Tag 1: Fachvorträge

NAMUR-Praxispapier zur VDI/VDE 2180-4

Freie Auswahl für Ausfallraten?!?

2021-09-21

Hablawetz // Knödler // Schmitt-Pauksztat

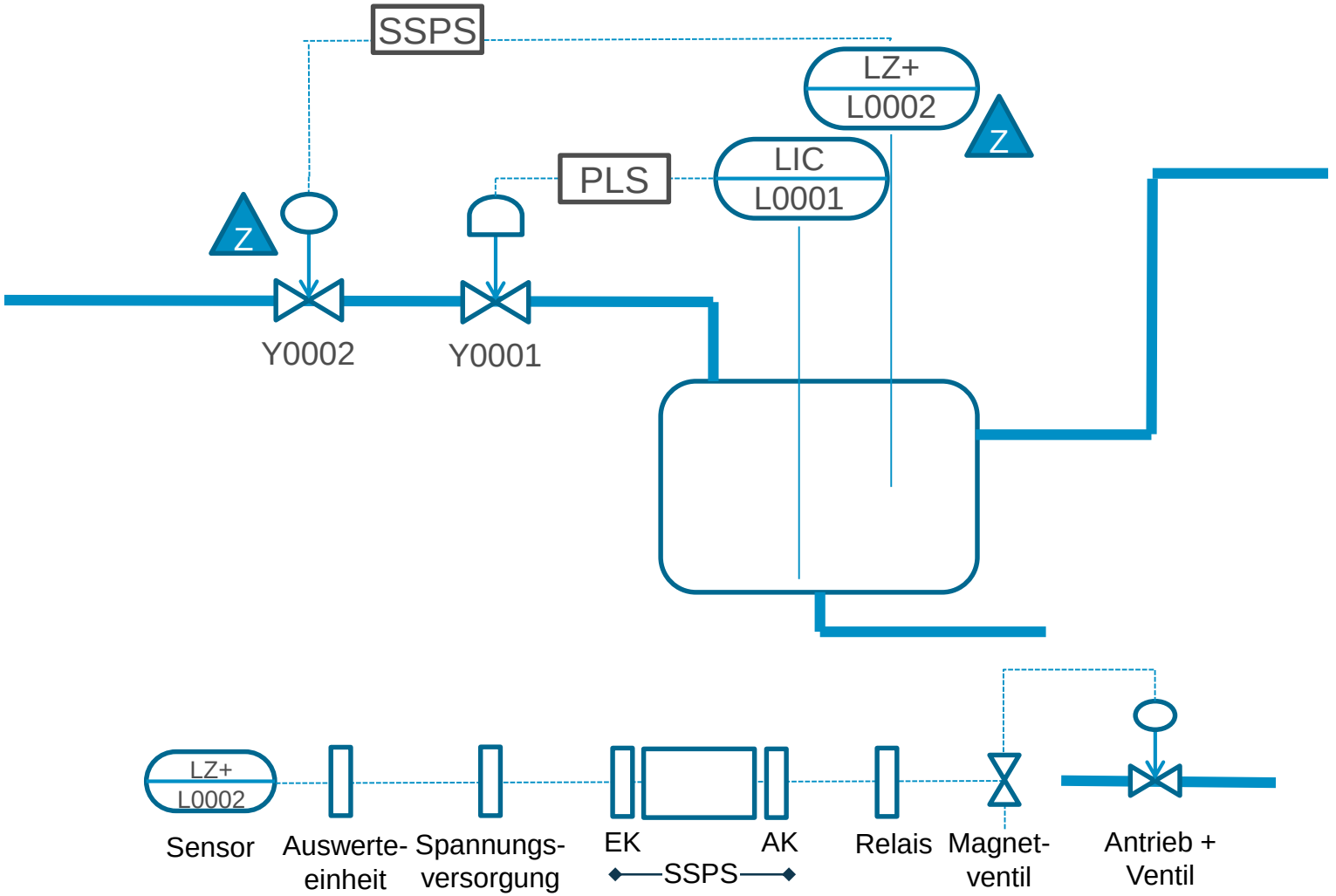
Wir basteln uns einen SIL-Nachweis

Umfrage: Wer von Euch erstellt SIL-Nachweise?

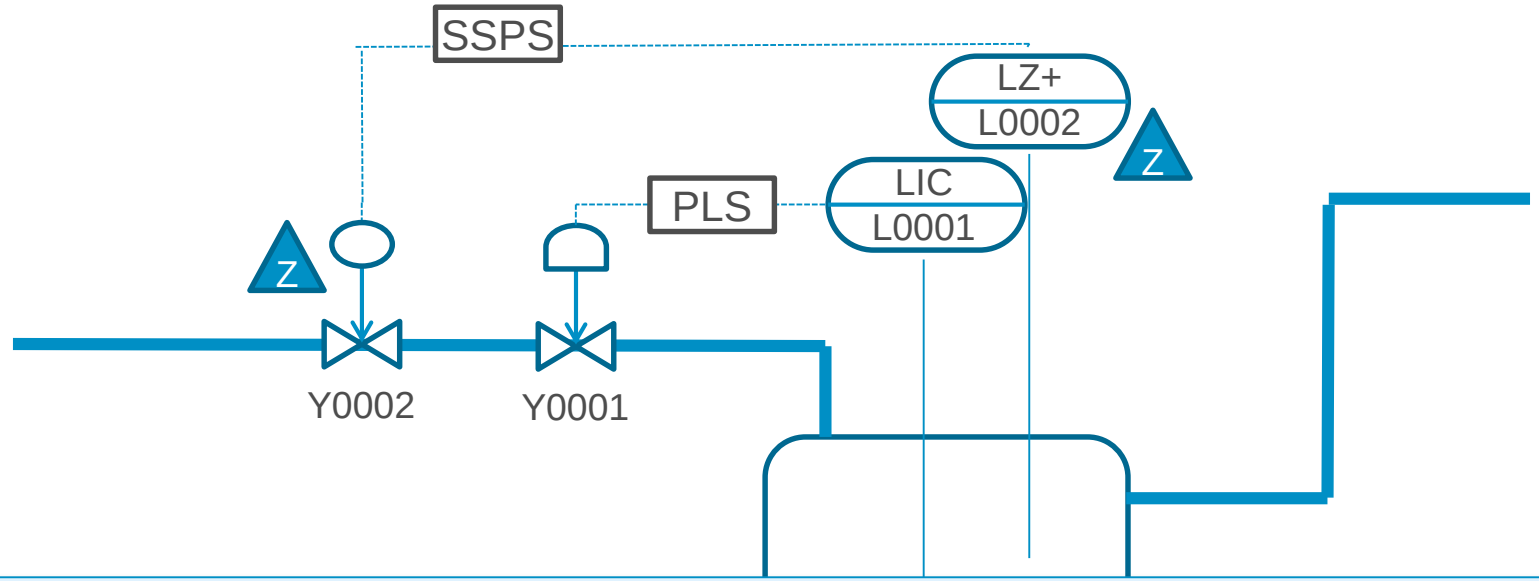
Wer von Euch erstellt SIL-Nachweise? (radio-button)

- erstelle regelmäßig SIL-Nachweise
- erstelle ab und zu mal einen SIL-Nachweis
- erstelle NIE SIL-Nachweise

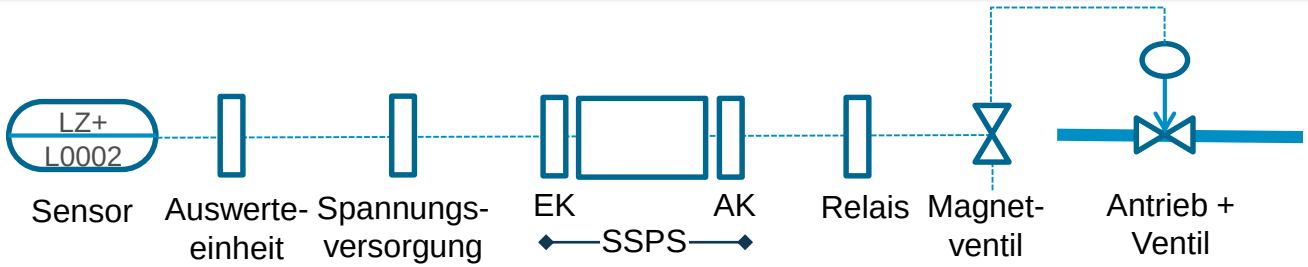
…aus dem Alltag der Funktionalen Sicherheit



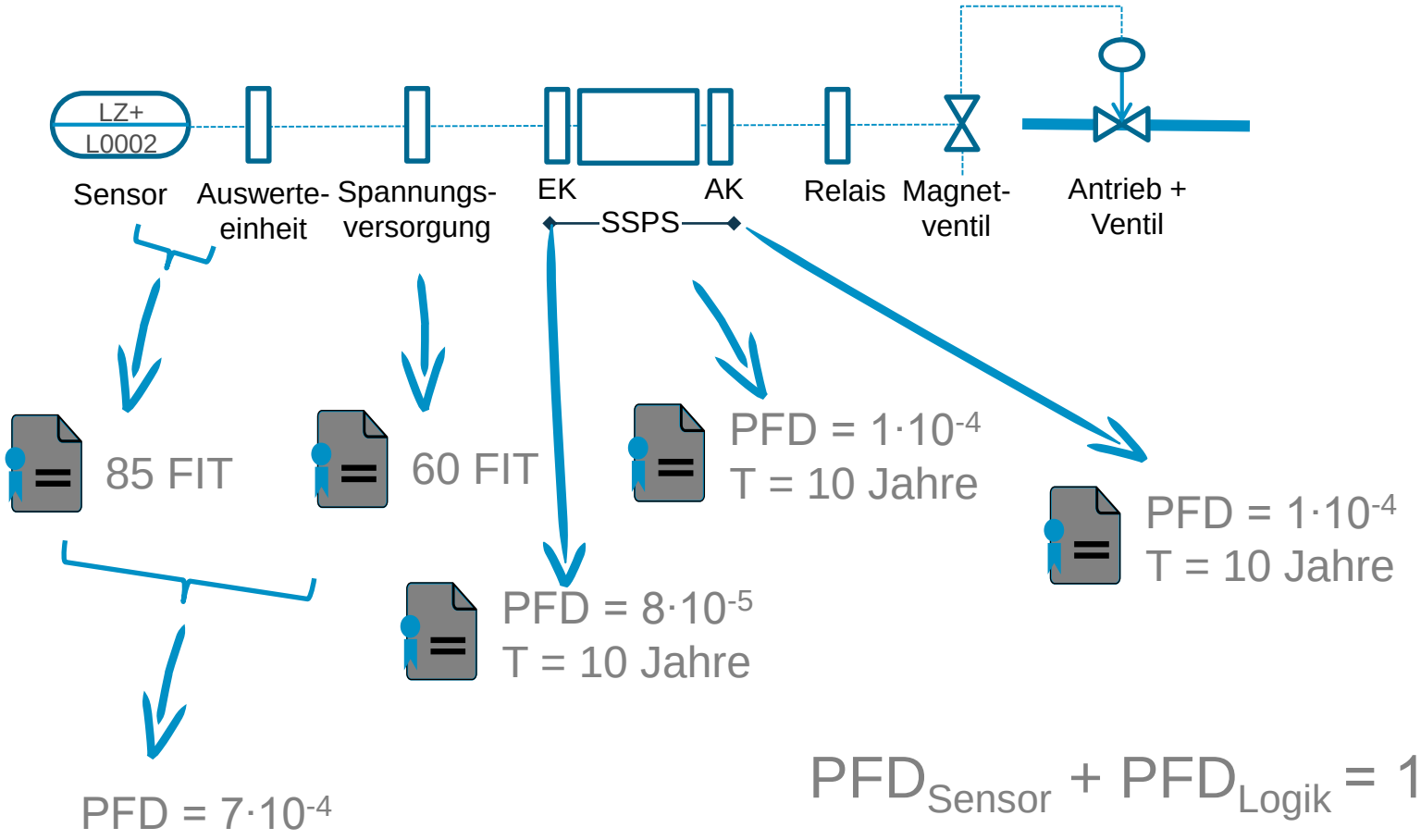
…aus dem Alltag der Funktionalen Sicherheit



Annahme: systematische Eignung (inkl Betriebsbewährung vorhanden)
-> Fokus auf PFD-Berechnung



PFD für Sensor-/Logik-Teilsystem simpel zu berechnen

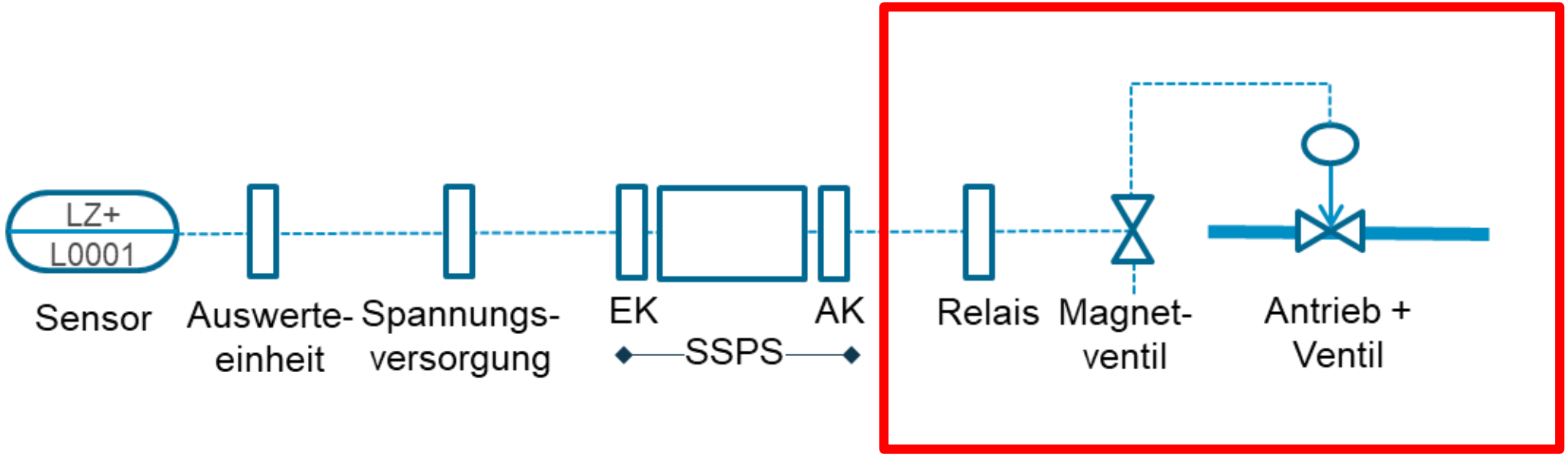


$PFD_{Sensor} + PFD_{Logik} = 1 \cdot 10^{-3}$

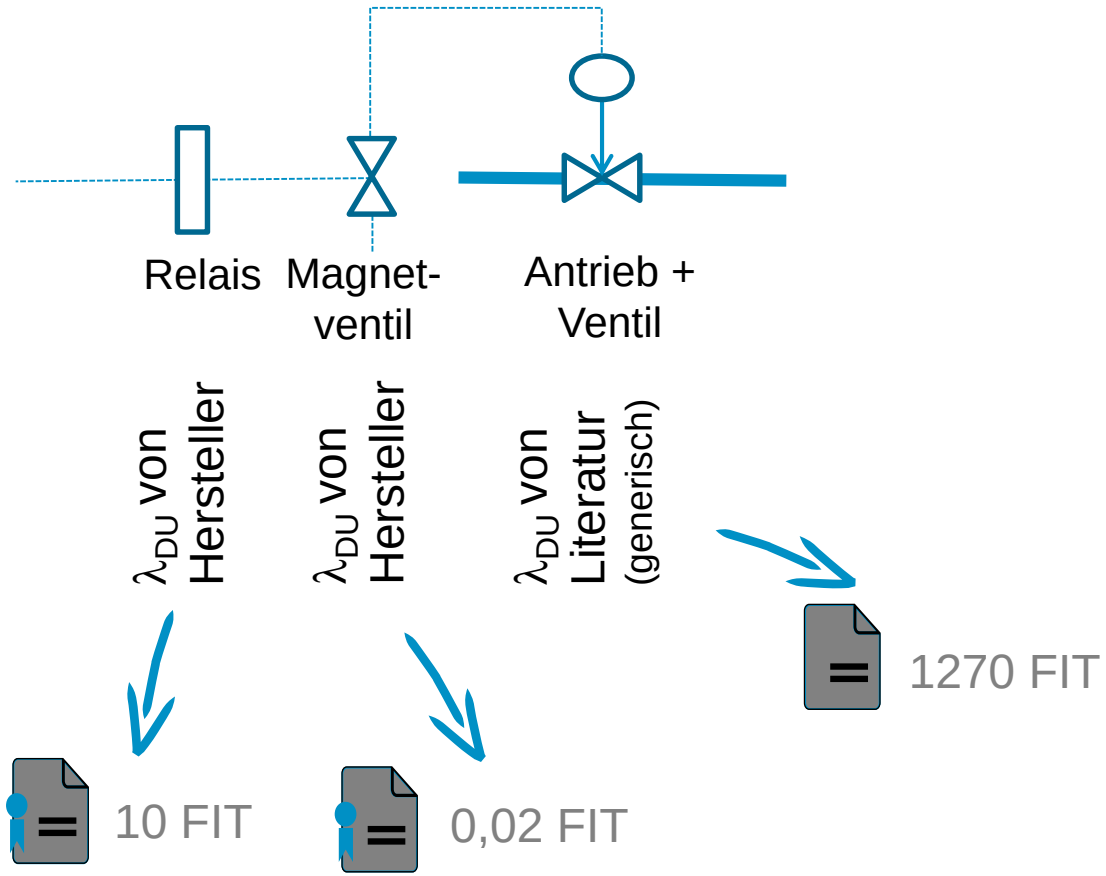
https://www.pepperl-fuchs.com/germany/de/32909.htm

*Berechnung nach VDI/VDE 2180-3, PTC=100%, PTI =1a

Was machen wir mit dem Aktor-Teilsystem?



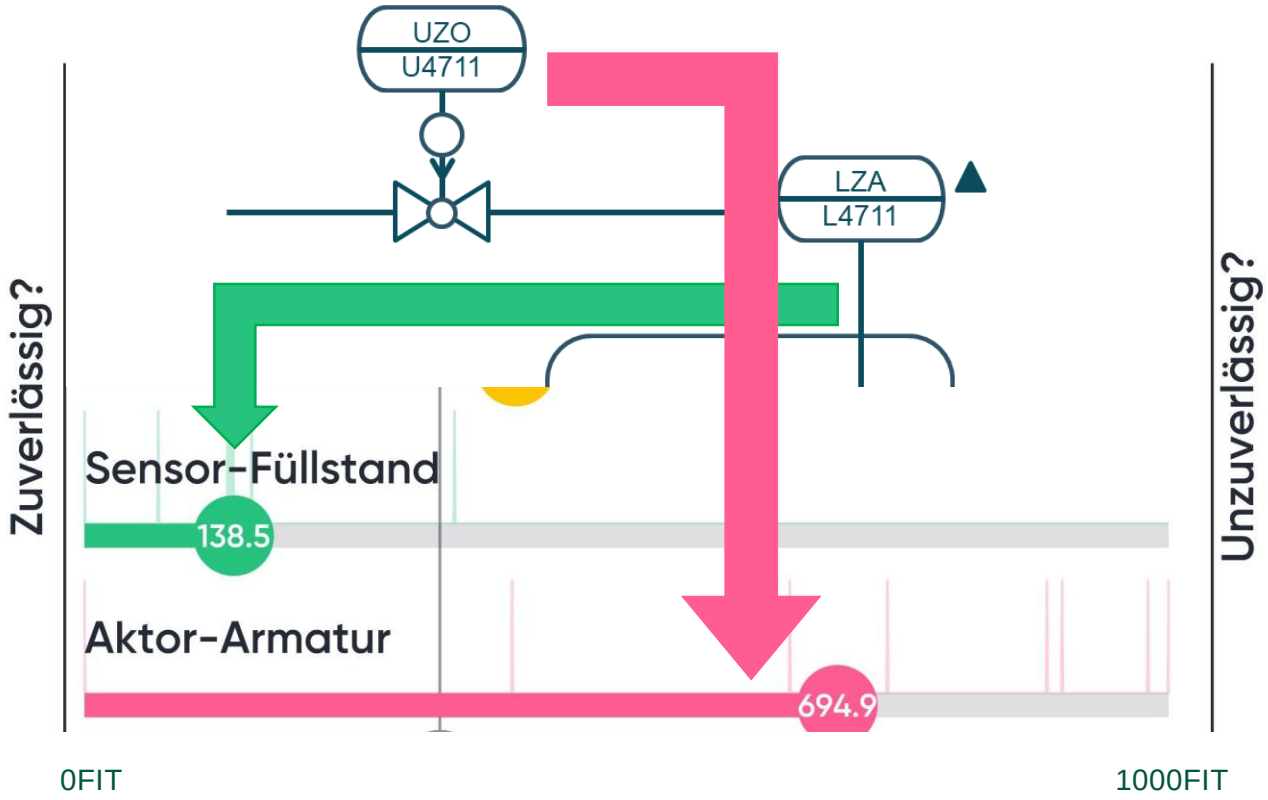
Nimm generische Werte aus Literatur…



$PFD_{Aktor} = 6 \cdot 10^{-3}$

*Berechnung nach VDI/VDE 2180-3, PTC=100%, PTI =1a

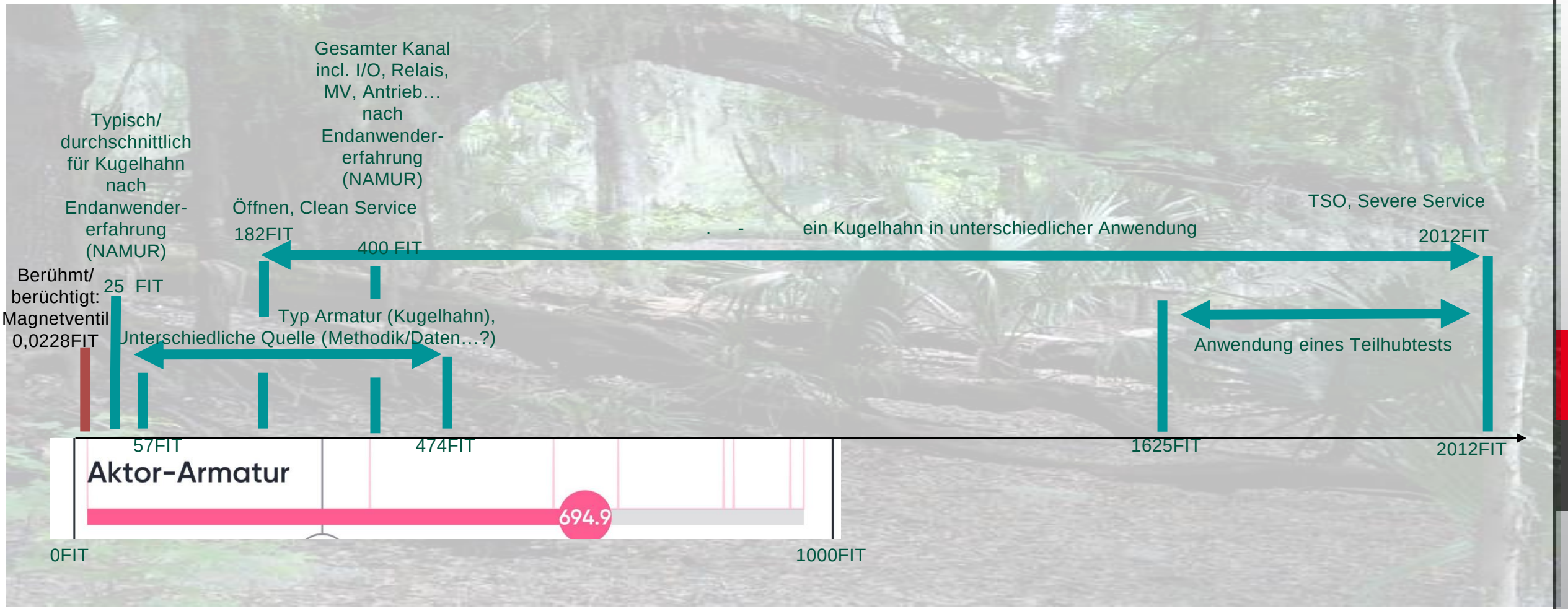
Ergebnisse einer Marktrecherche



LambdaDU = Rate gefährlicher (Dangerous) und unentdeckter (Undetected) „zufälliger“ Ausfälle in Failures In Time [FIT] = Ausfälle pro 10^9 Stunden

Ergebnisse einer Marktrecherche

LambdaDU = Rate gefährlicher (Dangerous) und unentdeckter (Undetected) Ausfälle in Failures In Time [FIT] = Ausfälle pro 10^9 Stunden



Mechanik – Beispiel Schraube – FIT ?

Klassifizierung von Edelstahl, z.B. A2-70 (Standard-Edelstahl)

A	Kennzeichen Werkstoffgruppe A = Austenitischer Edelstahl (Chrom-Nickel-Stahl)
2	Kennzeichen Stahlgruppe 1 = Automatenstahl 2 = Kaltstauchstahl legiert mit Chrom und Nickel (klassischer Edelstahl) 3 = Kaltstauchstahl mit Chrom und Nickel legiert und gehärtet mit Titan, Niob und Tantal 4 = Kaltstauchstahl mit Chrom, Nickel und Molybdän (hochsäurebeständig) 5 = Kaltstauchstahl mit Chrom, Nickel und Molybdän (hochsäurebeständig) und gehärtet mit Titan, Niob und Tantal
-70	Festigkeitsangabe: Zugfestigkeit 50 = 1/10 der Zugfestigkeit (mindestens 500 N/mm²) 70 = 1/10 der Zugfestigkeit (mindestens 700 N/mm²) 80 = 1/10 der Zugfestigkeit (mindestens 800 N/mm²) Regelzugfestigkeit für A1 A2, A4 (Standard) A4-80, A5

DN	Flanschtyp nach EN 5211	Zulässiges Drehmoment am Flanschbild 1) nach ISO 5211 [Nm]	Zulässiges Drehmoment für A4-70 Schrauben am Flanschbild 2) [Nm]	Zulässiges Drehmoment für A4-70 Schrauben auf Abscheren am Flanschbild 2) [Nm]	Md_{ref} Losreiß/ Grundmoment [Nm]	mit Sicherheitsfaktor 1,5 = Mdref	Md Lauf [Nm]	mit Sicherheitsfaktor 1,5 Md Lauf [Nm]	Md_{ref} Losreiß/ Grundmoment [Nm]	mit Sicherheitsfaktor 1,5 = Mdref	Md Lauf [Nm]	mit Sicherheitsfaktor 1,5 Md Lauf [Nm]	Maximal zulässiges Drehmoment Welle (1.4408) [Nm] Temperature [°C] 25	20	50	100	200	220
					(PTFE, PTFE X)				(PTFE/Glas, PTFE XC)									
15	F04	63	89	546	22	33	15	23	28	41	19	29	90		84	73		56
25	F05	125	151	922	43	65	30	45	54	81	38	56	200	200	186	162	129	125
40	F07	250	384	2348	66	99	46	69	83	124	58	87	290	290	269	235	186	181
50	F07	250	384	2348	106	159	74	111	133	199	93	139	600	600	557	486	386	374
80	F10	500	887	5420	140	210	98	147	175	263	123	184	600	600	557	486	386	374
100	F10	500	887	5420	200	300	140	210	250	375	175	263	810	810	752	656	521	505
150	F12	1000	1580	9652	434	651	304	456	543	814	380	570	1550	1550	1439	1255	996	967
200	F14	2000	3290	20099	534	801	374	561	668	1001	467	701	3200	3200	2971	2590	2057	1996
250	F14	2000	3290	20099	800	1200	560	840	1000	1500	700	1050	4500	4500	4179	3643	2893	2807
300	F16	4000	6059	37013	1066	1599	746	1119	1333	1999	933	1399	5350	5350	4968	4331	3439	3337
400	F25	8000	11938	72931	2120	3180	1484	2226	2650	3975	1855	2783	9880	9880	9174	7998	6351	6163

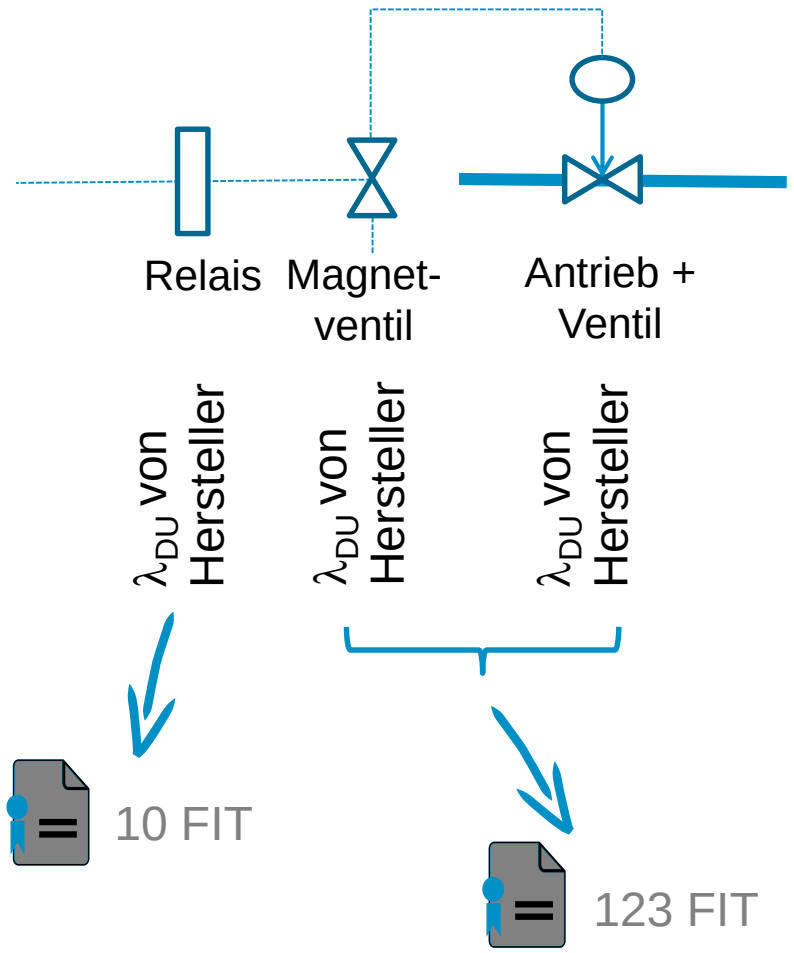
*1,5

1) Die Berechungen der zulässigen Momente basiert auf den Festigkeitswerten von Schrauben mit einer Zugbeansprachung > 290 MPa z.B. A2 -70

- Vorschlag in einem CEN-Normungs-vorhaben: Schraube=5 FIT -> PFD
- Realität: Welche Schraube verwenden wir? > Systematik – Zulässiges Drehmoment >1,5fache!

Mechanik FIT für die FUSI?

Nimm Herstellerangaben (wenn vorhanden)…



$PFD_{Aktor} = 1 \cdot 10^{-3}$

*Berechnung nach VDI/VDE 2180-3, PTC=100%, PTI =1a

Warum nicht eigene Ausfallraten nutzen als Betreiber?

NAMUR - Interessengemeinschaft
Automatisierungstechnik der Prozessindustrie e.V.

AK-PRAXIS

Praktische Anwendung der VDI/VDE2180-4

Stand: 2021-07-28

https://www.linkedin.com/posts/namur-ev_2021-07-28ak-praxisvdi2180-4-de-activity-6826146306482872320-9N6A

https://www.namur.net/fileadmin/media_www/Dokumente/AK-PRAXIS_4.5_VDI2180-4_DE.pdf

Warum nicht eigene Ausfallraten nutzen als Betreiber?

