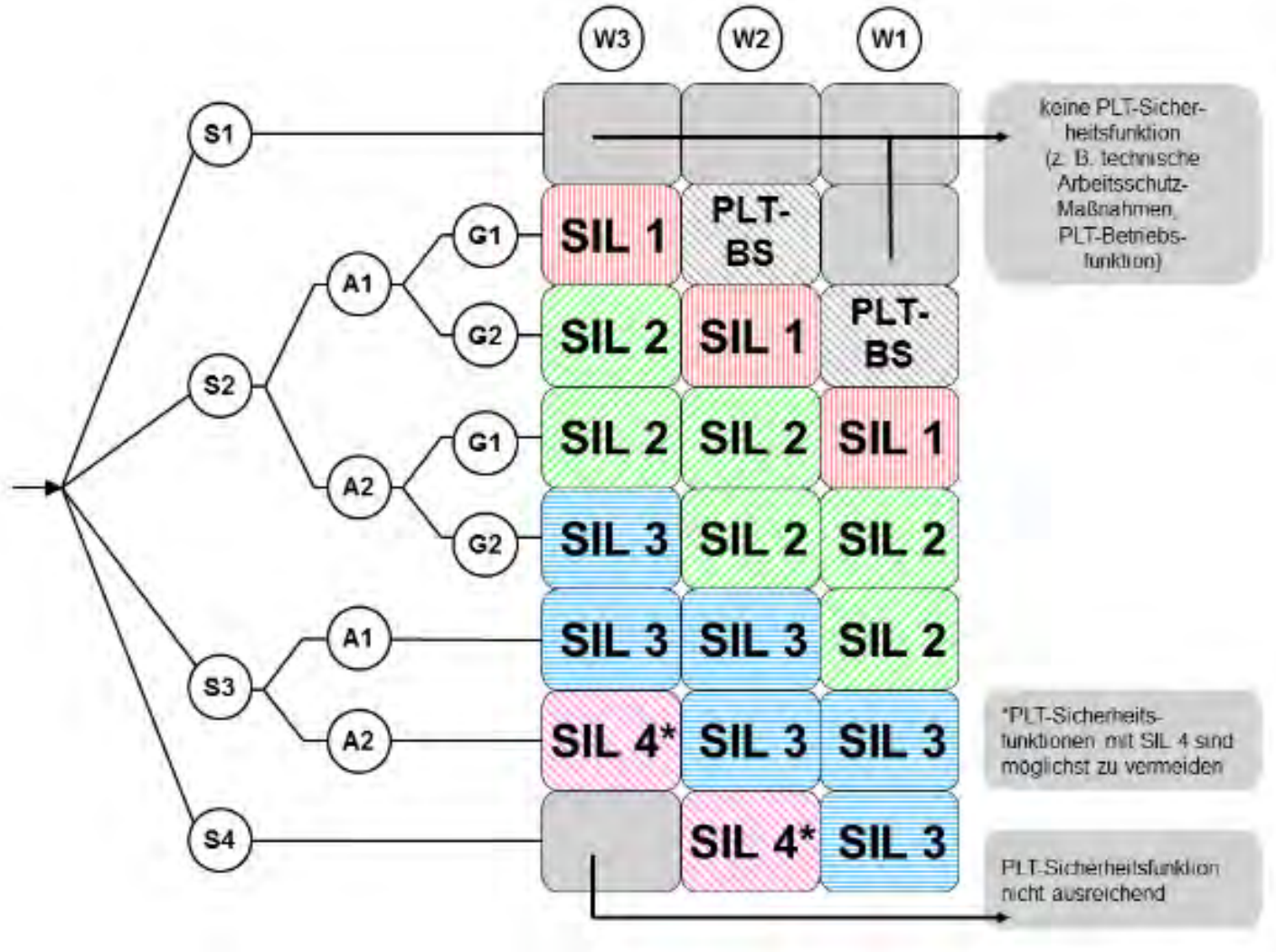
- „Kombination der Häufigkeit eines Schadenseintritts und seines Schadensausmaßes“
  VDE 2180 Blatt 1

=

- Eintrittswahrscheinlichkeit * Schadensausmaß

- Die Auswirkungen/ Schadensausmaß beziehen sich auf Personen- und Umweltschäden

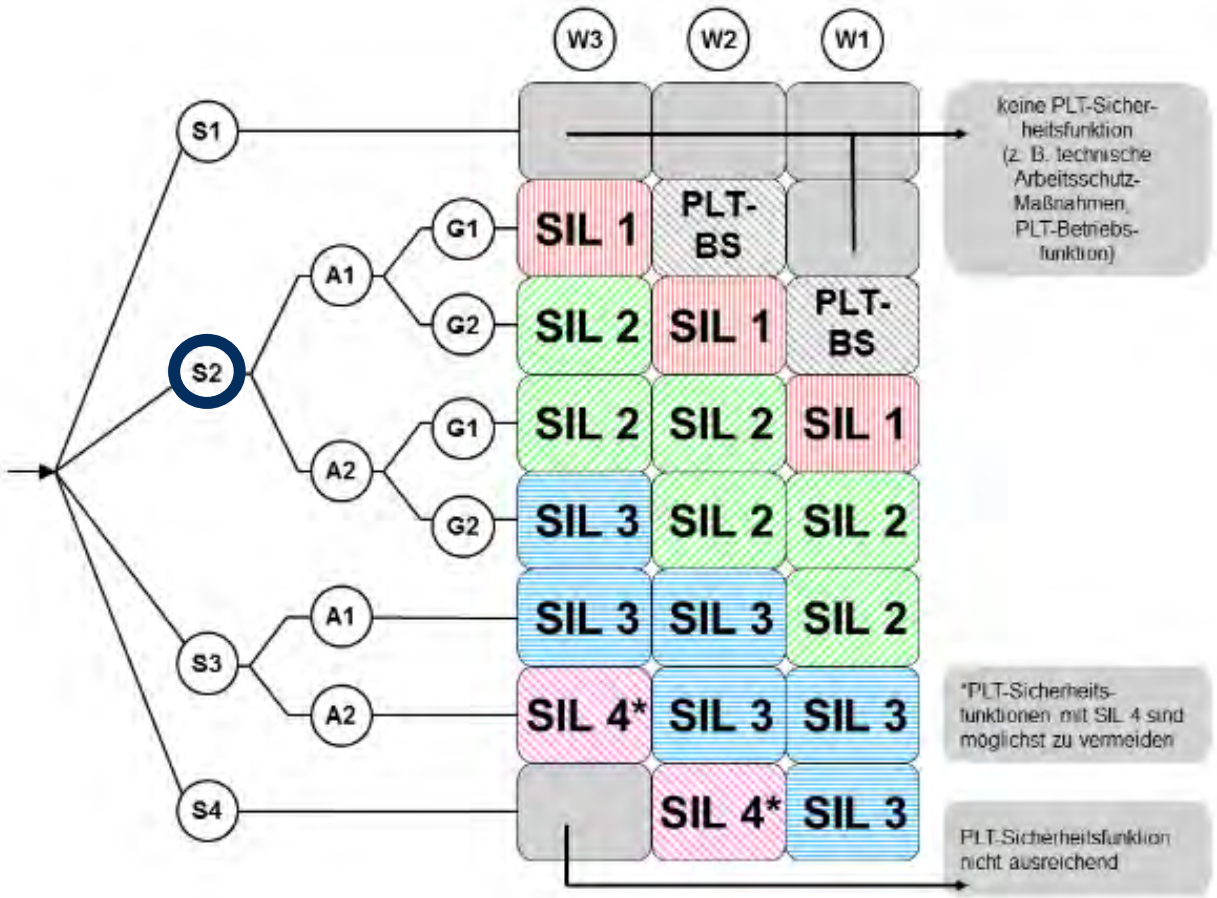
Methoden zur Risikoermittlung



Zuordnung zwischen Risikoparametern und den erforderlichen SIL anhand des Risikographen

Quelle: VDI/VDE 2180 Blatt 1, April 2019

Beispiel SIL 1:



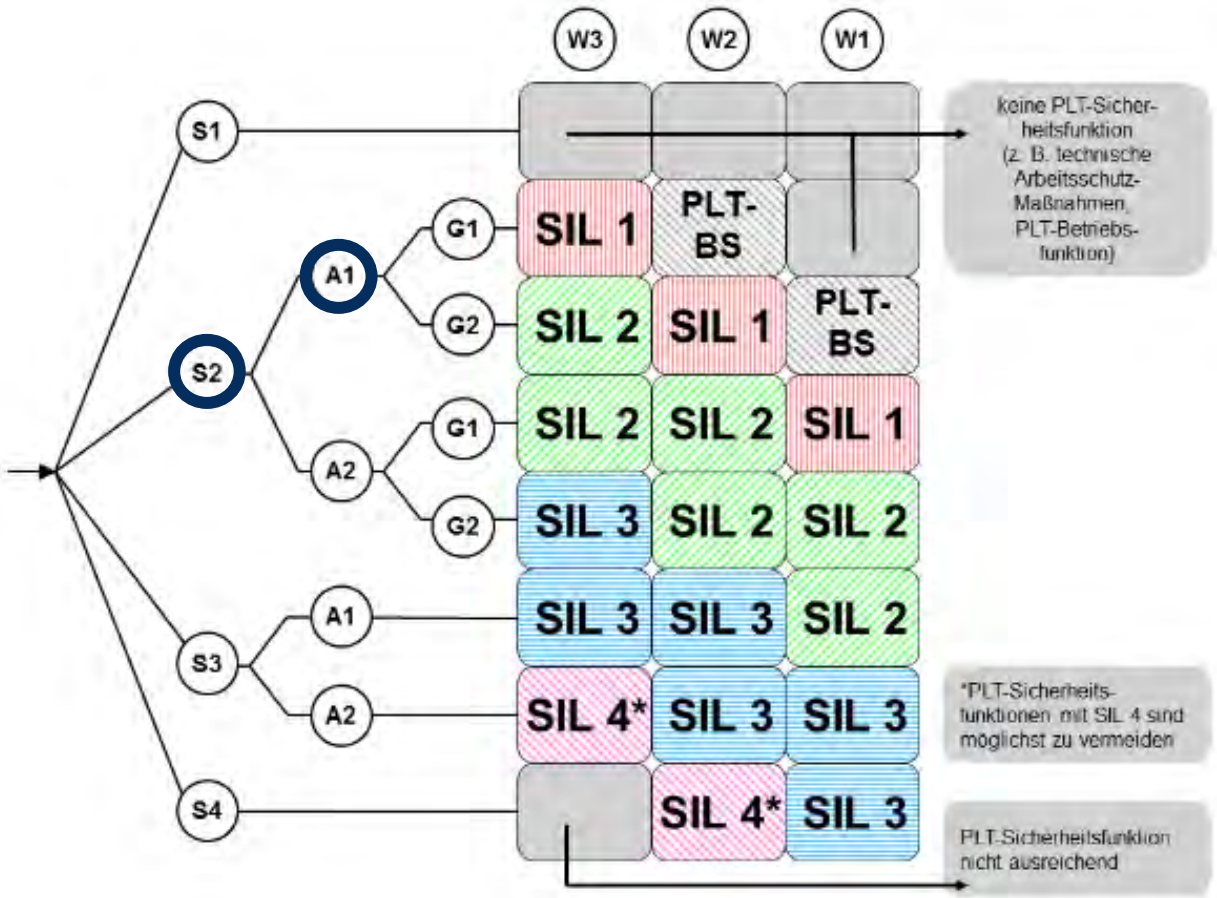
Zuordnung zwischen Risikoparametern und den erforderlichen SIL anhand des Risikographen

Quelle: VDI/VDE 2180 Blatt 1, April 2019

Schwere der Auswirkung (S):

- S2
  - schwere, bleibende Verletzung einer oder mehrerer Personen
  - Tod einer Person
  - vorübergehende größere schädliche Umwelteinflüsse, z.B. nach Störfallverordnung

Beispiel SIL 1:



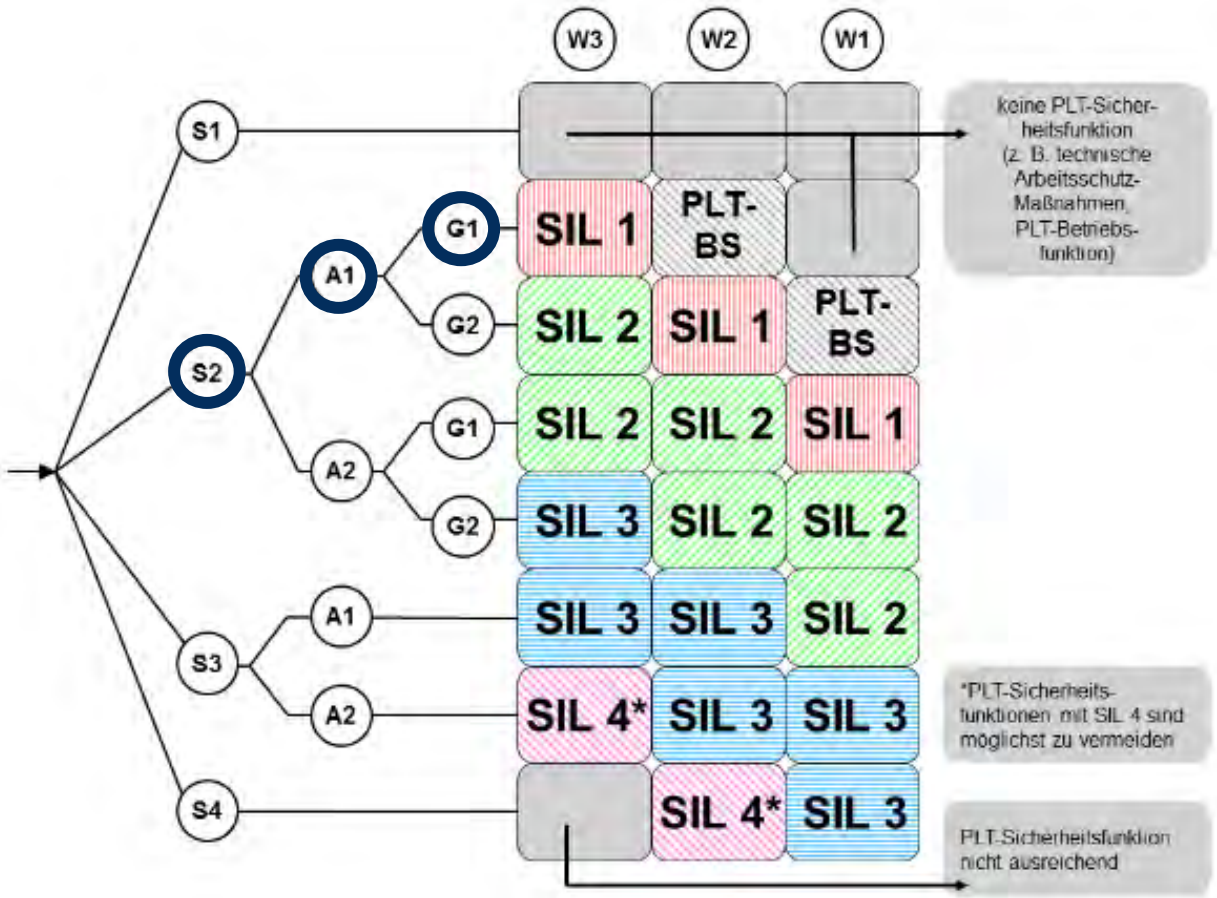
Zuordnung zwischen Risikoparametern und den erforderlichen SIL anhand des Risikographen

