Tag 1:
Fachvorträge

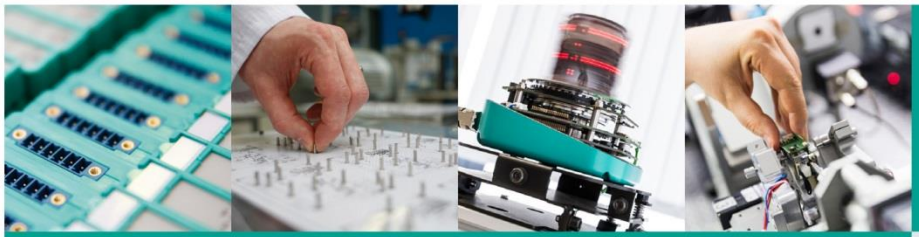
Motto 2025:
Außergewöhnliche
Praxisbeispiele

SIL Sprechstunde

PEPPERL+FUCHS



Kurt im Pech - oder warum sich ISA und NAMUR nicht einig werden



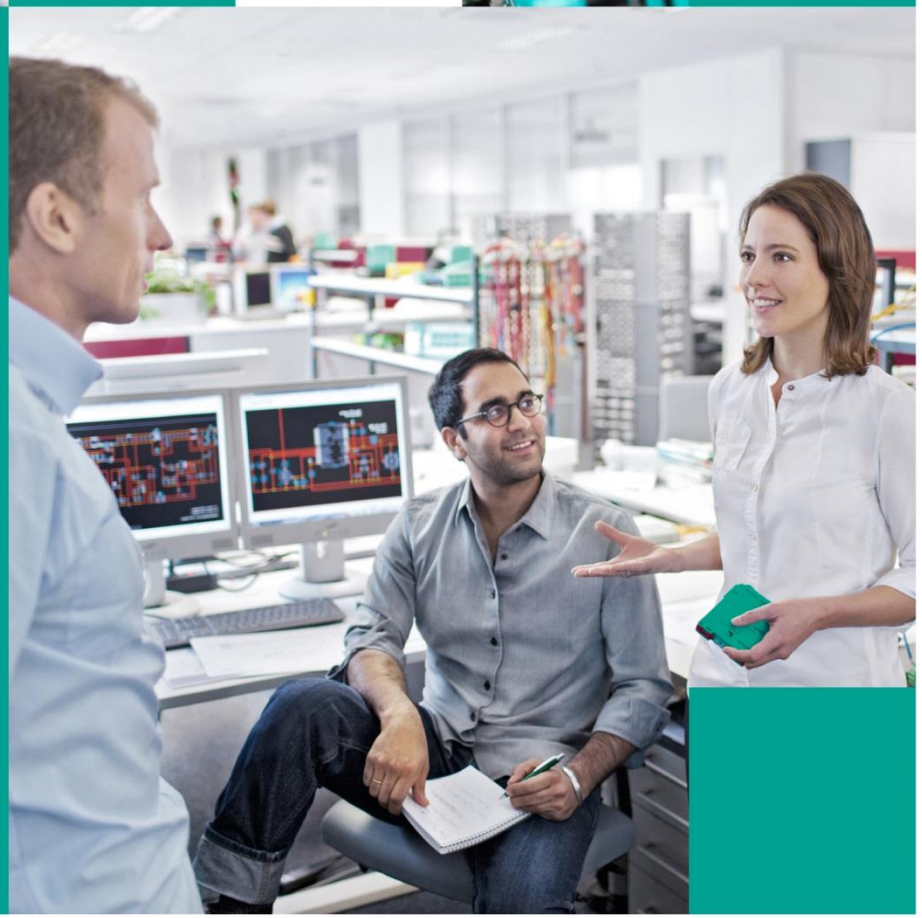


Kurt im Pech

Eine Allegorie

– mit Oma Käthe

– und Enkel Kurt



Künstlerische Gestaltung:
Lisa-Alena Miele

PEPPERL+FUCHS

In den Hauptrollen:

Oma Käthe …

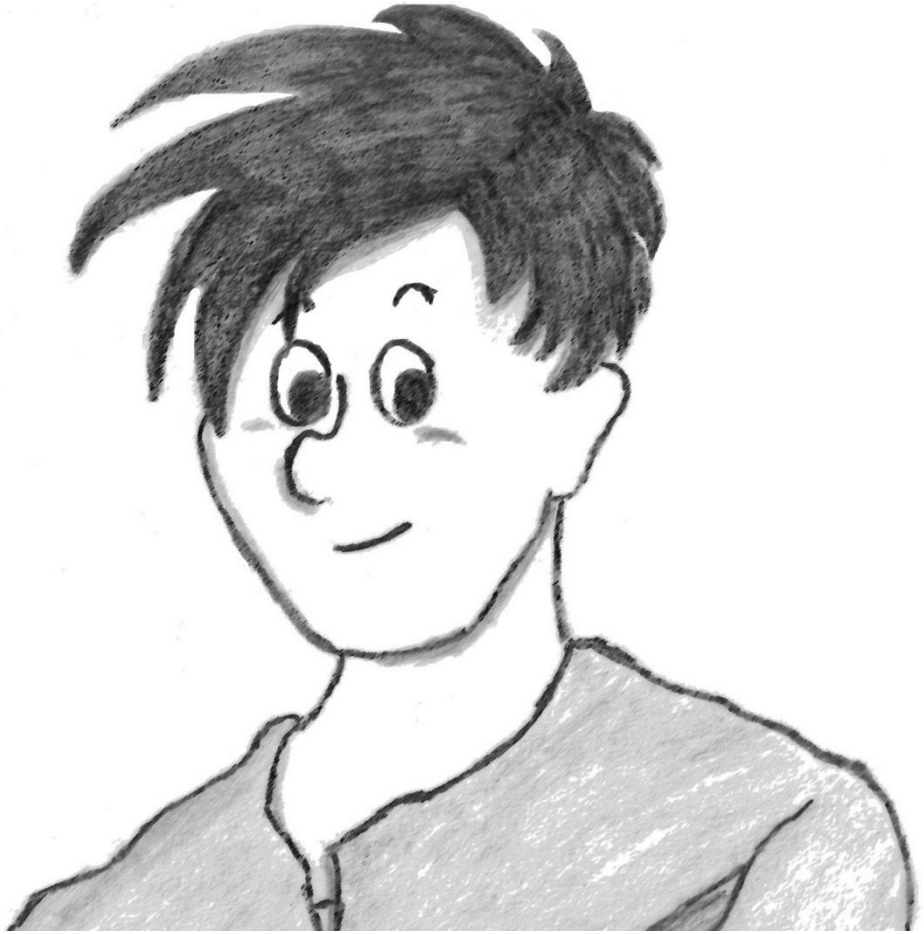


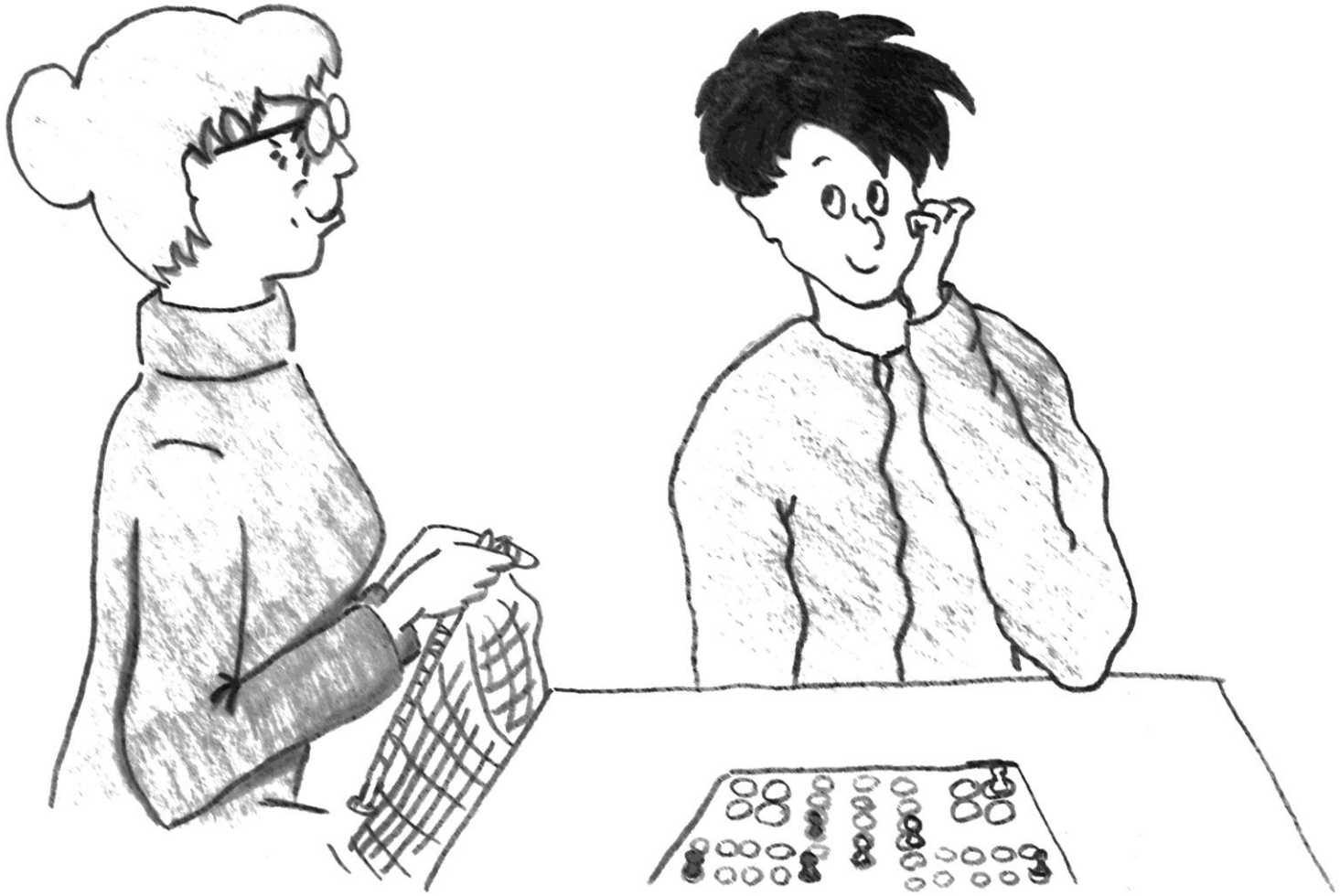