	Betreiber A	Betreiber B	Betreiber C	Betreiber D	Betreiber E	Betreiber F
Betriebszeit	$420 \cdot 10^6$ h	$56 \cdot 10^6$ h	$46 \cdot 10^6$ h	$43 \cdot 10^6$ h	$565 \cdot 10^6$ h	$83 \cdot 10^6$ h
Anzahl DU-Fehler in Betriebszeit	41	2	2	3	10	2
λ_{DU}	120 FIT	95 FIT	115 FIT	154 FIT	27 FIT	64 FIT
Anmerkung:	gesamter Aktorkanal (inkl. elektrische Komponenten)		inkl. Magnetventile	gesamter Aktorkanal (inkl. elektrische Komponenten)	ausschließlich mechanische Komponente	inkl. Magnetventile

Praxispapier zu VDI/VDE 2180-4

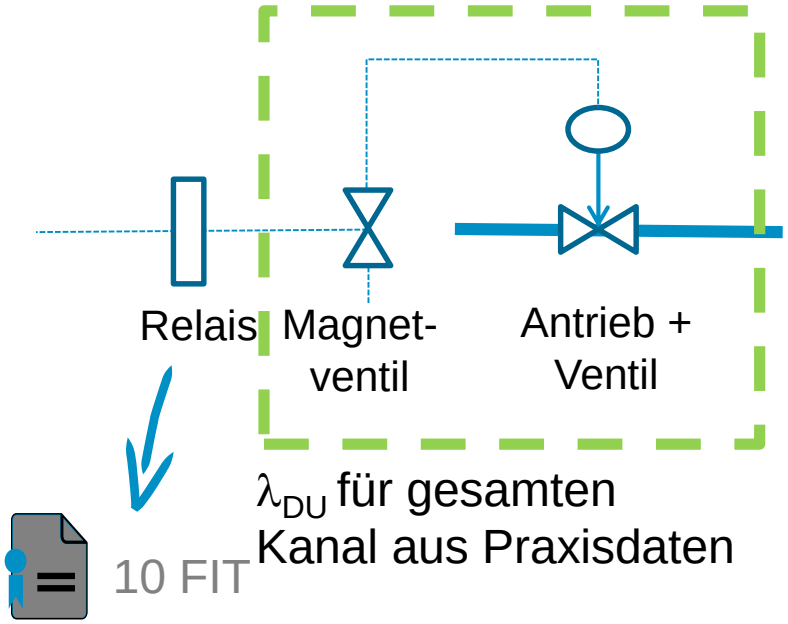
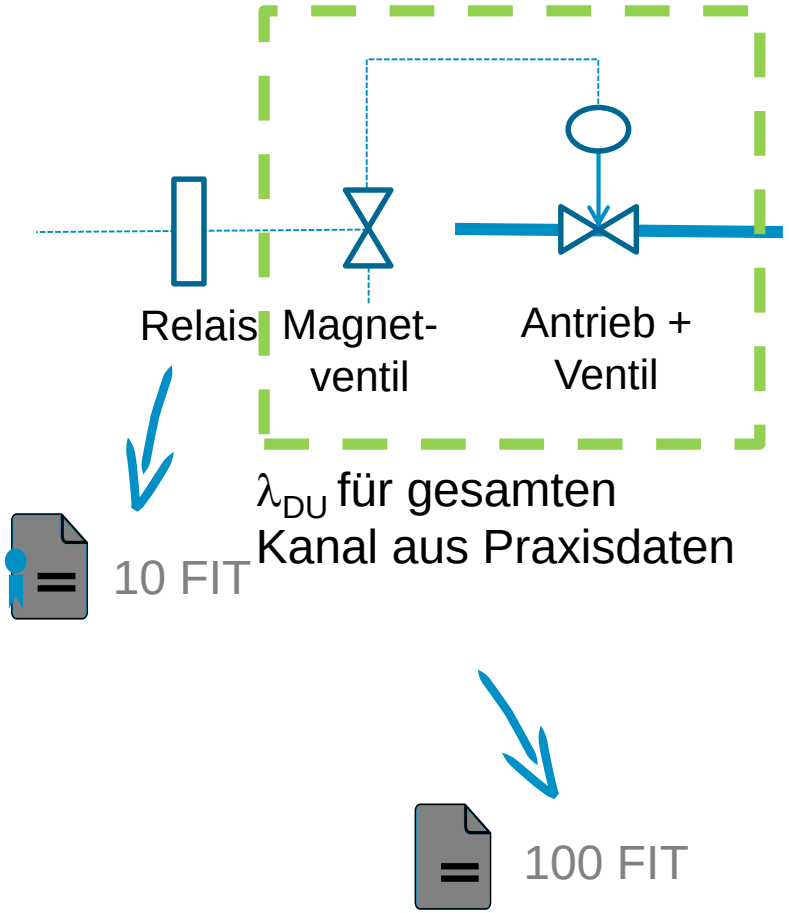


Tabelle 3: Ausfallraten zur praktischen Anwendung

Ausfallrate	Wert	Kommentar
$\lambda_{DU, erw.Aktor}$	100 FIT	Ersatzwert für Komponenten „Anbauteil“, „Antrieb“, „Diagnoseeinrichtung“, „Stellglied“ und „Ventilschaltverstärker“
$\lambda_{DU, mech}$	25 FIT	Ersatzwert für Stellglied inkl. Antrieb, wenn ALLE system. Fehler ausgeschlossen sind, d.h. insbesondere Fehler bzgl. Alterung/Verschleiß in den Stördaten NICHT auftreten

Praxispapier zu VDI/VDE 2180-4



$PFD_{Aktor} = 1 \cdot 10^{-3}$

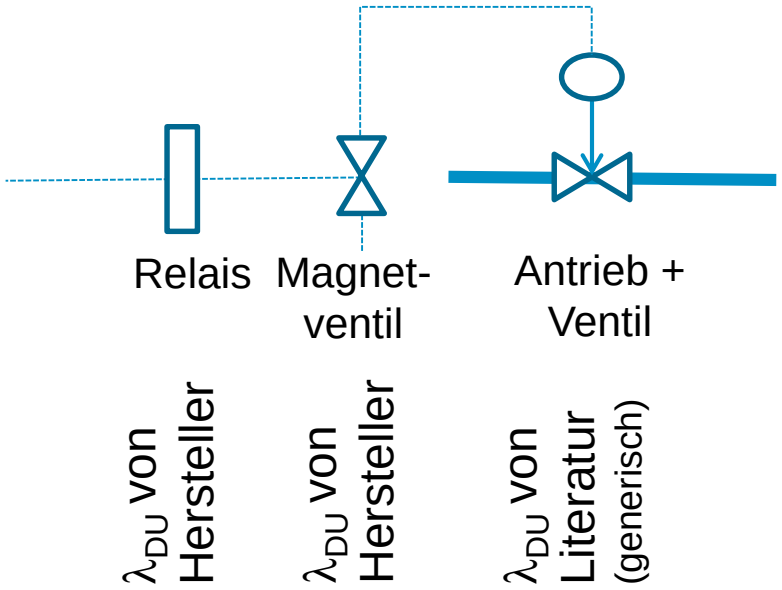
*Berechnung nach VDI/VDE 2180-3, PTC=100%, PTI =1a

Umfrage: Welche Variante bevorzugt ihr?

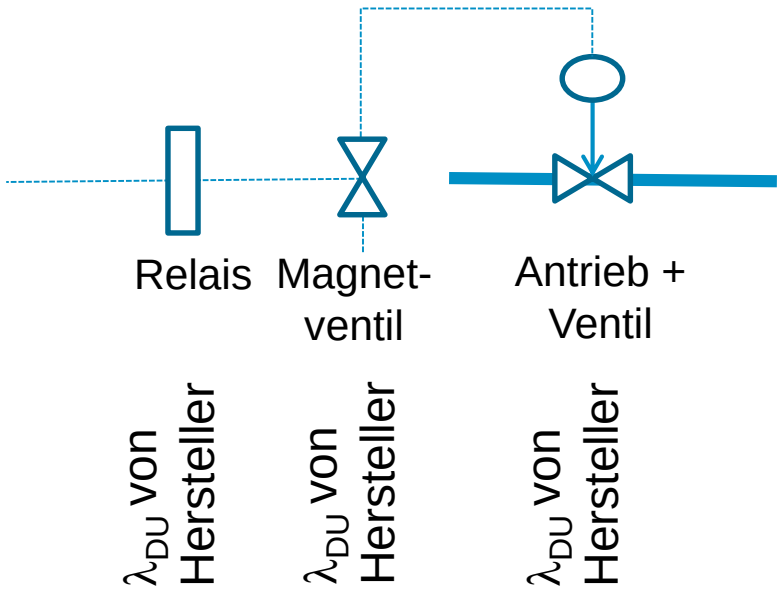
Welche Variante bevorzugt ihr? (multiple Choice)

- verwende am liebsten Literaturwerte
- verwende am liebsten Herstellerangaben
- verwende am liebsten Praxisdaten

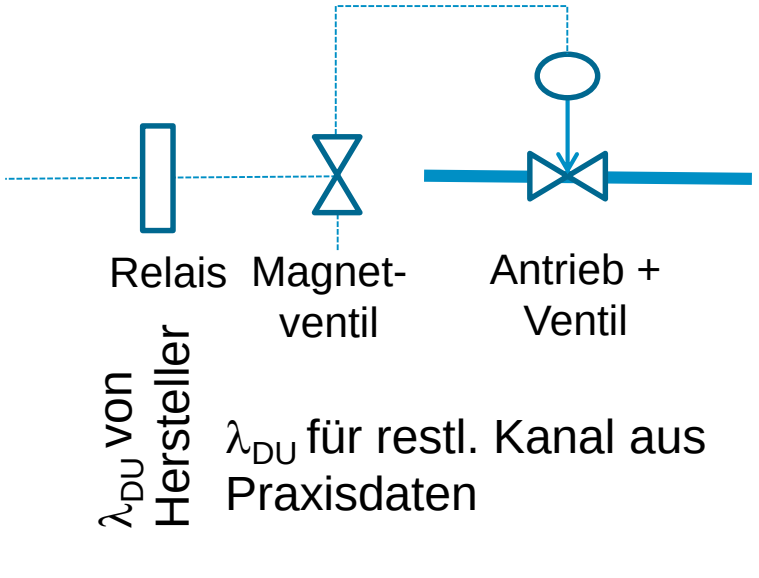
Ergebnis der PFD-Berechnung



$PFD_{Aktor} = 6 \cdot 10^{-3}$



$PFD_{Aktor} = 1 \cdot 10^{-3}$



$PFD_{Aktor} = 1 \cdot 10^{-3}$

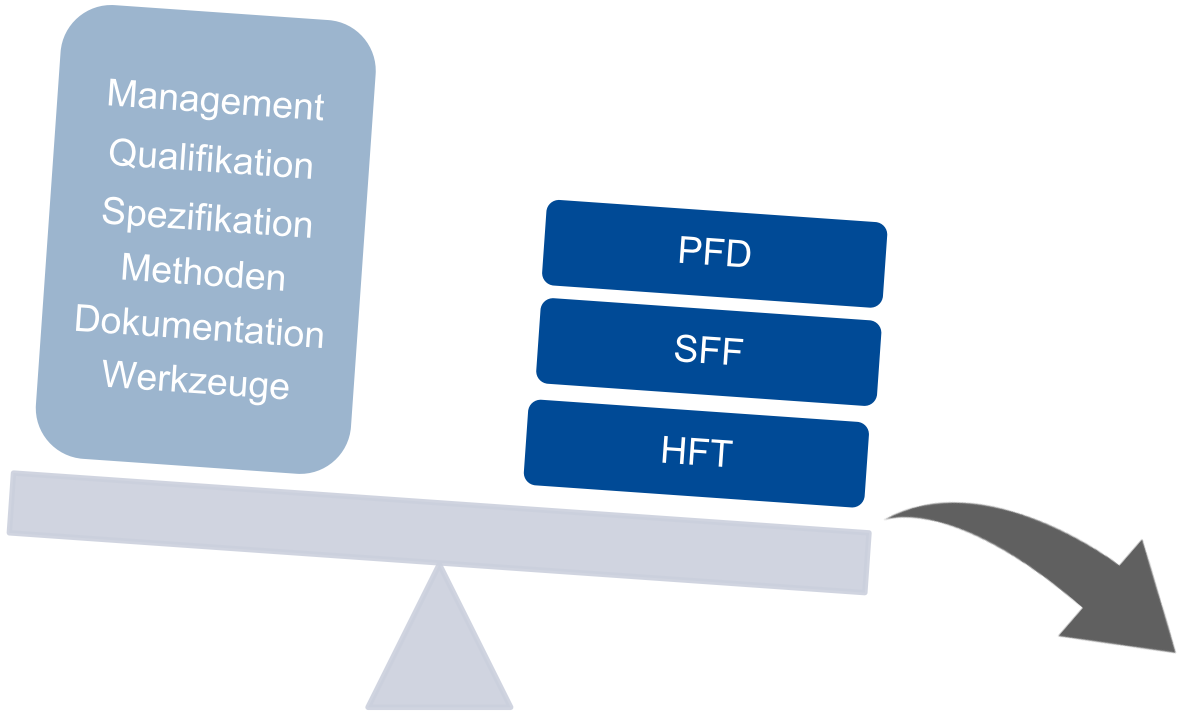
Umfrage: Welches Ergebnis ist richtig? und warum?

Welches Ergebnis ist richtig? (radio-button)

- Das Ergebnis mit Literaturwerten ist richtig.
- Das Ergebnis mit Herstellerangaben ist richtig.
- Das Ergebnis mit Praxisdaten ist richtig.
- Alle Ergebnisse sind richtig.
- Ab jetzt höre ich mit der Rechnerei auf.

Lieber systematisch richtig als zufällig falsch!

Gerechnet, alles gut! – Oder doch nicht?



Systematisc Fehler **vermeiden**

Zufällige Fehler **beherrschen**

Prio1: Systematische Fehler verhindern!

1. Undichtigkeit im Durchgang
2. Alterung / Verschleiß
3. Blockieren der Mechanik
4. Produktionsfluss
5. Undichtigkeit nach außen
6. Interner Gerätefehler (nicht durch Medium verursacht)
7. Planungsfehler
8. Sonstiger zufälliger Fehler
9. Korrosion
10. Umwelteinfluss

Umfrage: Was nehmt ihr aus dem Vortrag mit?

Freitext

Danke // Thanks

NAMUR@LinkedIN

NAMUR Homepage

RAMSYS
DAS machen Ingenieure

FSM und die Betrachtung des Prozessanschlusses

Agenda

- Vorstellung
- Systematische / Zufällige Fehler
- Fehlerverteilung in der Funktionalen Sicherheit
- Functional Safety Managementsystem
- Betrachtung des Prozessanschlusses

Agenda

- Praxisbeispiele
  - Projekte / As-Built Dokumentation
  - Beachtung anderer Regelwerke
  - Anlagenspezifische Daten (Unterschied bei SIL-Geräten)
  - Modifikation / Wartung
  - Unerwartete Fehler
  - Was kann ich tun, um diese Fehler zu vermeiden?

Kontaktdaten: Malika Mast

Persönliche Vorstellung:

Malika Mast

Geschäftsführerin

- 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

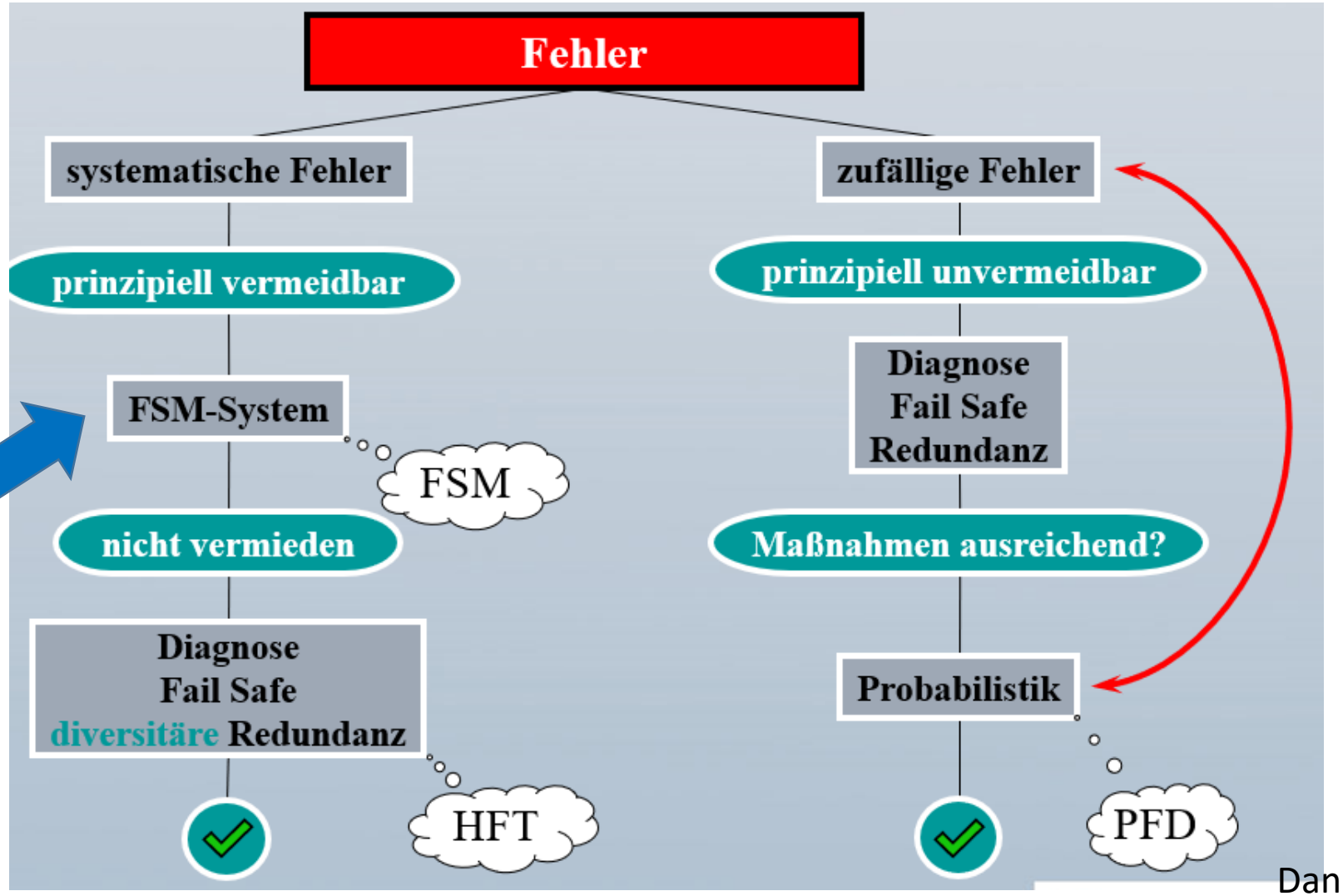
46286 Dorsten

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

m.mast@ramsys.org

www.ramsys.org

Systematische / Zufällige Fehler



Prozessanschluss

Danke Dr. A. Hildebrandt

Fehler Verteilung in der Funktionalen Sicherheit

Functional Safety Managementsystem

- Abdeckung des Sicherheitslebenszyklus
- Festlegung der Verantwortlichkeiten im Betrieb und Dienstleistern
  - In allen Betriebsphasen und während Projekten
- Automatisierte Abläufe im Betrieb
  - Festlegung welche Dokumentation benötigt und erstellt wird
- Welche Qualifikation müssen die Beteiligten haben
- Schnittstellenmanagement zu anderen Bereichen


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®

Prozessanschluss

- Innerhalb der Funktionalen Sicherheit wird der Fokus oft auf einige wenige Punkte gelegt:
  - SIL-Nachweisberechnung
  - Einsatzbewährung
  - Eignung der Geräte
  - FSM / Dokumentation

- Die Einflüsse und zu beachtenden Faktoren der eigentliche Anlage und die als „Standardplanung“ angesehen arbeiten werden meist vernachlässigt

- Speziell betrachtet wird folgend der Prozessanschluss und die dazugehörigen Einflüsse auf die Funktionale Sicherheit

Prozessanschluss

Was bezeichnen wir als Standardplanung

- Bestandteile der Standardplanung
  - Verfahrensdaten und zusätzliche Anforderungen (SIL, Ex, Werksnormen, etc.)
  - Erstellung der Spezifikation
    - Geräte
    - Leitsystem / SSPS
  - Anfrage an die Hersteller
  - Verdrahtung und Verschaltung der Geräte
  - Montagepläne
  - Erstellung der Prüfkonzepte
  - AS-Built Dokumentation

Praxisbeispiele

Projekte / AS-Built Dokumentation

- Kein Projekt läuft zu 100% perfekt ab, gewisse Einflüsse sind immer vorhanden
  - Führt zu möglicherweise unvollständiger oder nicht aktuellen Dokumentation
  - Verschiedene Projektteile haben mit unterschiedlichen Voraussetzungen gearbeitet
  - Kommunikation zwischen Betreiber und Dienstleistern
  - Unvollständige Bestandsdokumentation führt zu folge Fehlern

Praxisbeispiele

Beachtung anderer Regelwerke

- Welche Unterschiede habe ich zwischen einer Regeleinrichtung und einer PLT-Sicherheitseinrichtung
  - SIL-Eignung der Geräte
  - Anlagenspezifische Daten
- Beachtung aller relevanten Regelwerke und Vorschriften
  - Explosionsschutz
  - C-Normen
  - WHG
  - Etc.

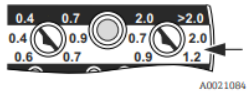
Praxisbeispiele

Anlagenspezifische Daten (Unterschied bei SIL-Geräten)

- Verfahrensdaten (Links mit SIL-Eignung / Rechts ohne SIL-Eignung)
  - Umgebungstemperatur
  - Mediums Temperatur
  - Drücke bis x Bar
  - Etc.
  - Beispiel: Prozesstemperatur

Prozesstemperatur

Der Temperaturbereich, in dem ein sicherheitsbezogener Betrieb zulässig ist, ist abhängig vom gewählten Dichtebereich.

Betriebsart MIN (weißer Bereich)	Dichtebereich	Dichte ρ_{Low}	Dichte ρ_{High}	Temperaturbereich	
				minimal	maximal
	1	0,4 g/cm³	0,7 g/cm³	−50 °C (−58 °F)	+60 °C (+140 °F)
	2	0,6 g/cm³	0,9 g/cm³	gemäß Merkmal 060, "Anwendung", → 🖹 6	
	3	0,7 g/cm³	1,2 g/cm³		
	4	0,9 g/cm³	2,0 g/cm³		

Quelle: Endress + Hauser: FTL 81

3 Produktbeschreibung

Der Liquiphant FailSafe ist ein Grenzschalter für die Minimum- oder Maximum-Detektion (MIN/MAX) zum Einsatz in Flüssigkeiten:

- Prozesstemperatur: –50…+150 °C (–58...+300 °F)

Praxisbeispiele

Anlagenspezifische Daten (Unterschied bei SIL-Geräten)

- Reaktionszeiten:
  - Innerhalb der Funktionalen Sicherheit muss der sichere Zustand in einem gewissen Zeitintervall erreicht werden, sonst kann das Schadenereignis nicht zu 100% verhindert werden.
  - Werden bei Regeleinrichtungen oft gar nicht mit betrachtet, daher gibt es außerhalb der Funktionalen Sicherheit auch nicht immer eine entsprechende Angabe

Reaktionszeit

Die kombinierte Fehlerdetektions- und Fehlerreaktionszeit ist die Zeit, in der das Gerät auf einen aufgetretenen Fehler reagiert.

Die Reaktionszeit (Ausschaltverzögerung) für die Sicherheitsfunktion ist < 100 ms.

Quelle: Pepperl + Fuchs: HiC 2873

Praxisbeispiele

Anlagenspezifische Daten (Unterschied bei SIL-Geräten)

- Eine zu hohe Messungenauigkeit kann das auslösen der Sicherheitseinrichtung verhindern
  - Bei der Planung die Geräte entsprechend der Messungenauigkeit auswählen
  - Oder die Messungenauigkeit bestimmen und entsprechend den Schaltpunkt anpassen
  - Beispiel für eine Messabweichung speziell in der Funktionalen Sicherheit:

- Bei der Berechnung der SFF wurde für die Abweichung des Ausgangsstroms bei Ausfall eines sicherheitsrelevanten Bauteils im Drucktransmitter ein Grenzwert von ±1 % zugrunde gelegt. Die ±1 %

Quelle: Endress+ Hauser: FMD 78

Praxisbeispiele

Modifikation / Wartung

- Modifikation an Geräten oder PLT-Sicherheitseinrichtungen dürfen nicht ohne entsprechende Bewertung durchgeführt werden
  - Was darf ich ohne großen Aufwand ändern?
  - Erneutes durchlaufen des Sicherheitslebenszyklus
  - Entsprechende Absprachen mit dem Betrieb / ZÜS / Hersteller, ob eine solche Modifikation überhaupt zulässig

- Wartung und Instandhaltung
  - Geräte mit SIL-Eignung haben oft eine spezielle Anforderung an die Lagerung der Geräte (Dauer)
  - Wie eben bereits gesehen, kann es das gleiche Gerät mit und ohne SIL-Eignung geben, dass muss beim Austausch beachtet und sichergestellt werden

Praxisbeispiele

Unerwartete Fehler

- Selbst wenn Sie alles beachten, kann es immer noch zu Fehler zu kommen
  - Beispiel Während der Planung: Trotz der Absprache und Bestätigung des Herstellers, hat eine Durchflussmessung für Quecksilber nicht funktioniert. Es konnte im Nachgang nicht festgestellt wurden, warum dies der Fall ist. Hier wurde bei der Planung alles richtig gemacht und trotzdem hat das System nicht wie erwartet funktioniert.
  - Der Faktor Mensch

Praxisbeispiele

Was kann ich tun, um diese Fehler zu vermeiden?

- Integration und Leben eines FSM

- Der Einsatz von entsprechend geschultem Personal / Dienstleistern / Lieferanten
  - Planung
  - Programmierung
  - Hersteller

- Das Bewusstsein das jeder Mensch Fehler macht und keiner alles wissen kann
  - gerade im Sicherheitsbereich sollte man keine Entscheidung alleine treffen
  - Nachfragen / Schulen wenn man etwas nicht weiß

RAMSYS
DAS machen Ingenieure

Vielen Dank für Ihre Aufmerksamkeit!

Ethik, Recht und KI – eine Debatte

Besonders im Zusammenhang mit der Verwendung Künstlicher Intelligenz gab es Initiativen menschliches Verhalten zu normieren (z.B. für Mensch-Maschine-Kollaboration) und sogar ethische Aspekte (z.B. ethische Risikobewertung). Diese Präsentation gibt etwas Hintergrund zu ethischen Konzepten, debattiert die Konflikte und Probleme hinter bestimmten Ansätzen, und analysiert mögliche Auswirkungen auf die Gesellschaft. Dies soll die Möglichkeiten und Herausforderungen der KI Systeme verstehen helfen und die überspannende Frage beantworten, ob wir uns auf deren Ergebnisse verlassen sollten.

erstellt von: Dipl-Ing. (FH) Holger Laible IEC ACOS Mitglied

IEC®
International Electrotechnical Commission

Warum die Debatte?

Schauen wir auf aktuelle Beispiele*…

*interessant ist auch der EU Regulierungsentwurf zu KI, auf den hier nicht eingegangen wird.

SMB Entscheidung 171/8 – SEG 10 Ethik in autonomen und KI Applikationen

SMB acknowledged that a refinement of the scope of the proposed Advisory Committee on Ethics in Standards (ACES) would be needed before making a final decision. SMB therefore requested SEG 10 to propose a revised scope, ensuring that it is not restricted to Autonomous and Artificial Intelligence Applications, that collaboration with ISO is included, and that comments made by SMB members, JTC 1 and ACOS are taken into account.

SMB further tasked Central Office to evaluate the interest from IEC Committees and their readiness to participate in the proposed ACES should it be created.

SMB also confirmed that the recommendation to complement existing standards for safety with a standard for **ethical risk assessment had not been approved**.

The recommendation for characterization of the environmental sustainability of Artificial Intelligence systems is referred to ACEA, TC 111, JTC 1/SC 39 and JTC 1/SC 42 for further consideration.

SC 42 and the Holistic AI Ecosystem Intelligence *

"A **new approach to standardization** is needed that

- Takes into account the context of use of the technology by looking at both technology capability and non-technical requirements such as business requirements, regulatory and policy requirements, application domain needs, **and ethical and societal concerns**
- Translating the above **into technical requirements**
- Building foundational standards that allow communities to build upon such as terminology, use cases, application guidance and reference architectures
- Linking technology innovation communities such as proprietary implementations, research, SDOs and open source communities"

"AI ethical and societal considerations not limited to SC 42 but extend to IEC/ISO TCs in their applications."

*zitiert von Obmann PPT

ISO/IEC JTC 1/SC 42 "Artificial intelligence"

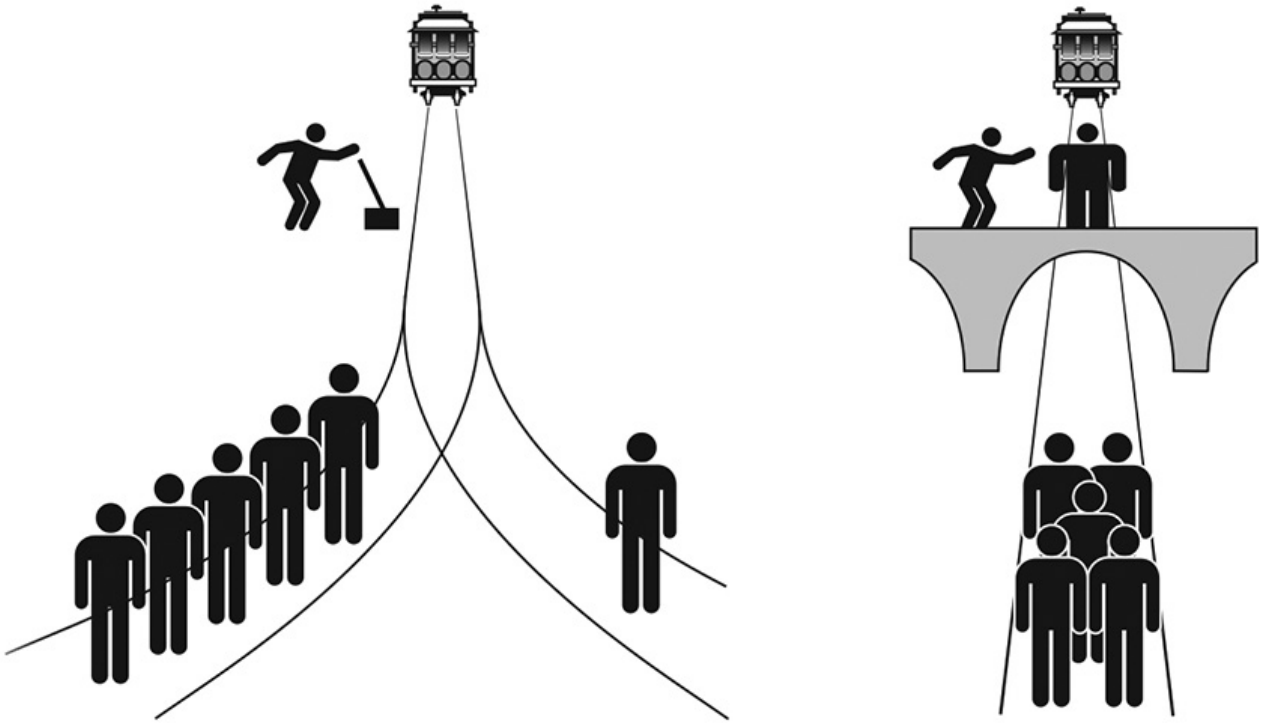
DTR Ballot Document - ISO/IEC TR 24368 - Information technology — Artificial intelligence — Overview of ethical and societal concerns

“4.3.3 **Utilitarianism**
Utilitarianism is an ethical framework that maximizes good and minimizes harm. A utilitarian choice is one that produces the greatest good and does the least amount of harm to all stakeholders involved. Once the ethical aspects of a problem are explained logically, **utilitarian approaches have the strength of being universally understandable and intuitive to implement**. Its primary disadvantage is that many moral considerations are difficult to quantify (e.g. dignity). Moral considerations vary enough that they are difficult to weigh against each other, for example environmental pollution versus societal truthfulness.”

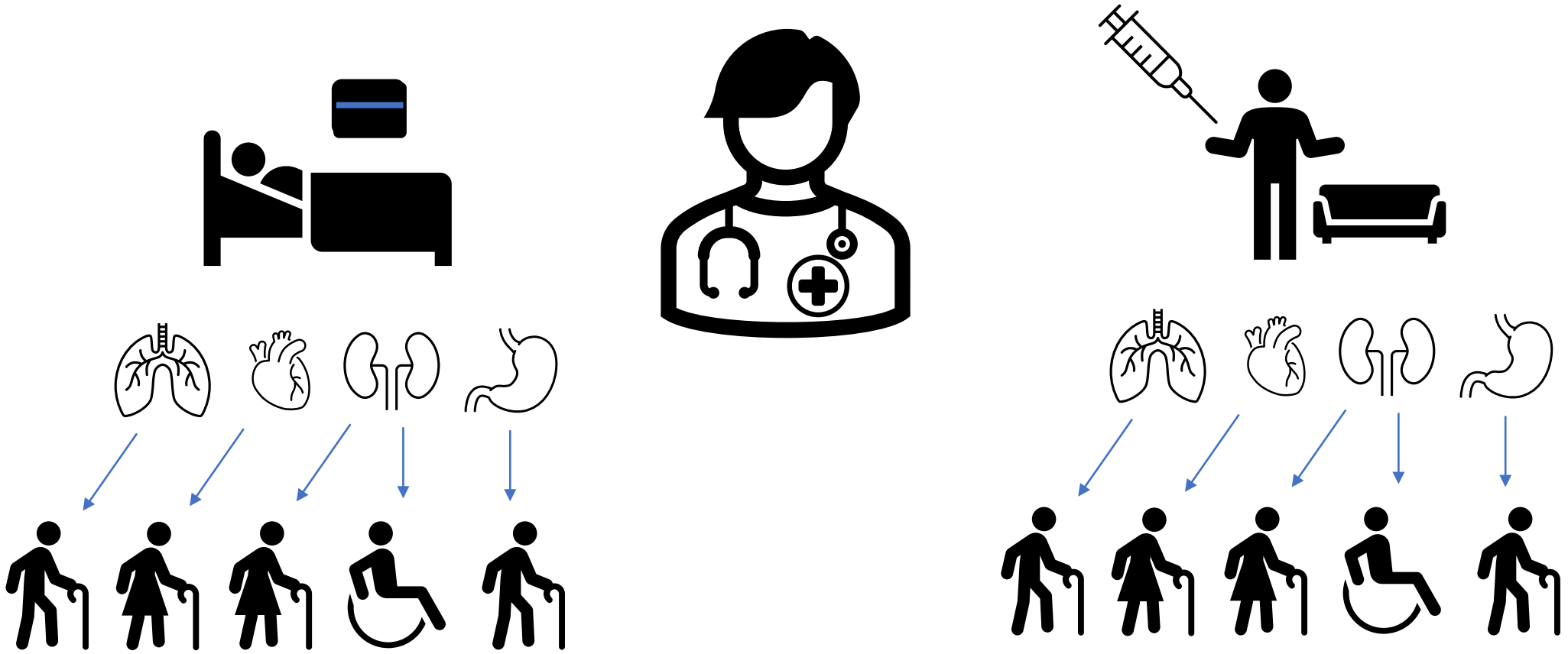
“Procedures, methods and criteria are needed to ensure that AI algorithms are sourced, designed and used to treat the individual in a representative and transparent manner, ensuring fairness and the respect of privacy.”