Quelle: VDI/VDE 2180 Blatt 1, April 2019

Aufenthaltshäufigkeit im gefährdeten Bereich multipliziert mit der Aufenthaltsdauer (A):

- A1
  - seltener bis häufiger Aufenthalt in der gefährdeten Zone

Beispiel SIL 1:



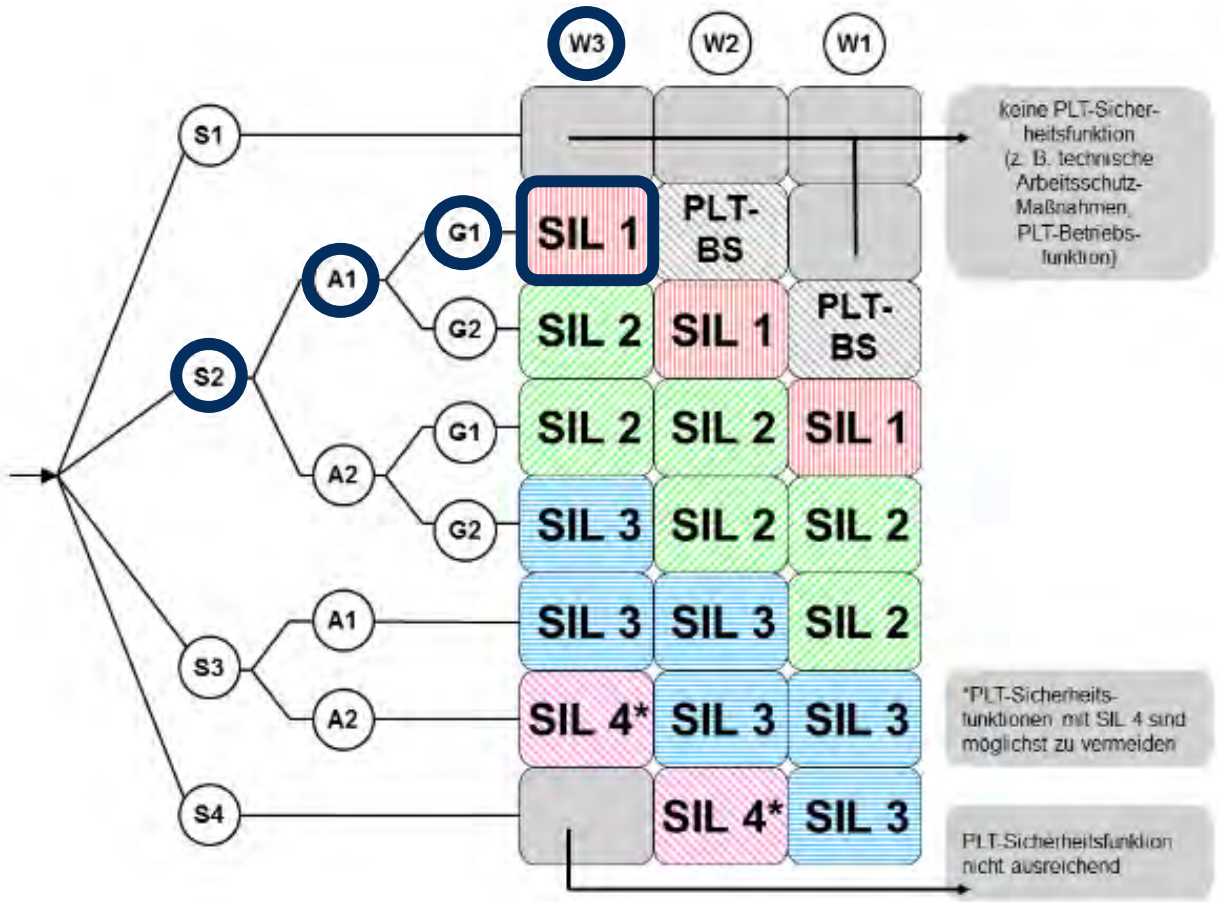
Zuordnung zwischen Risikoparametern und den erforderlichen SIL anhand des Risikographen

Quelle: VDI/VDE 2180 Blatt 1, April 2019

Möglichkeit, die Auswirkungen des gefährlichen Ereignisses zu vermeiden (G):

- G1
  - unter bestimmten Bedingungen möglich

Beispiel SIL 1:



Zuordnung zwischen Risikoparametern und den erforderlichen SIL anhand des Risikographen

Quelle: VDI/VDE 2180 Blatt 1, April 2019

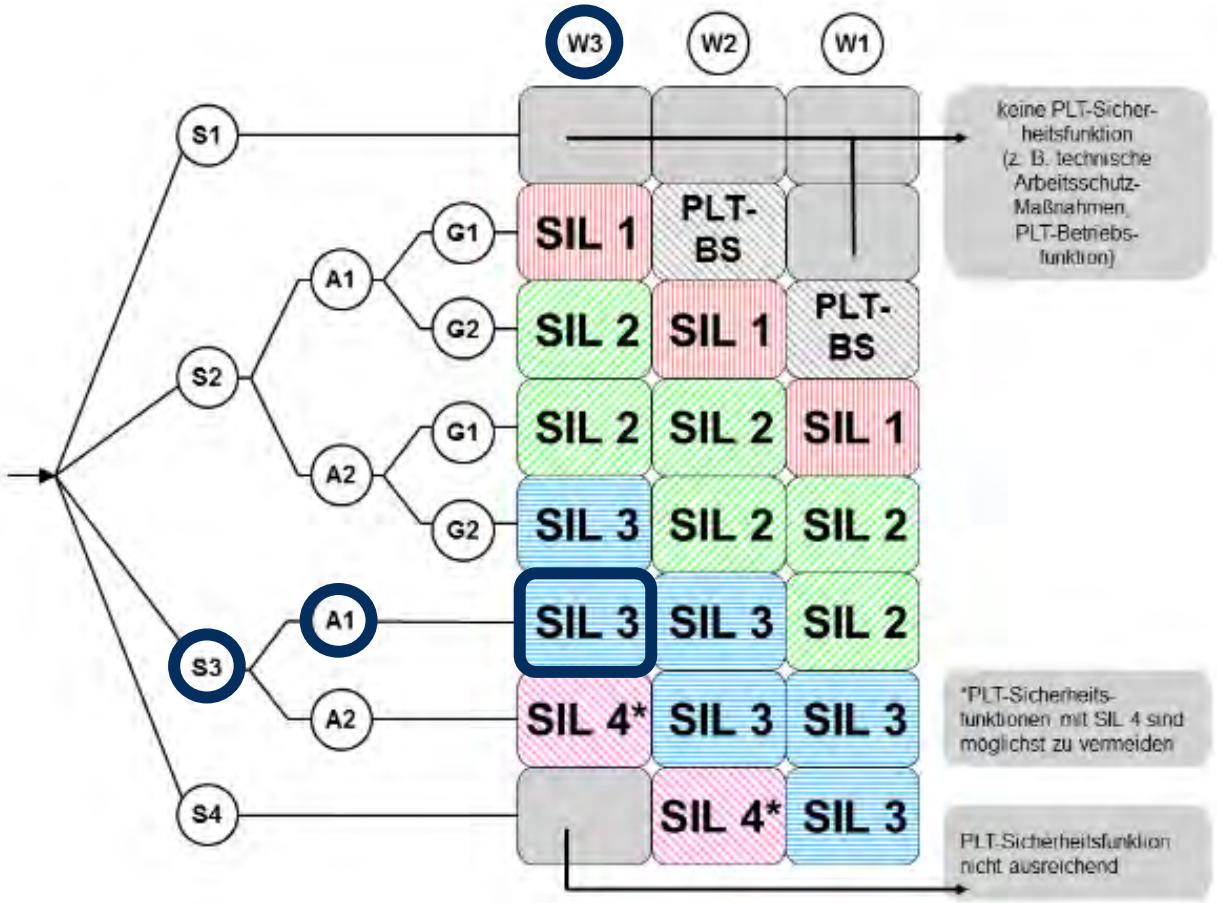
Wahrscheinlichkeit des unerwünschten Auftretens (W):

- W3
  - relativ hohe Wahrscheinlichkeit des unerwünschten Auftretens
  - häufige unerwünschte Ereignisse sind im betrachteten oder in ähnlichen Prozessen wahrscheinlich

Beispiel SIL 1:

- S2
  - schwere, bleibende Verletzung oder Tod einer Person
- A1
  - seltener bis häufiger Aufenthalt in der gefährdeten Zone
- G1
  - unter bestimmten Bedingungen möglich Auswirkungen zu vermeiden
- W3
  - relativ hohe Wahrscheinlichkeit des unerwünschten Auftretens

Beispiel SIL 3:



Zuordnung zwischen Risikoparametern und den erforderlichen SIL anhand des Risikographen

Quelle: VDI/VDE 2180 Blatt 1, April 2019

- S3
  - Tod mehrerer Personen
- A1
  - seltener bis häufiger Aufenthalt in der gefährdeten Zone
- ~~G~~
- W3
  - relativ hohe Wahrscheinlichkeit des unerwünschten Auftretens

Beispiel SIL 1:

- S2
  - schwere, bleibende Verletzung oder Tod einer Person
- A1
  - seltener bis häufiger Aufenthalt in der gefährdeten Zone
- G1
  - unter bestimmten Bedingungen möglich Auswirkungen zu vermeiden
- W3
  - relativ hohe Wahrscheinlichkeit des unerwünschten Auftretens

Beispiel SIL 3:

- S3
  - Tod mehrerer Personen
- A1
  - seltener bis häufiger Aufenthalt in der gefährdeten Zone
- ~~G~~
- W3
  - relativ hohe Wahrscheinlichkeit des unerwünschten Auftretens

Was passiert, wenn nicht gewissenhaft gearbeitet wird?

Planer	Ausführender	Problem
Plant richtig	Führt Planung richtig aus	nein
Plant richtig	Führt Planung falsch aus	ja
Plant falsch	Führt Planung richtig aus	ja
Plant falsch	Führt Planung falsch aus	ja
Plant falsch	Erkennt Planungsfehler	nein

Jeder muss sich seiner Verantwortung bewusst sein!

Problem = Risiko = Gefährdung von Leib und Leben!

Problemfaktor Mensch:

- Menschen machen Fehler
  - auf jeder Ebene
  - in jeder Projektphase

- Prüfungen zur Fehlervermeidung
  - in den Projektphasen
  - zur Inbetriebnahme und wiederkehrend
  - durch betriebsfremdes Personal
    - nicht betriebsblind
    - neutral und objektiv
    - sachverständig

Was passiert, wenn nicht gewissenhaft gearbeitet wird?

Planer	Ausführender	Problem	Prüfer	Problem
Plant richtig	Führt Planung richtig aus	nein	Prüft richtig	nein
Plant richtig	Führt Planung falsch aus	ja	Erkennt falsche Ausführung	nein
Plant falsch	Führt Planung richtig aus	ja	Erkennt falsche Planung	nein
Plant falsch	Führt Planung falsch aus	ja	Erkennt falsche Ausführung/ Planung	nein
Plant falsch	Erkennt Planungsfehler	nein	Prüft richtig	nein

Funktionale Sicherheit für Monteure und Techniker

Welches Wissen ist für Arbeiten im Feld relevant,

- zum Erkennen von Planungsfehlern?
- zum Erkennen von Ausführungsfehler?
- zum Erkennen von fehlerhaften Prüfanweisungen?

PLT-Grundlagen:

- Temperaturmessung
- Durchflussmesstechnik
- Füllstandsmesstechnik
- Druckmesstechnik
- Signaltechnik
- Regelungstechnik
- Elektrische Antriebe
- Armaturen

Jan-Niklas Stender, M. Sc.

Leiter Aus- und Weiterbildung
TUEG Schillings GmbH
Heisenbergstr. 18
50169 Kerpen

☎ +49 176 73504545
✉ jstender@tueg-schillings.de

Module der Akademie:

- Sensortechnik
- Kommunikation
- Verarbeitungslogik
- Aktorik
- Funktionale Sicherheit
- Elektr. Sicherheit
- Ex-Schutz

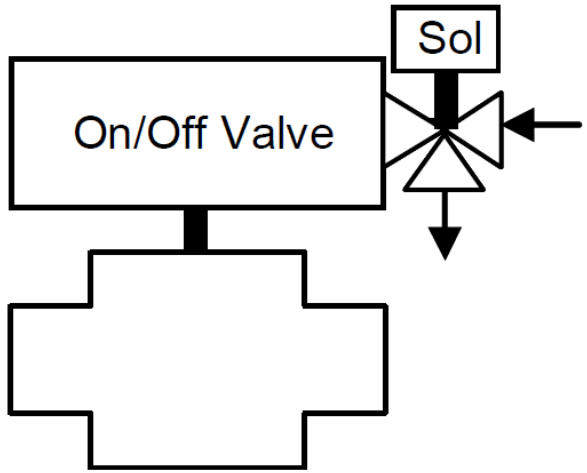
SIL SLAM
2023

Wann muss ein SIS Ventil erneuert werden?