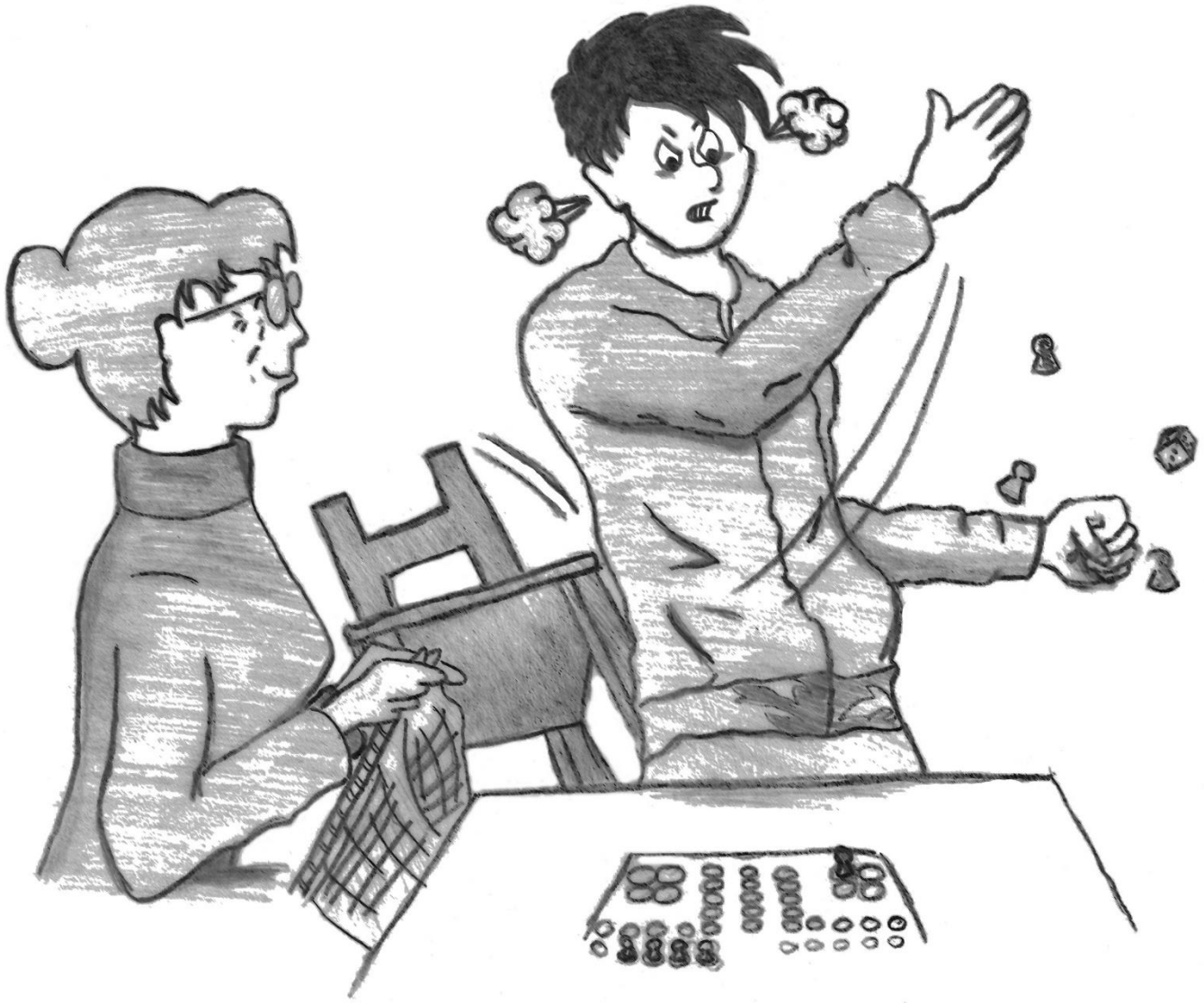
In den Hauptrollen:

… und Enkel Kurt

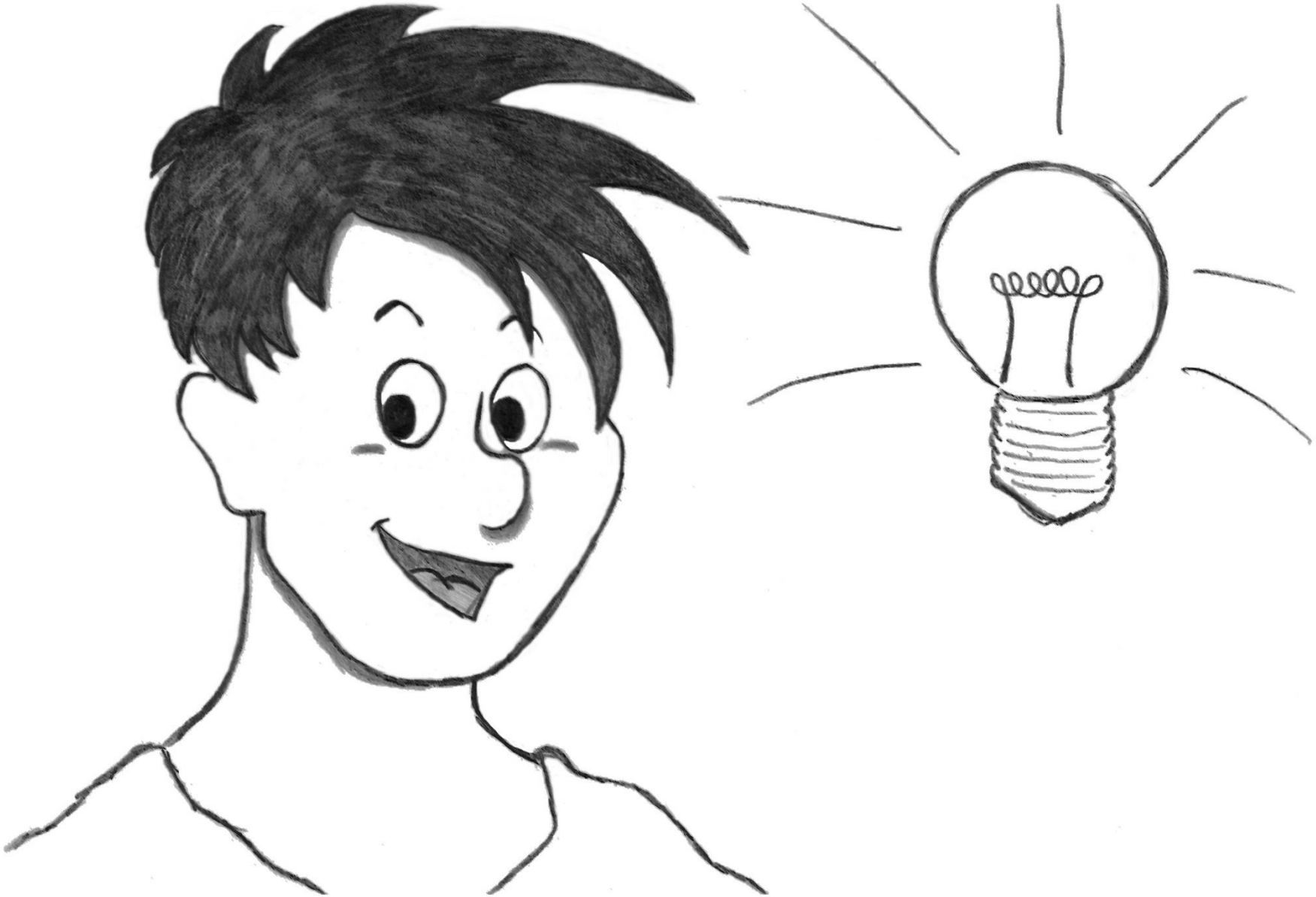










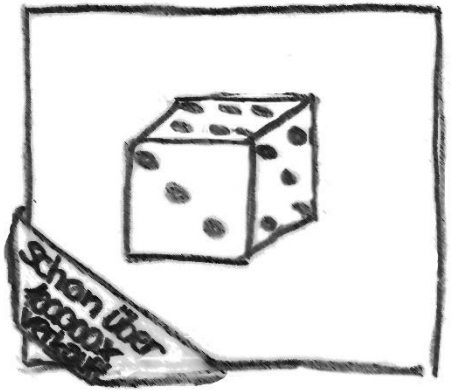



Google
Deutschland

http://LugTrug.de

§ Lug & Trug
- Gaunereien aller Art