Grundlagen von Ethik und Recht

Das Gleisarbeiter-Dilemma



Das medizinische* Dilemma

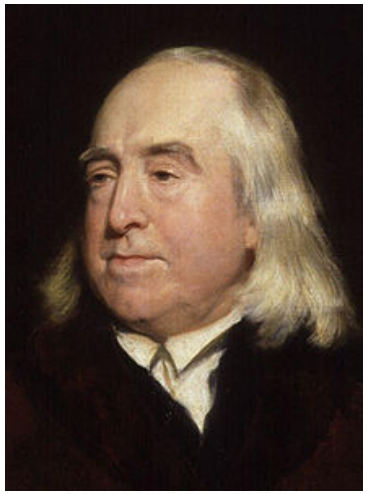


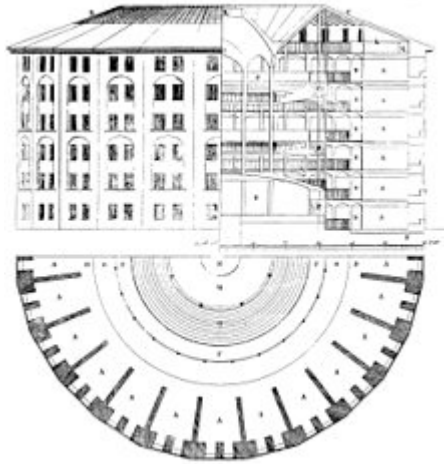
*Es gibt ähnliche Dilemmata, wie Rechtfertigung von Folter oder Abschuß eines entführten Flugzeugs.

Jeremy Bentham des moderen Utilitarismus

15 Feb. 1748 bis 6 Juni 1832 (84 Jahre)

- Das Prinzip des Nutzens: **“The greatest happiness of the greatest number is the foundatioun of morals and legislation.”** Mit Freude (Happiness) verstand er die Summe des Wohlergehens und die Abwesenheit von Schmerz und Leid.
- Scharfe Kritik wurde von Bentham’s Student John Stuart Mill formuliert, da beim **Ultilitarismus** die Motivation des menschlichen Gewissens unberücksichtigt bleibt.
    a. **Berücksichtigt nicht die individuellen Rechte**
    b. **Es ist nicht möglich alle Vorlieben und Werte zu erfassen.**
- Bentham’s Idee: Das Panoptikum das günstiger war als die Gefängnisse dieser Zeit, weil weniger Personal benötigt wurde; da die Wachmänner nicht gesehen werden, müssen sie nicht dauernd im Dienst sein und damit verbleiben die zu Beobachteten beobachtet.
- Bentham’s Wunsch seinen Korpus zu konservieren war im Einklang mit seiner utilitaristischen Philosphie.





Source: Wikipedia

Zweckorientierte Moralprinzipien

Jeremy Bentham – anwesend aber nicht abstimmend

Immanuel Kant Begründer des kategorischen Imperativs

22 April 1724 bis 12 Feb 1804 (79 Jahre)

- Kant wurde bekannt durch das einzig moralische Prinzip, dass er als "kategorischen Imperativ“ bezeichnete, übte Kritik an der praktischen Vernunft und Urteilskraft.

  “Handle nur nach derjenigen Maxime, durch die du zugleich wollen kannst, daß sie ein allgemeines Gesetz werde.”

- In der „Grundlegung zur Metaphysik der Sitten“ (1785), Kant postulierte die gegen den Utilitarismus gerichtete Idee, dass es einen Unterschied zwischen Vorlieben und Werten gibt, und dass individuelle Rechte schwer zu gewichten sind:
  Alles hat entweder einen Preis oder eine Würde. Was immer einen Preis hat, kann durch etwas anderes equivalent ersetzt werden; auf der anderen Seite existiert eine Würde ist oberhalb jedes Preises rangiert und deshalb kein Equivalent zuläßt.
- Er opponierte der “Demokratie“, welche zu dieser Zeit als direkte Demokratie verstanden wurde, im Glauben daran, dass die Mehrheitsherrschaft mit einer Gefahr der individuellen Freiheit verbunden ist. Er meinte sinngemäß, das Demokratie despotisch ist, weil ausführende Gewalt in der “alle” für oder gegen den Einzelnen entscheiden, der nicht zustimmt; das ist ein Widerspruch zum freien Willen und der Freiheit des Einzelnen.
- Kant, der lange arm war, litt unter gesundheitlichen Problemen und starb in Königsberg am 12 February 1804, mit den letzten Worten "Es ist gut”.

Source: Wikipedia

Kategorische Moralprinzipien

John Lockes Idee der “freien demokratischen” Gesellschaft

John Locke erweiterte die Idee des Sozialvertrags von Thomas Hobbes’s und entwickelte das **Konzept der natürlichen Rechte, das Recht auf Privatbesitz und das Prinzip der Zustimmung der Regierten**. Seine Ideen formen die ideologische Basis heutiger “freier demokratischer” Gesellschaften.

Source: Wikipedia

- **Vereinigte Staaten – Unabhängigkeitserklärung**
  “We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty and the **pursuit of Happiness**.”

- **Universelle Erklärung der Menschenrechte (UN)**
  https://www.un.org/en/about-us/universal-declaration-of-human-rights

  Auszüge:
  Artikel 3: “Jeder hat das Recht auf Leben, Freiheit und persönliche Sicherheit.”
  Artikel 9: “Niemand soll willkürlich verhaftet, festgesetzt oder verbannt werden.”
  Artikel 11: “Jeder der einer strafbaren Handlung bezichtigt wird hat das Recht als unschuldig behandelt zu warden, bis seine Schuld erwiesen ist…”

- **Grundgesetz der Bundesrepublik Deutschland**
  Es gibt subjektive allgemeine Rechte mit konstituierendem Rang an den alle Institutionen und Staatsorgane gebunden sind.

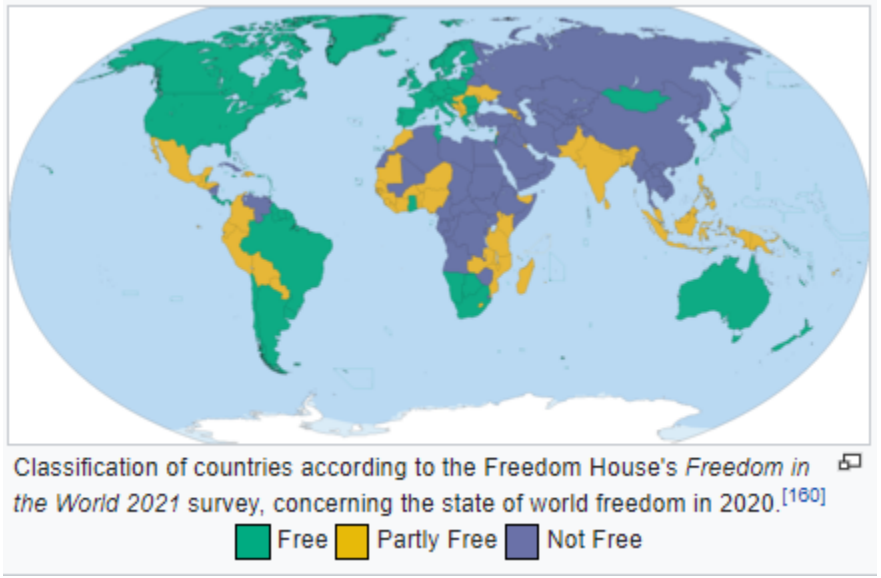
Der Schutz der Rechte des Einzelnen und
die Zustimmung ist der Schlüssel zu einer freien Gesellschaft!

Über welche Ethik sprechen wir?

Gesellschaften haben unterschiedliche Ethik.

Dies ist keine Frage von Standardisierung…
es ist hochpolitisch und hat enormes Konfliktpotential.

Nehmen wir mal an, dass die Anschauungen einer "freien demokratischen westlichen"Gesellschaft zugrunde gelegt werden.

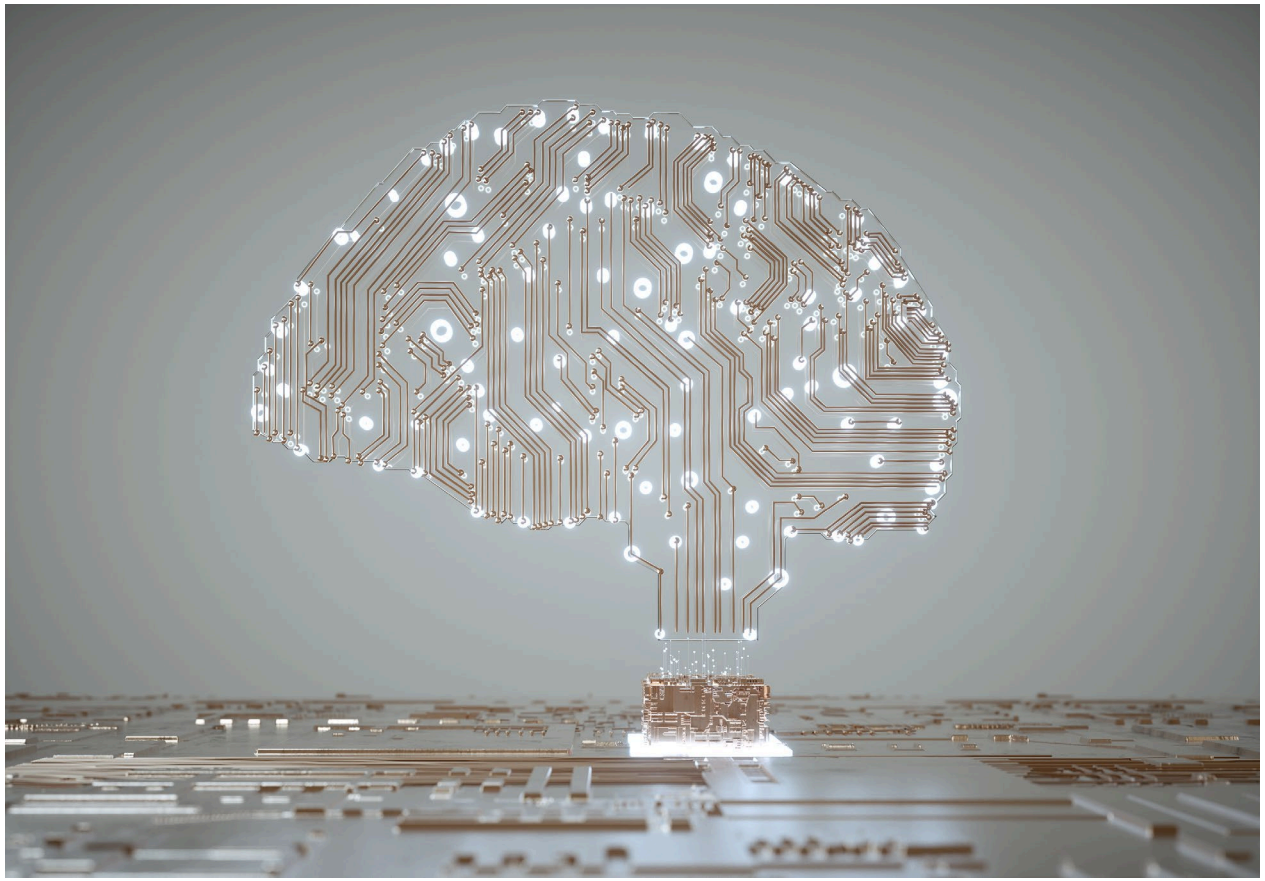


Classification of countries according to the Freedom House's *Freedom in the World 2021* survey, concerning the state of world freedom in 2020.[160]

Source: Wikipedia

Was kann realistischerweise durch KI Systeme geleistet werden?

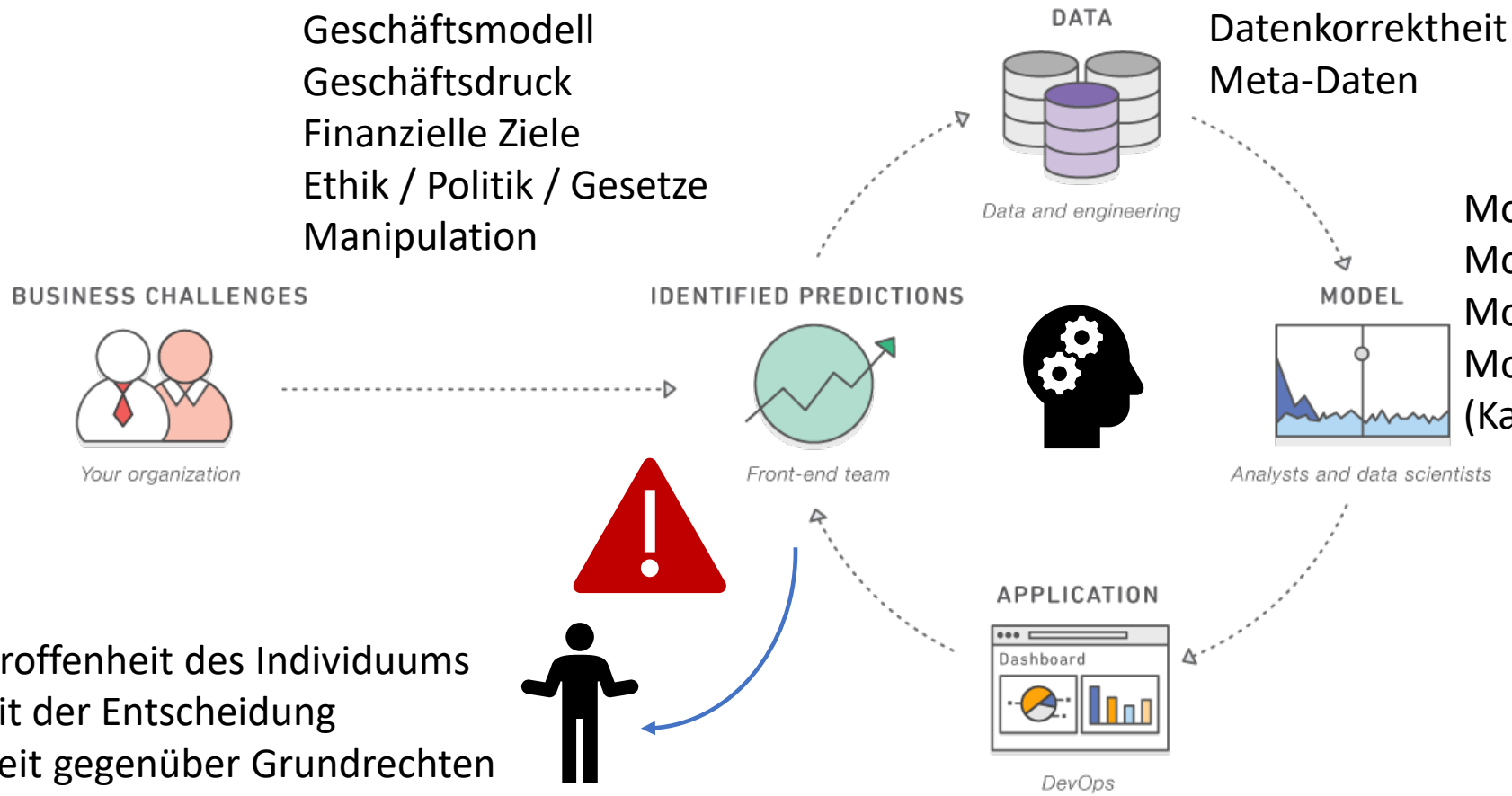
KI Systeme und deren Probleme



Generelles Konzept eines KI Systems

Datenauswahl
Datenschutz
Datenkorrektheit
Meta-Daten

Geschäftsmodell
Geschäftsdruck
Finanzielle Ziele
Ethik / Politik / Gesetze
Manipulation



Model Erstellung
Model KPIs
Model Abstraktion
Model Richtigkeit
(Kausalität vs. Korrelation)

Sofortige Betroffenheit des Individuums
Willkürlichkeit der Entscheidung
Gleichgültigkeit gegenüber Grundrechten

Intention des Bedieners
Verständnis des Bedieners (Transparenz)

Konflikte und ungleiche Macht

Begrenzte Transparenz der Algoritmen

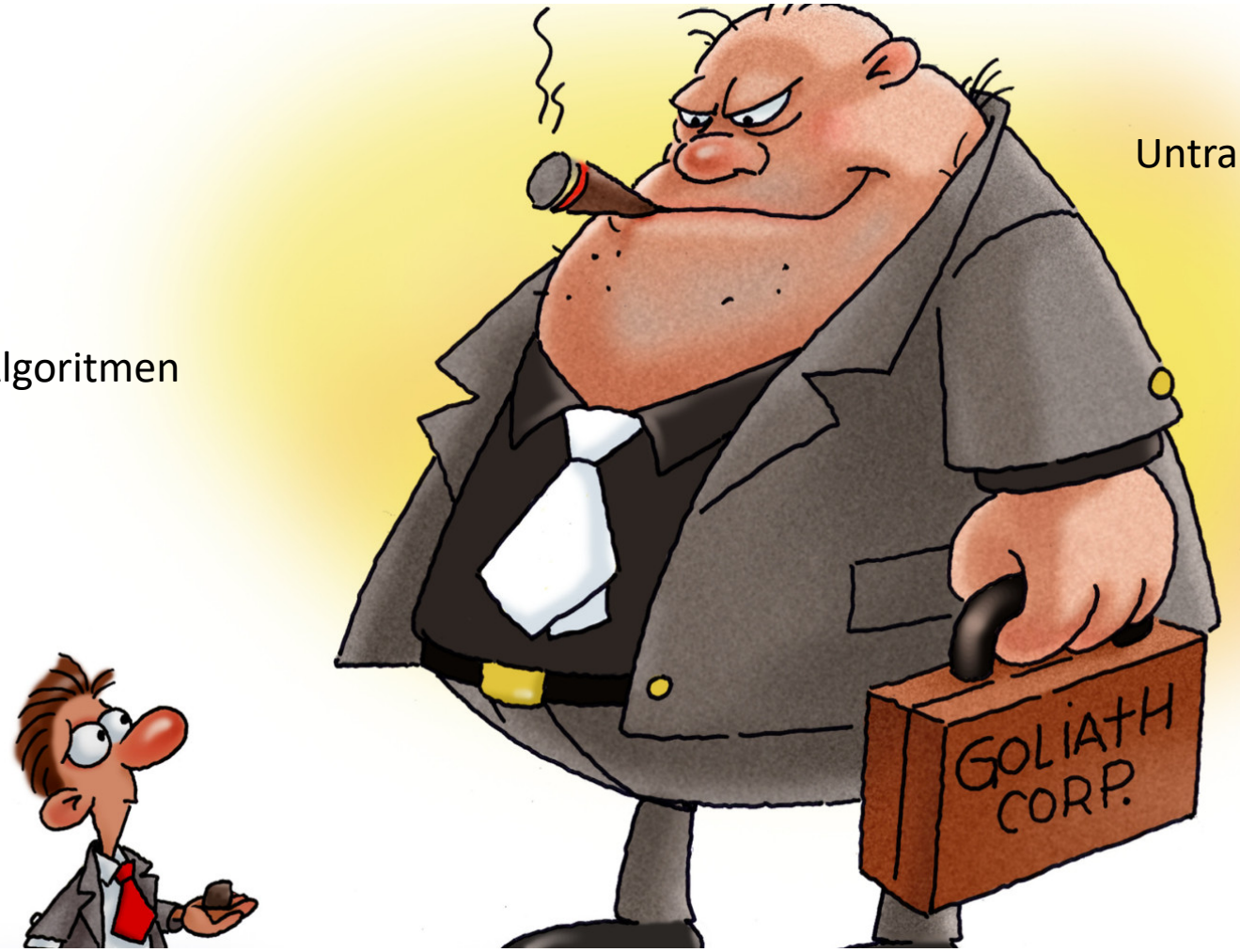
Begrenztes Wissen

Wenig Kontrolle über Daten

Sofortige Betroffenheit

Wenig Wahlfreiheit

Limitierte Rechtsmittel



Untransparent / Patente

Business Case

Expertenwissen

Kontrolle über Daten und Algoritmen

Politische Unterstützung

Globale Aufstellung

Auswirkungen von KI Systemen

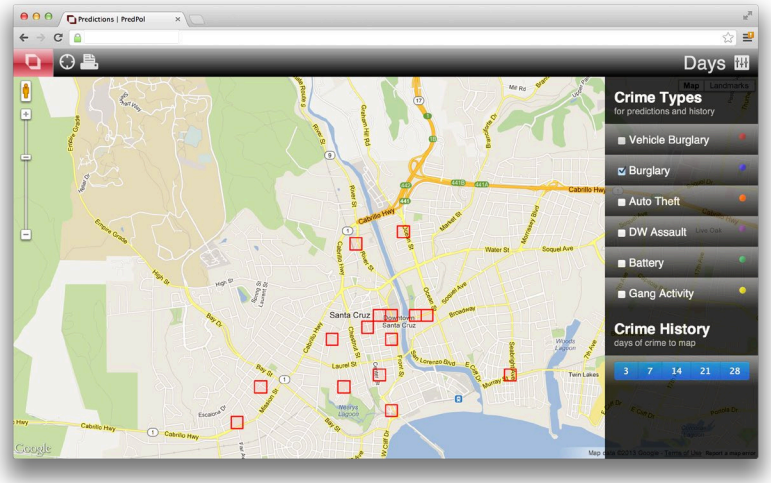
- Fast alle Aspekte des KI Einsatzes sind hinsichtlich der individuellen Grundrechte problematisch. Angefangen vom Datenschutz (Privacy), über die angewandten Algorithmen (Fairness, Transparenz), bis zu den Ergebnissen und Auswirkungen des KI Systems (Behandlung des Einzelnen).
- Die sofortige Auswirkung auf Einzelne verletzt das Recht auf Unschuldsvermutung, den KI Systeme entscheiden auf statistischer Basis und den Modellannahmen, unabhängig von einer Beweisführung.
- Cathy O'Neil beschreibt dies in ihrem Buch “Angriff der Algorithmen als “Weapons of Math Destruction” (WMDs) und gibt verschiedenste reale Beispiele.
- Bis heute gibt es keine Methode die Zuverlässigkeit von KI zu untersuchen.

Anmerkung:

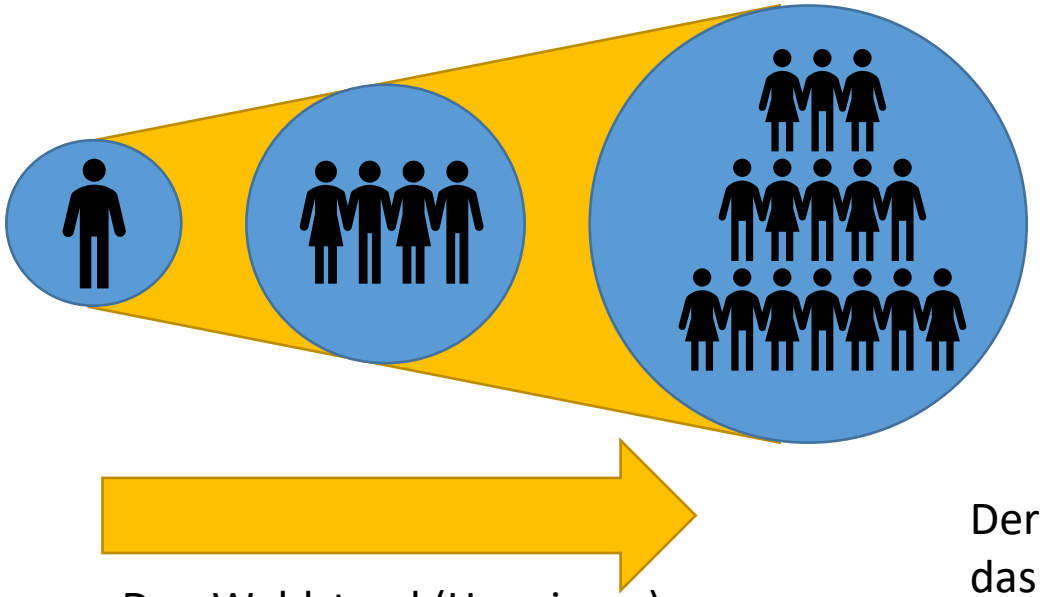
Es ist möglich KI zum gesellschaftlichen Nutzen zu verwenden, aber dies findet im Spannungsfeld mit politischen und geschäftlichen Interessen statt. Wenn es eine Methode zur Qualifizierung der Zuverlässigkeit von KI gäbe, wäre es möglich den WMD-Effekt zu verhindern.

Beispiel - PredPol

- PredPol ist eine Analyse-Software, die örtliche Vorhersagen über Eigentumsdelikte macht. PredPol hat einen patentierten Algorithmus, der auf einem Model zu Nachbeben (bei Erdbeben) basiert.
- Die Vorhersagen für Gebiete von möglichen Verbrechen basiert auf der Auswertung von historischen Verbrechensdaten (Theorie der zerbrochenen Fenster). In den verhergesagten Gebieten sollte die Polizei verstärkt patrollieren (stop In predicted areas police should patrol (stoppen und durchsuchen) und nach möglichen Verbrechern suchen. Im Ergebnis wurden viele unschuldige Menschen von der Polizei kontrolliert, was die Unschuldsvermutung verletzt.
- Es scheinte zu funktionieren, aber das Verfahren hat eine schlechte Feedback-Schleife, den je mehr man sucht umso mehr wird gefunden. Ferner gibt es einen Filter bzgl. bestimmter Verbrechenskategorien (z.B. wird Finanzkriminalität ausgeklammert).
- 2016 wurde PredPol als rassistisch hinsichtlich der Hautfarbe von Menschen erachtet. ng black people of crimes.
  Im April 2020, hat das LAPD, unter den längsten Nutzen von PredPol, das Programm eingestellt, ohne dass es möglich war die Effizienz des Einsatzes zu messen.



Gefahr von KI Systemen - Skalierbarkeit

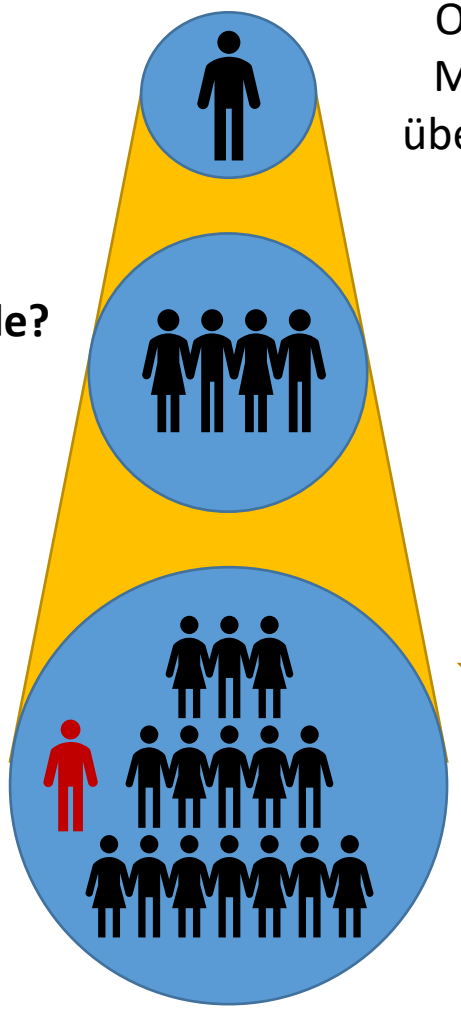


Den Wohlstand (Happiness) vieler Menschen mehren?

Wer ist in der Kontrolle?

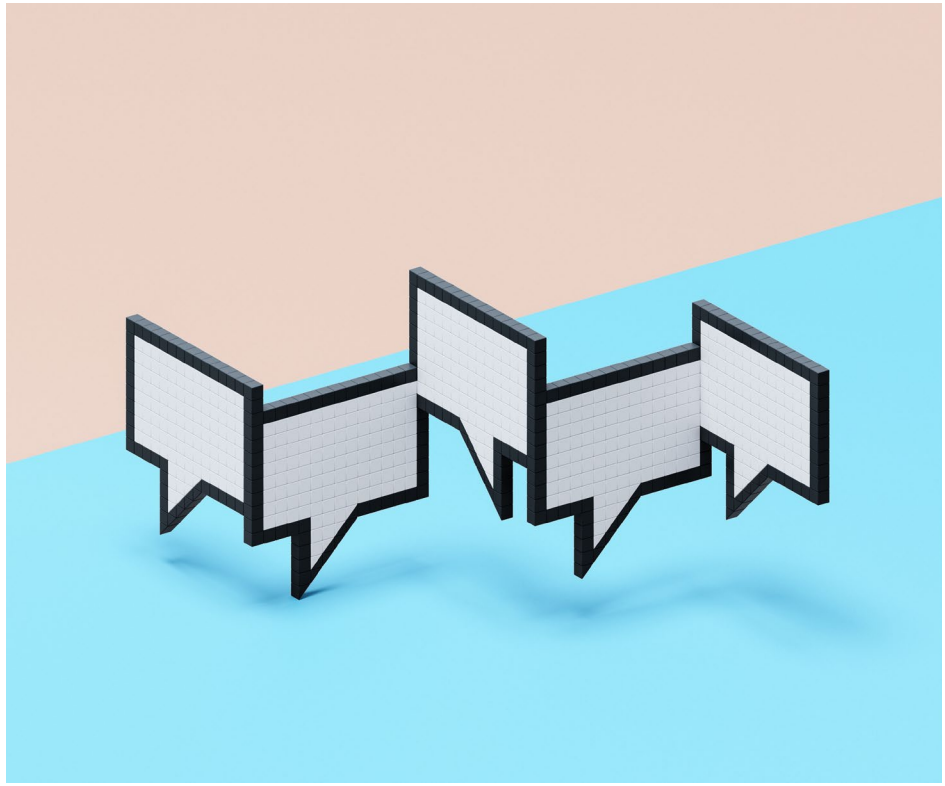
Was kann passieren?

Der Einzelne kann durch das KI System entweder indentifiziert oder ignoriert werden.



Oder viele Menschen überwachen?

Starten wir die Debatte!



„Die Entwicklung von vollständiger Künstlicher Intelligenz könnte des Ende der menschlichen Rasse bedeuten.
KI ist wahrscheinlich entweder das Beste oder das Schlechteste für die Menschheit."