3. Mai 2023 – Udo Menck – Dow Chemical (Stade)

Tätigkeiten am SIS Ventil

- **Prüfung**
  -> Überprüfung der spezifizierten sicherheitsrelevanten Parameter (meist Fahrzeit und Dichtigkeit)
  Wir stellen fest, ob das Ventil im Anforderungsfall sicher gewesen wäre.
  Wir finden Fehler, die die Sicherheitsfunktion blockiert hätten.
- **Wartung**
  -> Reinigung, Schmierung, Konservierung
  Sicherstellen, dass das Ventil bis zur nächsten Wartung funktioniert
- **Erneuerung von Komponenten**
  -> Austausch von einzelnen Komponenten
  Vorsichtsmaßnahmen, um sich anbahnende Fehler zu vermeiden
- **Gerätetausch**
  -> Wirtschaftliche Entscheidung
  Wenn der vorgefundene Zustand zuviel Aufwand zur Wiederherstellung benötigt, so dass ein Austausch wirtschaftlicher ist



Gelebte Praxis -Welche Intervalle ?

In welchen zeitlichen Abständen führen wir die Tätigkeiten aus?

- **Prüfung**
  Oft jährlich oder angepasst an die betrieblichen Belange, wenn die SIL Berechnung **und** die Einsatzbedingungen (Umgebung / Medium) es erlauben
- **Wartung**
  Gemäß den Einsatzbedingungen (Umgebung, Medium) nach Bedarf / Erfahrung während der Prüfung
- **Erneuerung von Komponenten**
  Gemäß den Einsatzbedingungen (Umgebung, Medium) nach Bedarf / Erfahrung während der Prüfung
- **Gerätetausch oder „Komplettüberholung *1“**
  Gemäß den Einsatzbedingungen (Umgebung, Medium) nach Bedarf / Erfahrung während der Prüfung

*1 Der Begriff „Komplettüberholung“ ist nicht definiert.
Man kann eine „Komplettüberholung“ so umfangreich definieren, dass die Praktiker sagen es ist wirtschaftlicher ein neues Ventil zu installieren.

Kann ich das Intervall für den Gerätetausch mit einer PFD Berechnung ausrechnen?

Berechnungsformel

1oo1

Kanal A / Channel A:

$$\lambda_{0,A} = PTC_{0,A} \cdot \lambda_{DU,A}$$

$$\lambda_{1,A} = \left(PTC_{1,A} - PTC_{0,A} \right) \lambda_{DU,A}$$

$$\lambda_{2,A} = \left(1 - PTC_{1,A} \right) \lambda_{DU,A}$$

Berechnung der PFD / Calculation of PFD:

$$PFD_{1oo1} \approx \lambda_{0,A} \frac{T_0}{2} + \lambda_{1,A} \frac{T_1}{2} + \lambda_{2,A} \frac{T_2}{2}$$

Quelle: VDI 2180 / Teil3 / September 2019

PTC: Proof Test Coverage

Ansatz …

Ich nehme einfach mal an, dass meine Prüfung im Intervall T1 nur 95% der gefährlichen zufälligen Fehler entdeckt und ich nach dem Zeitpunkt T2 das Ventil dann austauschen muss.

(auf eine Prüfung im Intervall T0 wird hier verzichtet)

Berechnungsergebnisse

*	Prüfung	Austausch
SIL 1	**3 Jahre**	**45 Jahre**
SIL 2	**6 Monate**	**1 Jahr**

Ergebnis:
Abhängig vom SIL muss das Ventil nach ***45 Jahren*** oder nach ***1 Jahr*** erneuert werden!

<u>Fragen an den Praktiker:</u>

Ist die Standzeit eines Ventils abhängig vom SIL?
(oder: Wer verrät dem Ventil vor Einbau, welchen SIL es einhalten muss?)

Ist die Standzeit eines Ventils immer gleich,
egal in welchem Medium und in welcher Umgebung ich es betreibe?

- Angenommene Fehlerrate Lamda DU Ventil: 2283 FIT - PTC Prüfung: 95% - PTC Austausch: 100% Berechnungsziel: 50% vom SIL für das Ventil

Diskussion

Ist es sinnvoll die Lebensdauer eines Gerätes in der PFD Berechnung zu berücksichtigen?

Wem nützt es, wenn in der PFD Berechnung von einer Prüftiefe kleiner 100% ausgegangen wird?

Ist es in der Praxis sinnvoller die Lebensdauer eines Gerätes unabhängig von der PFD Berechnung festzulegen (siehe auch NA106)?

BECKHOFF

What you always wanted to know about Markov Models

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

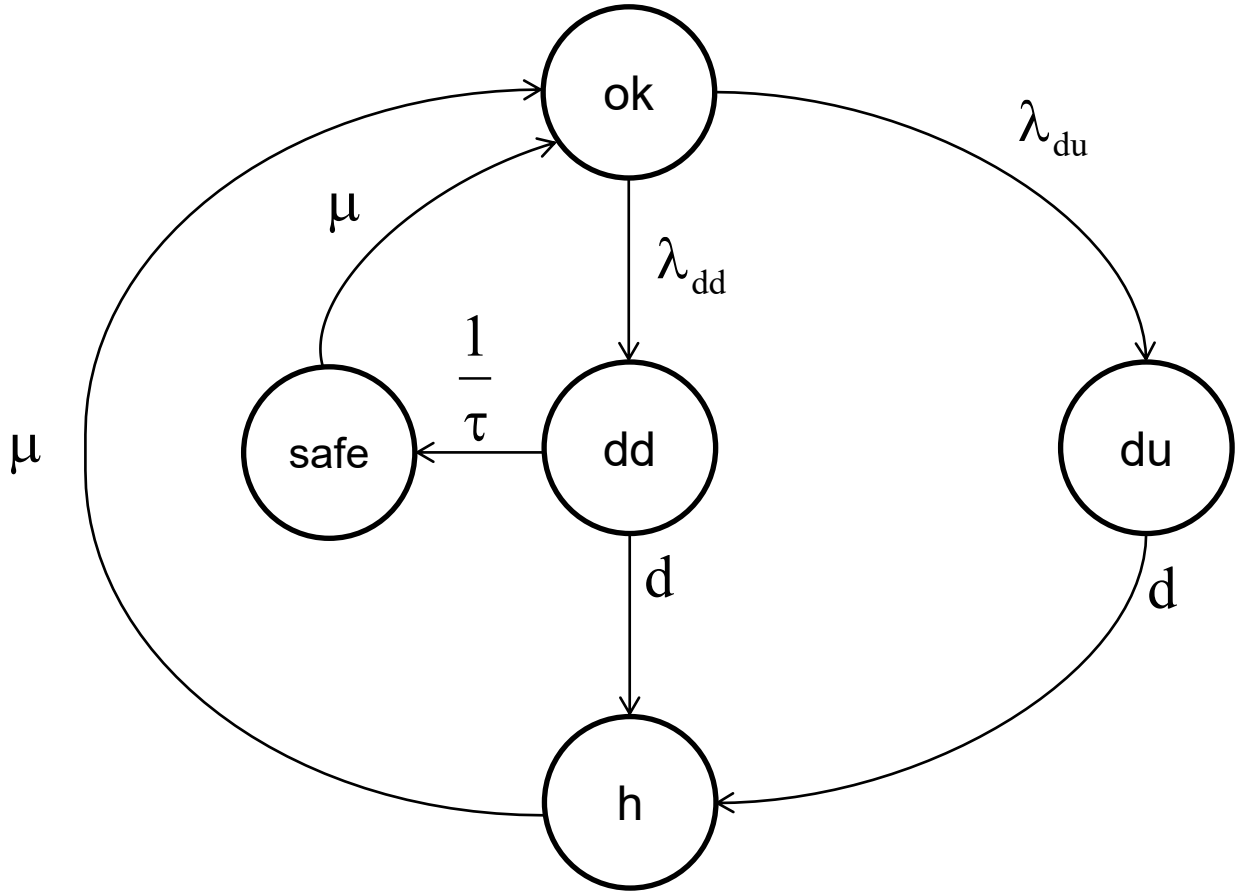
[1]IEC/TC 65/WG 12, Beckhoff Automation GmbH & Co. KG;
[2]Laboratory for Safe and Secure Systems, Ostbayerische Technische Hochschule Regensburg;
[3]IEC/TC 44, Siemens AG

Impact of Demand on Safety Analysis using Markov Models

BECKHOFF

- Markov Models
- PFD
- PFH
- Discussion
- Summary

Markov Model – Graphical Representation



λ_{du} rate of undetectable dang. errors

λ_{dd} rate of detectable dang. errors

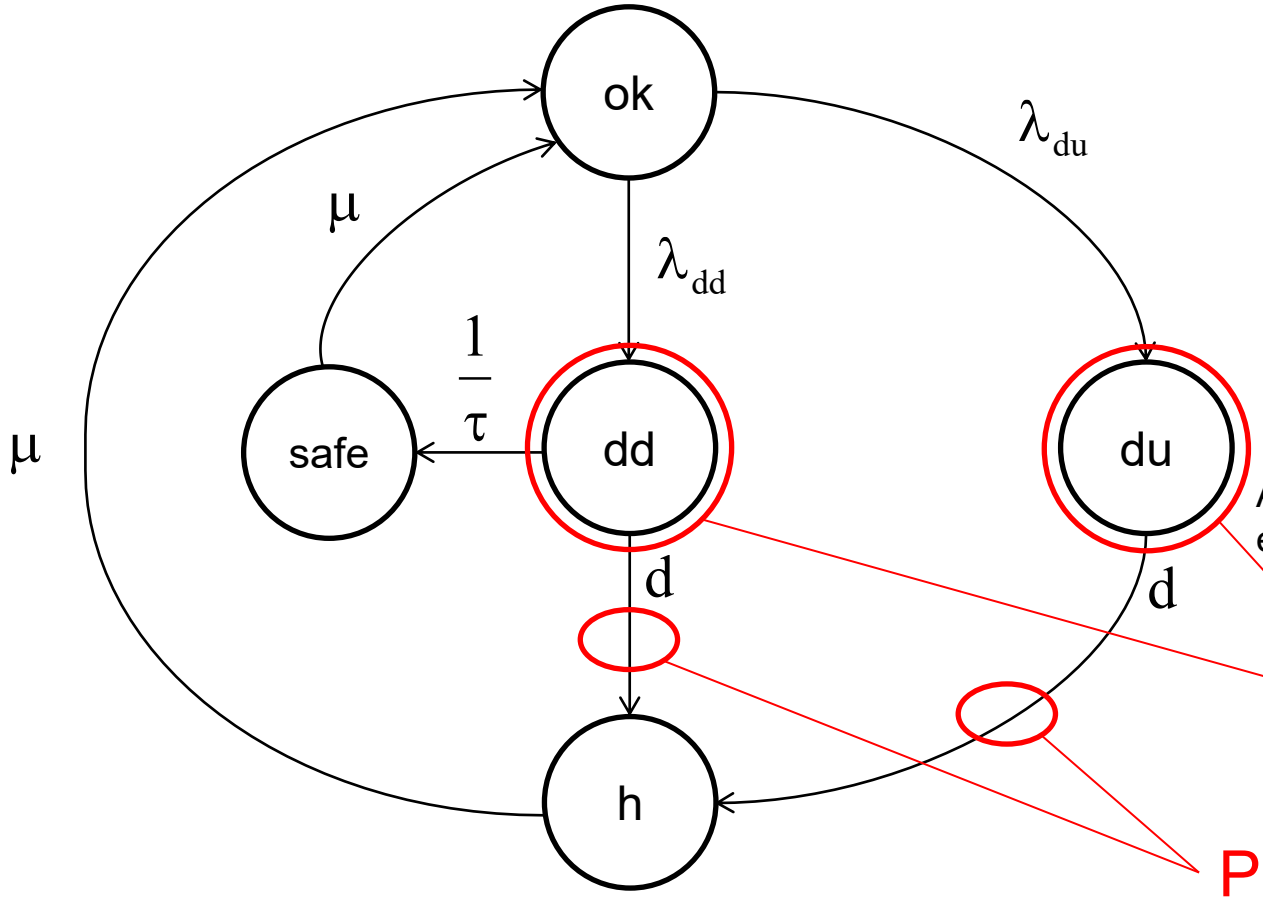
d rate of safety demands

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.