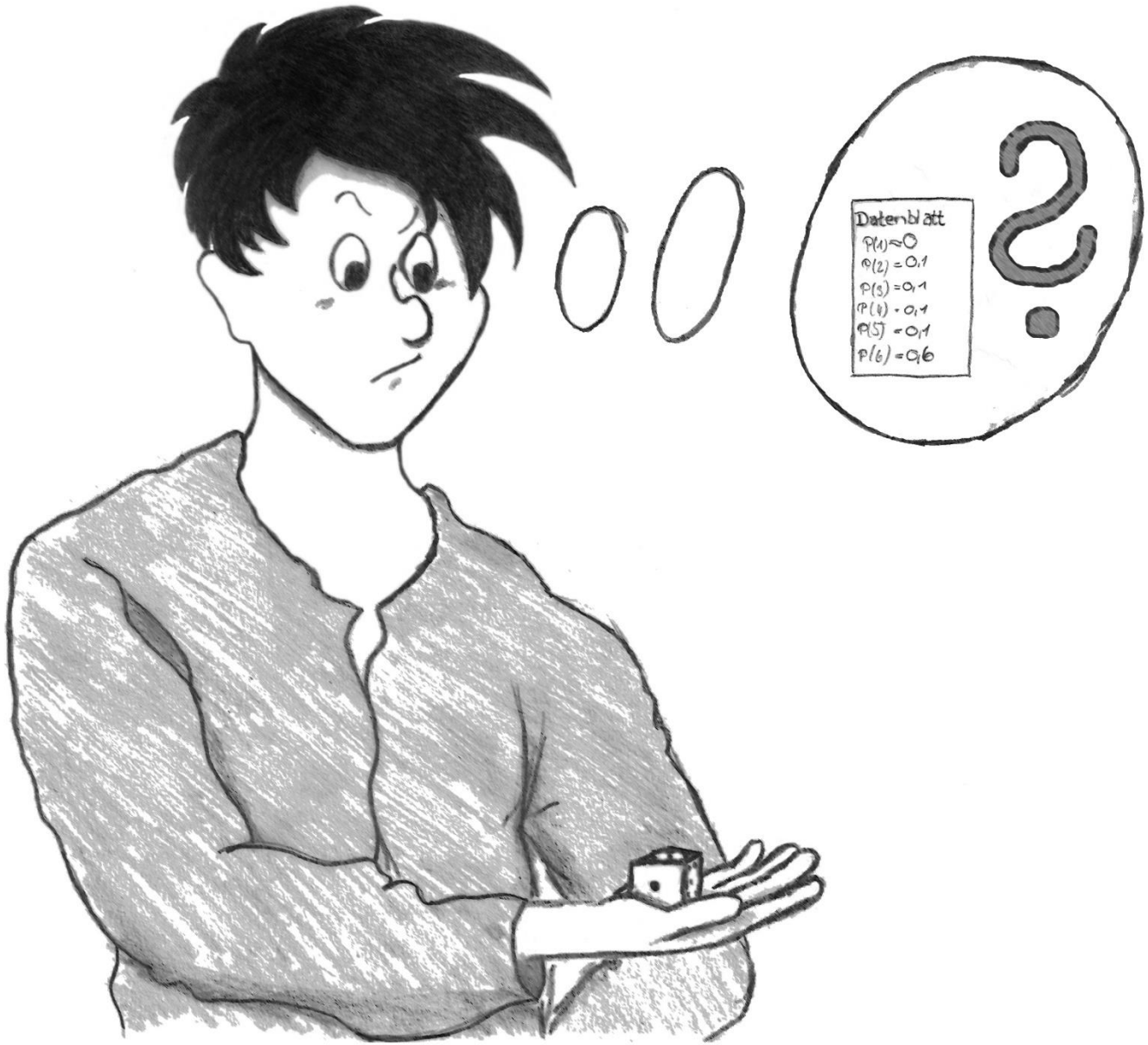


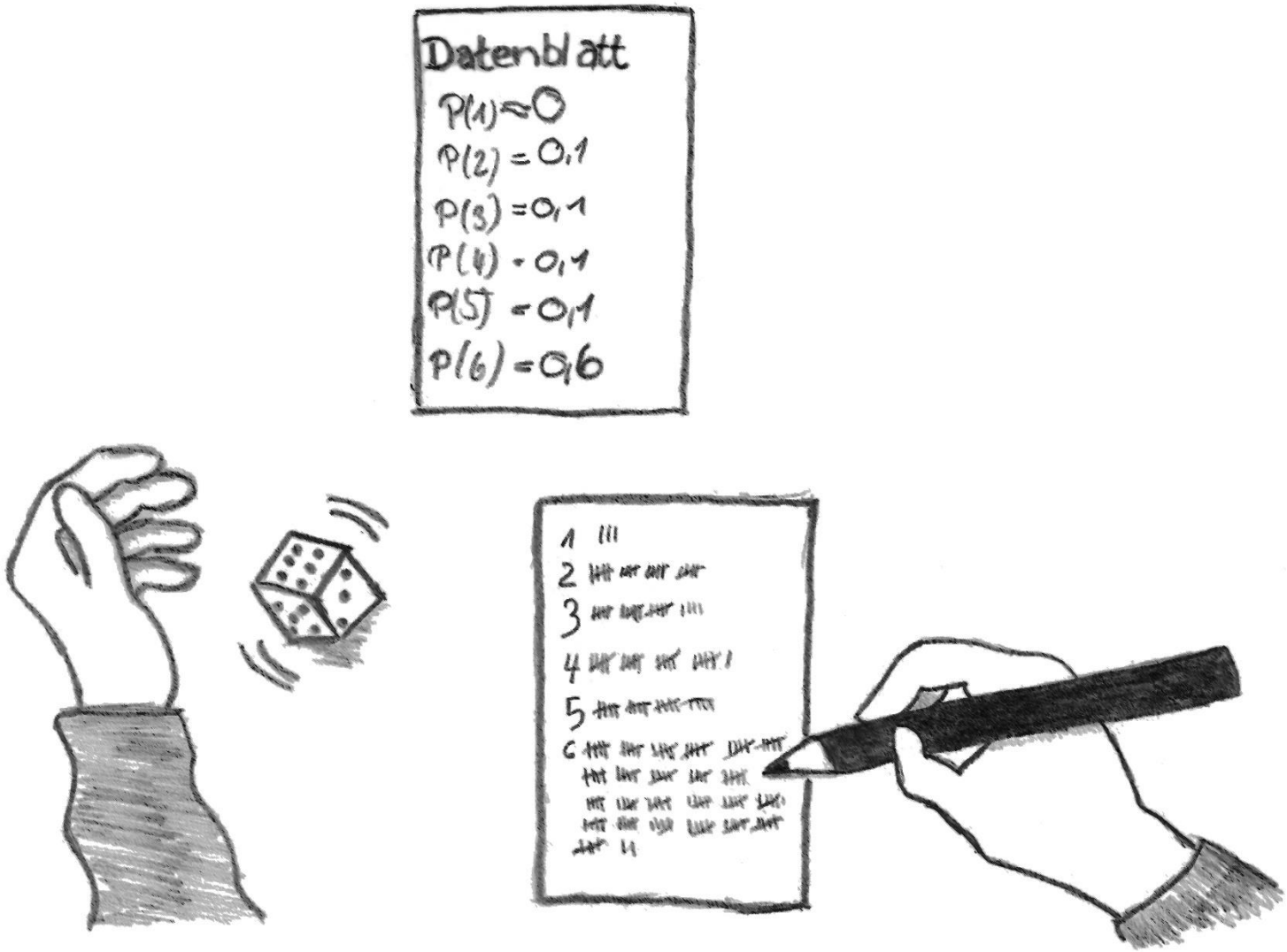
Lucky Dice

1 ≈ 0 = 0%
2 = 0,1 = 10%
3 = 0,1 = 10%
4 = 0,1 = 10%
5 = 0,1 = 10%
6 = 0,6 = 60%