Stephen Hawking

Betrachtung verschiedener PLT-Systemarchitekturen mit Ausblick auf zukünftige Cyber Security Anforderungen

Dieser Beitrag entstand aus unserer Mitarbeit in den folgenden Arbeitskreisen:

NAMUR AK 4.5 Funktionale Sicherheit
NAMUR AK 4.18 Automation Security

Vorstellung

Udo Menck

Dow Deutschland Anlagengesellschaft mbH Werk Stade

TES Core Engineering Technology Center

Current Position:

Global Functional Safety Manager

Please join my network at:

LinkedIn

Vorstellung

Please join my network at:

LinkedIn

Jan Rußmann

Dow Deutschland Anlagengesellschaft mbH Werk Stade

Operations IT/OT

Current Position:

Engineering and Maintenance IT Manager / Cyber Security Specialist

Agenda

- Einführung – PLT-Systemarchitekturen in der FuSi
- PLT-Systemarchitekturen (Rückblick NAMUR HS2017)
- Warum ist Cyber-Security für OT so wichtig geworden
- Gesetze und Normen bzgl. Cyber-Security
- PLT-Systemarchitekturen aus der Sicht von Cyber-Security
- Was man nicht vergessen sollte …

Einführung

Wenn man aus Sicht der funktionalen Sicherheit auf PLT-Systeme schaut, dann geht es primär um 3 Bereiche (Definition: VDI 2180-1 2019):

PLT-Betriebseinrichtung (prozessleittechnische Betriebseinrichtung)
Realisierung einer vorgegebenen →PLT-Betriebsfunktion
Englisch: **BPCS-C**

PLT-Betriebseinrichtung mit Sicherheitsfunktion
Realisierung einer vorgegebenen →PLT-Sicherheitsfunktion mit einem Risikoreduzierungsfaktor von bis zu 10 im Prozessleitsystem (PLS)
Englisch: **BPCS-P**

PLT-Sicherheitseinrichtung (prozessleittechnische Sicherheitseinrichtung, Sicherheitssystem)
Realisierung einer vorgegebenen →PLT-Sicherheitsfunktion mit einem SIL zwischen 1 und 4
Englisch: **SIS**

Sicherheitstechnische Bedeutung

Wenn man aus Sicht der funktionalen Sicherheit auf PLT-Systeme schaut, dann geht es primär um 3 Bereiche (Definition: VDI 2180-1 2019):

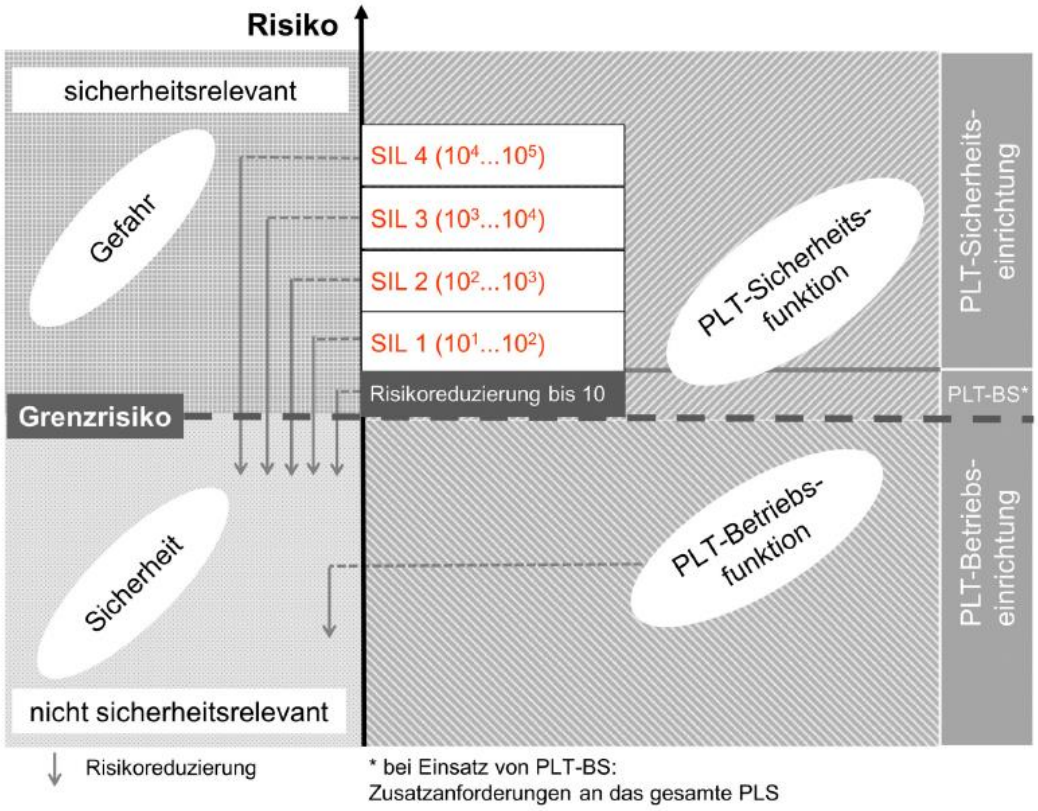


Bild 4. Risikoreduzierung durch PLT-Einrichtungen

NAMUR HS 2017 / Systemarchitekturen

Darstellung von 5 Varianten zur Realisierung der 3 Bereiche (BPCS-C, BPCS-P, SIS) in verschiedenen Systemarchitekturen mit Vor- und Nachteilen

Type 1: BPCS-CP SEPARATED

Type 2: BPCS-CP MIXED

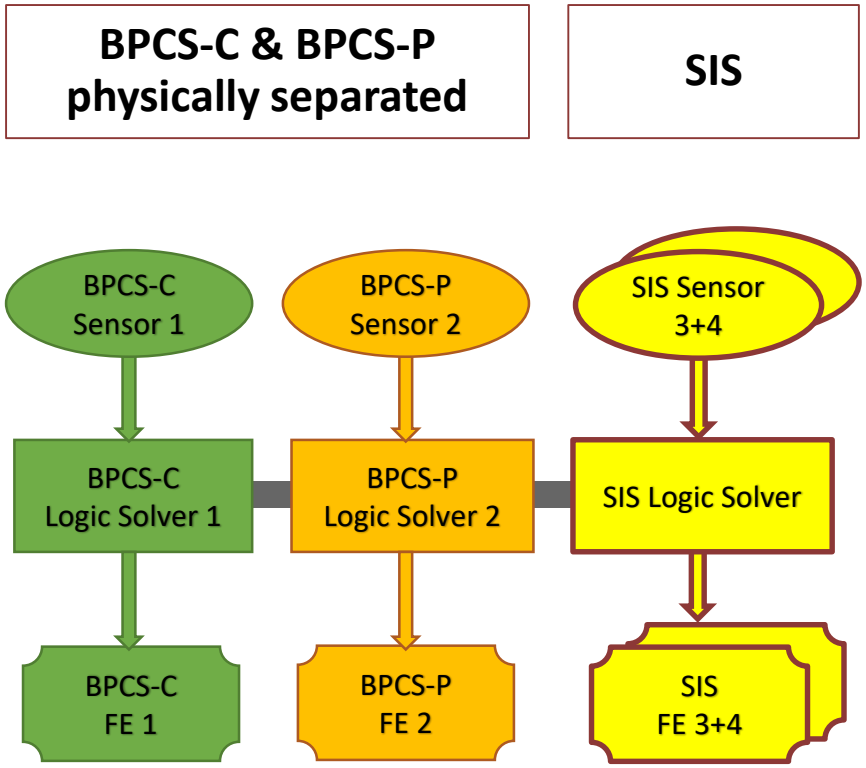
Type 3: DOUBLE SIS

Type 4: BPCS-C / P in SIS

Type 5: BPCS-CP P-BOXED (NAMUR Vision)

Type 1: BPCS-CP SEPARATED

BPCS-CP SEPARATED



Criteria:

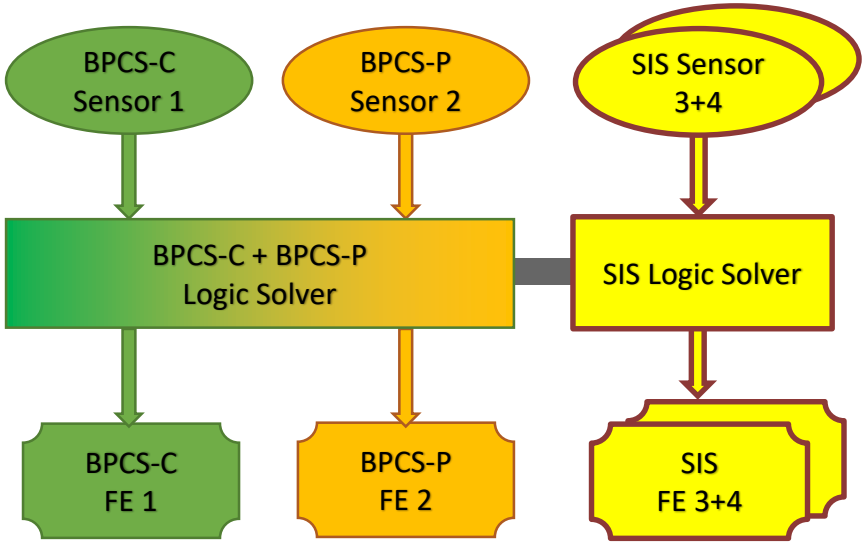
- Independency
- Design + Implementation
- Life-Cycle-Management
- **Cyber-Security**

Type 2: BPCS-CP MIXED

BPCS-CP MIXED

BPCS-C & BPCS-P in a single BPCS Logic Solver

SIS

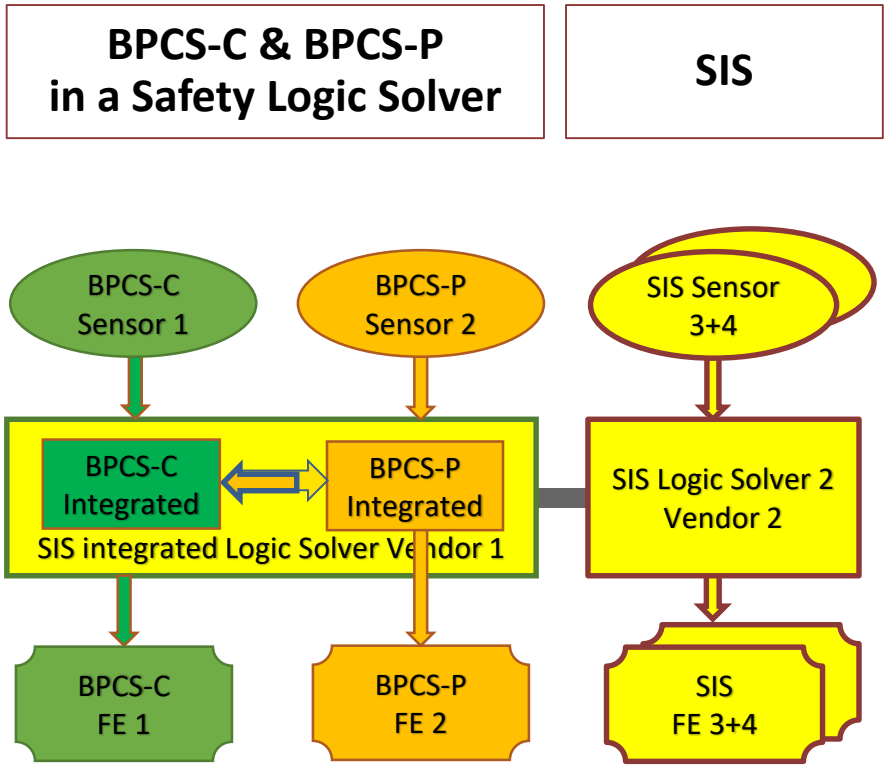


Criteria:

- Independency
- Design + Implementation
- Life-Cycle-Management
- **Cyber-Security**

Type 3: DOUBLE SIS

DOUBLE SIS



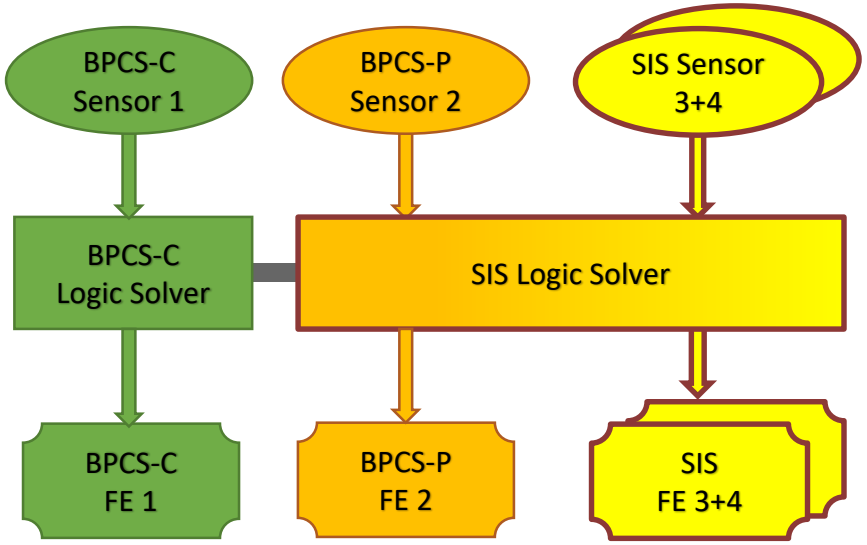
Criteria:

- Independency
- Design + Implementation
- Life-Cycle-Management
- **Cyber-Security**

Type 4: BPCS-C / P in SIS

BPCS-C / P in SIS

BPCS-C	BPCS-P & SIS in a Safety Logic Solver



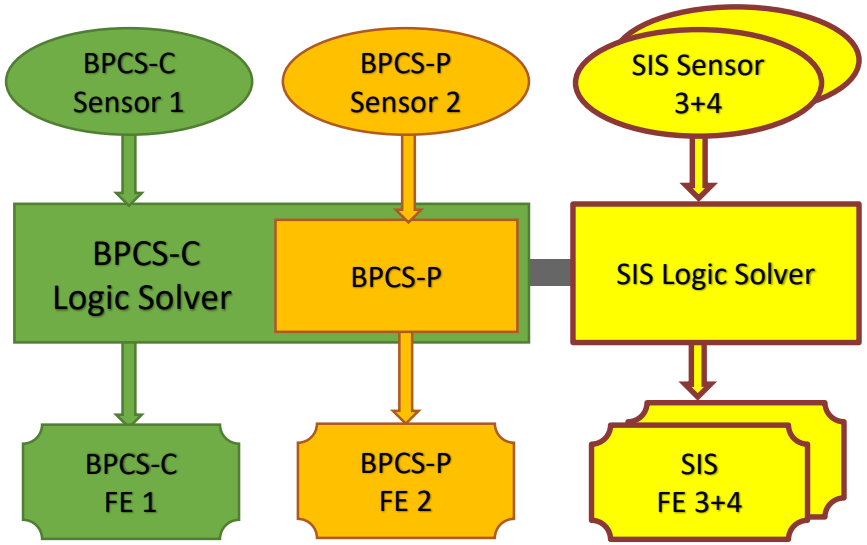
Criteria:

- Independency
- Design + Implementation
- Life-Cycle-Management
- **Cyber-Security**

Type 5: BPCS-CP P-BOXED (NAMUR Vision)

BPCS-CP P-BOXED

BPCS-C & BPCS-P in a BPCS Logic Solver BPCS-P area protected	SIS



Criteria:

- Independency
- Design + Implementation
- Life-Cycle-Management
- **Cyber-Security**

Umfrage NAMUR-HS 2017

Criteria:

WE WANT YOUR FEEDBACK !

Independency

Pain — Feel Good

Design + Implementation

Pain — Feel Good

Life-Cycle Management

Pain — Feel Good

Cyber-Security

Pain — Feel Good

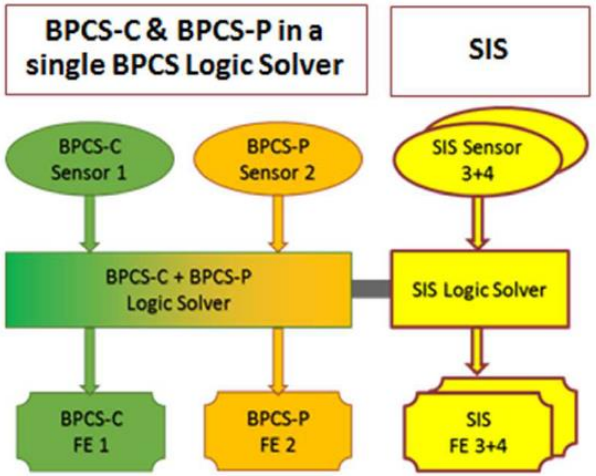
Overall Pain Level:

Feel Good

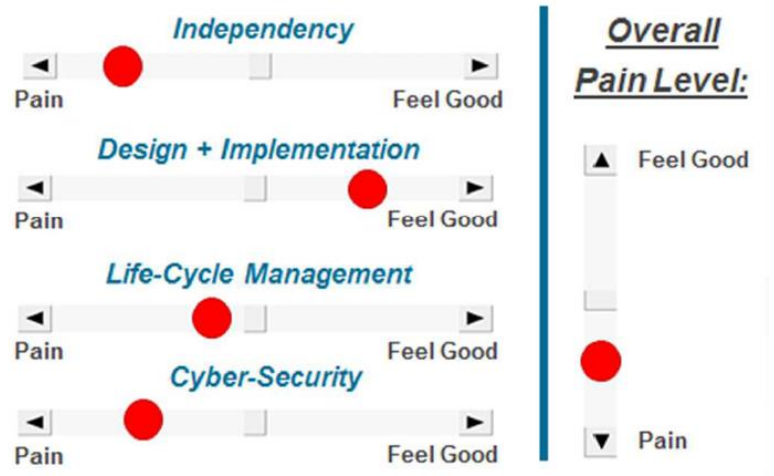
Pain

Ergebnis Umfrage NAMUR-HS 2017

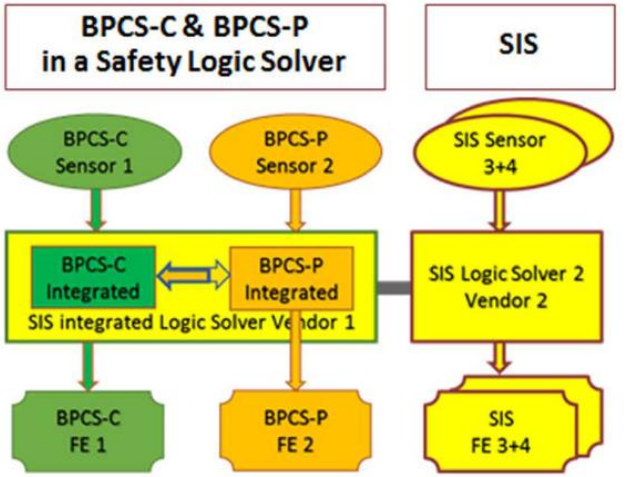
Type 2: BPCS-CP MIXED



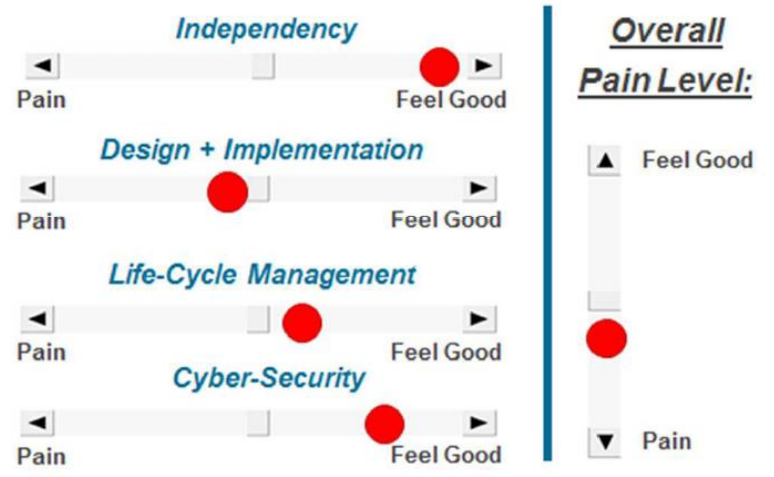
Type 2: BPCS-CP MIXED



Type 3: DOUBLE SIS

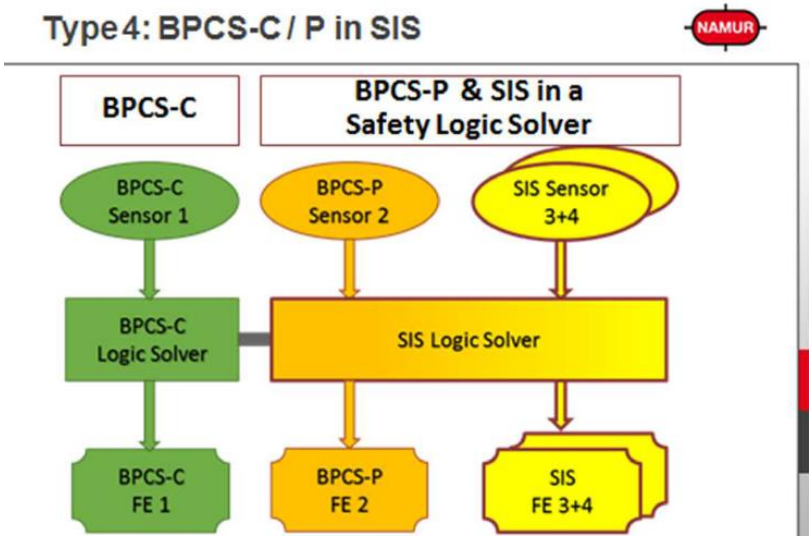


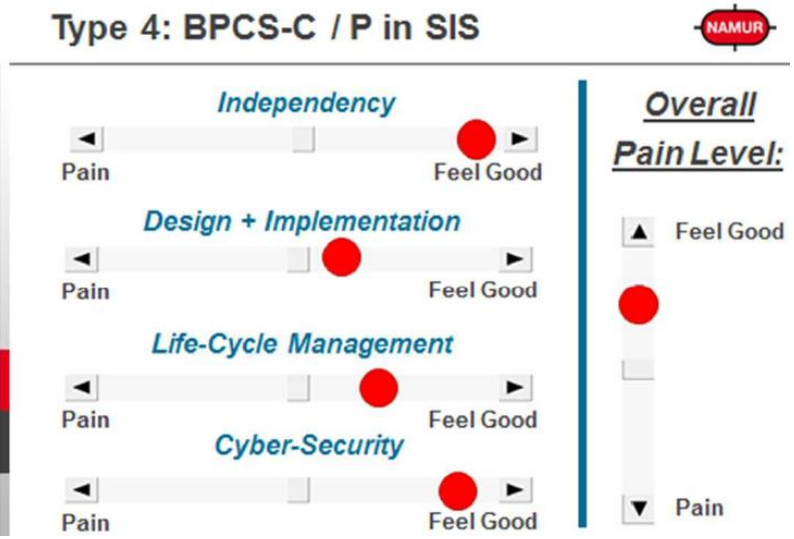
Type 3: DOUBLE SIS

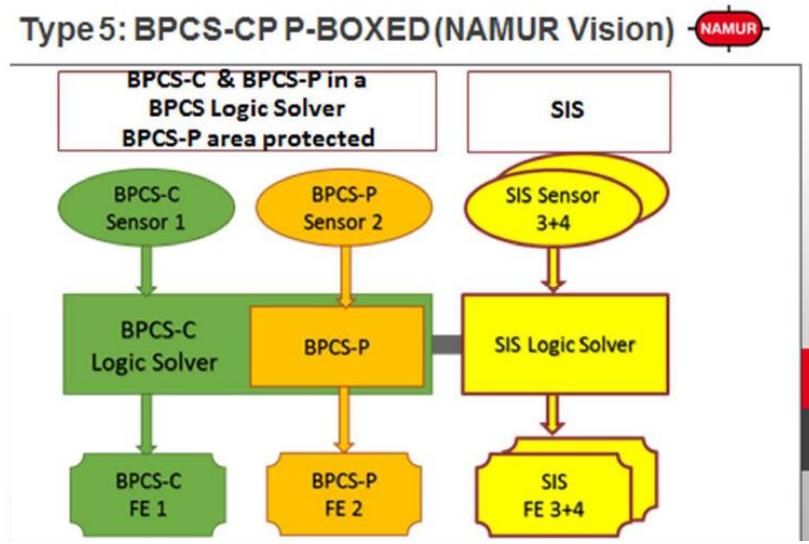


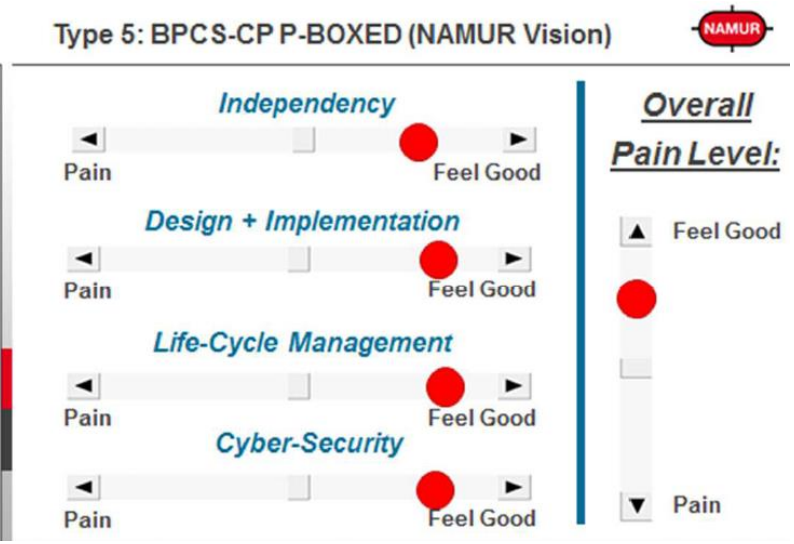
General Business

Ergebnis Umfrage NAMUR-HS 2017









Warum ist Cyber Security für OT so wichtig geworden?

(GEN2:IT)
Maersk: IT wurde von Computer Virus verschlüsselt
Schaden: **300.000.000 $**

(GEN2:IT) News
Hacker-Angriff über IT-Dienstleister Kaseya trifft Hunderte Unternehmen. Revil fordert **70.000.000 $ in Bitcoins**

(GEN3:OT)

SIS System shutdown in middle east (TRITON/TRISIS/HATMAN)

Erster bekannter Cyber-Angriff auf Safety Instrumented Systems (SIS)

Führte zu Kontrollverlust, System wurde von jemand anderem gesteuert

Sechs Monate Wiederherstellungsdauer!

Industry Trends continue in 2020,2021….

Atlanta Spent $2.6 Million to Recover from a $52,000 Ransomware Scare

Tesla worker admitted to sabotage of manufacturing systems

– June 2018)

Triton

America's Electrical Grid has a Vulnerable Back Door and Russia Walked Through It
Wall Street Journal – January 2019

Hexion and **Momentive** Respond To Cyber-Attacks
Chemical Engineering – March 2019

Arizona Beverages knocked offline by ransomware attack
TechCruch - March 2019

Hoya Hit By Cyber Attack In February
Japan Times – April 2019

Norway say **Norsk Hydro** cyber attack began Monday evening and escalated during the night
Reuters – March 2019

July 2021. Russian hac exploited a vulnerability in **Kaseya's** virtual systems/server administrator (VSA) software allowing them to deploy a ransomware attack on the network. The hack affected around 1,500 small and midsized businesses, with attackers asking for $

French IT service giant **Sopra Steria** was attacked by ransomware on the evening of 20th Oct con

Bayer Contains Cyber Attack It Says Bore Chinese Hallmarks
Reuters – April 2019

Manufacturing giant **Aebi Sch** by ransomware

September 2020. French shipping company CMA CGM SA saw two of its subsidiaries in Asia hit with a ransomware attack that caused significant disruptions to IT networks, though did

May 2021. The world's largest meat processing company, Brazilian-based ware ities in stralia.

July 2021. Transnet Port Terminals (TPT), South Africa's state-run ports operator and freight rail monopoly, had its rail services disrupted after a hack by unknown actors. Transnet reportedly declared it an act "force majeure."

May 2021. LineStar Integrity Services, a pipeline-focused business, was hit by a ransomware attack the same time as the Colonial Pipeline, with 70 gigabytes of its internal files being stolen

December 2020. Over 200 organizations around the world—including multiple US government agencies—were revealed to have been breached by Russian hackers who compromised the software provider SolarWinds and exploited their access to monitor internal operations and exfiltrate data.

Gegenmaßnahmen - Strategie

Welche Strategie wählen wir, um das Risiko zu mindern?

"Viele Wege führen nach…Rom"

- BSI IT Grundschutz
- MITRE ATT&CK®
- Common Criteria
- NIST Framework
- Grundschutzpapier Chemie
- IEC62443
- ISO/IEC 27001
- KAS 51
- NA163
- …
- Aber es ist auch eine Frage der Systemarchitektur !

SYSTEM SECURITY AS A DESIGN PROBLEM

"A combination of hardware, software, communications, physical, personnel and administrative-procedural safeguards is required for comprehensive security. In particular, software safeguards alone are not sufficient."

The Ware Report Defense Science Board Task Force on Computer Security, 1970

Ware W (1970) Security Controls for Computer Systems: Report of the Defense Science Board Task Force on Computer Security. (The Rand Corporation, Santa Monica, CA). Available at

https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/ware70.pdf

SYSTEMSICHERHEIT ALS DESIGNPROBLEM

Für eine umfassende Sicherheit ist eine Kombination aus Hardware-, Software-, Kommunikations-, physischen, personellen und administrativ-prozeduralen Schutzmaßnahmen erforderlich. Insbesondere sind Softwareschutzmaßnahmen allein nicht ausreichend.

The Ware Report Defense Science Board Task Force on Computer Security, 1970

Ware W (1970) Security Controls for Computer Systems: Report of the Defense Science Board Task Force on Computer Security. (The Rand Corporation, Santa Monica, CA). Available at

https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/ware70.pdf

Gesetze &Normen bzgl .Cyber Security

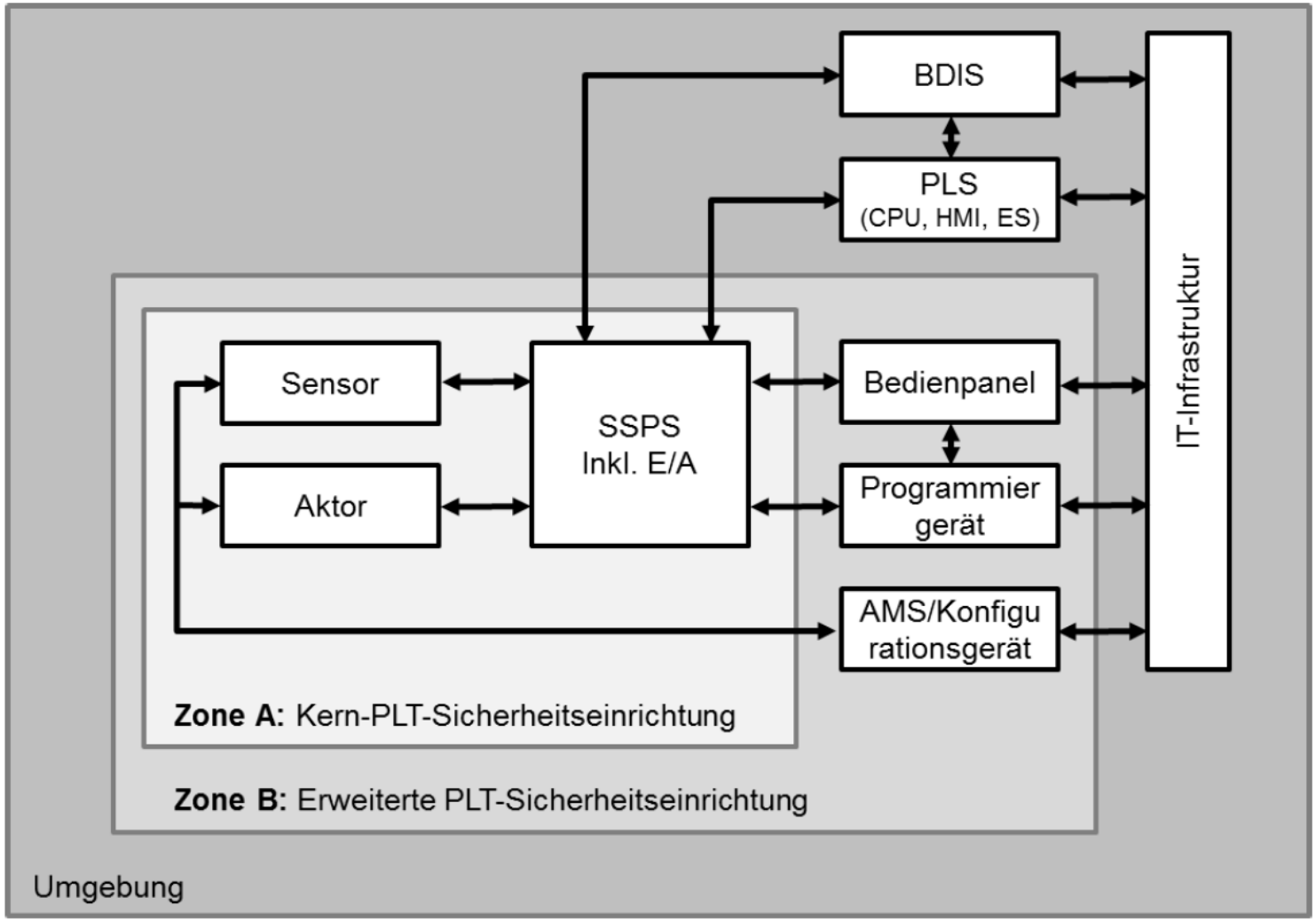
- IEC 61511…
  - Cyber Security Assessment nach IEC61511 erforderlich
- KRITIS VO
- IT SiG2.0
  - Unternehen im besonderen öffentlichem Interesse
  - Unternehmen “Obere Klasse StörfallVO”

  Wußten Sie schon: in ~5 Wochen (ab1.11.21)
  müssen Vorfälle an das BSI gemeldet werden?

- VDI2180

Zukünftig: NIS2 (EU) -> IT-SiG 3(?)