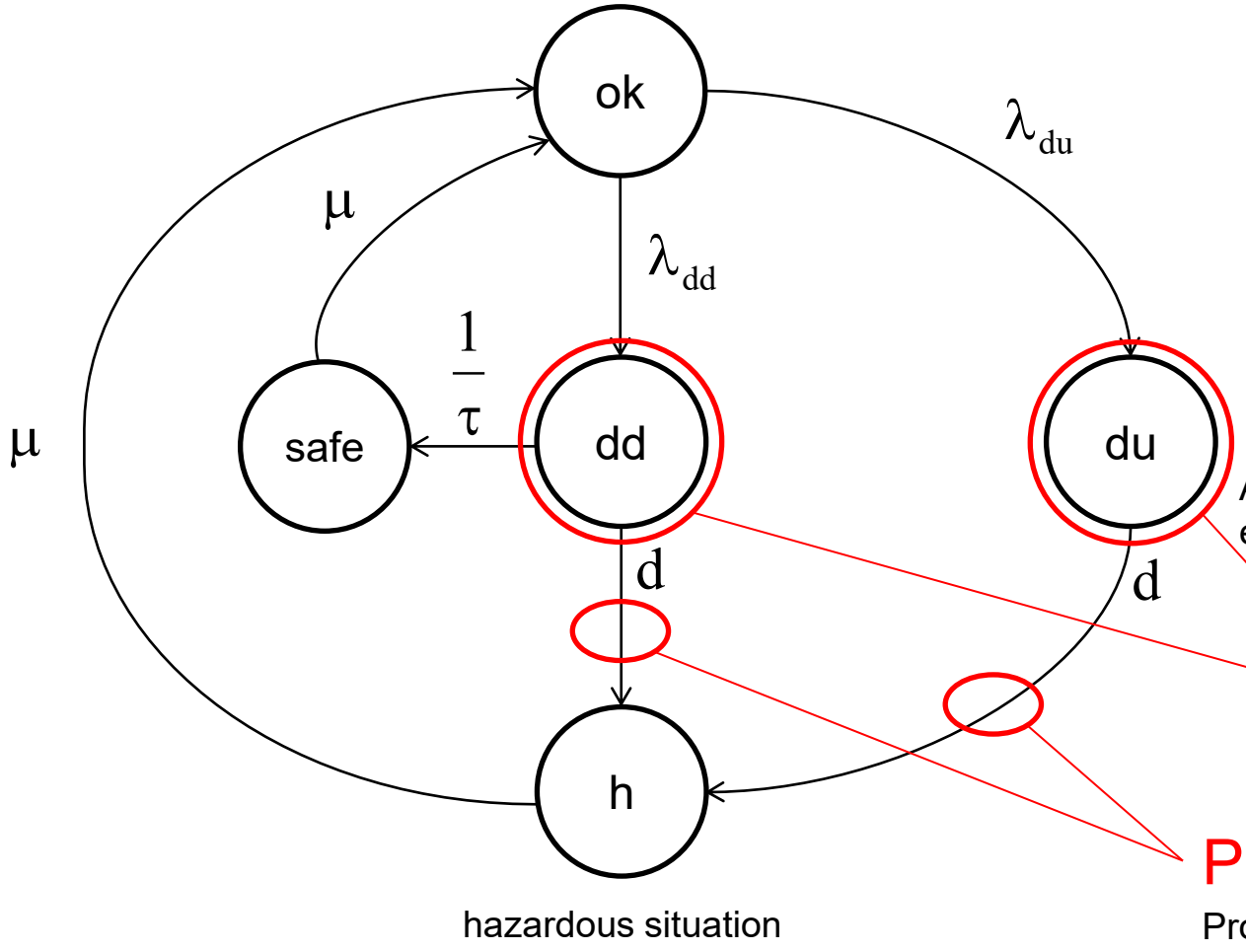
PFD

Probability of dangerous Failure on Demand

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}

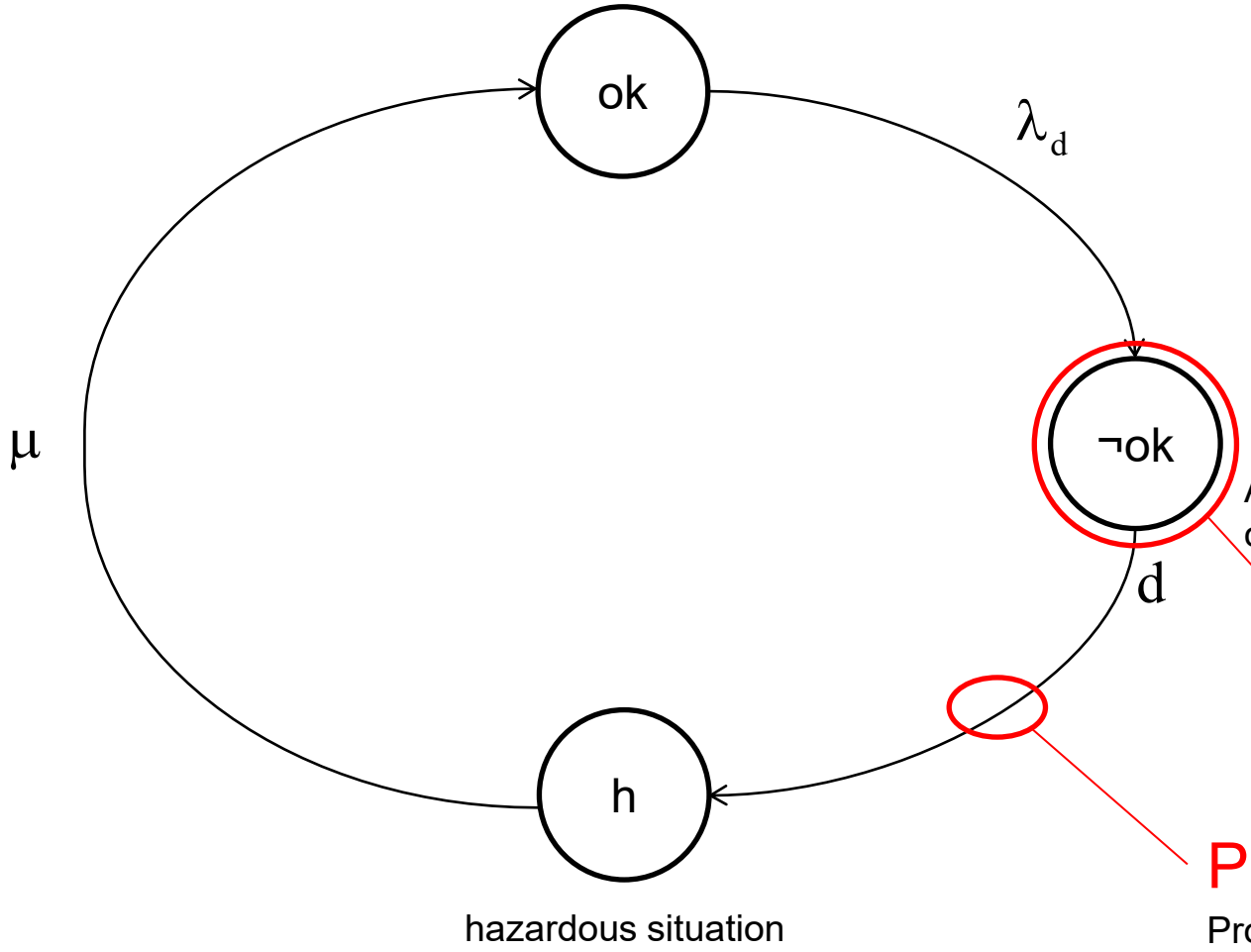
Probability of dangerous Failure per Hour (PFH of 1st edition IEC 61508)

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}

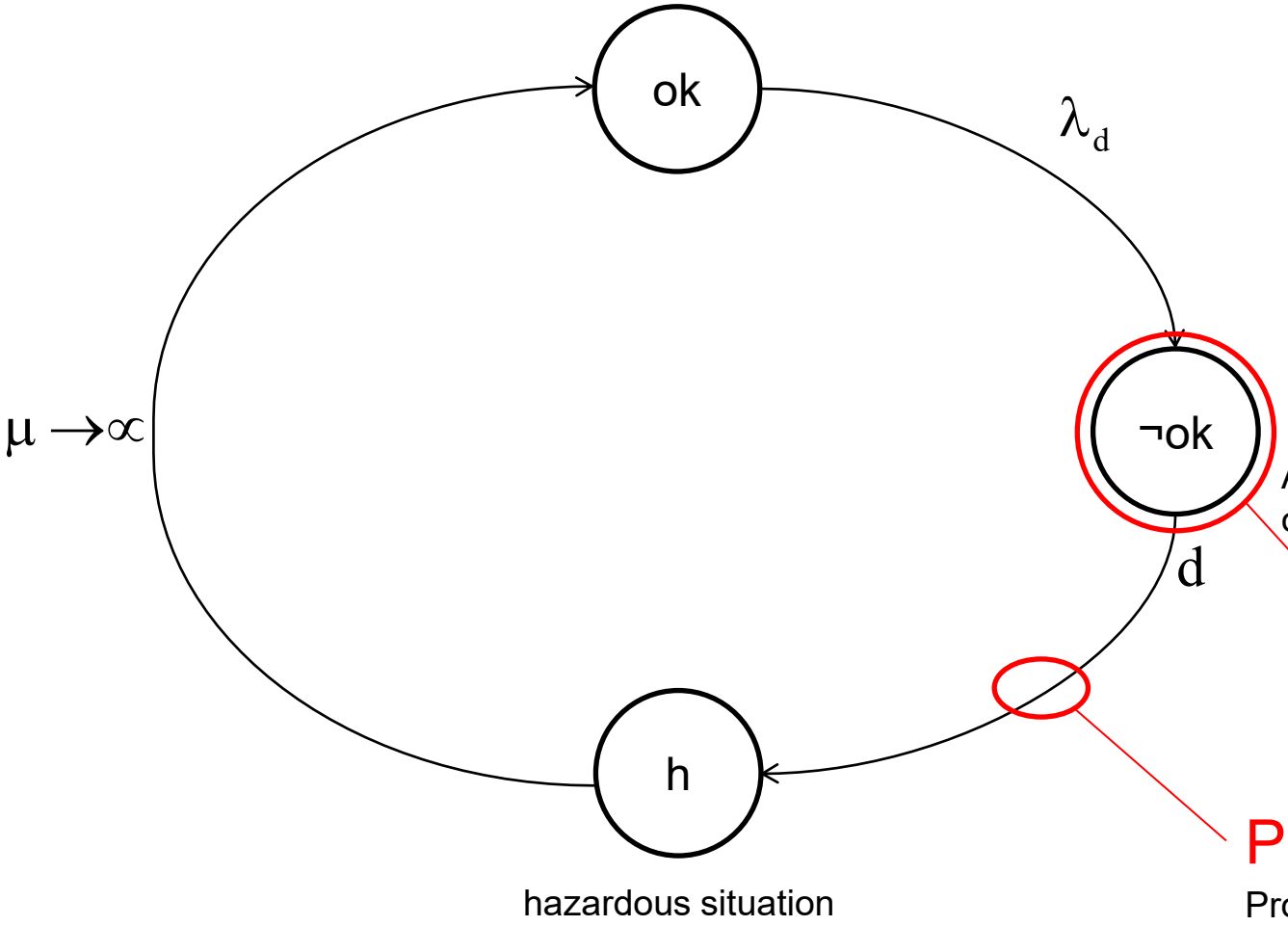
Probability of dangerous Failure per Hour (PFH of 1st edition IEC 61508)

PFH^{Ed2}

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

Markov Model – Worst Case Repair

BECKHOFF



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}

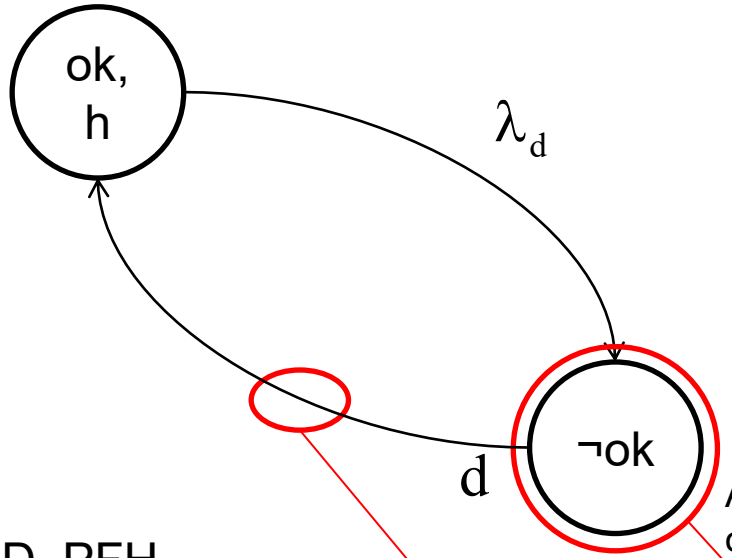
Probability of dangerous Failure per Hour (PFH of 1st edition IEC 61508)

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)

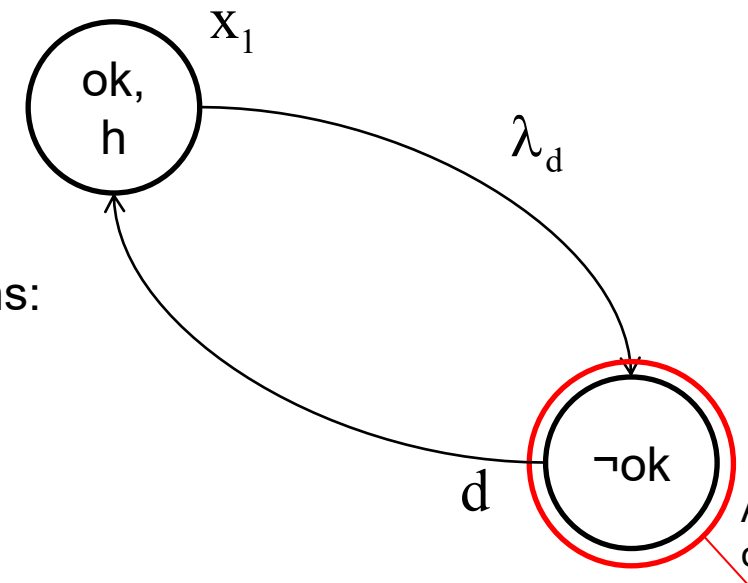
PFH^{Ed2}

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

Impact of Demand on Safety Analysis using Markov Models

BECKHOFF

- Markov Models
- PFD
- PFH
- Discussion
- Summary



λ_d rate of dangerous errors

d rate of safety demands

Set of differential equations:

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

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

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

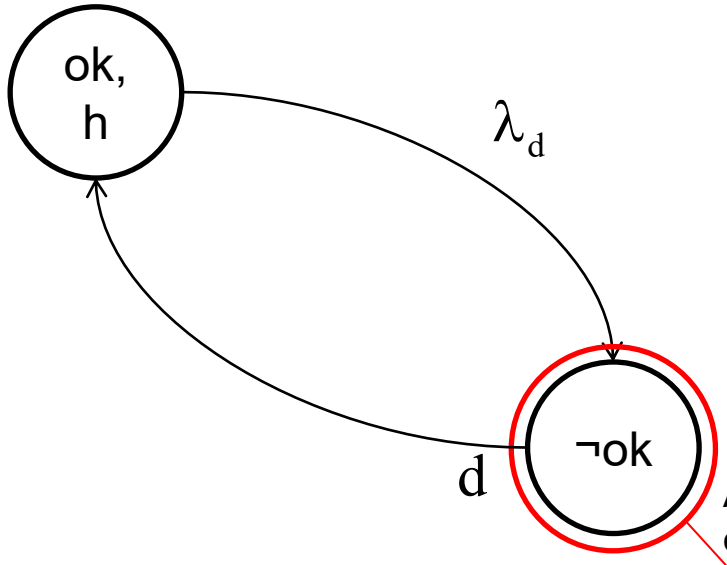
$$x_1 + x_2 = 1$$

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

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.

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

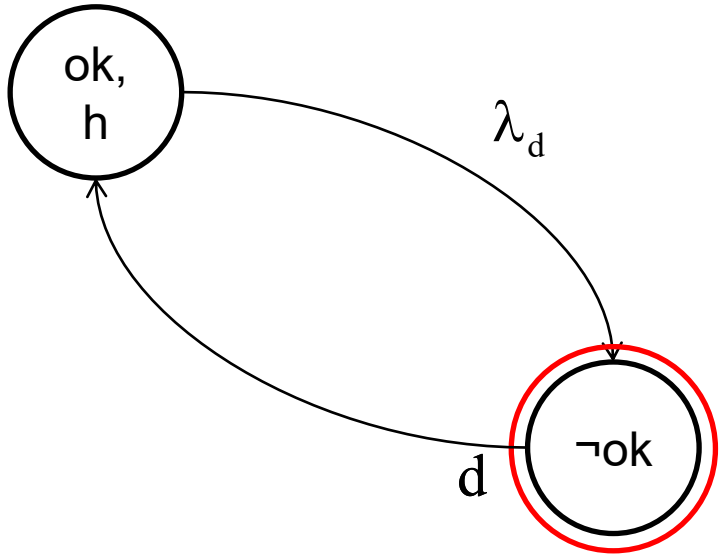
$$PFD_{avg}(T) = \frac{\lambda_d}{\lambda_d + d} \cdot \left(1 - \frac{1}{(\lambda_d + d) \cdot T} \cdot (1 - e^{-(\lambda_d + d) \cdot T})\right)$$

PFD

Probability of dangerous Failure on Demand

Worst case demand?

PFD – Worst Case Demand, d=0



λ_d rate of dangerous errors

d rate of safety demands

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

$d = 0$

Disadvantage:
- Greater value for PFD

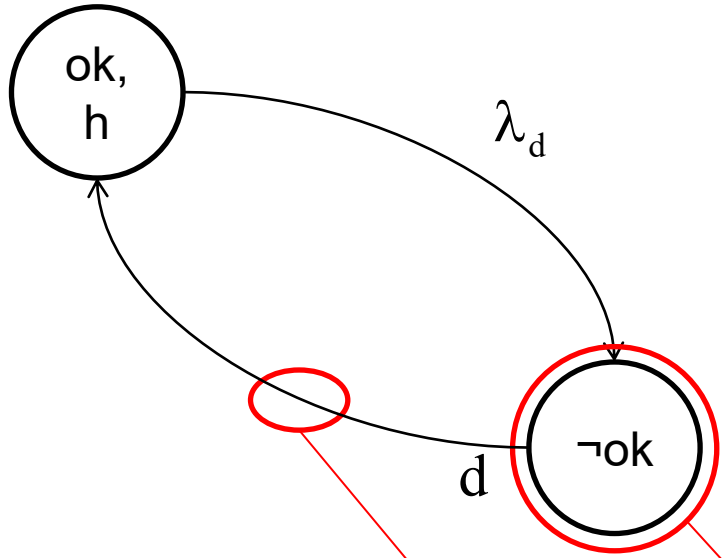
Advantage:
- No assumption about demand necessary, neither its rate nor its characteristic.

Impact of Demand on Safety Analysis using Markov Models

BECKHOFF

- 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

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

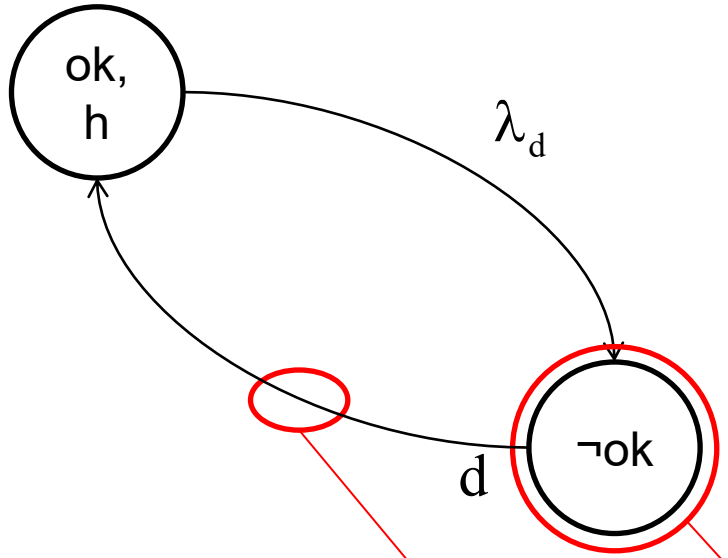
$$d \rightarrow \infty$$

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

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

Disadvantage:
- Greater value for PFH

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



λ_d rate of dangerous errors

d rate of safety demands

PFD

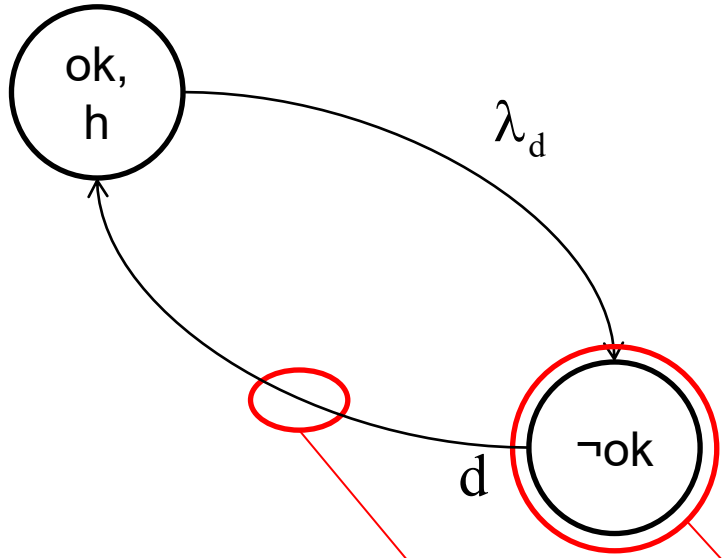
Probability of dangerous Failure on Demand

PFH^{Ed2}

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

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

BECKHOFF



λ_d rate of dangerous errors

d rate of safety demands

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

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

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

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

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

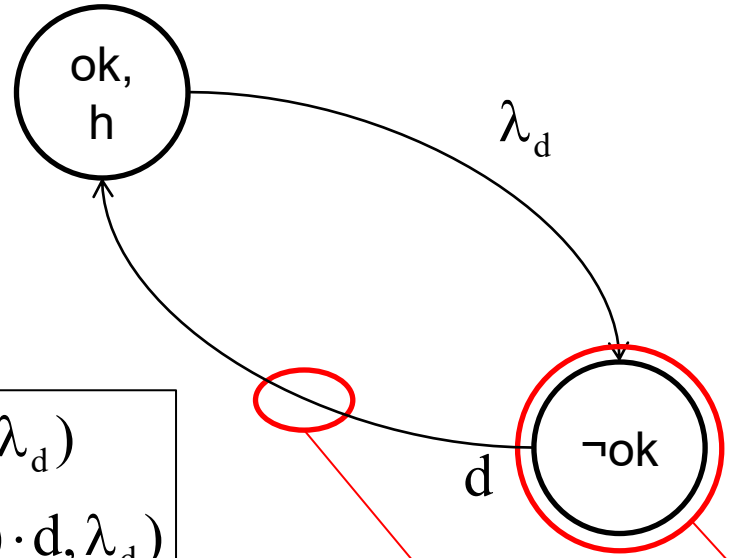
Probability of dangerous Failure on Demand

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

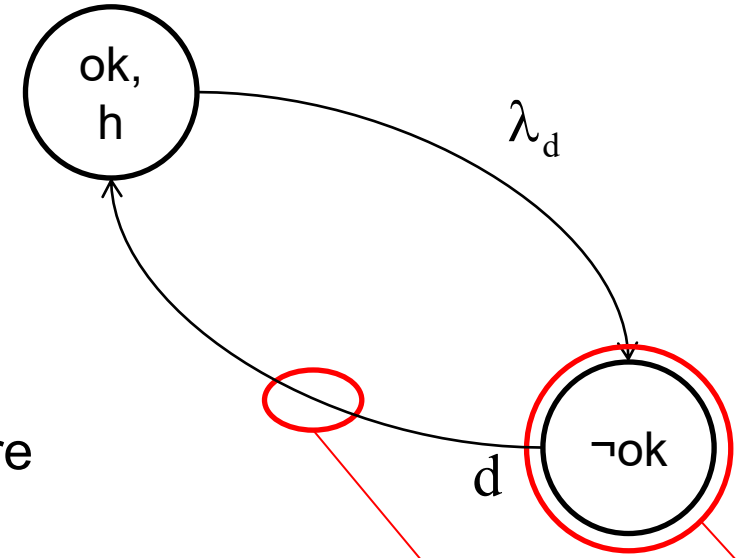
PFH^{Ed2}

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

Impact of Demand on Safety Analysis using Markov Models

BECKHOFF

- 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.

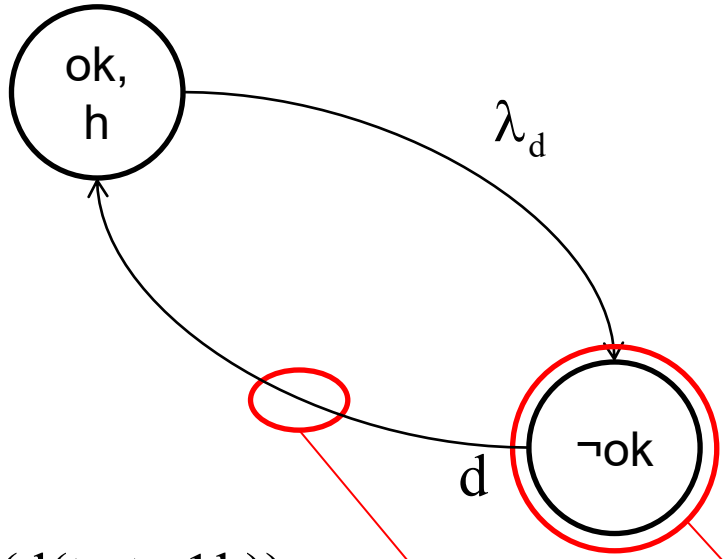
= Probability that a safety system is in state “¬ok” (“dangerous undetectable” and “dangerous detectable”) within one hour and at least one demand occurs within that hour.

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

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

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} – Demand

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

1. Random demand:

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

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

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.

Impact of Demand on Safety Analysis using Markov Models

BECKHOFF

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

Discussion – PFH^{Ed1} vs. PFH^{Ed2}

BECKHOFF

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

$$\cong$$

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

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

Impact of Demand on Safety Analysis using Markov Models

BECKHOFF

- 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.

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.

SIL SLAM 2023

Zufällige Fehler in Mechanik
Mythos oder Wirklichkeit?

Dipl.-Ing. Univ. Christoph Theilen

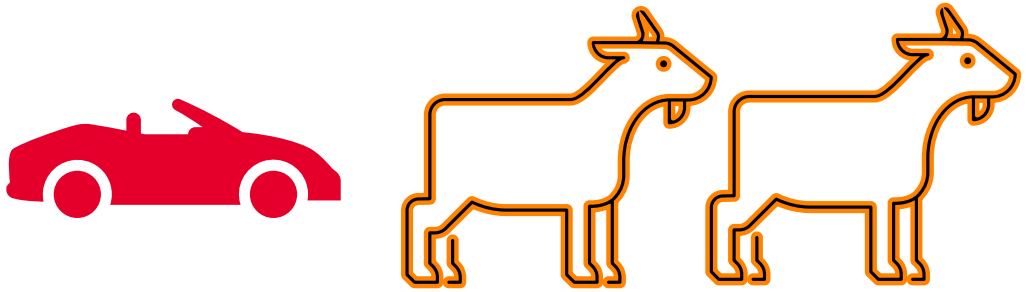
Mehr Wert.
Mehr Vertrauen.

Dipl.-Ing. Univ. Christoph Theilen

Vertrieb, Bereichsentwicklung, Strategic Account Manager

TÜV SÜD Industrie Service GmbH
Region Bayern
Westendstr. 199
80686 München
Germany

Tel. 0941/9910 416
Fax 089 5791-2425
Mobil 0160 704 3804
mail to: christoph.theilen@tuev-sued.de



Zufällige Fehler in Mechanik.
Mythos oder Wirklichkeit?

Der Fehler - Es gibt zwei Typen – eine theoretische physikalische Betrachtung

Exkurs in die physikalische Messtechnik

Zufällige Fehler xzuf

Bei vielen Wiederholungen der Messung ist nicht vorhersagbar, wie stark und in welche Richtung eine Abweichung des Bestwertes vom wahren Wert erfolgt. Der Zufall kann bei der Planung und Ausführung der Messung nicht ausgeschlossen werden.

- Die zufälligen Abweichungen vom wahren Wert haben gleichhäufig beiderlei Vorzeichen,
- vorausgesetzt man führt die Messung sehr oft durch.
- Es gibt also Messwerte, die größer, und solche, die kleiner als der wahre Wert sind.
- Die bei wiederholter Messung bestimmten Werte streuen um den Mittelwert $\bar{x}$ herum.

Systematische Fehler xsys

- Bei vielen Wiederholungen der Messungen wirken sich systematische Fehler stets gleich auf die Abweichung des Bestwertes vom wahren Wert aus.
- Die systematischen Abweichungen haben stets das gleich Vorzeichen. Bei wiederholter Messung
- sind die Werte sämtlich größer oder sämtlich kleiner als der wahre Wert.

Der Fehler in Sicherheitsfunktionen

Fehler bzw. fehlerhafte Schaltprozesse elektronischen Bautelen treten zufällig auf, das bedeutet:

- Sie sind nicht vorhersehbar.
- Sie sind nicht reproduzierbar.
- Sie sind den EIE / PE-Systemen immanent.

Diese zufälligen Fehler sind prinzipiell unvermeidbar, müssen also antizipiert und das Versagen der Bauteile somit einkalkuliert werden.

Dem gegenüber stehen die systematischen Fehler, die durch kausale Zusammenhänge gekennzeichnet sind:

- Sie treten immer dann auf, wenn bestimmte Rahmenbedingungen erfüllt sind.
- Sie haben eine nachvollziehbare und fest stellbare Ursache.
- Sie führen zu einer vorhersehbaren Wirkung und sind stets auf menschliches (Fehl-) Verhalten zurückzuführen.
- Ursache und Wirkung hängen kausal zusammen.

Der Fehler in Sicherheitsfunktionen

Woher kommt dann die Aussage vom Zufall in der Mechanik?

Klassifizierung von Fehlern

- Der Betreiber einer Prozessanlage hat von seinem Ventillieferanten 100 Ventile unterschiedlicher Bauart eingesetzt.
- Bei der jährlichen Funktionsprüfung wird ein gefährlicher Fehler eines Ventils festgestellt.
  – Ursache: Federbruch
- Der Betreiber führt eine Fehleranalyse durch um den Fehler zu klassifizieren (zufällig oder systematisch).
- Zur Analyse des Fehlers werden alle Ventile der gleichen Bauart ebenfalls geprüft.
  – Resultat: Bei keinem weiteren Ventil ist die Feder gebrochen, trotz gleicher Umgebungsbedingungen.
- Ergebnis: Der Betreiber erfasst den Fehler als zufällig in seiner Stördatenstatistik und meldet dies an den Hersteller zur Berechnung des PFD-Werts.