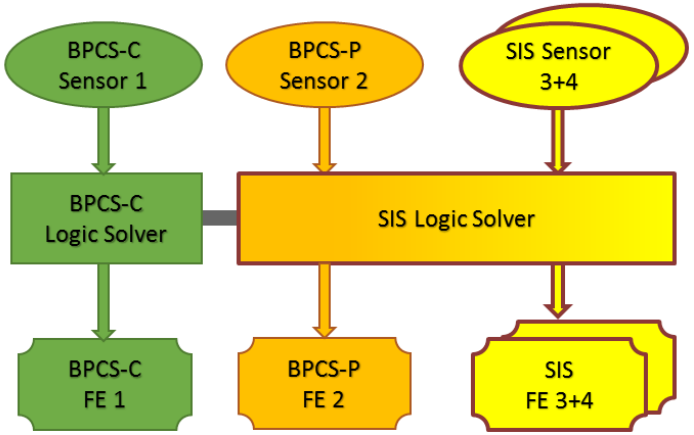
NAMUR NA 163 Modell

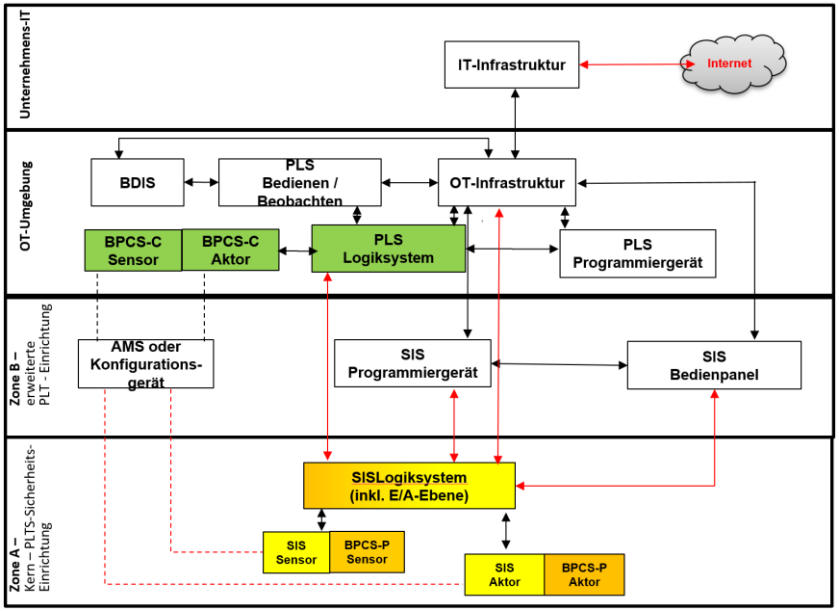


NAMUR NA 163 Modell

BPCS-C / P in SIS

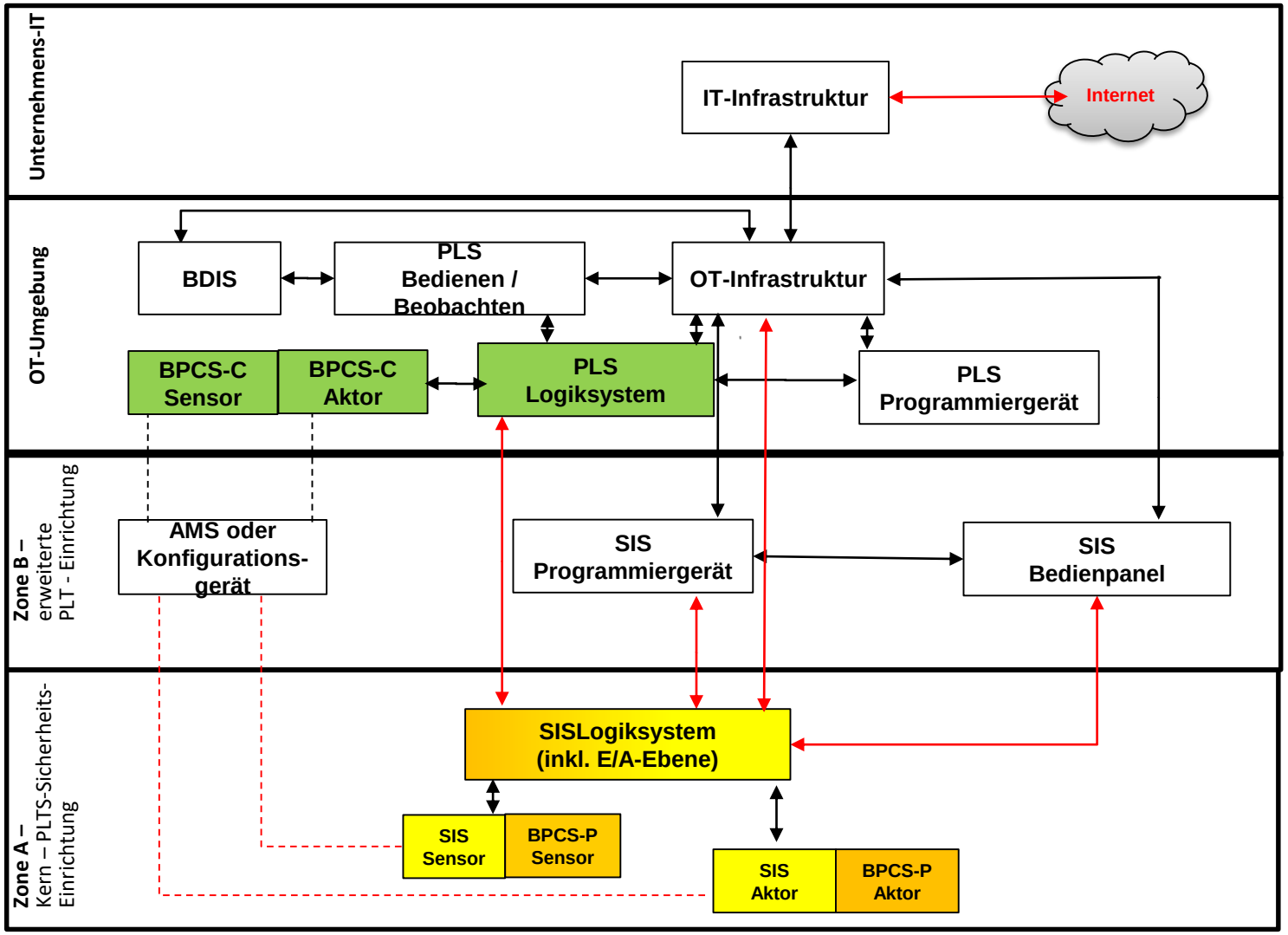
BPCS-C	BPCS-P & SIS in a Safety Logic Solver





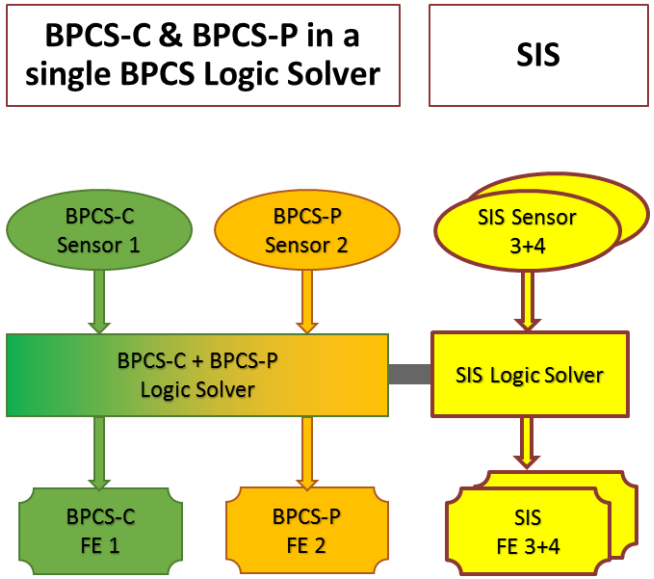
2017 → 2021

BPCS-C/P in SIS

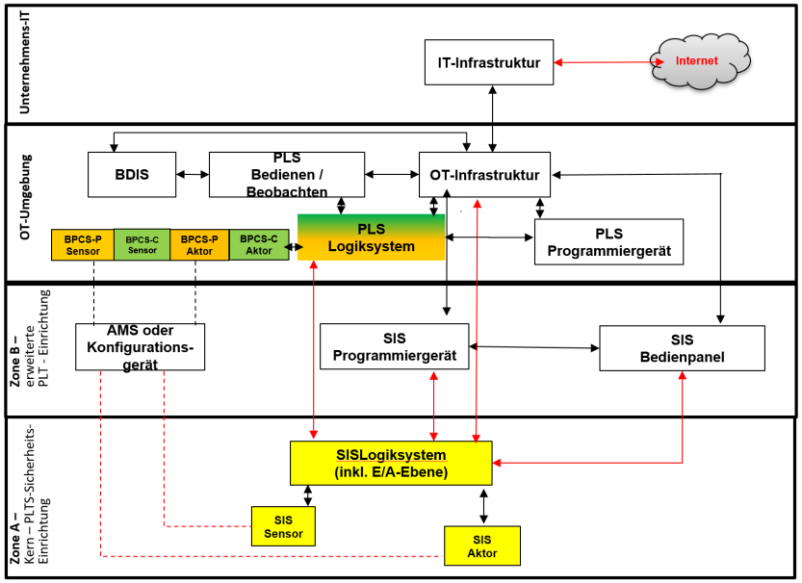


NAMUR NA 163 Modell

BPCS-CP MIXED

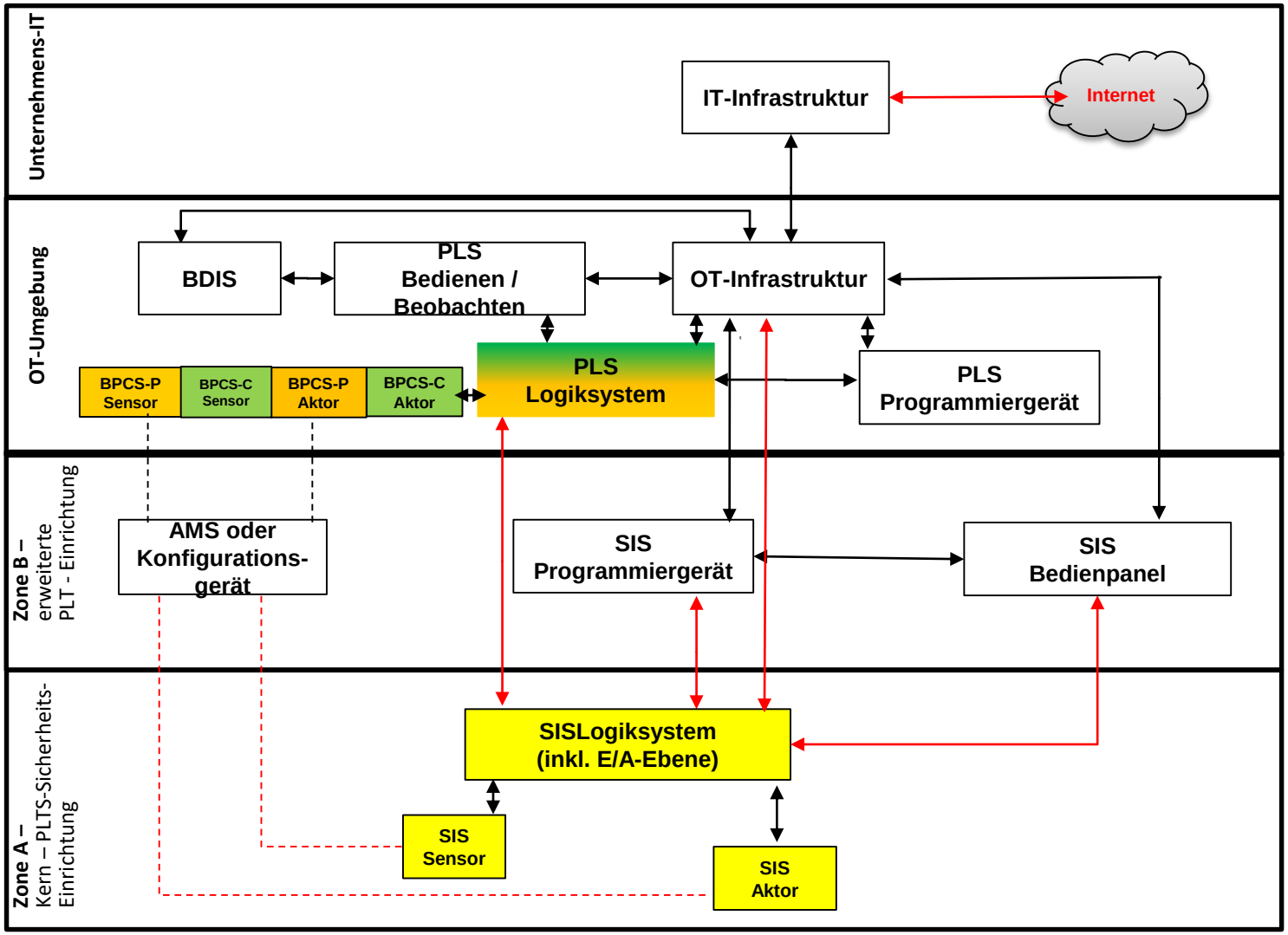


2017

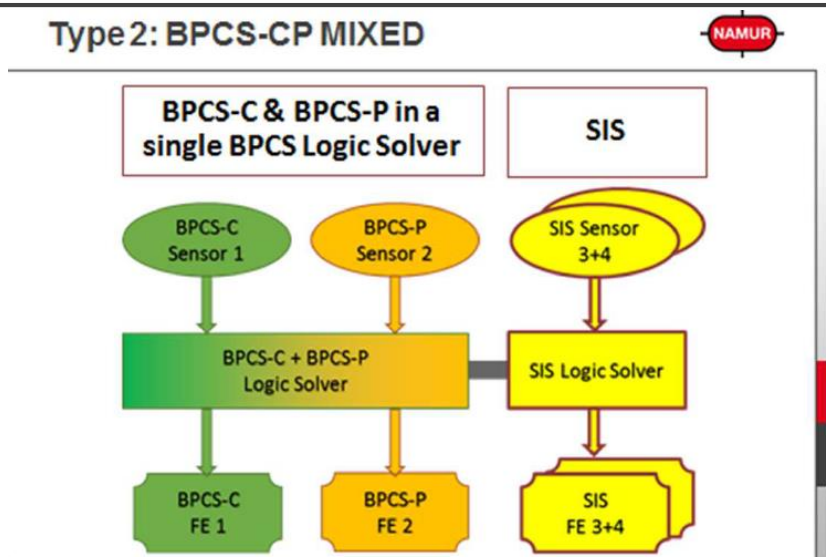


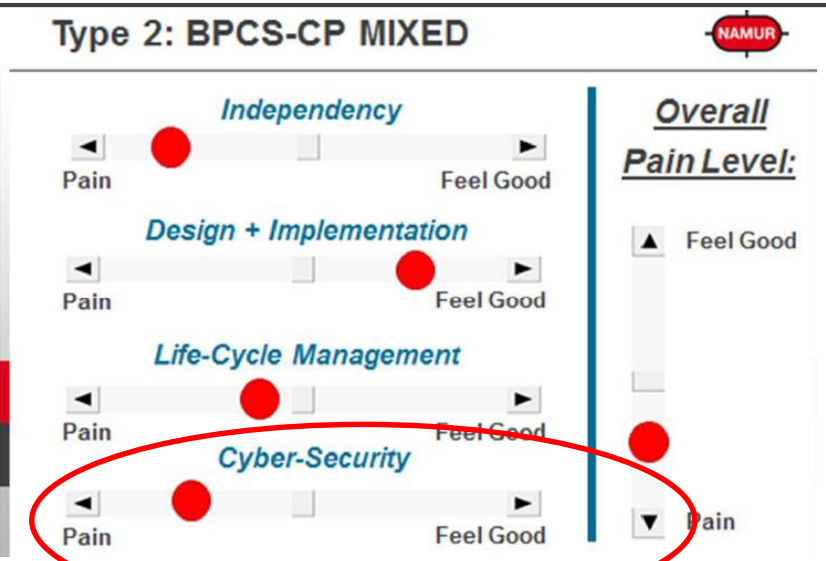
2021

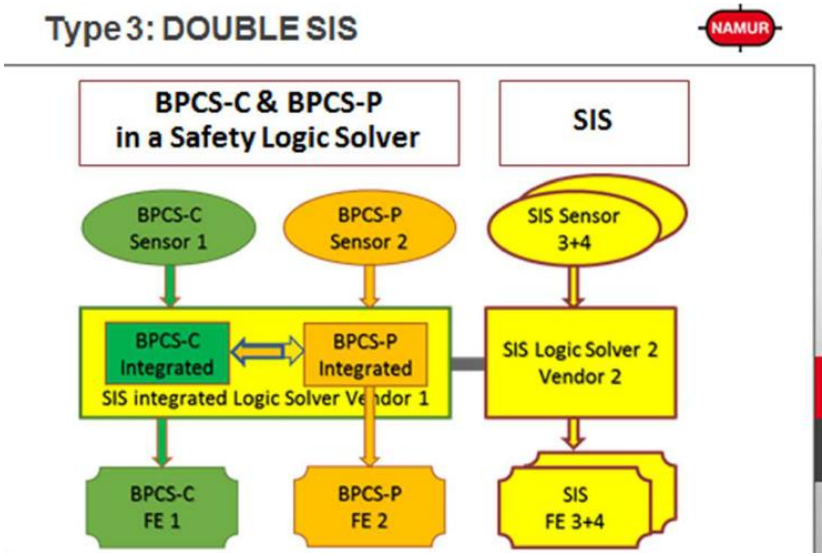
BPCS-C/P in SIS



Ergebnis Umfrage NAMUR-HS 2017







Anforderungen aus der VDE 2180

7.3 Realisierung als PLT-Betriebseinrichtungen mit Sicherheitsfunktion :

Werden PLT-Betriebseinrichtungen unterhalb von SIL 1 zur Realisierung von PLT-Sicherheitsfunktionen eingesetzt, sind gegenüber einer normalen PLT-Betriebseinrichtung **erhöhte Anforderungen** hinsichtlich ihrer Ausführung und ihres Betreibens zu beachten.

- **Sicherheitsmanagementsystem**
- **Qualitätssicherungssystem**
- **Betriebserfahrungen**
- **Trennung von Funktionen: PLT-Sicherheits-funktionen und PLT-Betriebsfunktionen müssen hinreichend voneinander getrennt sein**
- **Und Cyber Security?**

Anforderungen aus der VDE 2180

8.2 IT-Risikobeurteilung (& Maßnahmen)

Eine IT-Risikobeurteilung für PLT-Sicherheitseinrichtungen und PLT-Betriebseinrichtungen mit Sicherheitsfunktion kann unabhängig oder gemeinsam mit einer allgemeinen IT-Risikobeurteilung durchgeführt werden.

- Vollständige Dokumentation der Hard und- Softwarekomponenten
- Organisatorische Maßnahmen, die in Kommunikation und in entsprechende Maßnahmen münden
- Zugangsbegrenzung auf notwendige Minimum
- System- Funktionshärtung der Komponenten
- Klassifikation der Informationen der PLT-Sicherheitsfunktion
- Personen, Prozesse und Organisation weisen einen angemessenen Reifegrad auf
- Bedrohungszenarien als auch Wirksamkeit der Maßnahmen werden kontinuierlich bewertet und aktualisiert.

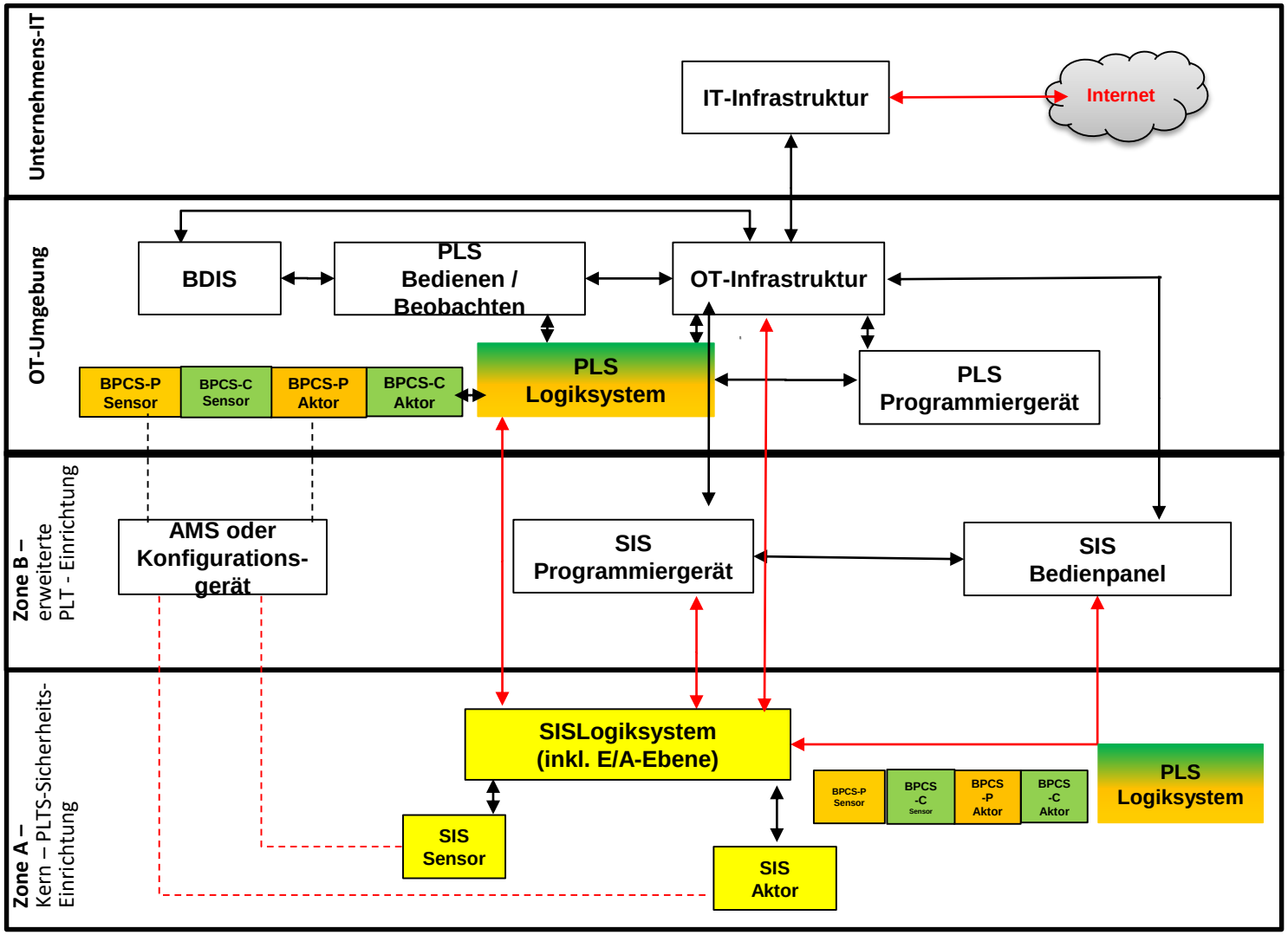
Anforderungen aus der VDE 2180

7.3 Cyber-Security: Wenn PLT-Sicherheitsfunktionen und PLT-Betriebsfunktionen innerhalb des gleichen Systems realisiert werden, besteht potenziell ein **„Common-Cause-Risiko**“. Dieses Risiko kann deutlich reduziert werden, wenn die in Abschnitt 8 beschriebenen Maßnahmen umgesetzt werden, insbesondere die physikalische/logische und organisatorische Trennung der Funktionen der PLT-Betriebseinrichtung und PLT-Sicherheitseinrichtung.

8 Cyber-Security
Im Management der funktionalen Sicherheit müssen IT-Sicherheitsaspekte in der Planung, der Beschaffung, der Validierung, im Betrieb, bei Änderungen und bei der Außerbetriebnahme berücksichtigt werden.

8.1 Risiken
Durch den Einsatz IT-basierter Technologien und die zunehmende Vernetzung von Systemen können Automatisierungssysteme inklusive der zugehörigen Programmier- und Konfigurationsgeräte zum Ziel von Cyber-Bedrohungen werden.

BPCS-C/P in SIS



… Erkenntnis

Das BPCS-P fällt fast unter die gleichen Regularien wie das SIS

7.3 Realisierung als PLT-Betriebseinrichtungen mit Sicherheitsfunktion :
Werden PLT-Betriebseinrichtungen unterhalb von SIL 1 zur Realisierung von PLT-Sicherheitsfunktionen eingesetzt, sind gegenüber einer normalen **PLT-Betriebseinrichtung erhöhte Anforderungen** hinsichtlich ihrer Ausführung und ihres Betreibens zu beachten.

… was ist mit dem Common Cause Fehler

7.3 Cyber-Security: Wenn PLT-Sicherheitsfunktionen und PLT-Betriebsfunktionen innerhalb des gleichen Systems realisiert werden, besteht potenziell ein **„Common-Cause-Risiko**“. Dieses Risiko kann deutlich reduziert werden, wenn die in Abschnitt 8 beschriebenen Maßnahmen umgesetzt werden, insbesondere die physikalische/logische und organisatorische Trennung der Funktionen der PLT-Betriebseinrichtung und PLT-Sicherheitseinrichtung**.**

Wie lässt sich dies in der Praxis umsetzen?

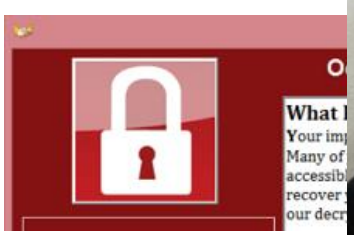
… und nun ?

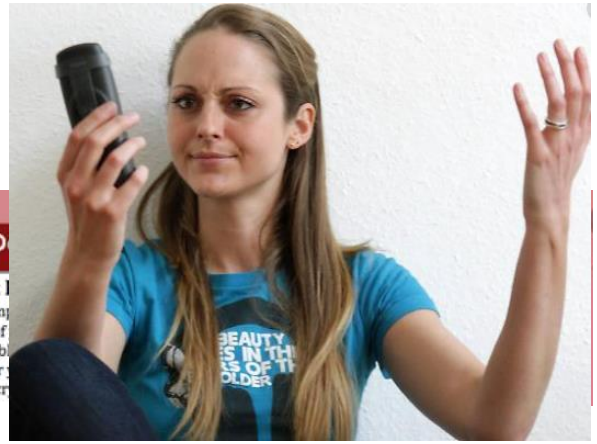
Cyber Angriff als „Common Cause“ Fehler

SIL SLAM 2020

Es ist Freitag der 13. und folgendes passiert um 22:30 Uhr in einer Meßwarte …

„Ich kann nicht auf den Server zugreifen. Der Computer zeigt mir etwas in Englisch an.“





Cyber Angriff als „Common Cause“ Fehler

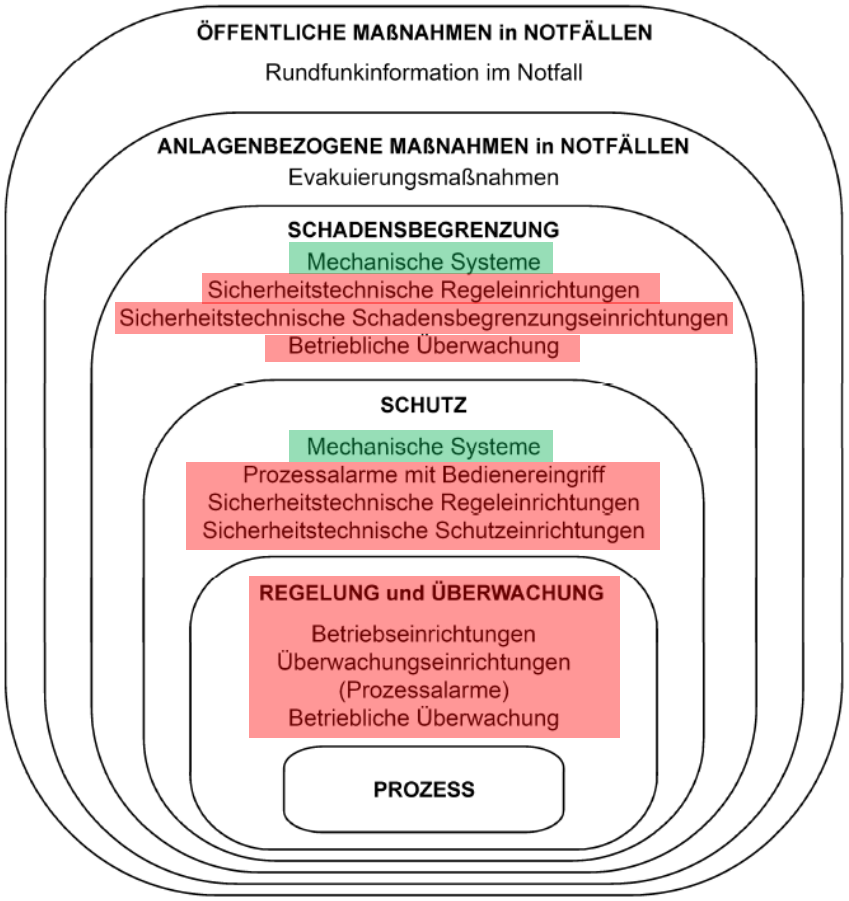


Bild 9 – Typische Schutzebenen und Maßnahmen zur Risikominderung

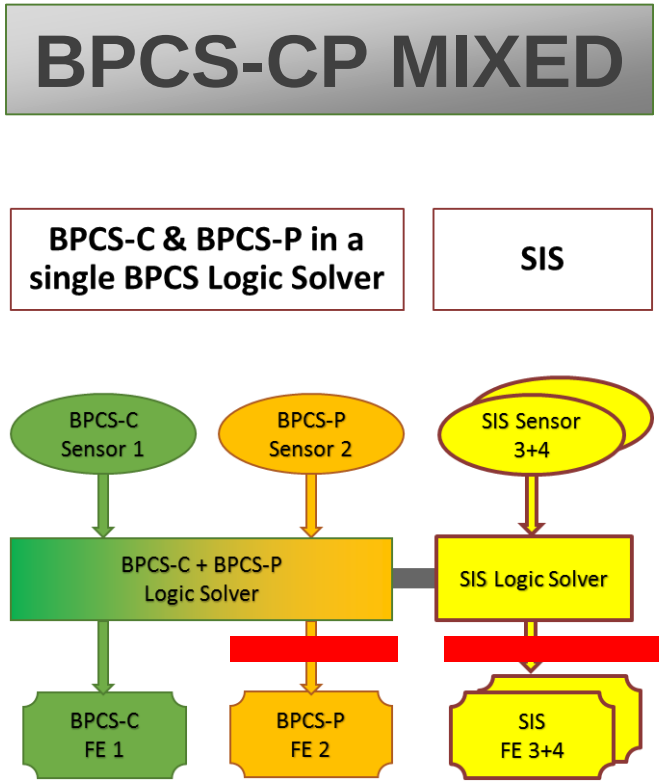
Ist es gut, wenn sämtliche primäre Schutzschichten auf angreifbare Technologie bauen?

Funktionieren Evakuierungsmaßnahmen im Falle eines Cyber Angriffs?

Haben wir die mechanischen Systeme noch, oder sind sie über die Zeit entfallen?

Quelle: IEC 61511-1 - 2019

LLoDD – Last Line of Defense Devices



Cybersichere LLoDD

- **Manuelle Abschalteinrichtung um PLT-Einrichtungen in den energielosen sicheren Zustand zu bringen**
- **Manuelle Absperrmöglichkeiten von Stoffströmen**
- **Manuelle Abschalteinrichtung für Hilfsenergien**

Unsere Empfehlung (1)

- **Prüfen Sie Ihren Alarm- und Gefahrenabwehrplan!**
- **Kann Ihre Anlage „cybersicher“ entsprechend einer trainierten Abfahrprozedur geordnet in den definierten sicheren Zustand gebracht werden?**
- **Greifen Sie bei der Durchführung des AGAPs ausschließlich auf cybersichere LLoDDs zurück?**

Unsere Empfehlung (2)

- **Trainieren Sie Ihre Anlagenfahrer!**
- **Schaffen Sie „Awareness“ zum Thema Cyber-Angriffe**
- **„Security Moment“ anstelle „Safety Moment“**
- **Fixieren Sie, WER entscheidungsbefugt ist die Anlage via LLoDDs abzuschalten und WANN dies geschehen soll!**

The End ….

Thank you
For your feedback!

Questions are welcome!

Anhang

LLODD – Last Line of Defense Devices

- **Manuelles Betätigen von Handarmaturen**
- **Hardverdrahtete Anlagen-Aus-Schalter**
- **Abschalten der Zuluft für pneumatisch angetriebene Armaturen durch:**
  - **Schließen der Hauptabsperrarmatur der MSR-Luft und Entspannung des MSR-Luftsystems**
  - **Abschalten der Spannungsversorgung der Magnetventile**
- **Abschalten der elektrischen Antriebe durch:**
  - **Abschalten der Steuerspannung**
  - **Abschalten der Versorgungsspannung**
  - **Betätigung von Wartungsschaltern an Motoren**
- **Abschalten der Versorgungsspannung des Prozessleit- und/oder Sicherheitssystems**
- **Abschaltung der Versorgungsspannung des Betriebes durch:**
  - **Trafonotschalter**
  - **Energieversorgung**

Erkennung von Cyberangriffen in der Anlage

Mögliche Szenarien, die auf einen Cyber-Angriff hinweisen, können die folgenden sein:

- unsinnige nicht gewohnte Bildschirmdarstellung,
- NICHT vom Bediener ausgeführte Tastatur- und Mausanzeigen,
- Fremdsteuerung,
- geldliche Erpressungsversuche,
- Beschränkung des Zugriffs auf das Prozessleitsystem
- Ungewöhnliche oder sich widersprechende Systemmeldungen auf dem Leitsystem oder dem Prozessinformationssystem, die im Normalbetrieb nicht auftreten (Bürocomputer, SPS)
- Keine oder eingeschränkte Bedienbarkeit des Leitsystems und von Bildschirmen usw.
- Angezeigte Zustände im Prozessleitsystem entsprechen nicht dem Anlagenzustand vor Ort
- Angezeigte Messwerte weit außerhalb der normalen Prozessfahrweisen
- Eingefrorene Bildschirme

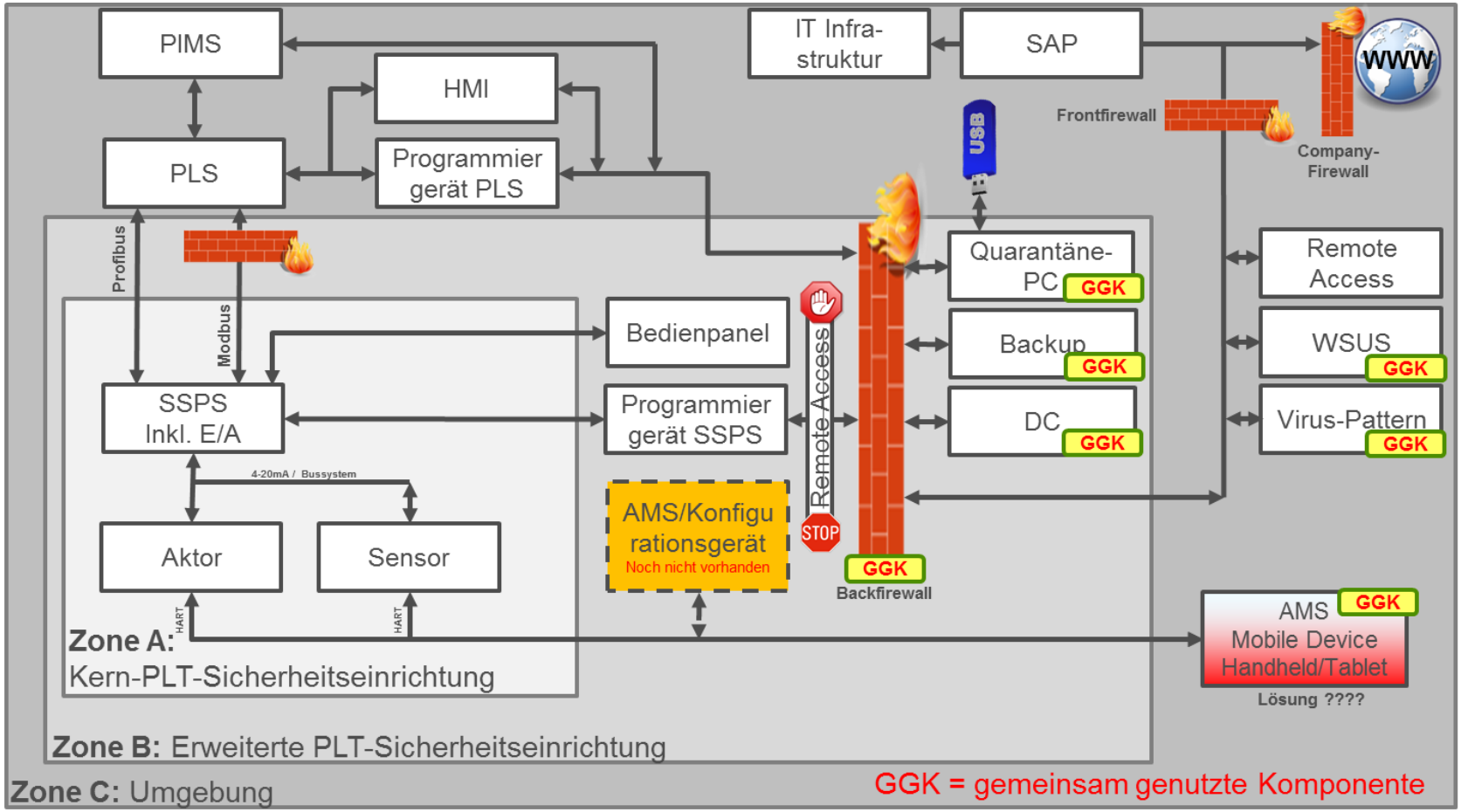
Erkennung von Cyberangriffen in der Anlage