Beispiel

Lieferant (Federn)	Ventilhersteller	Betreiber
Der Hersteller der Federn gießt seinen Stahl bei zu hoher Temperatur. Dadurch kommt es zu Lufteinschlüssen, welche Federbruch zur Folge haben können.	Der Ventilhersteller kauft 1000 Federn bei seinem Lieferanten.	Der Betreiber hat 100 Ventile des Herstellers im Einsatz.

Ursachen von systematischen Fehlern

- Fehler bei der Materialauswahl (z. B. Dichtungen oder Körper)
  - *Fehler in der Spezifikation*
- Fehler bei der Auslegung/Auswahl von Komponenten, z. B. zu schwache Auslegung von Stellantrieben
  - *Fehler in der Spezifikation*
- falsche Kalibrierung oder Justierung
  - *Fehler in der Installation*
- mangelhafte Montage oder Instandhaltung
  - *Fehler in der Installation oder dem Betrieb*
- Fehler im Fertigungsprozess aufgrund eines mangelhaften Qualitätsüberwachungssystems
  - *Gerade diese Fehler sind durch den Betreiber schwer zu klassifizieren*

Klassifizierung von Fehlern

Problem
Der Betreiber einer Anlage soll den Ausfall eines Ventils klassifizieren, ohne Einfluss oder detaillierte Kenntnis über den Herstellungsprozess des Ventils zu haben.

Folge
Aussagen über die Art eines Fehler im Feld unterliegen Unsicherheiten.
Es ist meist schlechthin nicht möglich eine eindeutige Einteilung zu machen, da das Wissen über den Fehler unvollständig ist.
Dadurch werden Fehler, die mit statistischen Verfahren ermittelt werden auch falsch einsortiert (Systematischer Fehler durch den Menschen aufgrund von Unkenntnis).

Bei einer theoretischen Betrachtung der physikalischen Eigenschaften der Mechanik, kommt man zu dem Schluss, dass Mechanik keine zufälligen Fehler enthalten kann, auch wenn es uns manchmal so erscheint.

RAMSYS
DAS machen Ingenieure

Betrachten Sie die Funktionale Sicherheit?

Was steckt hinter dieser Frage?

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

RAMSYS
DAS machen Ingenieure

I. Informationsquellen

(1) Was ist Stand der Technik

(2) Welche Quelle ist die richtige für mich

II. SIL-Einstufung → Umsetzung

(1) Ablauf Praxis

(2) Prozessanschluss

(3) Ablauf Theorie

III. Dokumentation

(1) FuSi-Dokumentation

(2) Zusammenspiel Engineering / FuSi

(3) Ablagemanagement

RAMSYS
DAS machen Ingenieure

I. Informationsquellen

(1) Was ist Stand der Technik

(2) Welche Quelle ist die richtige für mich

(1) Was ist Stand der Technik

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?

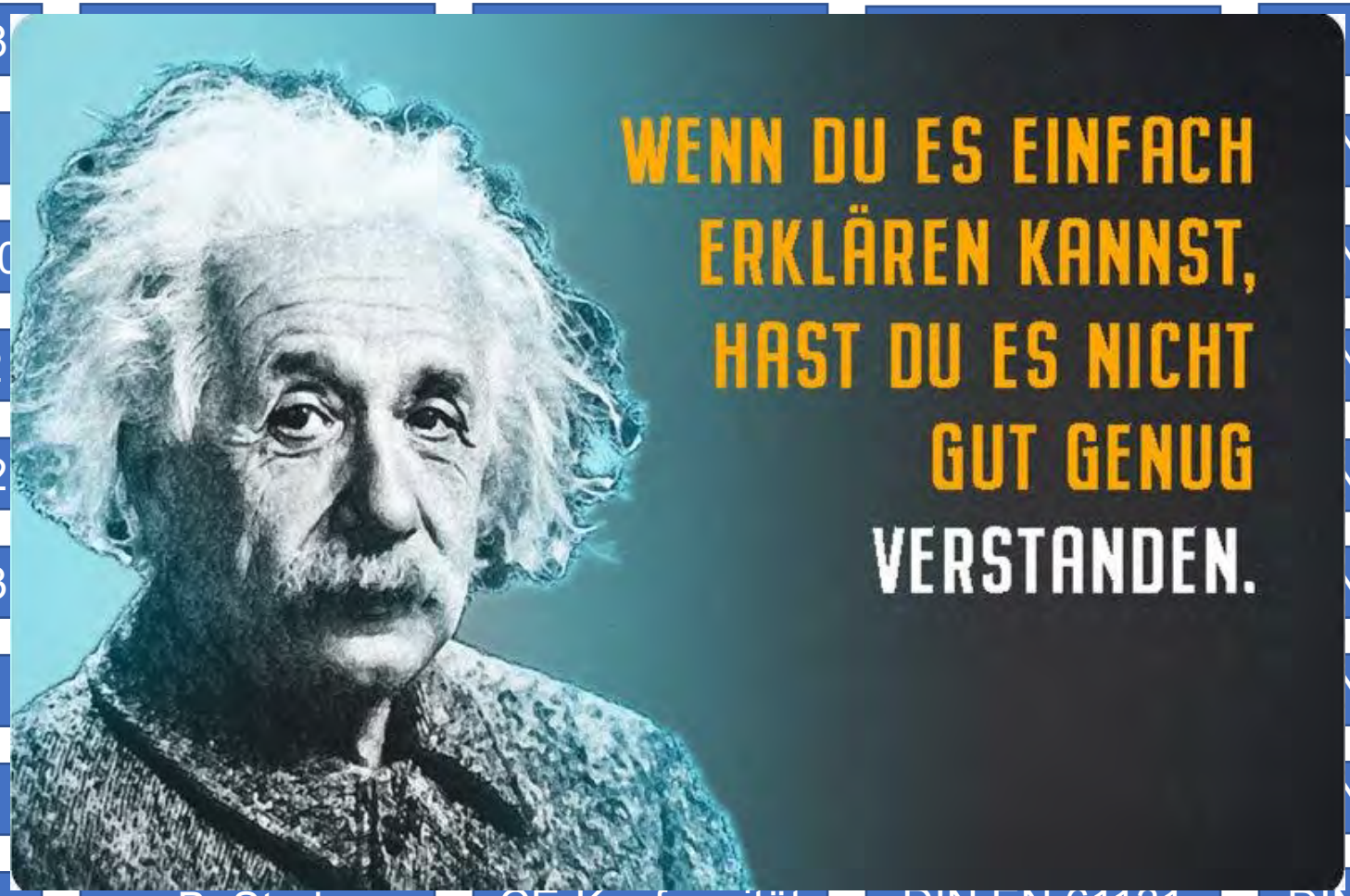
- „Der Stan… ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen od…isen, der die praktische Eignung einer Maßnahme zum Schutz der Gesundheit u…heit der Beschäftigten gesichert erscheinen lässt

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

(2) Welche Quelle ist die richtige für mich

RAMSYS
DAS machen Ingenieure

Prozessindustrie	Transportmittel	Maschinen	Verordnungen	Sonstiges
DIN EN 61508				DGRL
DIN EN 61511				N EN 60601
VDI / VDE 2180				N EN 62304
DIN EN 746-2				N EN 61513
DIN EN 12952				N ISO 15998
DIN EN 12953				N ISO 25119
NE 130				N EN 16590
NE 93				N EN 12999
NA 106	BoStrab	CE-Konformität	DIN EN 61131	DIN IEC 60880



(2) Welche Quelle ist die richtige für mich

RAMSYS
DAS machen Ingenieure

- Wie komme ich jetzt zu den Regelwerken die wirklich für mich relevant sind?
- Rücksprache mit der Zuständigen Behörde / ZÜS
- Nachfragen bei einem Experten auf dem Gebiet
- Aber selbst so haben Sie keine 100%ige Sicherheit. Sollte sich mal der Prüfer ändern, kann es gut sein das dieser andere Regelwerke ins Spiel bringt.
- Um diese Sicherheit zu verbessern, sollten Sie immer mehrere unabhängige Personen Fragen (z.B. ZÜS und einen Experte)