Mögliche Szenarien, die auf einen Cyber-Angriff hinweisen, können die folgenden sein:

- lange Systemantwortzeiten
- Unerwartete Veränderungen von Prozessparametern (ungewöhnliche und/oder plötzliche Veränderungen von Messwerten)
- Ungewöhnliche Zudosierung von Stoffen (bei Batchproduktion)
- Ungewöhnliche Änderungen von Drücken, Temperaturen oder weiteren Sensoranzeigen
- Abweichungen in der Qualitätskontrolle durch nicht nachvollziehbare Rezepturveränderungen
- Ungewöhnliches Ansprechen der mechanischen Überdrucksicherheitseinrichtungen (deutet auf ein Versagen der vorgelagerten Sicherheitskette hin)
- Ausfall der Telekommunikationssysteme (Telefon etc.)
- Ungewöhnliches Verhalten von Maschinen oder Anlagenkomponenten (z.B. Zentrifugen/Kompressoren drehen schneller oder langsamer als im Normalbetrieb)
- Ungewöhnliche Telefonanrufe von unbekannten Personen in der Messwarte mit der Aufforderung zu handeln

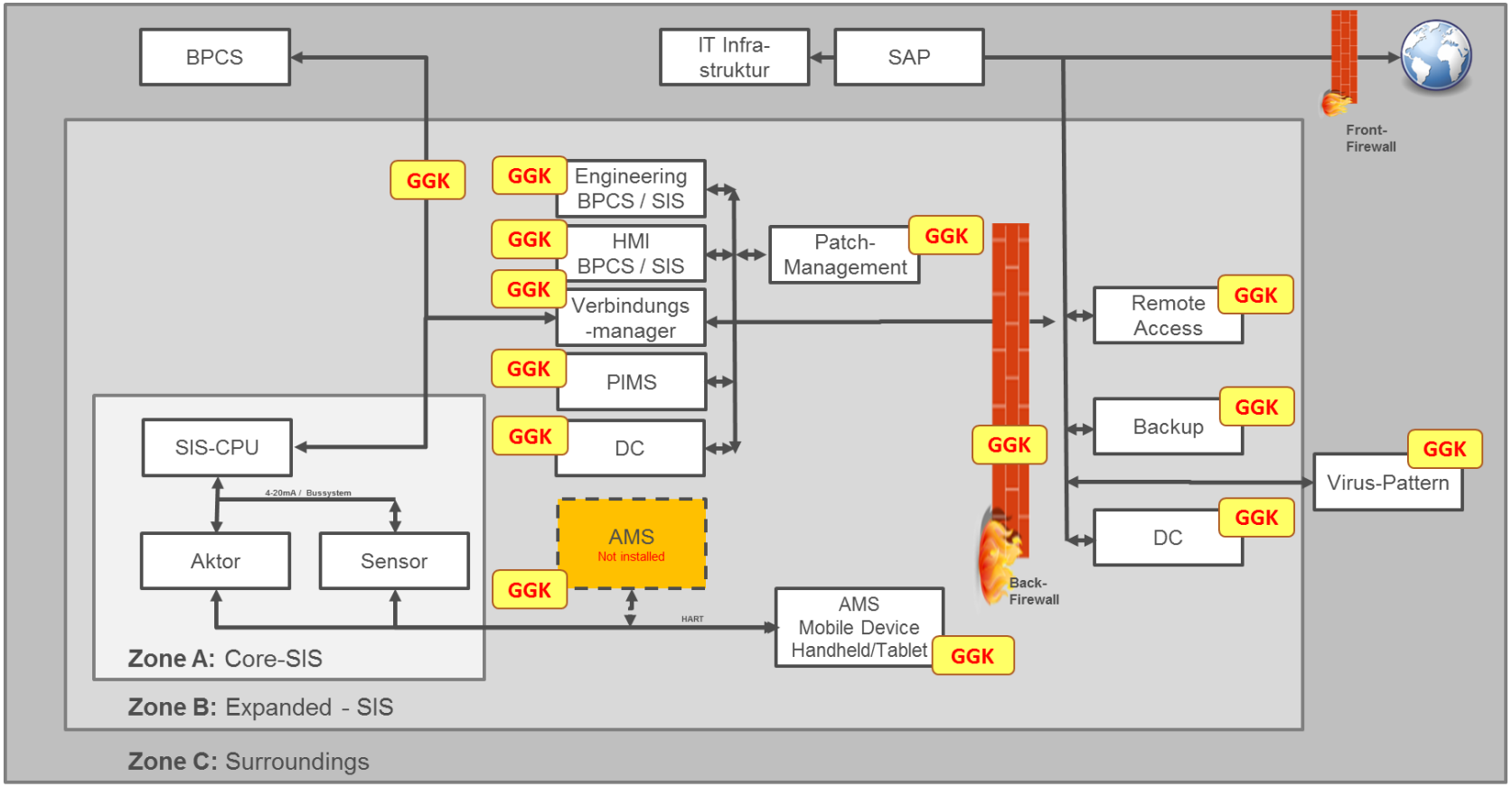
Type 2: BPCS-CP-MIXED im NA 163 Modell

Ausgeführt als „getrenntes System“ / verschiedene Lieferanten für BPCS - SIS

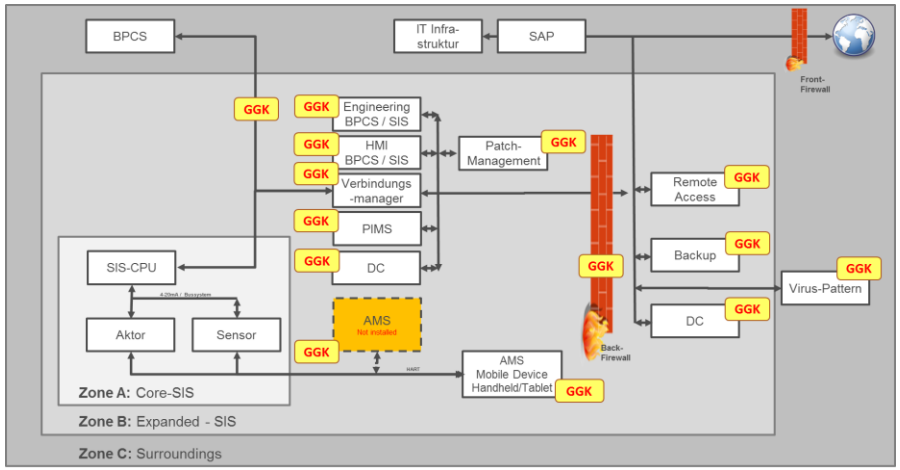


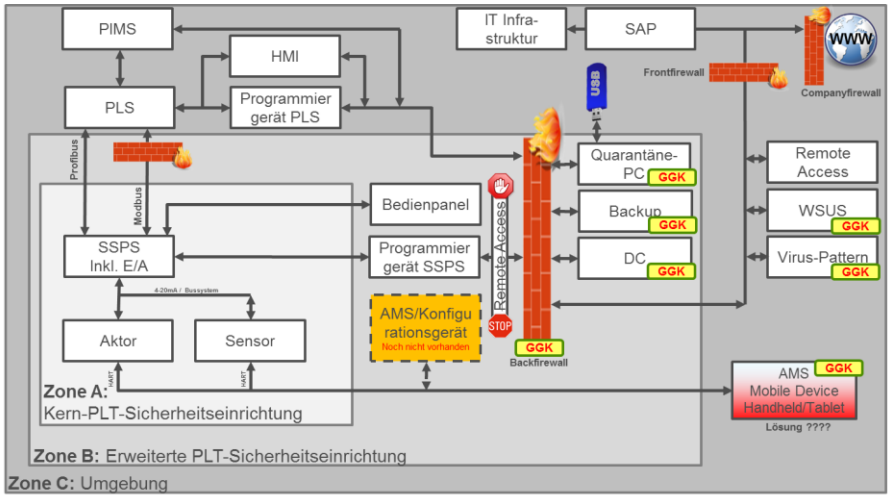
Type 2: BPCS-CP-MIXED im NA 163 Modell

Ausgeführt als „integriertes System“ / gleicher Lieferant für BPCS - SIS



NAMUR NA 163 Modell





- integriertes System

Was fällt auf ?

- getrenntes System

NAMUR NA 163

6.7. Umgang mit gemeinsam genutzten Komponenten

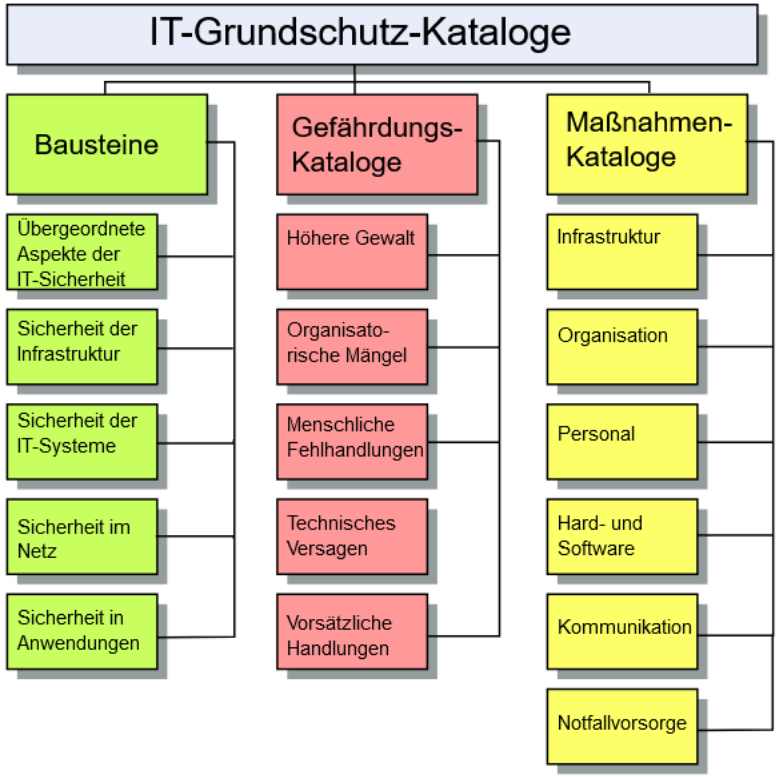
Zur Behandlung von gemeinsam genutzten Komponenten im Sinne der IT-Sicherheit kann wie folgt verfahren werden:

Lösung 1: Die Komponente ist im Management System der Funktionalen Sicherheit eingebettet (d.h. ist validiert UND unterliegt – auch für den nicht sicheren Teil – dem Change Management).

Lösung 2: Der NACHWEIS wird erbracht, dass innerhalb der gemeinsam genutzten Komponente eine – unter IT-Sicherheits- Gesichtspunkten- hinreichende Trennung und Unabhängigkeit zwischen dem „sicheren" Teil und dem „betrieblichen" Teil vorliegt. (Voraussetzung ist hier, dass der Nachweis der Konformität zu IEC 61508 oder IEC 61511 vorliegt.)

Lösung 3: In einer IT-Risikobeurteilung wird schriftlich dokumentiert, dass sich durch die gemeinsame Nutzung keine nicht tolerierbaren IT-Sicherheitsrisiken für die PLT-Sicherheitseinrichtung ergeben.

Beispiel: Aufbau des IT Grundschutz (BSI)



Functional Safety Discipline

SIL Sprechstunde 2021
Safety & Availability





10 10 10 BY2020

Christian Demski

Technical Expertise and Support

Leverage Globally, Act Regionally, Execute Locally – ***Faster and Smarter***

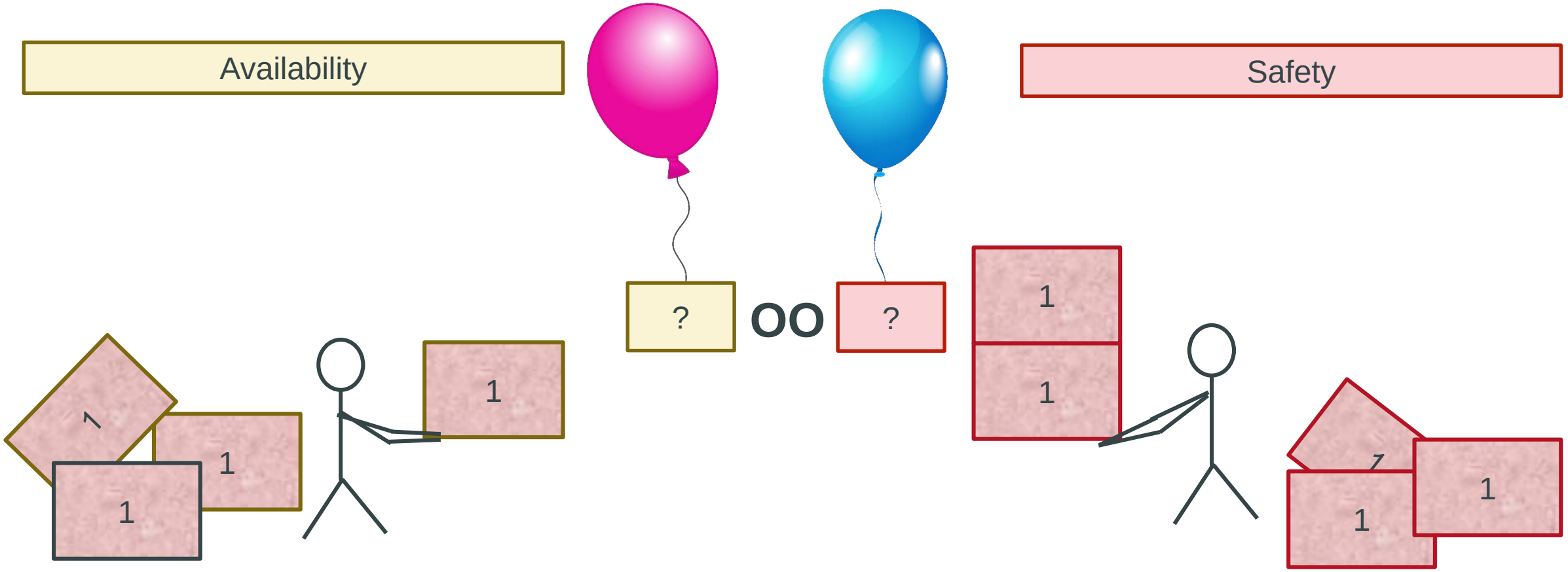
Definitions

- **safe failure (IEC 61511-1 ed. 2 3.2.62)**
  - failure which favors a given safety action
  - Own summary of the notes:
    - What is safe for one function my not be safe for another
    - Redundancy plays a role
    - And it might significantly impact the production availability

Note 1 to entry: A failure is "safe" only with regard to a given safety function.
Note 2 to entry: When fault tolerance is implemented, safe failure can lead to either:
– operation where the safety action is available but with a higher probability of success on demand (demand mode of operation) or a lower likelihood to cause a hazardous event (continuous mode of operation);
– a spurious operation where the safety action is initiated.
Note 3 to entry: When no fault tolerance is implemented, safe failures result in the initiation of the safety action regardless of the process condition. This is also known as a spurious trip.
Note 4 to entry: A spurious trip may be safe with regard to a given safety function but may be dangerous with regard to another safety function.
Note 5 to entry: Spurious trips may also have detrimental effects on the production availability of the process.

- **safe failure (IEC 61508-4 ed. 2 3.6.8)**
  - failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that:
    a) results in the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state; or
    b) increases the probability of the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state

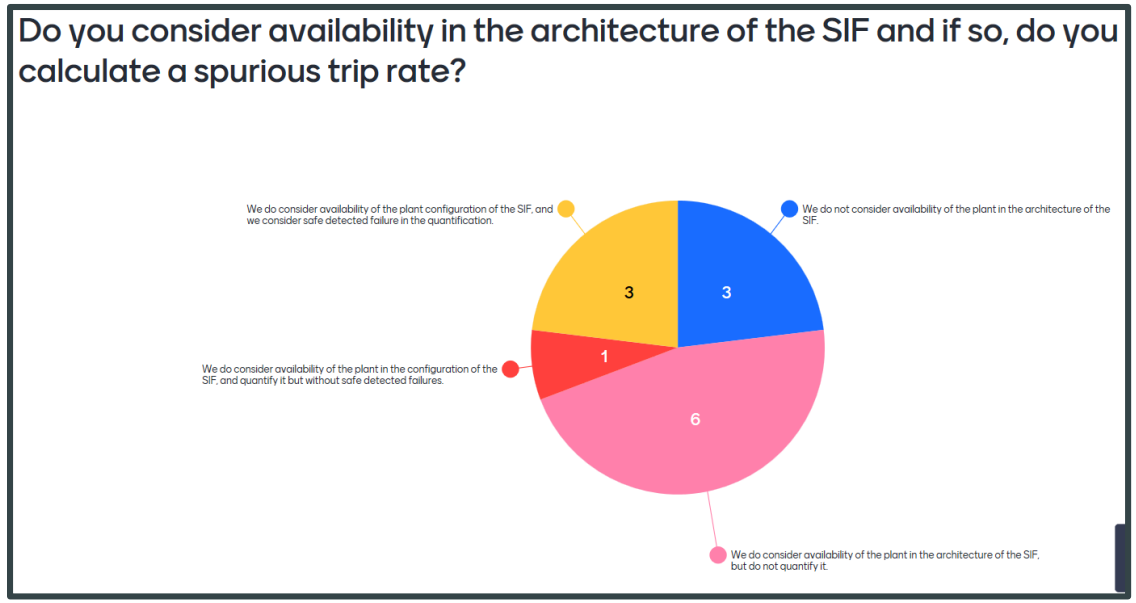
This is the discussion we know.



Questions to the audience?

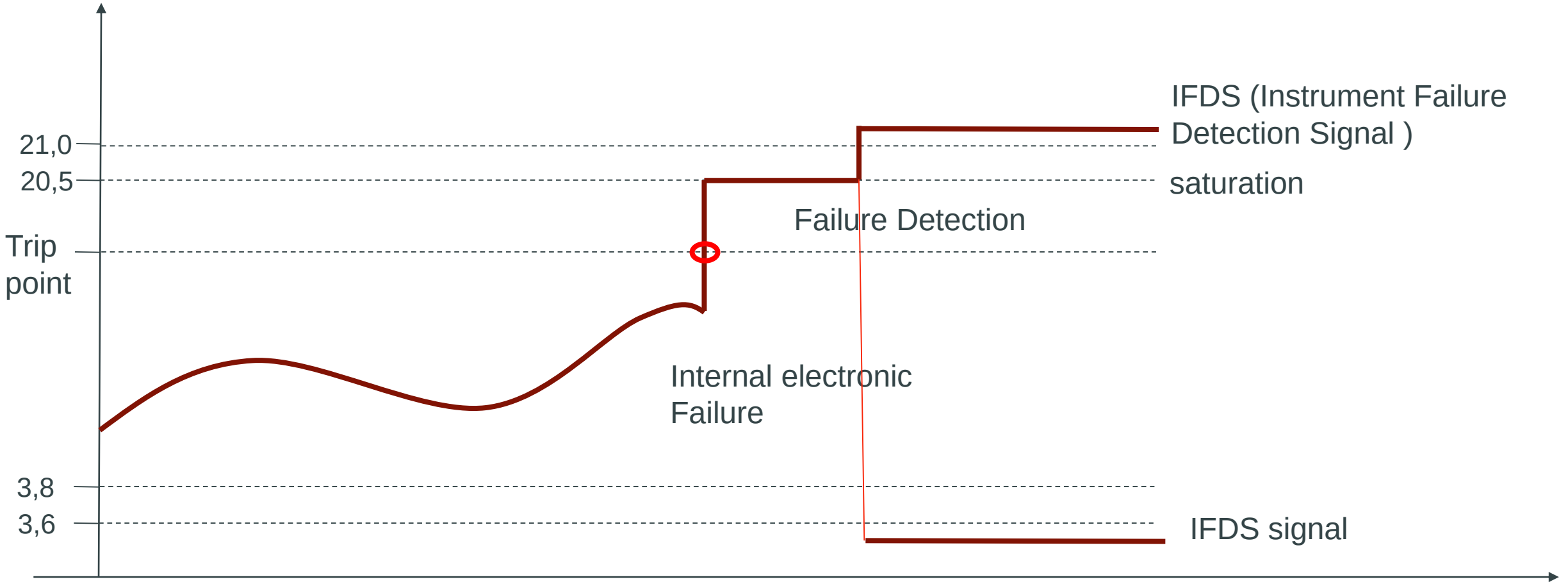
Do you consider availability in the architecture of the SIF and if so, do you calculate a spurious trip rate?

- We do not consider availability of the plant in the architecture of the SIF.
- We do consider availability of the plant in the architecture of the SIF, but do not quantify it.
- We do consider availability of the plant in the configuration of the SIF, and quantify it but without “safe detected” failures.
- We do consider availability of the plant configuration of the SIF, and we consider “safe detected” failure in the quantification.



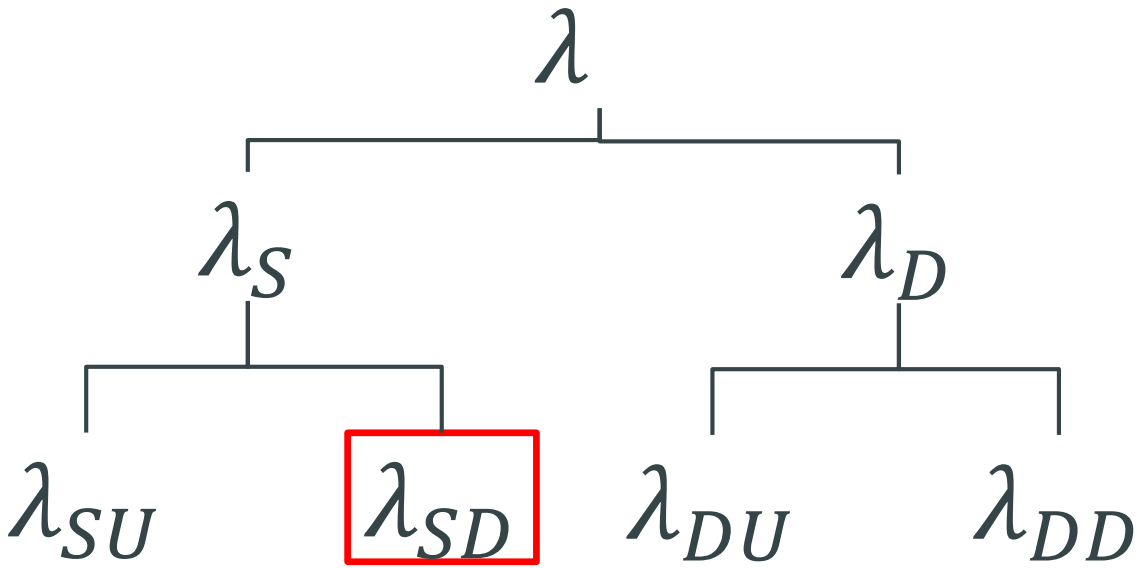
Result: SIL Slam 09/13/2021

An actual event in the plant led to some thoughts…..



Basics

- Four Failures:
  - Safe:
    - Detected
    - Undetected
  - Dangerous:
    - Detected
    - Undetected



Do safe detected failure exist?

Looking from a manufacturer point of view

- We (manufacturer) can only say that in case the output signal is beyond a certain accuracy, it is considered to be dangerous.
- Within a certain bandwidth (and without a frozen signal) it is considered to be safe

Anything to add from our manufacture colleagues?

Consequence for the user:
Failures that are considered to be dangerous by the manufacturer turn out to be safe at the user side.

(this is applicable for detected and undetected)

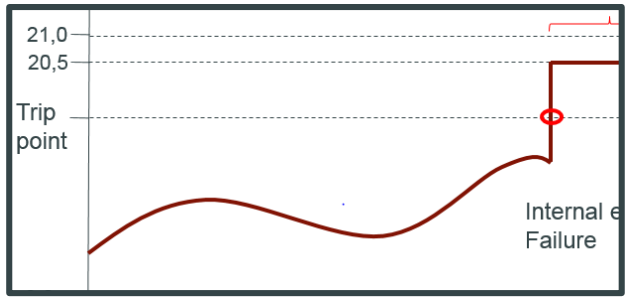
Example in a certification.

Table 2: Summary – IEC 61508 failure rates

Failure category	Failure rates (in FIT)
Fail Safe Detected (λ_{SD})	**0**
Fail Safe Undetected (λ_{SU})	**0**
Fail Dangerous Detected (λ_{DD})	**527**
Fail detected (detected by internal diagnostics)	382
Fail high (detected by safety logic solver)	23
Fail low (detected by safety logic solver)	87
Annunciation detected (λ_{AD})	35
Fail Dangerous Undetected (λ_{DU})	**38**
Fail Dangerous Undetected (λ_{DU}) with Display	**39**

The value shown by the instrument is leaving the accuracy boundary to the high side. In case the trip is a high trip, this means this trip may be activated even if the process is still in a normal operating parameters.

Is this a safe failure rather than a dangerous one?

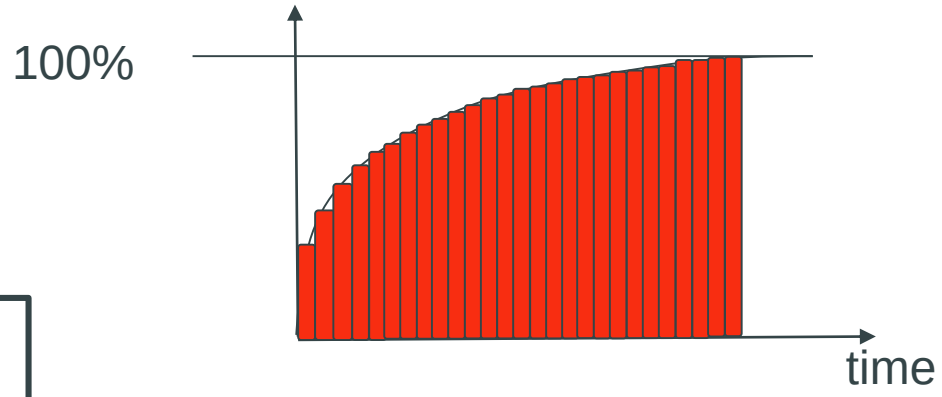


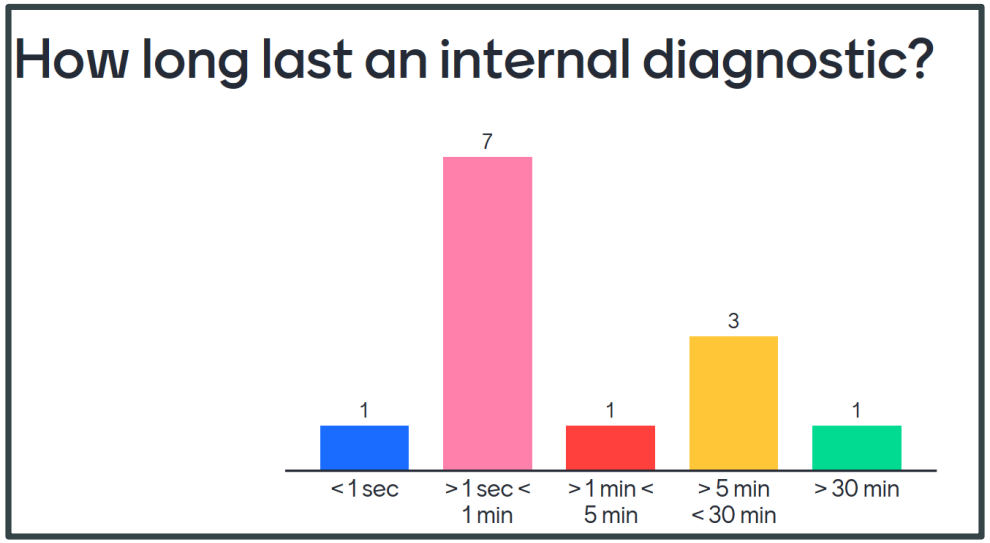
How long does internal diagnostic take?

- < 1 sec
- > 1 sec < 1 min
- > 1 min < 5 min
- > 5 min < 30 min
- > 30 min

In most of the cases it takes more than 30 min…..

SUM (Number of failures * frequency of occurrence)



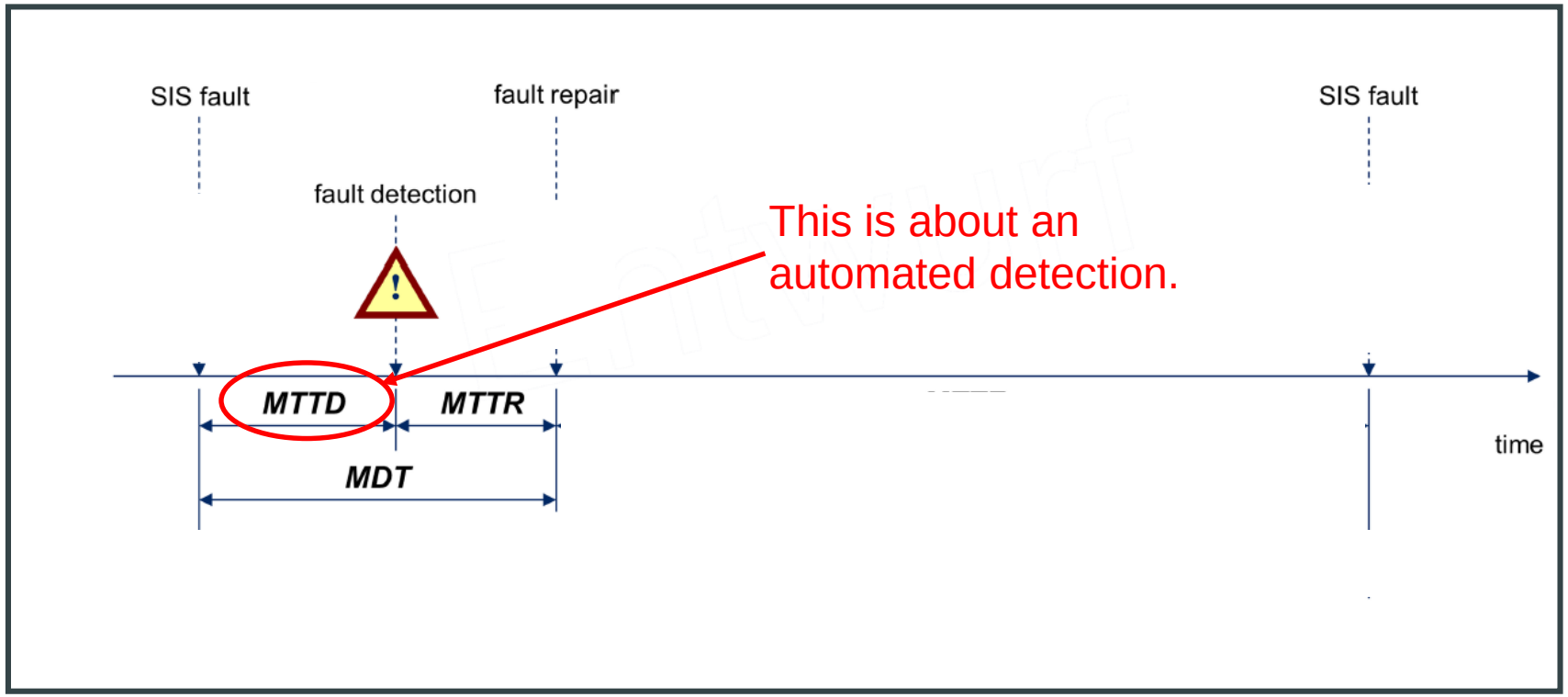


Result: SIL Slam 09/13/2021

What does a detection do?

- An internal detection detects failures of an electronic device.
- What is the effect of the detection time from a safety point of view?
- The failures we are looking at, are the λ_D (Dangerous) ones. These failures would never cause the plant to trip, even if the trip condition is reached.

Effect from a safety point of view



Graph: based on VDI 2180 part 3 (2019)

MTTD: Mean time to detect
MTTR: mean time to restoration
MRT: Mean recovery time
MDT: Mean down time

MTTR according IEC 61508-4 and 11-1 ed. 2)

MRT according IEC 61508-4 and 11-1 ed. 2)

Table B.1 – IEC 61508-6

MTTR = MRT = 8 (72) hours is based on the assumption that the time to detect a dangerous failure, based on automatic detection, is << MRT

Effect from a safety point of view

- In this context and with a MTTR of often 8 to 72 hours, it has no significant effect if the failure is detected in one second or in 3 hours.
- In a safety loop, test intervals from 1 up to 6 years proof testing (~ 45,000 hours) are used.
- From the safety point of view, the cycle time for an internal failure detection is not essential.

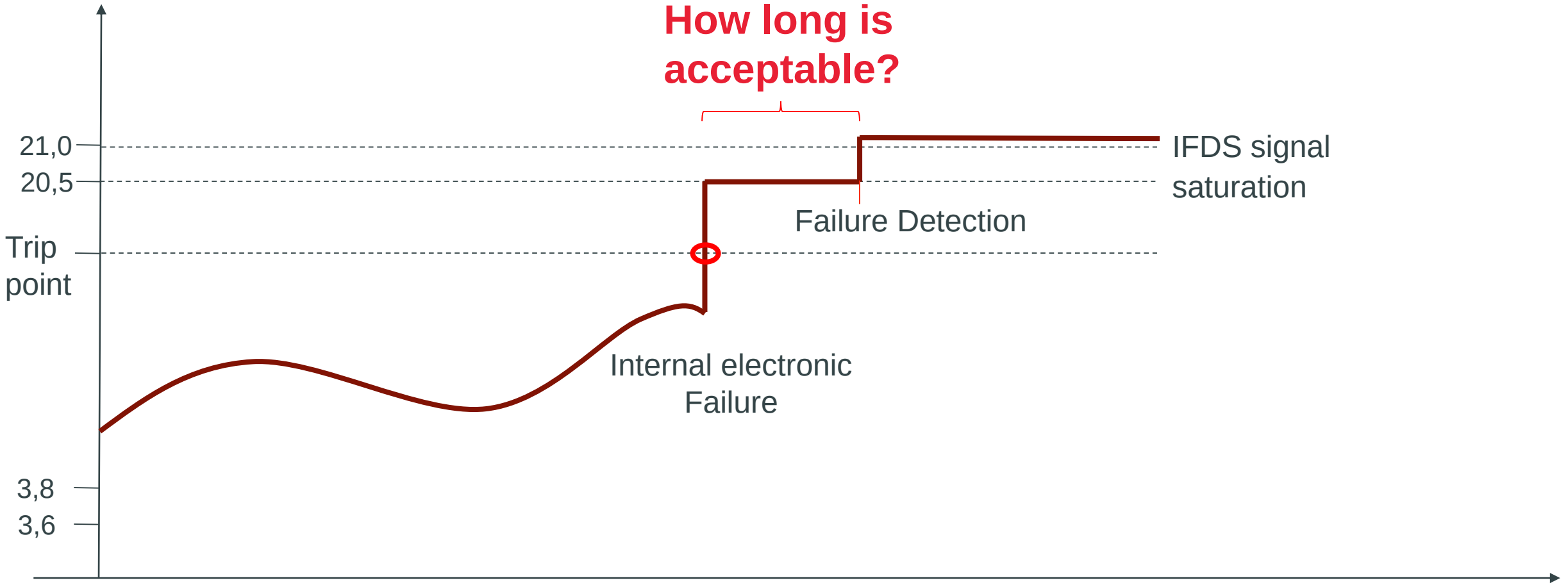
Table B.1 – IEC 61508-6

MTTR = MRT = 8 hours is based on the assumption that the time to detect a dangerous failure, based on automatic detection, is << MRT

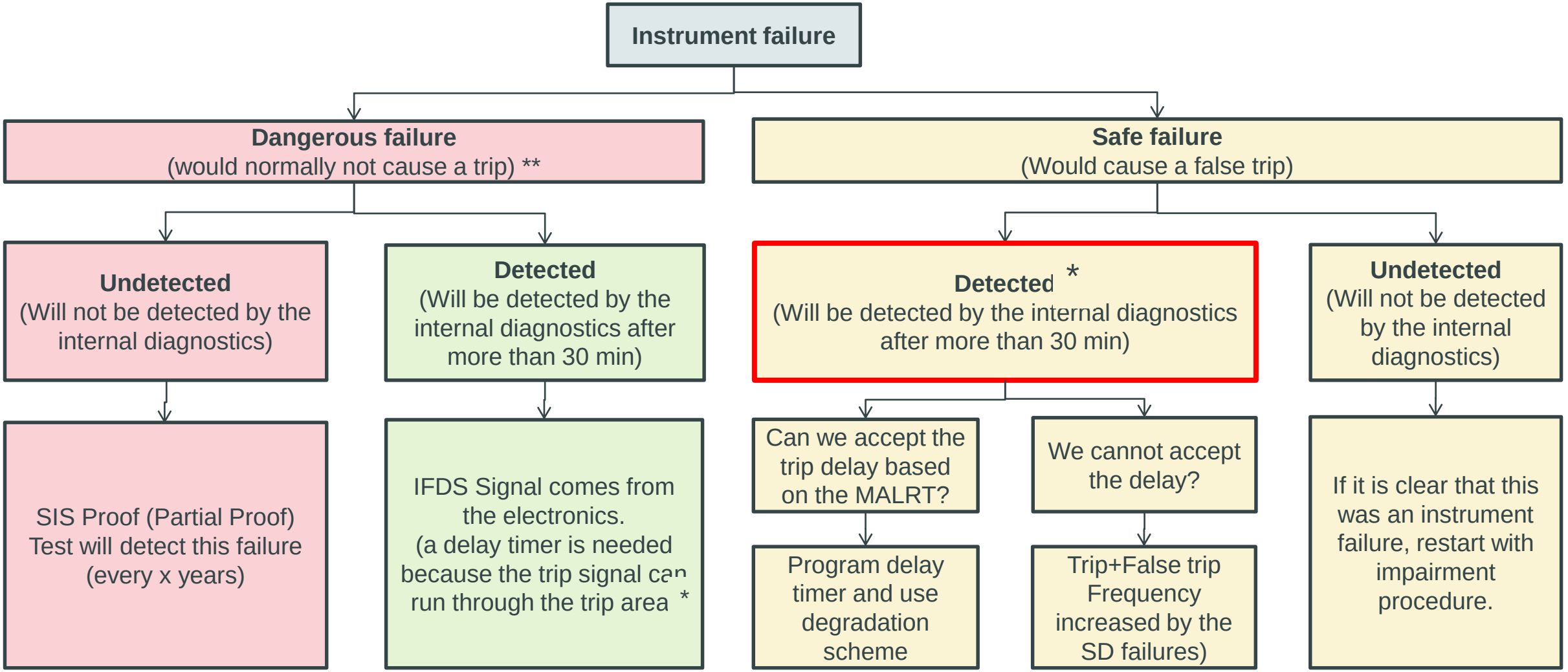
Effect from a availability point of view.

- An internal detection detects failures of an electronic device.
- What is the effect of the detection time from a availability point of view?
- The failures we are now looking at, are the λ_S (Safe) ones. These failures would cause the plant to trip even if the trip condition does not take place.

An actual event in the plant lead to some thoughts…..



Effect of failures impact of IFDS

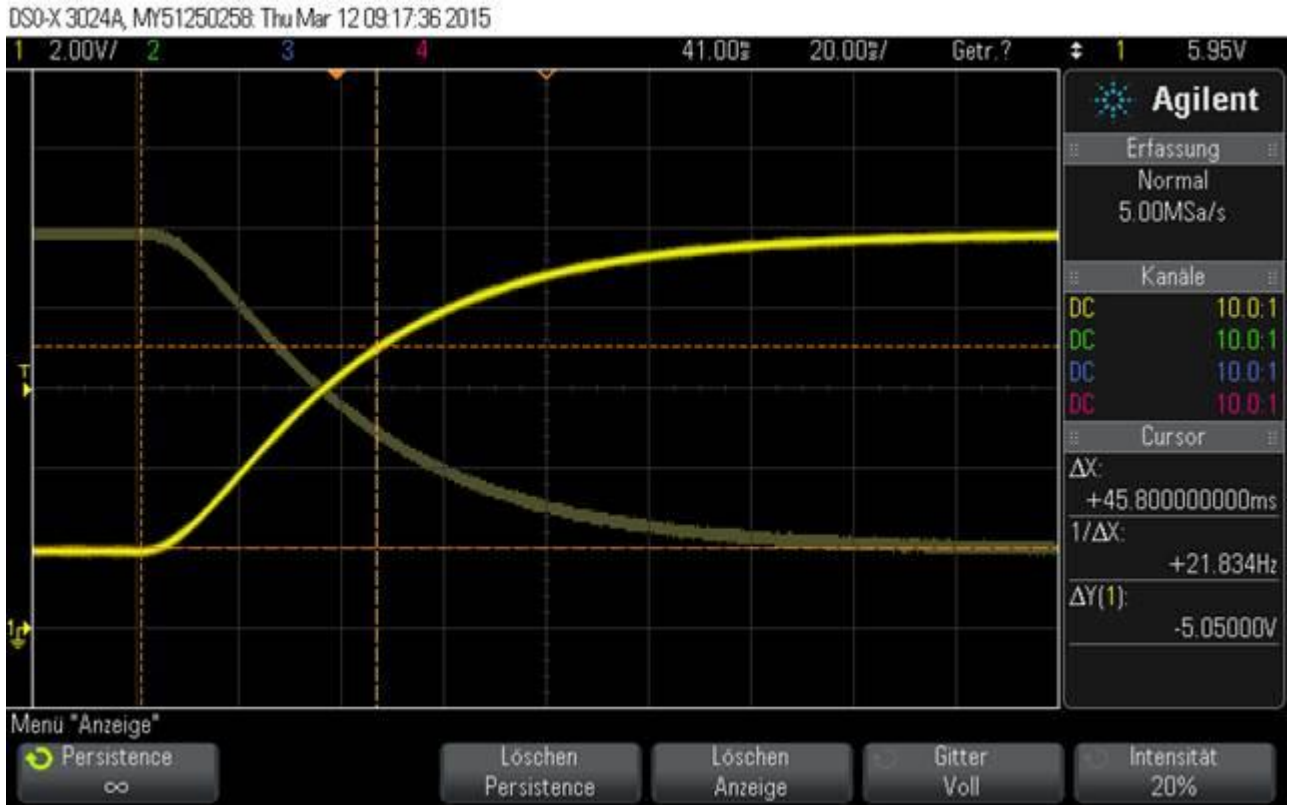


** Only for IFDS. Some other diagnostic together with configurations offer different abilities. See following discussion*

*** Except dangerous detected 1oo1.. etc*

MALRT = Maximum allowable loop response time.

Signal if the failure is detected.



It is not a step it is a ramp. 300 ms in this case. So a delay timer on the AI is needed anyway. (just 1 or 2 sec)

What is available outside of IFDS
Different modes of diagnostic

- **Hi/Lo:** This is programmed in the DCS to detect a shortcut or an open circuit
- **Diagnostics (fail safe):** is the internal diagnostic of the device that leads to the output signal in the area of the current indicting a failure (Namur < 3.6 mA or > 21.0 mA)
- **Intercomparison:** comparing the signals of devices against each other
- **Rate of change:** algorithm programmed in the DCS meant to detect changes in the signal that cannot happen under process condition indicating a failure of the device.

How do other methods of diagnostic change the picture for safe detected failures

		MooN (N>M)		MooN (M=N > 1)	
	1oo1	1ooN	MooN (M>1)	redundant	non redundant
Hi/Lo (device)	No λ_{SD}	λ_{SD}	λ_{SD}^{**}	λ_{SD}^{**}	No λ_{SD}
IFDS	No λ_{SD}	No λ_{SD}	λ_{SD}^{**}	λ_{SD}^{**}	No λ_{SD}
Deviation alarm	na	λ_{SD}^{*}	λ_{SD}^{**}	λ_{SD}^{**}	na
Rate of change	No λ_{SD}	No λ_{SD}	λ_{SD}^{**}	λ_{SD}^{**}	No λ_{SD}

- ** Deviation alarm failure are considered to be able to detect upcoming failures before the trip set point is reached.*
- *** In this application the failures going to the safe side which means that the failed unit is voting for trip. In case it is taken out of service it needs to be kept in a "vote for trip" situation. (Be aware this that this is not so easy for calculated trip points)*

Summary

- Safe failures do exist
- IFDS can only reveal them and prevent an unnecessary shut down in some configurations.
- „External diagnostic“ offer different points of detecting safe failures and increase availability.
- Different configuration offer different portions of revealed failures.

Thank you for the attention

Questions, comments, discussion points?

In case of any comment or want to have a later discussion and please contact me

Christian Demski
Dow Deutschland Anlagenge...
IEA SIS Expertise Area Leader
Technical Expertise & Support
+49 41469 13814 Work
Other
CDemski@dow.com
Postfach 1120
Stade, ND 21677

Technical Expertise & Support
Leverage Globally
Act Regionally
Execute Locally
Faster and Smarter

Safety Architectures

Prüfen von Anwender-Software

Peter Sieber

Dep. SN/HCH

Agenda

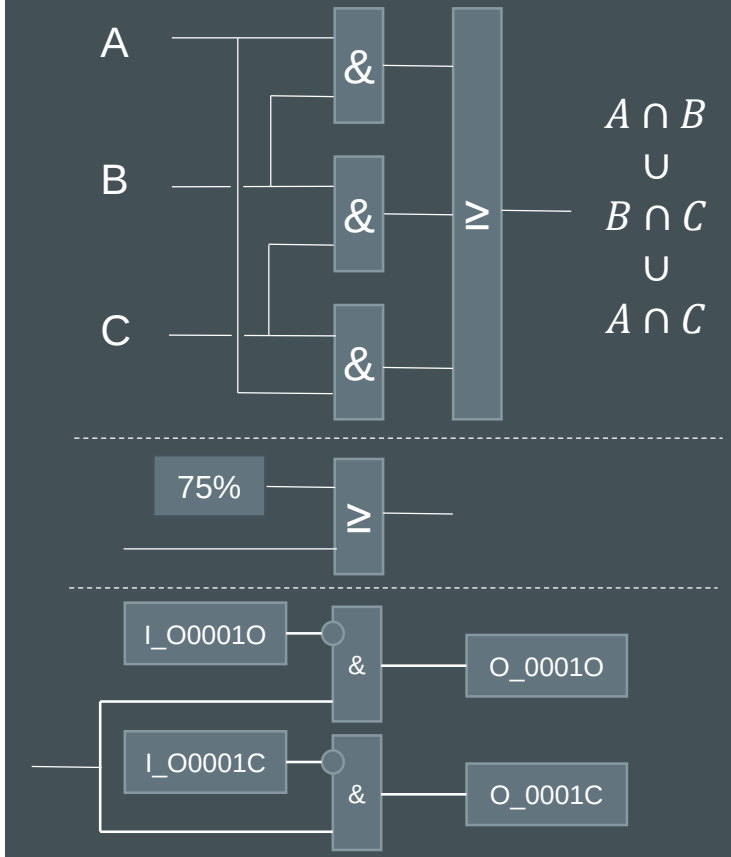
1. Fehlerarten und deren Beherrschung
2. Spezifikation und deren Umsetzung (what you get is what you **did not** expect)
3. Erstellen einer Architektur für sichere Applikationen
4. Zusammenfassung

Fehlerarten und deren Behandlung

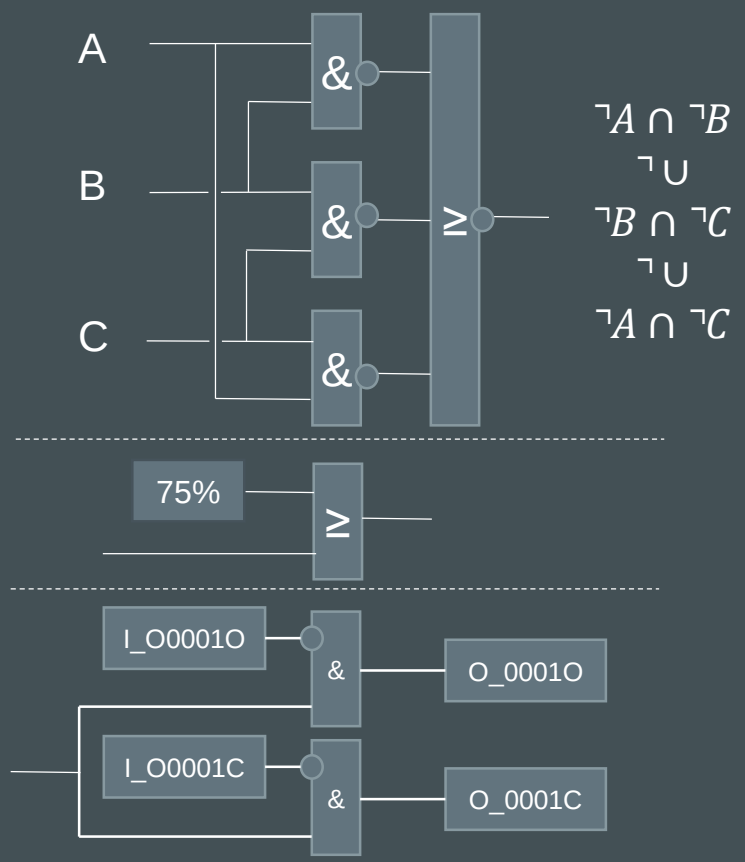
Fehlerart	Auftritt	Fehlerbeherrschung durch
Zufällige Fehler	Statistisch verteilt	➢ Fail Safe Design (SN; Planar) ➢ Architectur der Lösung (Redundanz) ➢ Komponenten Zuverlässigkeit (Route 2H acc. IEC 61508) ➢ Kombination aus Zuverlässigkeit und Test
Systematische Fehler	Immer wenn die Fehlerbedingungen Erfüllt sind	➢ Design Zuverlässigkeit (Prozess Qualification) ➢ Architektur der Lösung (Diversität) ➢ Kombination aus zuverlässigem Design und Test

Entstehung eines systematischen Fehlers

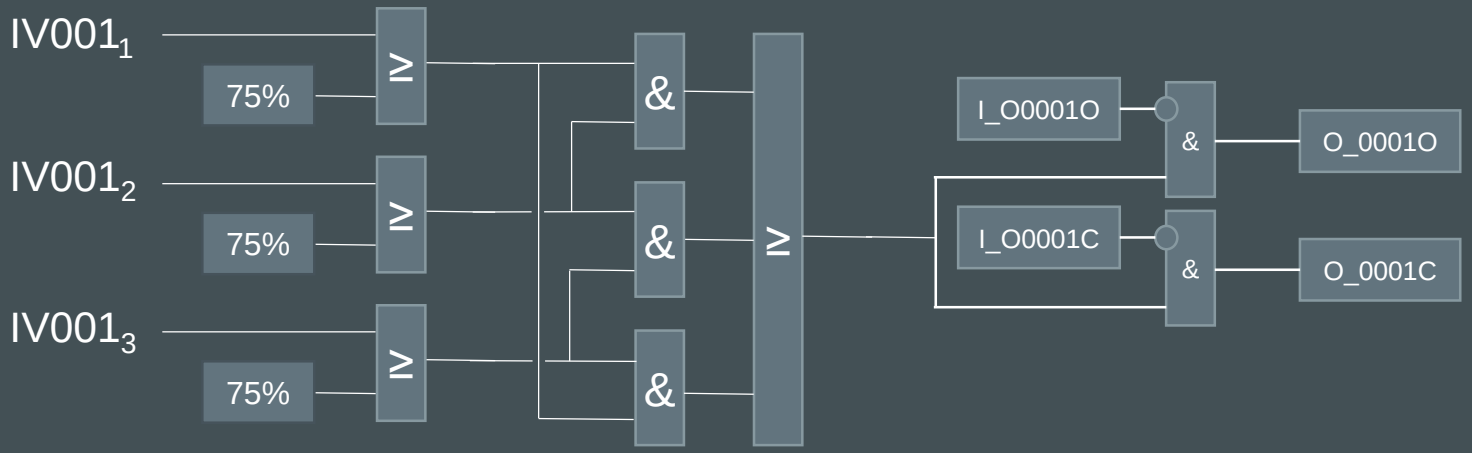
Spezifiziert



Programmiert



Die Applikation



Potentielle Fehler und deren Beherrschung

- Verdrahtung
  (ungewollte Querverbindungen)
- Tag Namen
  (Tippfehler, Zuordnungsfehler)
- Fehler in den Typicals
  (funktionale Fehler der Templates)
- Kopierfehler
  (Falsches Typical, E/A Zuordnungsfehler)

- SpezifiKation
  (Eindeutigkeit der Spezifikation)
- Definiere ein Test Programm für
  - E/A Zuordnung
  - Funktion der Templates
  - Funktion der Typicals
  - Korrektheit der Instanzen
- Implementieren der Lösung
- Testen der Lösung
- Dokumentieren der Testergebnisse

Application Design Process

Specification
(Safety Requirement Specification)

Safety Assessment 3
Acc. IEC 61511

Review Test Results
(Application)

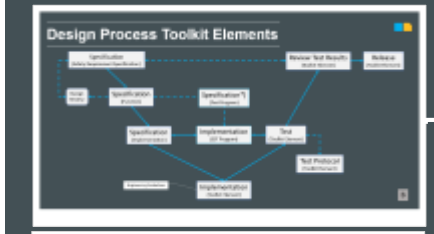
Release
(Application)

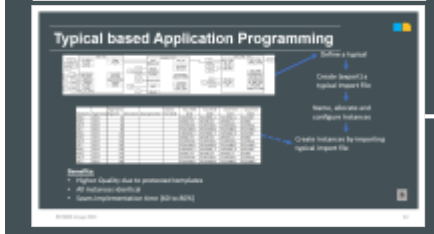
Design Review

Functional Specification
(C&E acc IEC 62881)

Specification*)
(Test Program)

*) to be done/reviewed by owners Representative





Software Specification
(Acc. T2 as per 61508-3)

Implementation
(SST Program)

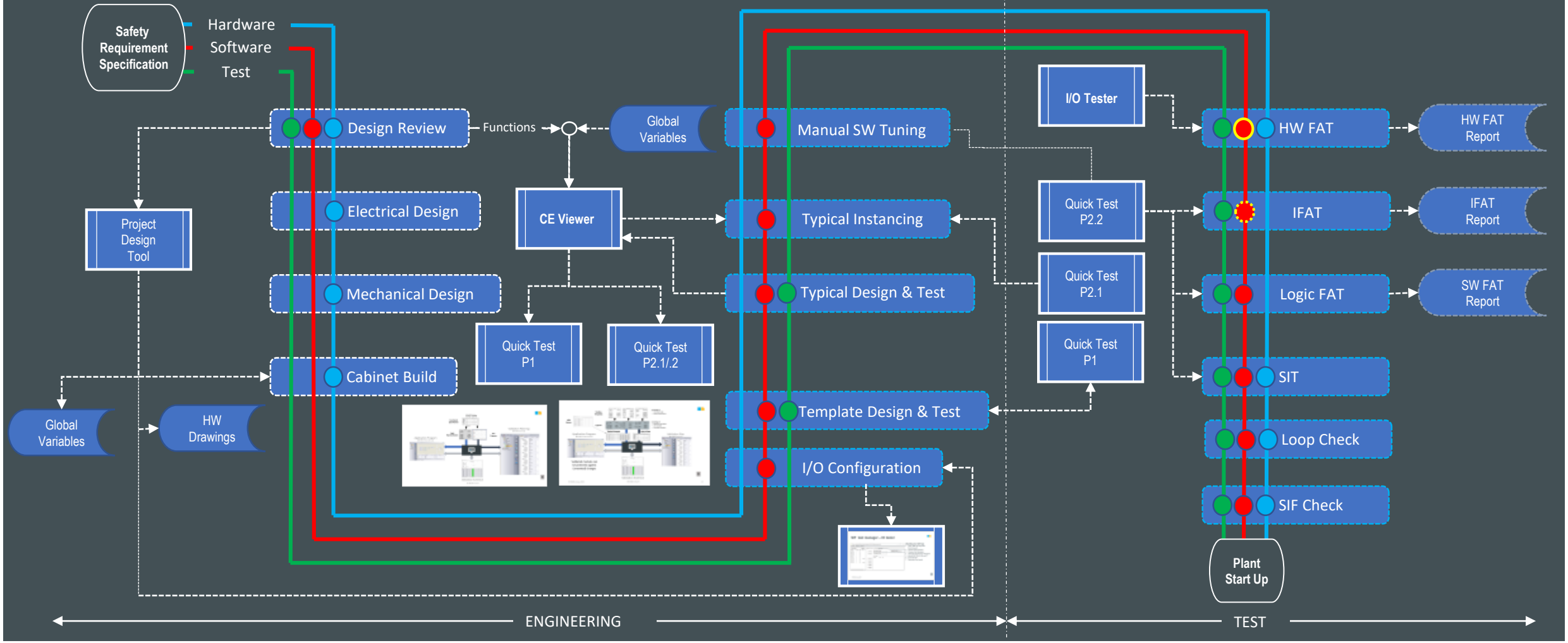
Test
(Application)

Test Protocol
(entire Application)

Engineering Guidelines

Implementation
(Acc. T3 as per 61508-3)

Digitalized Programming & Test



Smart Application Programming & Testing

Define Typicals

- Structure SRS Functions
- Use pre-tested Toolbox

Instance Typicals

- Define Instances (count; I/O)

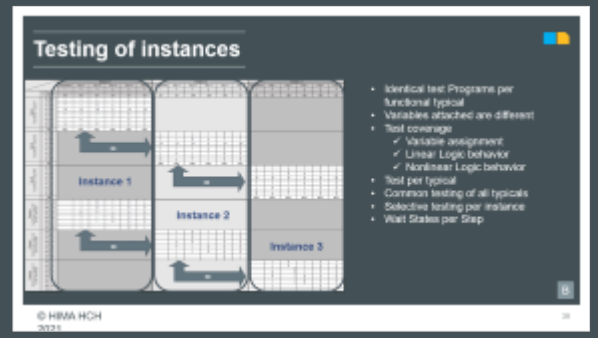
Test Application

- Create & Run Test

Full IEC 61511 compliance

Saving 75 to 85 execution Time

Example:
200 X 200 I/O
53K lines Test Program (8s)
50 K test cases to execute (1.5 h)



Zusammenfassung

Bei der Implementierung von Lösungen der funktionalen Sicherheit

- Braucht die Anwendungsprogrammierung besondere Aufmerksamkeit
- Es muss eine Scherheitsarchitektur verwendet warden, welche Fehler aufdecken kann
- Automatisches Testen ist auf Anwendungsniveau durchaus anwendbar

Thank You.

HIMA Paul Hildebrandt GmbH

Albert-Bassermann-Str. 28
68782 Brühl, Germany

Phone: +49 (0) 6202 / 709-0
Fax: +49 (0) 6202 / 709-107

Email: info@hima.com
Website: www.hima.com

Tag 2: Fragen und Antworten

PEPPERL+FUCHS

Your automation, our passion.

SIL-Sprechstunde 2021

Mitschrift der Fragen und Antworten

Frage 1: Laut 61508 ist es möglich, ein einzelnes Gerät in SIL3 zu verwenden, wenn auch die SC entsprechend SC3 ist. Wie sieht das die 61511 vor? Kann der Nachweis über die SC ausreichend sein? Sollte somit in der Bewertung dokumentiert werden? Konkretes Beispiel: KCD2-SCD-Ex1.ES

Die IEC 61508 fordert für SIL3 normalerweise eine HFT1. Für Typ A – Elemente ist unter bestimmten Bedingungen nach Teil 2 Kap. 7.4.4.3 eine HFT0 gestattet. Die IEC 61511 bestätigt dies in Teil 1 Kap. 11.4.

Bei der Sprechstunde anwesende Industrievertreter gaben an, dass die meisten Firmen der Prozessindustrie Redundanz für SIL3 nutzen. Daher sollte unbedingt eine SC3 angegeben sein. Es gab zwar auch den Hinweis auf eine Einzelfallbetrachtung, dies wäre aber sehr Prozess abhängig. Dann könne man mit nur einem Gerät mit SIL3 und einer SC3 einen SIL3 erreichen.

Beide Aussagen deckten sich auch mit einem Erfahrungsbericht einer Anlagenplanerin. Ihre Firma habe zwar auch schon einen SIL3 mit nur einem Gerät realisiert, habe dabei aber eine sehr enge Absprache mit dem TÜV gepflegt und es sei auch nur realisiert worden, weil die sehr engen Platzverhältnisse 2 Geräte nicht zugelassen haben.
Dazu kam von einem anderen Teilnehmer der Hinweis, dass eine lange Diskussion mit dem TÜV und ein aufwändiges Dokumentieren der Begründung (wieso nur ein Gerät verwendet wird) nicht unbedingt eine „Ersparnis“ (finanzieller Art) erbringen würde.

Frage 2: Wie kritisch ist es, die Sicherheitsbudgets von Sensor, Logik und Aktor zu ignorieren? Es könnte immer wieder Anwendungen geben, wo es ein komplettes Übergewicht in eines der Bereiche gibt.

Sicherheitsbudgets in der PFD-Berechnung wurden in der veralteten NE106 angegeben. Dort unter Kapitel 6.4 stand: „die typischen PFD-Anteile für die einzelnen Teilsysteme müssen allerdings beachtet werden - für das Sensorsystem ca. 35 % der PFD, für das Aktorsystem ca. 50 % der PFD."

Es gab aber den Hinweis, dass die NE106 überarbeitet wurde, und nun NA106 lautet. In dieser neuen Fassung sei diese Angabe auf PFD-Anteile entfallen.

Daher gab es in der anschließenden Diskussion Stimmen aus der Industrie, für die eine Verteilung, oder Aufteilung des PFD-Wertes keine Rolle spielt, da dies ja auch kein Bestandteil in einer Norm sei.
Es gab aber auch Teilnehmer, die angaben, dass bei Ihnen versucht würde eine solche Gewichtung einzuhalten (auch ohne Rechnung) um einzelnen Komponenten kein übermäßiges Gewicht in der Sicherheitsfunktion zu geben. Dies hätte sogar Einfluss auf die Geräteauswahl. Für Gerätehersteller ist es wichtig, ein realistisches Budget für die Erstellung eines Sicherheitskreises angeben zu können.

Einigkeit bestand nur darin, dass auch aus Erfahrungsberichten heraus bei der Abnahme vom TÜV eine solche Verteilung keine Rolle spielen würde. Da würde nur das Gesamtbudget nach Norm geprüft.

Quintessenz: je nach Anwendung agieren und den Sachverstand nutzen. Nicht stur nach Vorgaben oder Mustern bewerten.

Frage 3: Was wird getan (Instandhaltungsmaßnahmen, Dokumentation, Betriebsbewährtheit), um die Geräte nach End of Life weiter betreiben zu können?

Eigentlich ist der Begriff „End of Life“ mit dem Ausmustern der Komponente (verschrotten) verbunden – damit wäre die Frage nicht sinnvoll. Es könnten das Ende der Gebrauchsdauer oder die Angabe im Handbuch gemeint sein. Auf Rückfrage wurde die Angabe im Handbuch (z.B. 8-12 Jahre) diskutiert.

Die Betreiber fordern eine „Öffnungsklausel“ um eigene Stördatenerfassung zu erlauben - in Firmen in denen mehrere Hundert oder gar Tausend gleiche Komponenten im Einsatz sind können Ausfallgrenzen gut beobachtet, ermittelt und bestimmt werden. Daher würden in solchen Firmen die Geräte wesentlich länger eingesetzt. Manchmal wird die Angabe „8-12 Jahre“ schon als „Öffnungsklausel“ angesehen wenn der Hersteller nicht explizit eine Entsorgung nach dem Zeitraum vorschreibt. Komponenten mit solchen Vorgaben würden sonst nicht eingesetzt (gekauft) werden. **Der Nachweis und die Begründung sind dann natürlich selbst zu führen.** Auch die Proof Tests sind dann näher zu betrachten. **Sinnvoll erscheinen dann kürzere Prüfintervalle.** Hier kommt es aber wieder auf die Einzelfallbetrachtungen an.

Fragestellungen:

- Handelt es sich um einen Sensor oder Aktor?
- **Wird die Komponente in einem redundanten System verwendet oder nicht?**
- Macht der Hersteller eine Aussage was das begrenzende Element ist und ob das speziell geprüft werden kann?

Ein Teilnehmer vertrat die Meinung, dass auch ein Austausch als neue Fehlerquelle gelten kann – auch weil nach Jahren kein identisches Ersatzgerät zu bekommen ist.
Bei einer SSPS (als sehr komplexe Komponente) kann eine solche Prüfung allerdings nicht erbracht werden - daher sehen deren Hersteller die Angabe der Nutzungsdauer als verbindlich an.

Fazit: Bei einer Nutzung über die vom Hersteller angegebene Nutzungsdauer, geht die Verantwortung an den Betreiber über. Die Proof Tests (Intervalle) sind für eine solche Nutzung zu überdenken. Wo möglich können diese Komponenten noch in Nicht-Sicherheits-Anwendungen eingesetzt werden.

Die aktuelle DIN EN 61508-2 beschreibt Möglichkeiten in einer Fußnote, die NA106 gibt konkretere Hinweise.

Frage 4: Ist eine (vollständige) Abnahme eines Schutzkreises durch einen Sachverständigen erforderlich, wenn Komponenten im Kreis nicht 1:1 ausgetauscht wurden? Beziehungsweise welchen Maßnahmen werden in solch einem Fall ergriffen?

Grundsatzfrage: was ist überhaupt ein 1:1 Austausch? Reicht die HW, oder muss auch die SW identisch sein? Genügt es schon wenn die Ex-Kenndaten identisch sind?
Hierzu wurde auf die TRBS1115 Kapitel 8.3.3 verwiesen: *„Falls der Austausch von Bauteilen zu einer Änderung der sicherheitsrelevanten Eigenschaften der sicherheitsrelevanten MSR-Einrichtung führt, ist eine Überprüfung der Wirksamkeit der Schutzmaßnahmen der sicherheitsrelevanten MSR-Einrichtung notwendig.“*
In Kapitel 8.3.2 ist beschrieben, wann es sich um eine prüfpflichtige Änderung handelt.

Es wurde auch darüber diskutiert, ob es eine ZÜS (Zugelassene Überwachungs-Stelle) sein muss. Allerdings sei dieser Begriff nicht geschützt. In der TRBS seien aber auch Kriterien für Prüfer beschrieben.

In der Diskussion wurde darauf hingewiesen, dass die kritischen Punkte übereinstimmen müssen. (Einzelfallbetrachtung). Um eine Beeinträchtigung der Sicherheitseinrichtung auszuschließen, wäre eine neue Betrachtung mit unabhängigem Dritten (Sachverständiger) erforderlich.

Des Weiteren wurde auf die NE126 (bezüglich Bestandsschutz) hingewiesen. Bei Überarbeitung entfällt aber der Bestandsschutz. Man müsse immer darüber nachdenken, bewerten und dokumentieren, ob die Sicherheit beeinträchtigt ist und ggf. Maßnahmen ergreifen. Sich auf Bestandsschutz zu berufen sei der falsche Weg.

Frage 5: Was sollen Prüfanweisungen für die Erst- und Wiederholungsprüfung enthalten bzw. gibt es Beispiele dafür wie diese aufgebaut sind?

Ein Anwender gab folgend „Schlagworte als Beispiel: – Sichtprüfung außen, Sichtprüfung Anschlüsse, „wedded parts“. Genauigkeit, Settings, Delay, Fehlergrenzen, - stimmen diese mit dem PLS überein; Prozessarbeitsschritte. Er verwies auch darauf, dass Reparaturen zu protokollieren seien.
Die „useful lifetime“ wird innerhalb des Maintenance Management separat geregelt.

Eine Teilnehmerin verwies auf die Handbücher. Dort sind mittlerweile gute Vorgaben gegeben.

Ein weiterer verwies auf die VDI 2180 Blatt 2 und NA106.

Frage 6: Welche Qualifikation wird bei den Prüfern bei Erst- und Wiederholungprüfungen gefordert?