II. SIL-Einstufung → Umsetzung

(1) Ablauf Praxis

(2) Prozessanschluss

(3) Ablauf Theorie

(1) Ablauf Praxis

RAMSYS
DAS machen Ingenieure

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

(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) Ablauf Theorie

RAMSYS
DAS machen Ingenieure

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

RAMSYS
DAS machen Ingenieure

III. Dokumentation

(1) Zusammenspiel Engineering / FuSi

(2) FuSi - Dokumentation

(3) Ablagemanagement

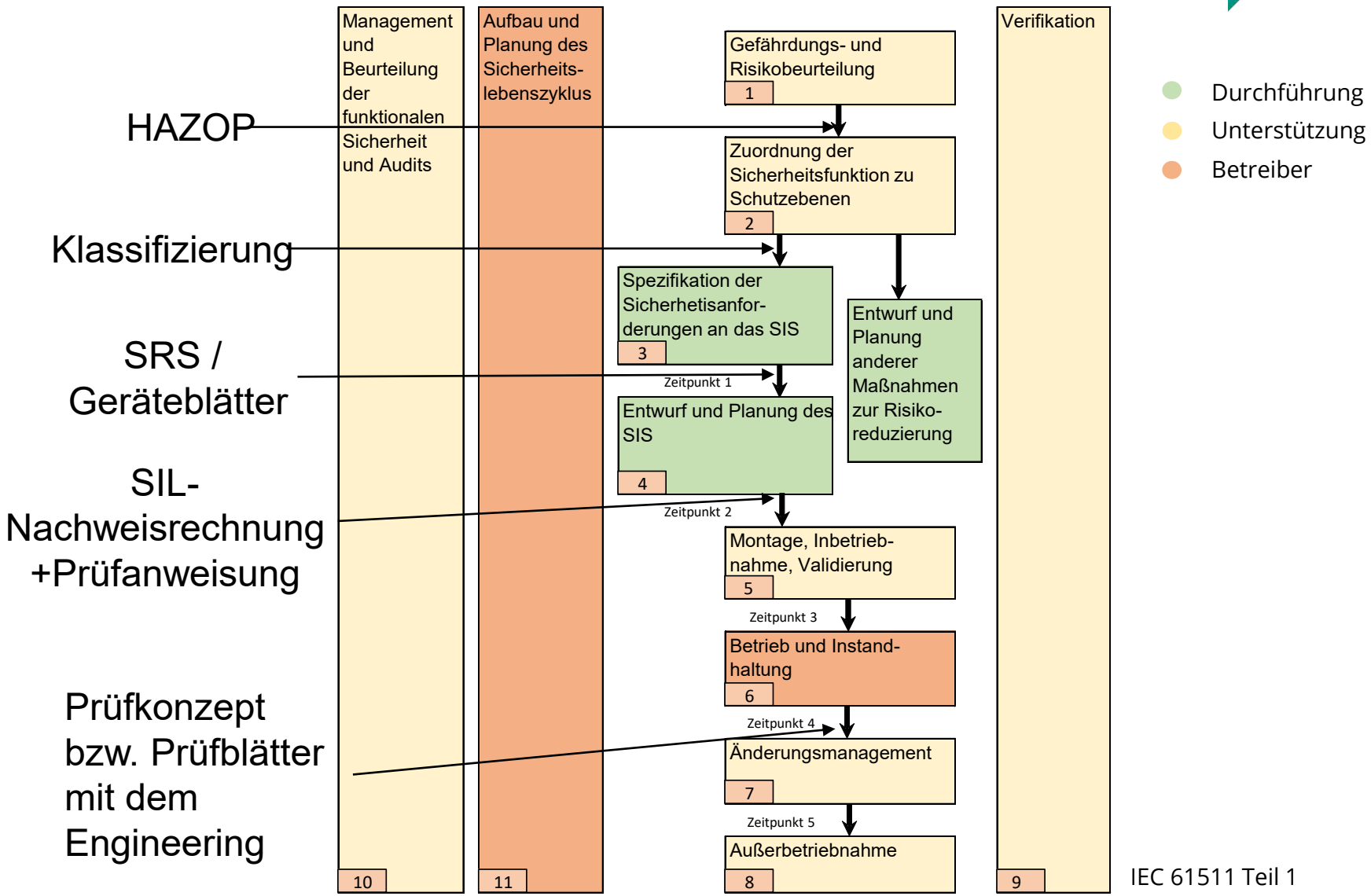
(1) Zusammenspiel Engineering / FuSi

uf kann je nach Firma /
kt variieren

- Funktionale Sicherhei
- Engineering

Normal Betrieb

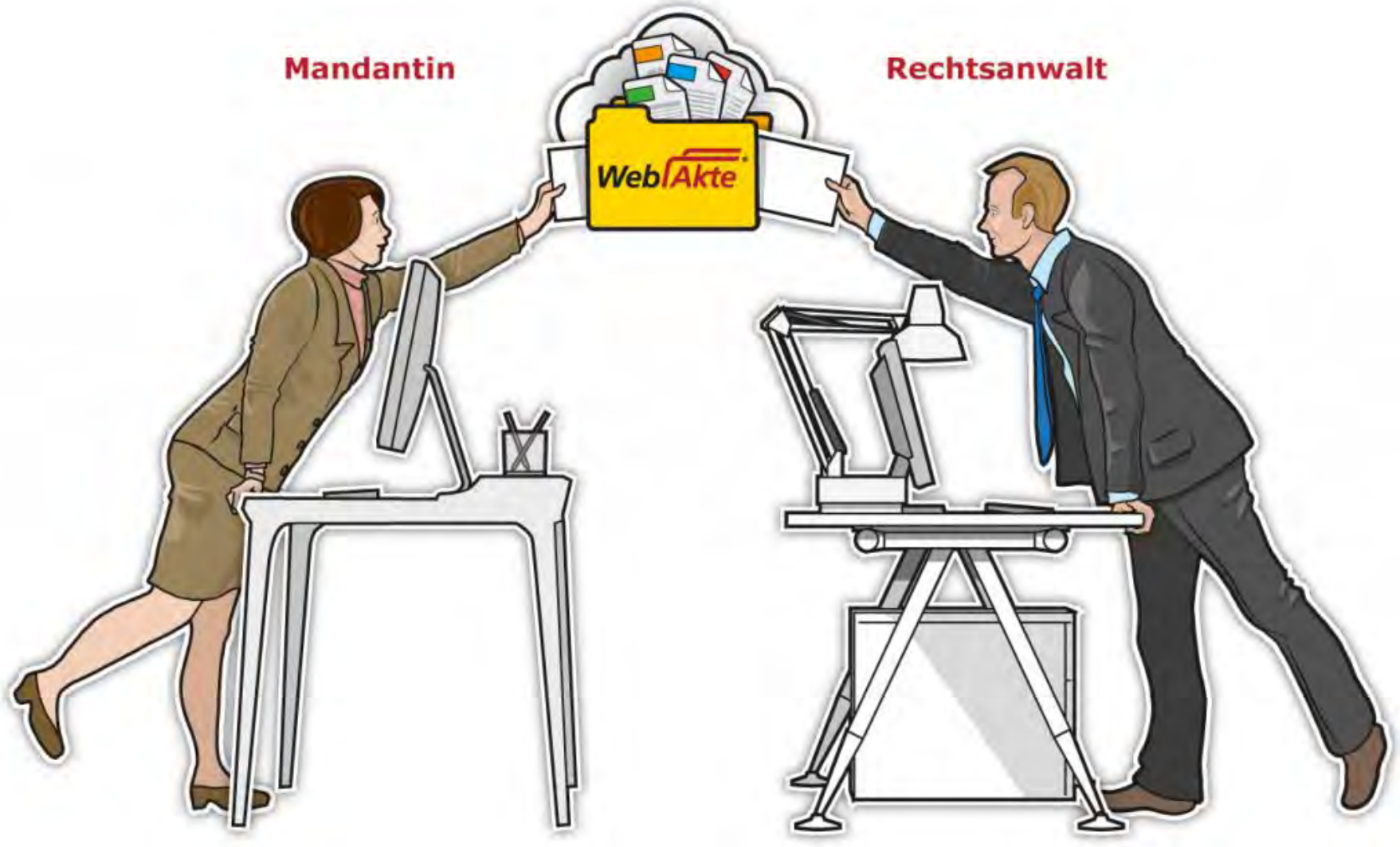
(2) FuSi-Dokumentation



- Durchführung
- Unterstützung
- Betreiber

IEC 61511 Teil 1

(3) Ablagemanagement



RAMSYS
DAS machen Ingenieure

Vielen Dank für Ihre Aufmerksamkeit

Malika Mast Dipl. Ing / Geschäftsführerin

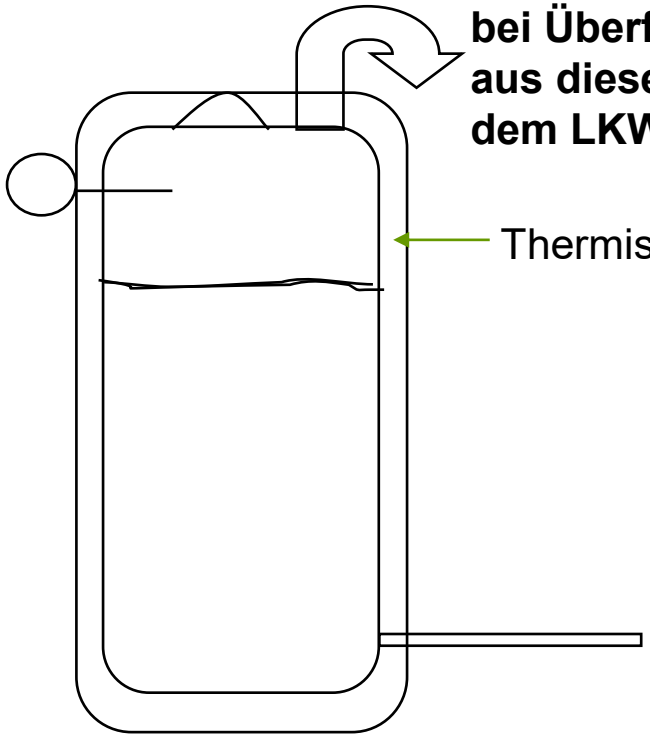
E-Mail: M.Mast@ramsys.org

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

Mobil: 0171 / 3037392

Vorlesung funktionale Sicherheit 1 – Fallstudie: Eine Anlage mit einem eingebetteten System versagt (1) (Script 1.1)

Füllstandsgeber, an SPS angeschlossen zur Auslösung einer Hupe



bei Überfüllung sollte die Flüssigkeit aus diesem Schwanenhals auslaufen, dem LKW-Fahrer "direkt vor die Füße"

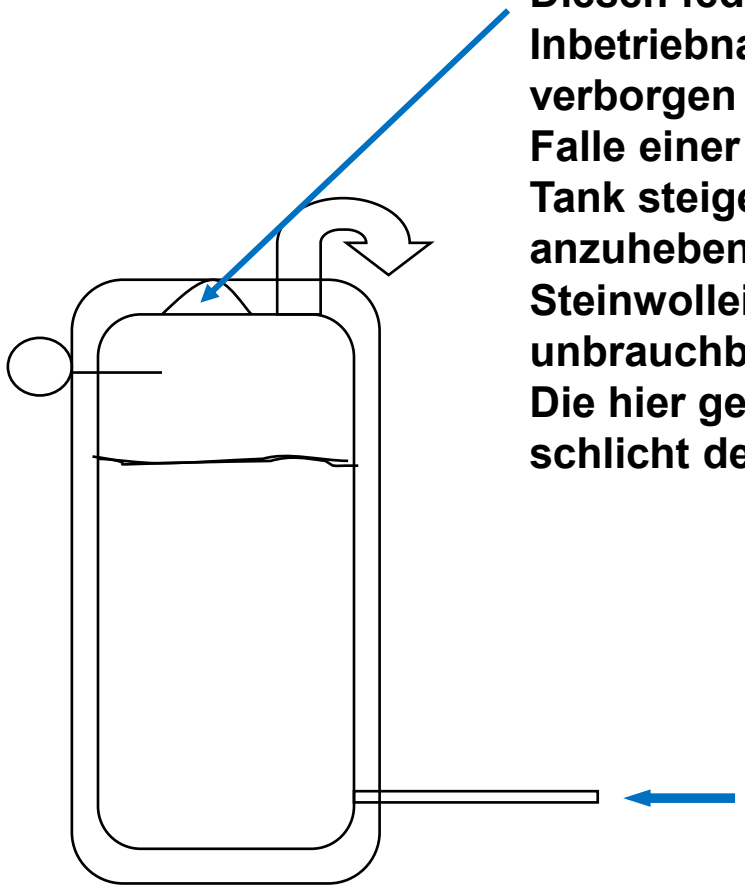
Thermische Isolierung

Flüssigkeitseinlauf vom LKW, gesteuert vom Fahrer

Aufgabe: Überfüllung dieses Tanks verhindern.
Lösung: Zwei unabhängige Schutzmaßnahmen.

Vorlesung funktionale Sicherheit 1 – Eine Anlage mit einem eingebetteten System versagt (2) (Script 1.1)

Das SPS-Programm zur Auswertung des Gebersignals erwartete, dass nach jeder Betätigung von extern ein Hilfsmerker zurückgesetzt wurde. Da das nirgends dokumentiert war, funktionierte es nach einem Reset oder Einschalten der SPS genau einmal. Das war bei dieser Anlage der Test. Zum Auslösen des Gebers musste man am Tank hinaufsteigen, so dass der Test nicht wiederholt wurde.



Diesen federbelasteten Deckel kannte das Inbetriebnahmepersonal nicht, da er unter der Isolation verborgen war. Sein Zweck war Druckentlastung im Falle einer Verpuffung im Tank. Der Auftrieb der im Tank steigenden Flüssigkeit genügte, um ihn anzuheben. Die Flüssigkeit lief in die Steinwolleisolation und machte diese dadurch unbrauchbar.
Die hier gelagerte Flüssigkeit war unbrennbar. Es war schlicht der falsche Tank bestellt worden

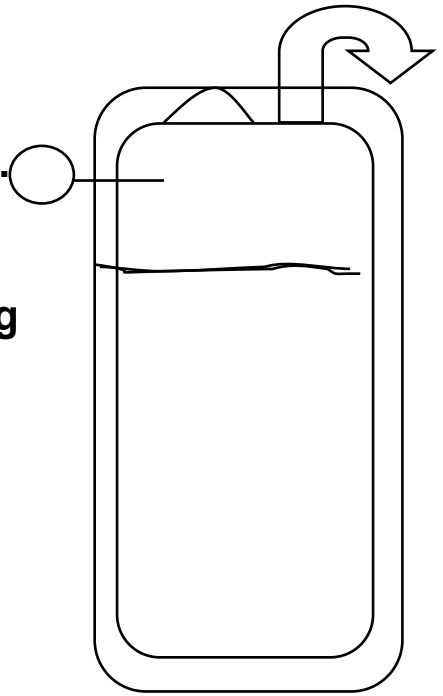
Der LKW-Fahrer bemerkte, dass ihm die Flüssigkeit nicht durch den Schwanenhals, sondern durch die Isolierung entgegenkam

Wir dachten, wir hätten Schutz unter normalen und den Bedingungen eines Einzelfehlers gehabt, aber in Wirklichkeit hatten wir überhaupt keinen

Vorlesung funktionale Sicherheit 1 – Eine Anlage mit einem eingebetteten System versagt (3) (Script 1.1)

Oft wird nach solchen Ereignissen gesagt: „Was da passierte, war so blöd, dass wirklich niemand darauf kommen konnte. Aber so etwas passiert dennoch:

- **Ein unzureichend dokumentiertes Stück Software**
- **Jemand bestellte den falschen Tank. Es war viel Hektik in diesem Projekt und es ging auch niemand aus dem Bereich der Projektleitung zum fertig aufgebauten Tank und sah ihn sich an. So wurde er unbesehen mit Steinwolle isoliert und eingehaust.**



Um solche Ausfälle zu vermeiden

- **ist es nicht ausreichend, sich nur mit der elektronischen Steuerung zu beschäftigen, weil viele Ursachen um Umfeld liegen,**
- **ist eine Richtschnur für die Projektabwicklung notwendig, um Managementfehler zu vermeiden. Diese dürfen gar nicht erst in das Projekt hineinkommen, denn es ist sehr schwierig, sie durch Prüfungen alle aufzufinden und wieder zu entfernen (der unbekannte Tankdeckel)**
- **müssen trotzdem gründliche Prüfungen ausgeführt werden. Sie sollten stufenweise erfolgen und bei den kleinsten Modulen beginnen. In diesem Beispiel hätte das SPS-Programm im Prüffeld gründlich getestet werden müssen, bevor es auf der Baustelle geladen wurde.**
- **sind probabilistische Vorhersagen nur begrenzt geeignet**
- **muss besonderes Augenmerk auf die Software gerichtet werden und ihre Erstellung unter klaren Richtlinien (In diesem Fall hätten mit dem Modul auch die Schnittstellenbeschreibung übergeben werden müssen)**


2023
SIL Slam
PEPPERL+FUCHS

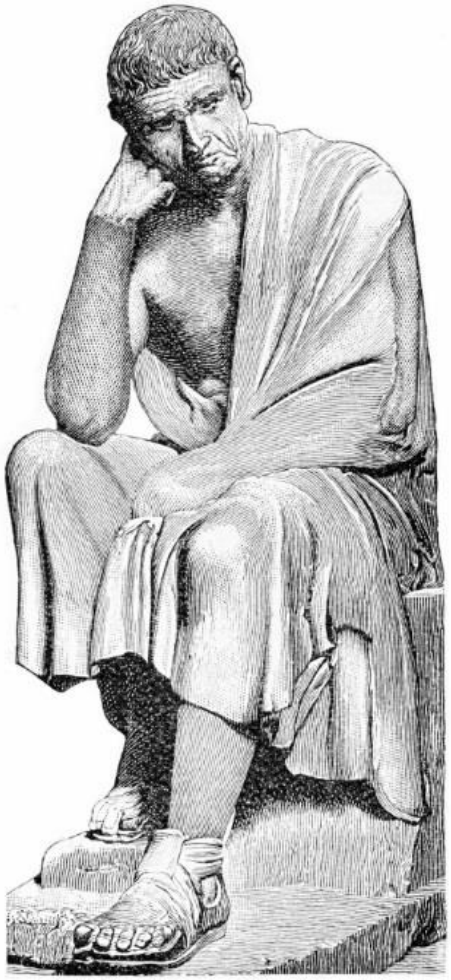
pixabay

Brauchen wir einen LDM und einen HDM?