Der Referent einer Prüfstelle verwies darauf, dass dies jeder Betreiber selbst entscheiden müsse. **Oft werden 3 Jahre für Stufe 1 mit externer Prüfung, dann weitere Qualifikationen für die Stufe 2, bis zur Stufe 3 (z.B. Mitarbeit im Normengremium) genutzt.**
Dies gelte auch für externe Dienstleister. Diese müssten sich auch Gedanken über die Qualifikation ihrer Mitarbeiter machen. Der Auftraggeber sollte diese Nachweise der Qualifikation prüfen (verlangen).

Ein weiterer Teilnehmer aus der Industrie meinte dazu: „Ausbildung, Erfahrung, Training ist die übliche Reihenfolge. Im Arbeitsprozess stellt sich die Frage: „Was mache ich wenn ein Fehler auftritt und was muss im Prozess beachtet werden.“ Auch verschiedene Regelwerke (TRBSen) geben das vor.

Frage 7: Müssen nach einem Austausch einer SPS E/A Karte (Karte wird gesteckt, Verkabelung ist nicht betroffen) die entsprechenden Signalkreise wieder geprüft werden? Falls ja, in welchem Umfang?

Bei HIMA muss das nicht geprüft werden. Laut Anwender wurde im speziellen Fall eine HIMax – XDO Karte getauscht aber es gab Diskussionen ob und in welchem Umfang nun geprüft werden muss.
Der Referent antwortete, dass bei der HIMax keine Verwechslungsgefahr bestünde, und daher keine Prüfung durchgeführt werden muss.

Ein Referent gab zu bedenken, dass es bei speziellen 19“ Karten leider aus Ex-Gründen eine andere Steckleistenbelegung gab. Daher hatte die Nachfolgekarte eine andere Funktion und es musste daher getestet werden. Daher hängt es wohl auch vom Einzelfall ab.

Frage 8: SIL-Berechnung: Armatur nicht bekannt – Reicht das Rechnen bis zum Magnetventil aus? Da Aktorik (Armatur) Mechanik?

Ein Referent aus der Industrie verwies auf die VDE 2180 - Blatt 4 – bei Mechanik würde mit typischen Werten (100 FIT) gerechnet.

Prüfstellen richten sich auch nach der VDE 2180 und schauen nach der Applikation, systematische Eignung muss stimmen (z. B. geeignete Materialbeständigkeit der Armatur und Dichtungen, Auslegung des Antriebs, etc.). Rechnen sei nicht so relevant.

Die Anlagenplanerin gab zu bedenken, dass bei einer unbekannten Armatur Eignung nicht bekannt wäre weil auch nicht geprüft. Fraglich, wie dann systematische Fehler ausschließbar sind. Es sollte doch Prüfanweisungen und / oder Nachweise geben um auf Eignung rückzuschließen.

Es wurde auch auf die Unterscheidung zwischen berechnen und betrachten hingewiesen. Ein SIL-Nachweis ist nicht nur die Berechnung. Man könne auch bis zum Ventil rechnen, muss aber die Betrachtung für den kompletten „Zweig“ (Pfad) durchführen.

Frage 9: Ist es von Nöten beim Tausch (anderer Hersteller) einer sicherheitsgerichteten Steuerung eine Neubetrachtung vorzunehmen? Software, Sensorik, Aktorik und Sicherheitsfunktionen bleiben dabei unberührt. Handelt es sich um eine wesentliche Veränderung? Allgemein: Wann kann ich von Bestandsschutz ausgehen? Welche Voraussetzungen müssen erfüllt sein? Die Fragen beziehen sich in Hinsicht auf die Funktionale Sicherheit und die Maschinenrichtlinie.

Ein Hersteller meinte dazu, dass es dafür auch in der MRL (Maschinenrichtlinie) Papiere gäbe. Bei einer Modernisierung ohne wesentliche Änderung (wie definiert) sei keine Neubetrachtung not wendig.

Auch von Betreibern kam die Einschätzung, dass eine Neubetrachtung des Risikos oder der gleichen Technik, bei Modernisierung nicht nötig / zwingend sei aber ausgiebige Tests erfolgen sollten.

Der Fragesteller wollte weiterhin wissen, ob er validieren und verifizieren muss, oder was getan werden müsse. Aus der Industrie wurde auf die NE 126 Anhang 4 verwiesen - verifizieren auf jeden Fall. Validierung nicht wenn wie hier beschrieben alles gleich bleibt. Vorsicht ist aber bei Bewertung von Relais durch einen SPS-Eingang geboten - dann sei die SPS schneller und reagiere auch auf EMV oder Schalterprellen. Es gebe einen fließenden Übergang in der Norm zwischen V&V. Daher sei dies auch eher eine Grauzone.

Ein Teilnehmer gab an, dass bei Änderung an einer alten Anlage auch die Sicherheitsbetrachtung neu durchgeführt werden muss - da gibt es keinen Bestandsschutz. Das gibt auch die BetrSichV so vor. Wenn keine wesentliche Änderung vorgenommen wird, dann kann auch nur eine Teilbetrachtung erfolgen. Aber bei einer wesentlichen Änderung gebe es keine Ausrede. Dann muss alles neu betrachtet werden, nach allen Regeln.

TRBS verlangt immer einen risikobasierten Ansatz. Daher muss immer eine Risikobewertung durchgeführt werden.

Frage 10: Ist bei einer schadensbegrenzenden Maßnahme, wie bei einer schadenverhindernden Maßnahme ebenfalls ein rechnerischer Nachweis der Ausfallwahrscheinlichkeit (SIL-Berechnung) vorzuweisen?

Ein Referent antwortete: „Wenn man bei der Risikobetrachtung Kredit daraus zieht ja, sonst nicht.“ Dies ist wie so oft von einer Einzelbetrachtung abhängig.

Frage 11: Welche Funktionen müssen in der Firmware eines Feldgerätes implementiert sein, um SIL2 Zertifizierung zu erreichen? Wie hoch ist der Entwicklungsaufwand für die Software, wenn von NULL gestartet wird? Wie komme ich zu weiteren Unterlagen/Spezifikation, in denen zu implementierende Funktionen beschrieben werden?

HIMA gibt für 1 Stunde Änderung ca. 10 Stunden Prüfung als Richtwert. Der Unterschied in der SW für SIL2 und SIL3 sei nicht sehr hoch. Eine generische Antwort ist schwierig, hängt von Faktoren wie der Risikoanalyse, Aufbau, erforderliche Komponenten und Maßnahmen, common cause und Diagnose ab. Der größte Aufwand ist die Dokumentation.

Andere Teilnehmer gaben an, dass der Mehraufwand vermutlich mit einem Faktor zwischen 3-5 beziffert werden kann.

Frage 12: Häufig wird in Multi Purpose-Anlagen eine Abhängigkeit einer Sicherheitsfunktion von einer Betriebsart oder einer Wegstellung/Wegwahl gewünscht. Wie kann ich damit umgehen? Ist es zulässig z.B. eine Stellungsrückmeldung einer Armatur als "Freigabe" einer Sicherheitsfunktion zu verwenden? Wenn ja, wie muss ich diese Abhängigkeit im Nachweis darstellen/berechnen?

Ein Teilnehmer meinte dazu, dass die Pumpensteuerung nicht sicherheitsrelevant sein müsse. Nur die Armatur da diese das sicherstellende Element ist.

Prüfstellen sehen kritisch dass z.B. die Pumpe nicht mehr Drehmoment hat als die Armatur verkraften kann. Dann könne auch das Schaltsignal von der tatsächlichen Stellung abweichen. Da sie die Sicherheitsfunktion beeinträchtigen kann muss die Überwachung in die Betrachtung / Berechnung mit berücksichtigt werden.

Frage 13: NAMUR Papier - Gerätegebrauchsdauer – Umgang mit Herstellerangaben: Die Betrachtungen im genannten NAMUR Dokument beziehen sich auf „PLT-Geräte“. Sind darin auch die fehlersicheren Steuerungen inklusive der IO-Module eingeschlossen? Können aus Sicht des NAMUR AK die ursprünglich von den Herstellern ermittelten PFD-Werte und die damit verbundenen SIL-Berechnungen auf Basis dieser Betrachtungen auch jenseits der zugrundeliegenden Gebrauchsdauer / Mission Time als weiterhin gültig angesehen werden, insbesondere wenn keine Proof-Tests vorgesehen bzw. möglich sind?

Ein Referent gab dazu an, dass es ab und an den Fall gäbe, dass der Betreiber keinen Proof Test machen möchte. Doch wie kann man dann sicherstellen, dass ein Ventil nach der Lebensdauer noch das tut was es soll. Es müsse auch bei einem Austausch das Gerät noch einmal geprüft werden, um nachzuweisen, dass das Gerät bei Ende der Gebrauchsdauer noch die Funktion erfüllt hätte. Dies trage entscheidend zur Ermittlung einer realen Gebrauchsdauer bei.

Ein Hersteller gab an, dass niemand gezwungen würde das Gerät nach 20 Jahren zu tauschen, aber ein Nachweis, dass man sich als Betreiber noch im Rahmen der geforderten PFD befindet (Ausfallrate) wäre erforderlich.
Der Kunde muss mehrere dieser Geräte in Betrieb haben um die Ausfallrate auch bestimmen zu können. Dazu gehöre auch die Betrachtung von gleichen Geräten, die nicht in sicherheitsgerichteten Anwendungen genutzt werden. Wenn die Ausfallrate ansteigt, egal ob in sicherheitsgerichteten Anwendungen oder nicht stellt das einen Hinweis auf die Notwendigkeit eines Austauschs dar.
Es kam noch der Hinweis, dass nur der Hersteller einen Proof Test angeben könne.

Eine weitere Anmerkung verwies darauf, dass das Gerät unendlich betrieben werden könnte wenn im Prozess alle gefährlichen Fehler aufdeckbar sind - alle gefährlichen Fehler können aber meist nicht aufgedeckt werden.
Es ist eigentlich davon auszugehen, dass z.B. ein Sensor eine Stunde nach proof Test immer noch funktioniert - wenn das Ende der theoretischen Lebensdauer schon überschritten sei wäre das aber nicht immer gegeben.

Fazit: Der Betreiber übernimmt bei Abweichung von Herstellerangaben die Verantwortung – er muss sich sicher sein.

Frage 14: Herr Laible hat in seinem Vortrag erwähnt, dass bei Sicherheitsfunktionen eine "Fail Safe"-Verhalten gefordert wird. Woher kommt diese Forderung (Quelle) und gibt es eine Definition, was "Fail Safe" bedeutet?

Laible: Im Rahmen von KI (Article 15 of proposal for a regulation of the eu parliament and of the council) für “high risk” Systeme ist fail safe gefordert.

Ein anderer Referent gab zu bedenken, dass die 61508 das Gegenteil aussage.

Frage 15: Dokumentation – SSPS Firmware update Dokumentation: Welche Arten von Änderungen an den Steuerungssystemen erfordern ein MOC (Management of Change)?

Prüfstellen verweisen auf die Vorgaben des Herstellers. Wenn sich die Signatur ändert müsse das dokumentiert werden. Bei HW-Änderungen erst recht.

Der Referent von HIMA meinte, man könne die Firmware von der Applikation trennen. Wenn es Änderungen am CRC gibt dann muss das in der MOC beschrieben werden. Bei Firmware Änderungen (z.B. im Modul) ist das Zertifikat maßgebend. In TÜV-Revisionslisten sind die Ausgabestände gelistet. Wenn das Upgrade dem Zertifikat entspricht, dann muss keine MOC Dokumentation erfolgen.
Wenn Funktionsänderungen (der Firmware) eine CRC Änderung der Applikation ergeben, und das vom TÜV Dokumentiert ist (vom Hersteller), dann muss auch kein MOC erfolgen.

Ein Referent aus der Industrie hielt entgegen, dass nicht jeder Hersteller so sei. Ein Hersteller hatte ihm einmal angeboten den Aufbau im Werk selbst zu prüfen was der Anwender gar nicht kann.

Frage 16: Wie werden BPCS Funktionen betrachtet? Diese sind zwar nicht SIL, aber zumindest die vorgeschaltete Maßnahme, um in den low demand mode zu kommen. Wie oft und in welche Tiefe sollten diese geprüft werden?

Der Referent der Firma HIMA antwortete darauf, dass eine BPCS (BPCS=Basic Process Controll System (also die “normale” Prozessleittechnik)) keine probabilistischen Werte hätte, und man daher nicht rechnen könne. In der EN 61511 Teil 2 soll das aber ausführlicher erklärt sein.

Von Betreiberseite kam der Hinweis auf die NE165. Ein Teilnehmer meinte, dass sich diese Regelwerke unterscheiden (Widersprüchlich seien). Eine Erklärung dazu von Dr. Hildebrandt:

Die IEC 61511 und die VDI/VDE 2180 unterscheiden sich an dieser Stelle. Der Grund dafür ist folgender:

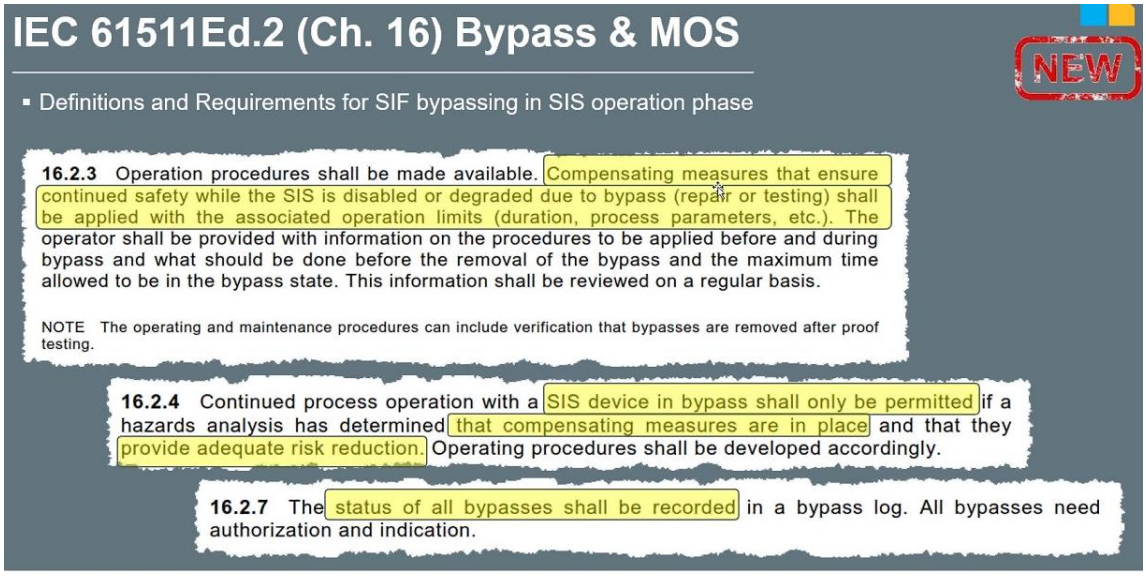
Wenn die Amerikaner (also IEC 61511) von BPCS sprechen, dann haben sie ein System vor Augen, das typischerweise aus mehreren unabhängigen Teilsystemen besteht. Wenn die Anlage ausfällt und nicht mehr so läuft wie es sein soll, dann ist nach deren Sicht nicht das gesamte BPCS ausgefallen, sondern nur ein bestimmter Teil davon. Andere Teile des BPCS laufen noch und daher können diese (noch funktionierenden Teile) eine Sicherheitsfunktion übernehmen. Also kann man mit dem BPCS ohne „Klimmzüge“ risikomindernde Funktionen realisieren.

In Deutschland versteht man das BPCS eher als eine homogene Einheit. Wenn das BPCS nicht mehr wie vorgesehen funktioniert, dann unterstellt man, dass auch eine Sicherheitsfunktion, die mit diesem (kaputten) BPCS realisiert wurde, evtl. nicht mehr funktioniert. Daher fordert die VDI/VDE2180, dass man mit besonderen Maßnahmen die „BPCS-Sicherheitsfunktionen“ so realisiert, dass dies nicht geschehen kann.

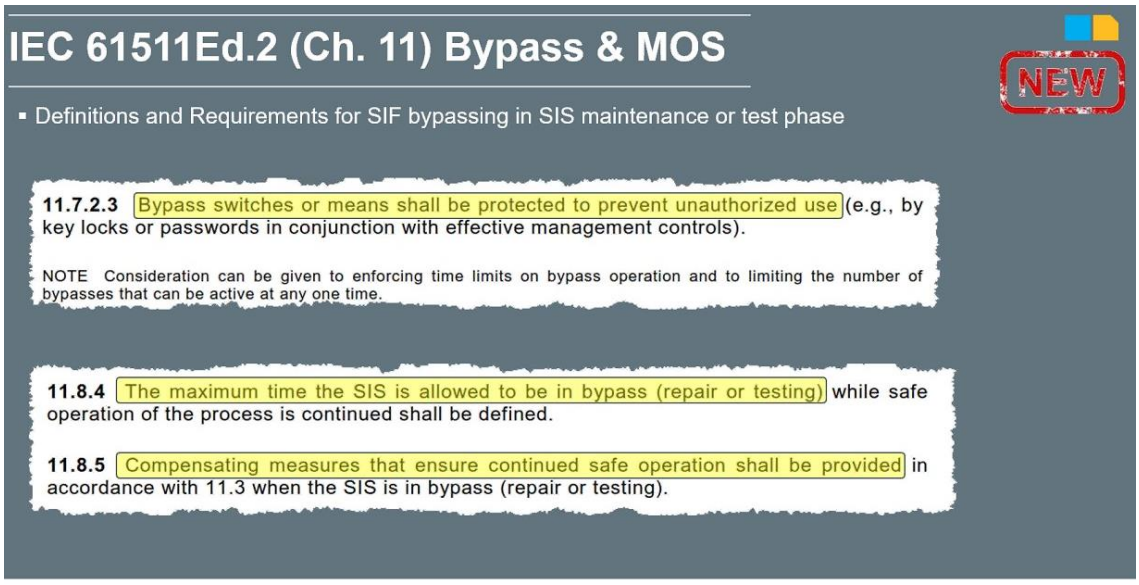
Diese Diskussion wird schon sehr lange und leidenschaftlich geführt.

Frage 17: Gibt es normative Anforderungen oder betriebliche Leitfäden, z.B. NAMUR-Empfehlungen, zur Realisierung von Bedienfunktionen, die im laufenden Betrieb des SIS durch einen Operator durchgeführt werden können. Z.B. • Quittierung von Gerätefehlern und anschließende Wiedereingliederung in die SIF • Ändern von Grenzwerten im Rahmen von vorher fest definierten Bereichen • Überbrückungen von Signalen zur vorbeugenden Instandhaltung von Geräten

In der 61511-1 Kap. 16 werden „compensating measures“ gefordert.



Kompensierende Maßnahmen sind erforderlich.



Die Anlagenplanerin berichtete, dass nur sie als Dienstleister das Passwort wenn sie bei sehr kleinen Firmen die SPSS programmieren. Als weiterer Hinweis kam ein Verweis auf die VDE 2180 Blatt 2 für eine genauere Erklärung – oder die NE154 für Batchbetrieb).

Von Betreibern kam der Verweis auf die NE154. Typischer Fehler bei Änderung von Schaltpunkten ist die Befragung des Instrumentierers – der kenne die Anlage am besten.

Ein weiterer Teilnehmer gab an, dass das HAZOP Team darüber spreche und es würde abgestimmt.

Ein Schlüssel-Schalter ist normativ nicht vorgegeben, sei aber vorzusehen aus gesundem Menschenverstand.

SIL Sprechstunde 2021 Vorbereitung

C. Demski

1

Laut 61508 ist es möglich, ein einzelnes Gerät in SIL3 zu verwenden, wenn auch die SC entsprechend SC3 ist. Wie sieht das die 61511 vor? Kann der Nachweis über die SC ausreichend sein? Sollte somit in der Bewertung dokumentiert werden?
Konkretes Beispiel: KCD2-SCD-Ex1.ES

- Wir verwenden kein einzelnes Gerät für SIL 3.
- Die Tabelle der IEC 61511 fordert bei SIL 3 Redundanz. Anders als die Tabelle der 61508 spielt hier auch keine SFF eine Rolle.
- Die Säule der HFT muss unabhängig von der PFD erfüllt sein. (siehe nächste Seite)
- In der 61511 wird trotzdem davon gesprochen, dass die HFT reduziert werden kann s. 11.4.6 ich habe davon noch nie gebrauch gemacht.

Table 6 – Minimum HFT requirements according to SIL

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

11.4.6 For a SIS or SIS subsystem that does not use FVL or LVL programmable devices and if the minimum HFT as specified in Table 6, would result in additional failures and lead to decreased overall process safety, then the HFT may be reduced. This shall be justified and documented. The justification shall provide evidence that the proposed architecture is suitable for its intended purpose and meets the safety integrity requirements.

1 Grundlagen der funktionalen Sicherheit

Dokumentation

HFT
(Hardware fault tolerance)

Wie groß muss die Redundanz sein, um gegen den Ausfall einer Komponente resistent zu sein?

Systematic Failure

Wie groß ist das Risiko für systematische Fehler sowohl beim Hersteller [SC (Systematic Capability) - Wert im Zertifikat] als auch beim Anlagenbauer und auch beim Betreiber?

PFD (Probability of failure on demand)
PFH (Probability of failure per hour)

Wie groß ist die mittlere Wahrscheinlichkeit, dass eine Sicherheitseinrichtung im Bedarfsfall nicht funktioniert?

Prüfungen

Wie häufig muss von einem Prüfer mit welcher Qualifikation in welcher Tiefe gegen welche Bedingungen geprüft werden?

Fit for purpose/ fit for application:

Genaues Engineering für den speziellen Fall

2

Wie kritisch ist es, die Sicherheitsbudgets von Sensor, Logik und Aktor zu ignorieren? Es könnte immer wieder Anwendungen geben, wo es ein komplettes Übergewicht in eines der Bereiche gibt.

- Es gibt immer wieder solche Fälle… Kuriositäten sind dann…
  - 2oo3 Sensoren mit Prüfintervall 6 Monate eine SIL 3 SSPS, und 2oo2 Ventile mit Prüfintervall von 6 Jahren da man dort nicht rankommt.
    - Budget: 1% SE; 1%LS; 98% FE
  - Bei uns muss man sich das Überschreiten von einem FE budget von 70% noch mal jemanden fragen.

  - Aber so lange es sicherheitstechnisch kein systematisches Problem darstellt und keine Erfahrung dagegenspricht… warum nicht.

3

Was wird getan (Instandhaltungsmaßnahmen, Dokumentation, Betriebsbewährtheit), um die Geräte nach End of Life weiter betreiben zu können?

- Sensor: Ensure diagnostic:
  - Deviation alarm
  - IFDS programmed
  - Regular visual inspections between Proof test
  - Regular proof test (anyhow)
- Final Element: Overhaul on fixed intervalls

4

Ist eine (vollständige) Abnahme eines Schutzkreise durch einen Sachverständigen erforderlich, wenn Komponenten im Kreis nicht 1:1 ausgetauscht wurden? Beziehungsweise welchen Maßnahmen werden in solch einem Fall ergriffen?

- Was ist ein 1:1 Austausch? (NE 53; 126 Bsp. 2)
  - Hardware
  - Technology
  - Ex Schutzt
  - Software version
- Gerät
  - Betriebsbewährt
- Selektion:
  - Kann die Abschaltung wirklich erfüllen
  - Technology ist OK
- Installation
  - Kann so installiert werden, Installation muss verändert werden
- Einstellungen
  - Welche Einstellungen muss ich ändern?
  - Auf welche Einstellungen muss ich achten
  - Hat das Auswirkungen auf das Anwenderprogramm

Beispiel 2

- Instandsetzung: Ein Feldgerät wird 1:1 durch ein gleiches Feldgerät (Gerätetyp) ersetzt

Maßnahme:
Dokumentation des Austauschs (z. B. Vermerk auf dem Prüfblatt).

Beispiel 3

- Ein Feldgerät wird durch ein anderes Feldgerät (welches für Einsatz in PLT-Schutzeinrichtungen zugelassen ist) ersetzt, gleiche sicherheitstechnische Aufgaben-stellung und Funktion (z. B. bei Betrieb oder Instandhaltung des Feldgerätes haben sich systematische sicherheitstechnische Probleme oder Probleme bei der Instandhaltung ergeben).

Maßnahme:
Anlagenänderungsblatt erstellen, sicherheits-technische Betrachtung der Eignung des Feldgerätes für den Einsatzfall wie bei einer Neuplanung. Dokumentation des Austausches (z. B. Vermerk auf dem Prüfblatt).

5

Was sollen Prüfanweisungen für die Erst- und Wiederholungsprüfung enthalten bzw. gibt es Beispiele dafür wie diese aufgebaut sind?

- Welche Fehler wollen wir damit aufdecken?
  - Fehler, die mit Diagnostic nicht aufgedeckt werden müssen (Reaktive Fehler)
- Wollen wir nur sehen das das Gerät funktioniert oder auch, dass es wahrscheinlich bis zur nächsten Prüfung funktioniert
  - Wettet parts
  - Internals
  - Dichtigkeit 45% von der minimal erforderlichen Dichtigkeit

5

Was sollen Prüfanweisungen für die Erst- und Wiederholungsprüfung enthalten bzw. gibt es Beispiele dafür wie diese aufgebaut sind? 2

Tag Number		Work Order	
Transmitter model number:		Control system ID	
Transmitter serial number:			
Serial number(s) calibration device(s):			
Remote Seal model no.: (if applicable):			

If small activities are performed to achieve good condition, the quick fix field and comments have to be filled out.

☐ **Visual Inspection**

	N/A	Yes	No	Quick Fix
Labels for instrument, cable, SIS and accessories are well fastened and can be read clearly?		☐	☐	☐
No obvious process leaks visible?		☐	☐	☐
Instrument free from corrosion or other damage?		☐	☐	☐
No vibration that would cause damage or affect instrument performance?		☐	☐	☐
Instrument mounting stand, brackets and other mountings parts are in good condition and all bolts are in place and not loose?		☐	☐	☐
All unused openings are plugged or caped?		☐	☐	☐
Electrical conduit and/or cable installation are in good condition? Conduit drains and/or cable glands OK?		☐	☐	☐
Model number(s), recorded in the CMMS are the same as the installed instrument?		☐	☐	☐
Instrument capillaries, tubing or remote seal in good condition and supported properly?		☐	☐	☐
Insulation is in good condition and complete?	☐	☐	☐	☐
Heat tracing and/or enclosure is in good condition and functional?	☐	☐	☐	☐

Comment to Quick Fix:

☐ **Additional Visual checks during calibration**

	Yes	No	Quick Fix
No moisture inside transmitter, and O-ring in good condition?	☐	☐	☐
Process taps and remote seals OK? No plugging or build up?	☐	☐	☐
No Seal damages? No Material effects from corrosion, degeneration or temperature?	☐	☐	☐
No Plugging, build up or restrictions?	☐	☐	☐
Electrical connections and insulation on wiring and in good condition?	☐	☐	☐

Note any items found that need repair:

Example of Dow

☐ **Calibration / Performance Test**

	Target / Spec Data Points		0%	50%	SIS Alarm point or 100%	50%	0%
		[unit]					
Check of the transmitter performance	Actual Points set	[unit]					
	Actual point should have this output signal	mA					
	As found data	mA					
	Allowed error in mA to pass	mA					
	As left results (if any changes made)						
	Pass or Fail for transmitter	P or F					

☐ **Calibration test results / protocol of calibrator / manufacturer are attached to this test record sheet (Note: no data needs to filled out in the table)**

	Documented Data (Spec data)	Actual Data Value
Settings	Instrument Range to [unit]	Instrument Range: to [unit]
	Control System Range to [unit]	Control Sys Range: to [unit]
	Instr. Failure expected: High ☐ Low ☐	Failure actual Cont. Sys.: High ☐ Low ☐
	Instr. Failure value expected: mA	Actual in control system: mA
	Instrument Output: Linear ☐ Square root ☐	Actual in Contr. Sys.: Linear ☐ Square root ☐

Loop Simulation - Testing of the Instrument signal incl. barrier (if installed)									
	in %	NFS	0	25	50	75	100	PFS
	in mA		4	8	12	16	20	
	[unit]							
	CS reading [unit]							
	Pass or Fail	Pass ☐				Fail ☐		

Comments and Note any items found that need repair:

Final Evaluation and Signature Section		Yes	No
The Proof Test of the equipment pass without any deficiency?		☐	☐
Instrument is ready to return to operations?		☐	☐
Is any repair needed? Than create a new WO for the repair. Record required repairs.	Repair WO no.:	☐	☐
Is a safety relevant failure detected? Please inform Reliability Engineer and/or the site Instrument DAS.		☐	☐

Date:		Testing Person : **Print name**	
Signature:		Company:	

Welche Qualifikation wird bei den Prüfern bei Erst- und Wiederholungprüfungen gefordert?

- TRBS 1115 (wie alle TRBS):
  - Ausbildung
  - Erfahrung
  - Training (Workprozess)

7

Müssen nach einem Austausch einer SPS E/A Karte (Karte wird gesteckt, Verkabelung ist nicht betroffen) die entsprechenden Signalkreise wieder geprüft werden? Falls ja, in welchem Umfang?

- Siehe 1:1 Austausch.
  - Muss ich die Karte im Programm neu einbinden
  - Muss ich für die Karte Security Communikations Settigs setzen
  - Muss ich für die Karte neue Delay oder andere Timer setzen
  - Muss ich die Kanäle noch einzeln vom Messbereich neu konfigurieren
  - Kann die Karte das Signal auf dem ganzen Bereich lesen? (Loop Check 3.5 bis 22.0 mA)
  - Stecken alle Stecker wirklich richtig?
  - Hat die Karte auch eine Elektronik enthalten… (nicht das wir nicht schon einmal nur ein Gehäuse bekommen hätten…. ☺

SIL-Berechnung: Armatur nicht bekannt – Reicht das Rechnen bis zum Magnetventil aus? Da Aktorik (Armatur) Mechanik?

- Solange man nicht zu 100% vom Budget rechnet…
- 100 fit
- Wenn das Ventil nicht bekannt kurzes Prüfintervall (Betriebsbewährung)

9

Ist es von Nöten beim Tausch (anderer Hersteller) einer sicherheitsgerichteten Steuerung eine Neubetrachtung vorzunehmen? Software, Sensorik, Aktorik und Sicherheitsfunktionen bleiben dabei unberührt. Handelt es sich um eine wesentliche Veränderung? Allgemein: Wann kann ich von Bestandsschutz ausgehen? Welche Voraussetzungen müssen erfüllt sein? Die Fragen beziehen sich in Hinsicht auf die Funktionale Sicherheit und die Maschinenrichtlinie.

- NE 126 sinngemäß:

Beispiel 4

- Eine VPS wird durch eine SSPS ersetzt, Funktionen (Funktionsplan) unverändert. (Grund: z. B. keine Ersatzteile mehr erhältlich, Modernisierung)

Maßnahme:
Anlagenänderungsblatt erstellen, Festlegungen für die Funktionsprüfung überarbeiten; Prüfblatt anpassen. Bei vorhandener SIL 3-Zulassung der SSPS entsprechend der Rahmenbedingungen der VDI/VDE 2180 keine SIL-Einstufung der Schutzfunktionen erforderlich, da Anforderungen aller Schutzfunktionen abgedeckt sind (Schutzfunktionen mit SIL 4 in VDI/VDE 2180 ausgeschlossen). Bei Zulassung der Steuerung nur für SIL 2 muss die SIL-Einstufung der Schutzfunktionen überprüft werden.
Entwurfsprüfung und Funktionsprüfung nur der Steuerung, wie bei Neuerrichtung.

10 Ist bei einer Schadensbegrenzender Maßnahme, wie bei einer Schadenverhindernden Maßnahme ebenfalls ein rechnerischer Nachweis der Ausfallwahrscheinlichkeit (SIL-Berechnung) vorzuweisen?

- Grundsätzlich ja,
- Bei Ex (tertiärer Explosionsschutz) gibt es häufig sehr integrierte Systeme, die vom Anwender nicht designed werden.

11

Welche Funktionen müssen in der Firmware eines Feldgerätes implementiert sein, um SIL2 Zertifizierung zu erreichen? Wie hoch ist der Entwicklungsaufwand für die Software, wenn von NULL gestartet wird? Wie komme ich zu weiteren Unterlagen/Spezifikation, in denen zu implementierende Funktionen beschrieben werden?

12

Häufig wird in Multi Purpose-Anlagen eine Abhängigkeit einer Sicherheitsfunktion von einer Betriebsart oder einer Wegstellung/Wegwahl gewünscht. Wie kann ich damit umgehen? Ist es zulässig z.B. eine Stellungsrückmeldung einer Armatur als "Freigabe" einer Sicherheitsfunktion zu verwenden? Wenn ja, wie muss ich diese Abhängigkeit im Nachweis darstellen/berechnen?

- Ich würde zwischen zwei Fällen unterscheiden:
  - Permissive SIF, die eine Freigabe für einen Prozessschritt geben und NE 154 (WIB M-2796-X-15)
  - den Freigaben, die für eine Aktivierung einer Sicherheitsfunktion verwendet werden. Jede Freigabe kann auch eine Sicherheitsfunktion verhindern, also ist es für mich Teil der Architektur (und der PFD)

13

NAMUR Papier - Gerätegebrauchsdauer – Umgang mit Herstellerangaben: Die Betrachtungen im genannten NAMUR Dokument beziehen sich auf „PLT-Geräte“. Sind darin auch die fehlersicheren Steuerungen inkl. der IO-Module eingeschlossen? Können aus Sicht des NAMUR AK die ursprünglich von den Herstellern ermittelten PFD-Werte und die damit verbundenen SIL-Berechnungen auf Basis dieser Betrachtungen auch jenseits der zugrundeliegenden Gebrauchsdauer / Mission Time als weiterhin gültig angesehen werden, insbesondere wenn keine Proof-Tests vorgesehen bzw. möglich sind?

- Bitte einen Punkt beachten. Ein Austausch ersetzt NICHT den Proof test.
  - Wie bestimme ich den „As found“ Zustand?
  - Wie beweise ich, dass die Funktion noch funktioniert hätte.