Nein! Aber …

Hohe und niedrige Anforderungsrate

- Warum unterscheidet man zwischen der hohen und der niedrigen Anforderungsrate?
- Übliche Antwort: Weil Mechanik auf völlig unterschiedliche Art und Weise versagt, je nachdem, ob diese häufig oder nur sehr selten betätigt wird.
- Anwendungsbereich EN 61508: „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.“
- Warum die Unterscheidung zwischen HDM und LDM auch bei rein elektronischen Sicherheitsfunktionen?
- Warum die Grenze zwischen HDM und LDM bei einer Anforderung pro Jahr?
- Warum unterschiedliche Berechnung der Versagens-wahrscheinlichkeit (PFH bzw. PFD)?



iStockphoto

„Alte“ EN 61508 Teil 4

Edition 1

3.5.12
Betriebsart (en: mode of operation)
Verwendung, für die ein sicherheitsbezogenes System bestimmungsgemäß vorgesehen ist, hinsichtlich seiner Anforderungsrate, die folgende Ausprägungen annehmen kann:

- **Betriebsart mit niedriger Anforderungsrate (en: low demand mode):** wobei die Anforderungsrate an das sicherheitsbezogene System nicht mehr als einmal pro Jahr beträgt und nicht größer als die doppelte Frequenz der Wiederholungsprüfung ist,

D. h. LDM nur dann, wenn max. 2 Anforderungen innerhalb von T_1 erwartet werden
(ISA-TR84.00.02-2022: max. 0,5 Anforderungen innerhalb von T_1)

VDMA 4315-1: Turbomaschinen, Generatoren

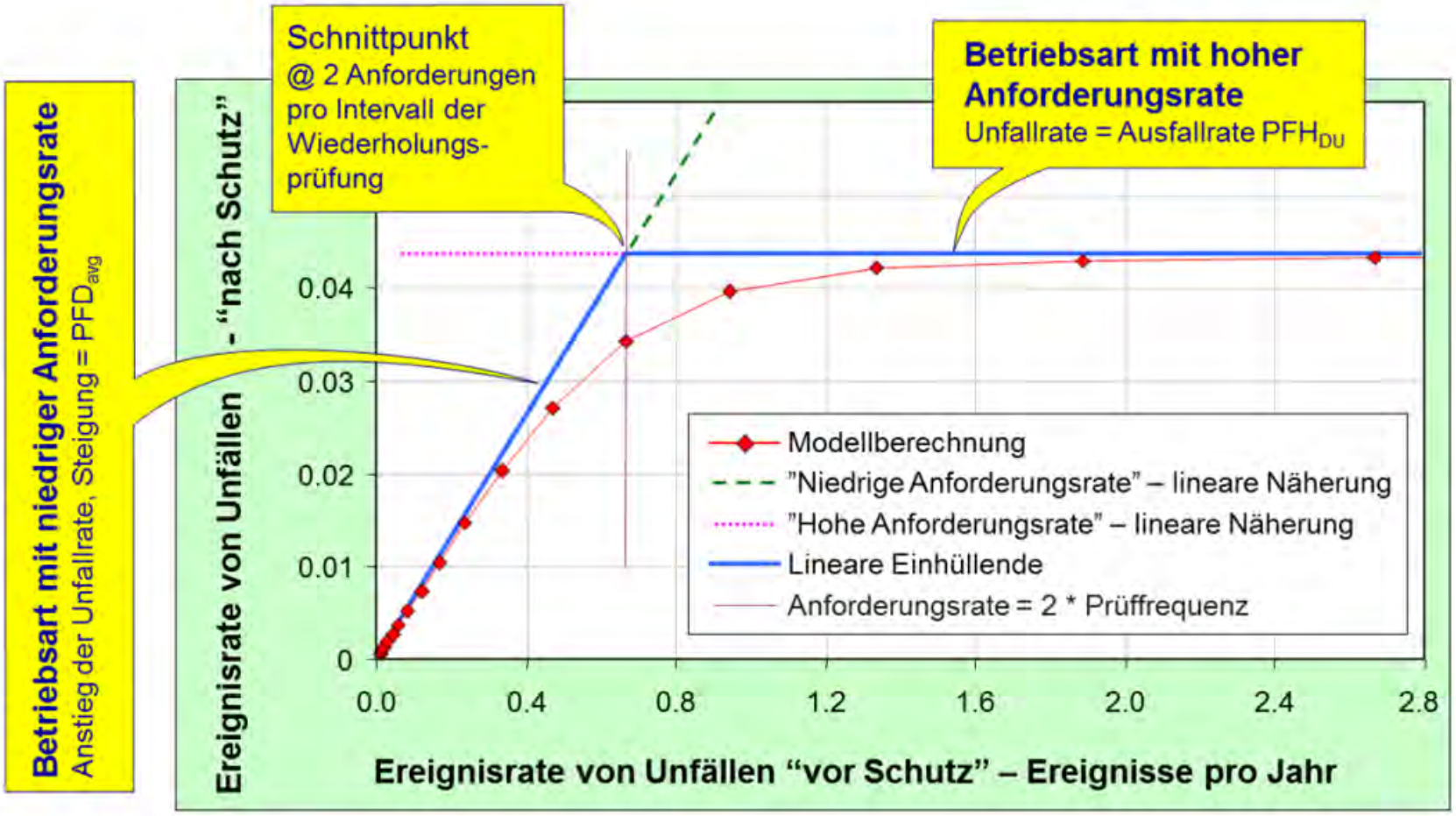


Bild 5 – Häufigkeit von Unfallereignissen „nach Schutz“ als Funktion der Anforderungsrate

Alte und neue EN 61508 Teil 4

Edition 1

3.5.12
Betriebsart (en: mode of operation)
Verwendung, für die ein sicherheitsbezogenes System bestimmungsgemäß vorgesehen ist, hinsichtlich seiner Anforderungsrate, die folgende Ausprägungen annehmen kann:

– **Betriebsart mit niedriger Anforderungsrate (en: low demand mode):** wobei die Anforderungsrate an das sicherheitsbezogene System nicht mehr als einmal pro Jahr beträgt ~~und nicht größer als die doppelte Frequenz der Wiederholungsprüfung ist~~,

~~**D. h. LDM nur dann, wenn max. 2 Anforderungen innerhalb von T_1 erwartet werden**~~

(ISA-TR84.00.02-2022: max. 0,5 Anforderungen innerhalb von T_1)

Edition 2

3.5.16
Betriebsart
(en: mode of operation)
Art der Verwendung einer Sicherheitsfunktion, welche entweder sein kann

– **Betriebsart mit niedriger Anforderungsrate (en: low demand mode):** wobei die Sicherheitsfunktion nur auf Anforderung ausgeführt wird, um die EUC in einen festgelegten sicheren Zustand zu überführen, und wobei die Häufigkeit von Anforderungen nicht mehr als einmal je Jahr beträgt, oder

Beispiel: Sicherheitsfunktion in SIL 1

- Sicherheitsfunktion mit λ_{DU} = 9,9·10^{-6} 1/h, alle 20 Jahre eine Anforderung, T_1 = 50 Jahre
- Nach EN 61508 Edition 1 wird die Sicherheitsfunktion im HDM betrieben
  - → *Anforderungsrate ist größer als die doppelte Frequenz der Wiederholungsprüfung.*

$$\frac{1}{20\ Jahre} > 2 \cdot \frac{1}{50\ Jahre} \quad \rightarrow \quad \frac{5}{100\ Jahre} > \frac{4}{100\ Jahre}$$

- Es muss die PFH berechnet werden!

EN 61508 Ed. 1

Wenn angenommen wird, dass das Sicherheitssystem bei jedem erkannten Ausfall die EUC in den sicheren Zustand bringt, wird für eine 1oo1-Architektur Folgendes erreicht:

$$PFH_G = \lambda_{DU}$$

Sicherheits-Integritätslevel	**Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung** (Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde)
4	$\geq 10^{-9}$ bis $< 10^{-8}$
3	$\geq 10^{-8}$ bis $< 10^{-7}$
2	$\geq 10^{-7}$ bis $< 10^{-6}$
1	$\geq 10^{-6}$ bis $< 10^{-5}$
ANMERKUNG Siehe nachfolgende Anmerkungen 3 bis 9 für Einzelheiten zur Interpretation dieser Tabelle.	

$\lambda_{DU} = 9{,}9 \cdot 10^{-6}$ 1/h, d. h. PFH-Anforderung für SIL 1 wird erfüllt

Anforderung nach 20 Jahren

$$F(t) = 1 - e^{-\lambda_{DU} \cdot t}$$

$$F(20\,Jahre) = 1 - e^{-9{,}9 \cdot 10^{-6} \cdot 20 \cdot 8760} = 0{,}824$$

Ist es akzeptabel, dass eine Sicherheitsfunktion mit einer Wahrscheinlichkeit von mehr als 80% versagt, wenn man sie braucht?

Falls nicht, dann muss die **PFD auf einen vertretbaren Wert begrenzt** werden.

Sicherheits-Integritätslevel	Betriebsart mit niedriger Anforderungsrate (mittlere Ausfallwahrscheinlichkeit der entworfenen Funktion bei Anforderung)
4	$\geq 10^{-5}$ bis $< 10^{-4}$
3	$\geq 10^{-4}$ bis $< 10^{-3}$
2	$\geq 10^{-3}$ bis $< 10^{-2}$
1	$\geq 10^{-2}$ bis $< 10^{-1}$
ANMERKUNG Siehe nachfolgende Anmerkungen 3 bis 9 für Einzelheiten zur Interpretation dieser Tabelle.	

Idee: Statt PFH immer die PFD berechnen

- Sicherheitsfunktion mit λ_{DU} = 8,3·10^{-3} 1/h, alle 20 Minuten eine Anforderung, T_1 = 1 Tag
- Eine PFD-Berechnung ergibt:

$$PFD_{avg} = \lambda_{DU} \cdot \frac{T_1}{2} = 8,3 \cdot 10^{-3} \cdot \frac{24}{2} = 9,96 \cdot 10^{-2} \approx 10\%$$

- Die PFD erfüllt die Anforderung für SIL 1
- Jede zehnte Anforderung „geht schief“

PEPPERL+FUCHS

Wieviel Unfälle passieren in einem Jahr?

$$F(t) = 1 - e^{-\lambda_{DU} \cdot t}$$

$$F(20\ Minuten) = 1 - e^{-8{,}3 \cdot 10^{-3} \cdot \frac{1}{3}} = 2{,}76 \cdot 10^{-3}$$

Jedes Jahr wird die Sicherheitsfunktion 26280 mal angefordert. Bei jeder Anforderung ist die Wahrscheinlichkeit, dass diese versagt, 2,76 Promille. Daraus folgt, dass jedes Jahr mehr als 72 Unfälle zu erwarten sind.

Ist es akzeptabel, dass eine SIL 1 Sicherheitsfunktion so „schlecht“ ist, dass jede Woche ein oder mehrere Unfälle zu beklagen sind?

Falls nicht, dann muss die **Unfallrate (PFH) auf einen vertretbaren Wert begrenzt** werden.

PEPPERL+FUCHS

Erkenntnis

Für die Beurteilung, ob eine Sicherheitsfunktion ausreichend zuverlässig ist, müssen **zwei Aspekte** betrachtet werden:

1. Anzahl der zu erwartenden Unfälle pro Jahr
2. Wahrscheinlichkeit des Versagens bei Anforderung

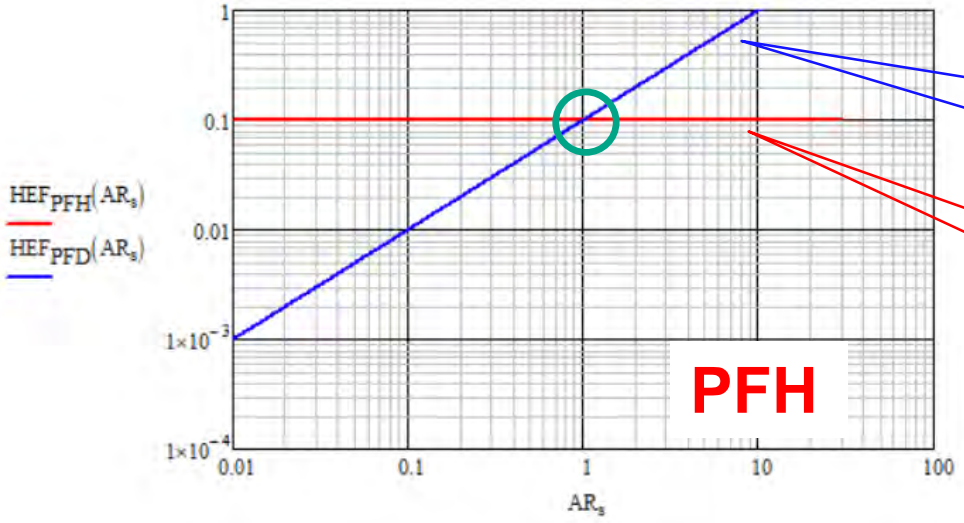
Über Punkt 1 gibt die PFH Auskunft, für Punkt 2 ist die PFD ausschlaggebend

Es muss immer beides berechnet werden, die PFH und die PFD

IMMER?

Unfallrate u. PFD über der Anforderungsrate

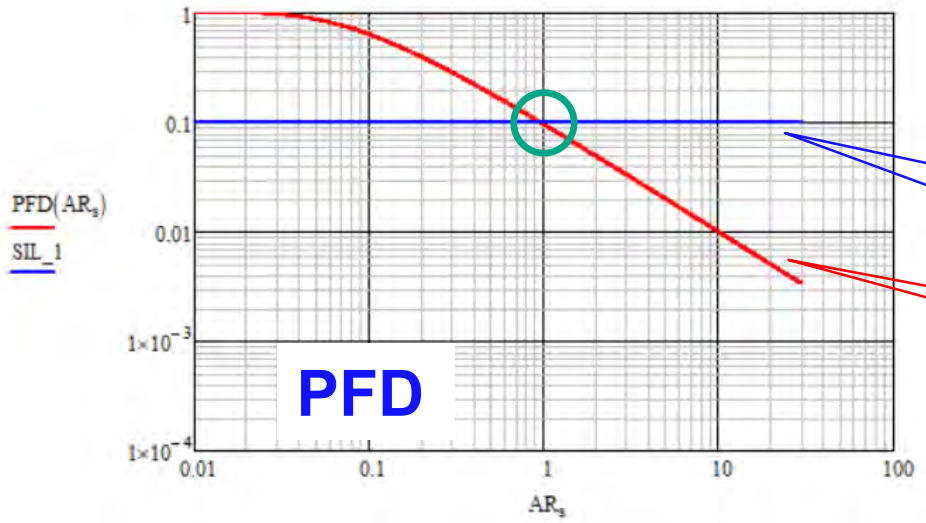
1. Unfallrate



Unfallrate in Abhängigkeit der Anforderungsrate bei **PFD = 0,1**

Unfallrate in Abhängigkeit der Anforderungsrate bei **PFH = 1·10^{-5}**

2. PFD



Maximale PFD für SIL 1 **PFD = 0,1**

PFD in Abhängigkeit der Anforderungsrate bei **PFH = 1·10^{-5}**

PEPPERL+FUCHS

LDM und HDM unnötig?

Wir brauchen im Prinzip keinen LDM und HDM …

… aber wir brauchen eine PFD- und PFH-Berechnung!

Je nachdem, wie Häufig eine Anforderung stattfindet, reicht es aus, eine der beiden Größen zu berechnen. Die Anforderung der jeweils anderen Größe wird dann automatisch ebenfalls erfüllt.

Wo ist das Problem bei der alten Definition?

Edition 1

3.5.12
Betriebsart (en: mode of operation)
Verwendung, für die ein sicherheitsbezogenes System bestimmungsgemäß vorgesehen ist, hinsichtlich seiner Anforderungsrate, die folgende Ausprägungen annehmen kann:

- **Betriebsart mit niedriger Anforderungsrate (en: low demand mode):** wobei die Anforderungsrate an das sicherheitsbezogene System nicht mehr als einmal pro Jahr beträgt und nicht größer als die doppelte Frequenz der Wiederholungsprüfung ist,

Durch den gelb hervorgehobenen Zusatz kann die PFD-Berechnung bei seltener Anforderung umgangen werden!

Um das zu verhindern, wurde der gelb markierte Teil in der Edition 2 der EN 61508 ersatzlos gestrichen.

PEPPERL+FUCHS

Manchmal geht Redundanz über alles