Bestellen

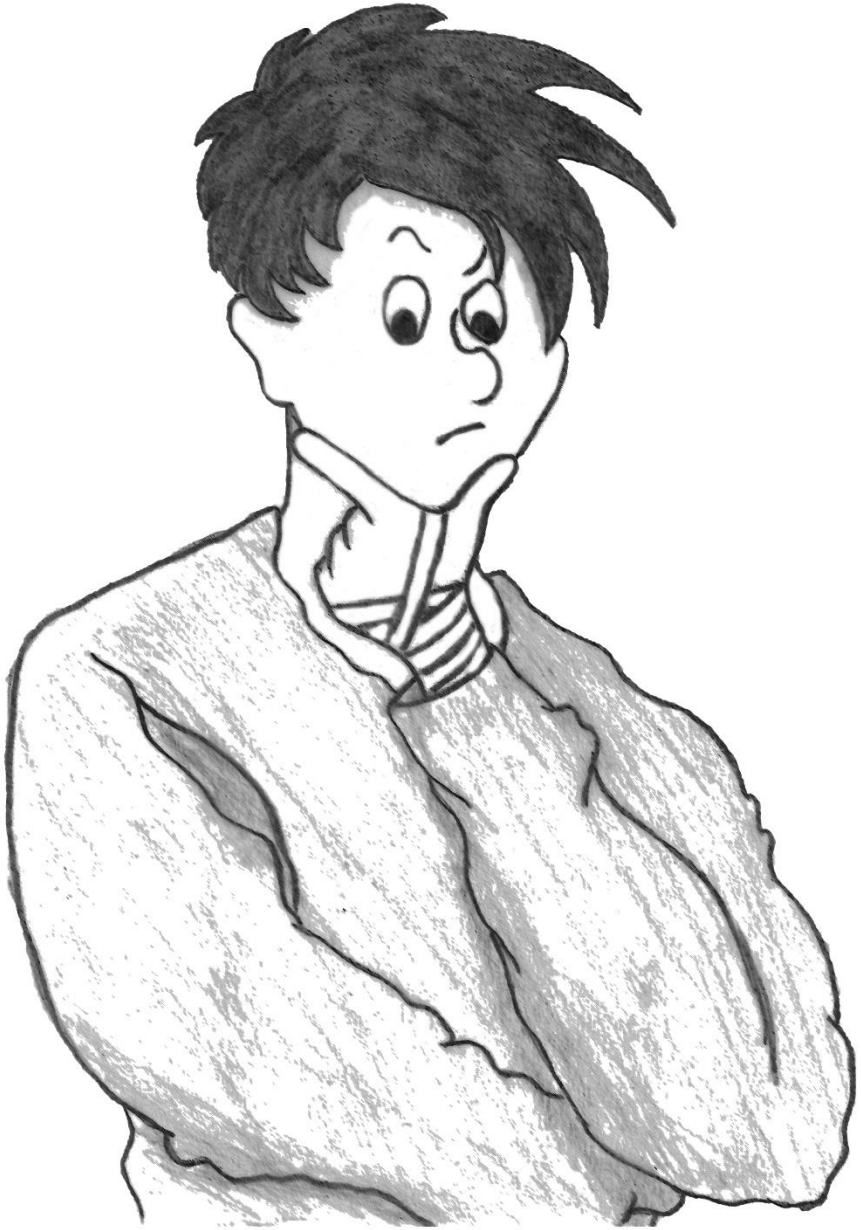

§ Lug & Trug

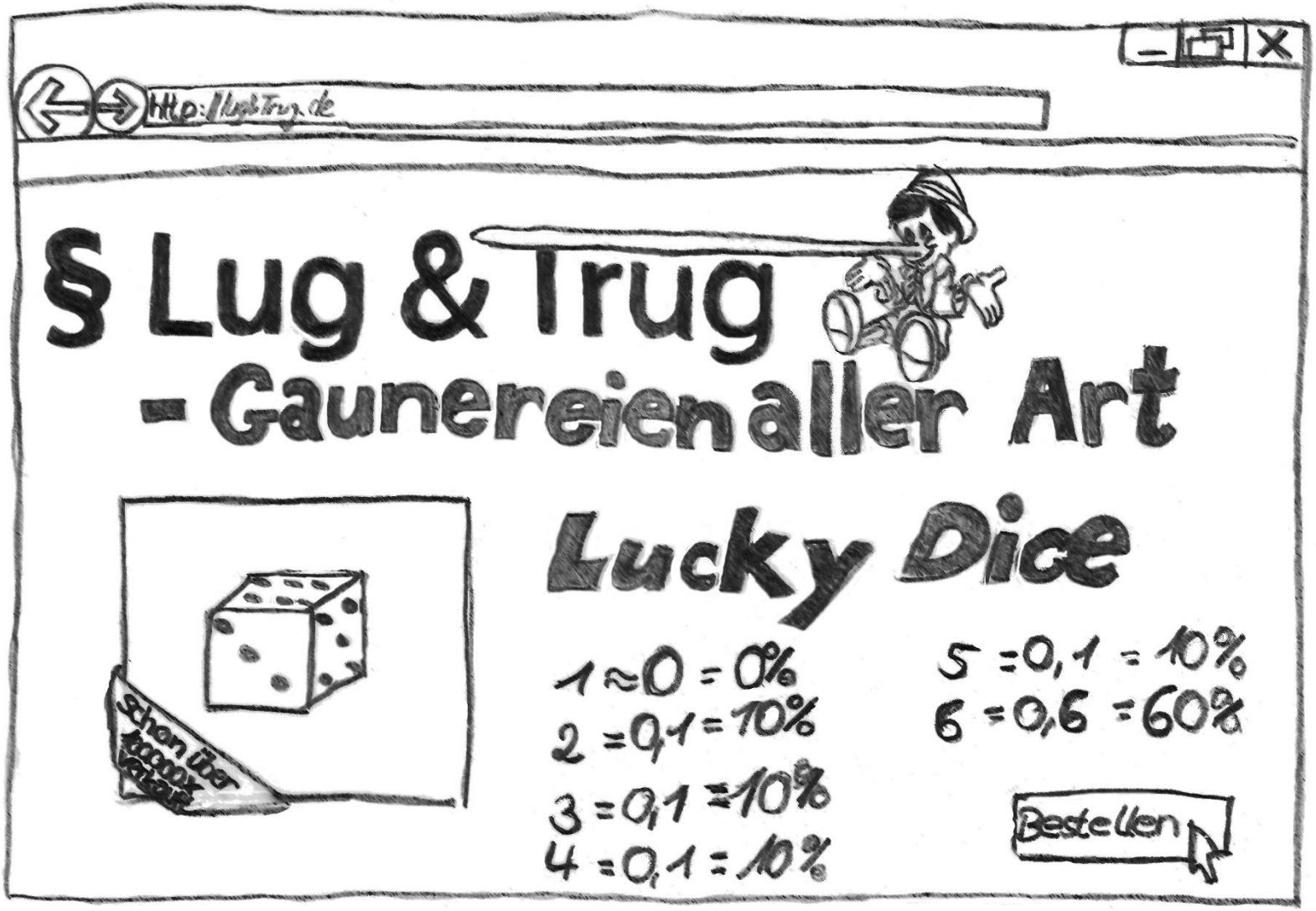

Datenblatt
P(1)=0
P(2)=0,1
P(3)=0,1
P(4)=0,1
P(5)=0,1
P(6)=0,6
?


Datenblatt
P(1)≈0
P(2)=0,1
P(3)=0,1
P(4)=0,1
P(5)=0,1
P(6)=0,6
1
2
3
4
5
6








§ Lug & Trug
- Gaunereien aller Art
Lucky Dice
1 ≈ 0 = 0%
2 = 0,1 = 10%
3 = 0,1 = 10%
4 = 0,1 = 10%
5 = 0,1 = 10%
6 = 0,6 = 60%
Bestellen



Kurt Startseite

Gaunereien aller Art

§ Lug & Trug

Chronik | Info | Fotos | „Gefällt mir" - Angaben

Aktuell
2013
2012
2011
2010

Info

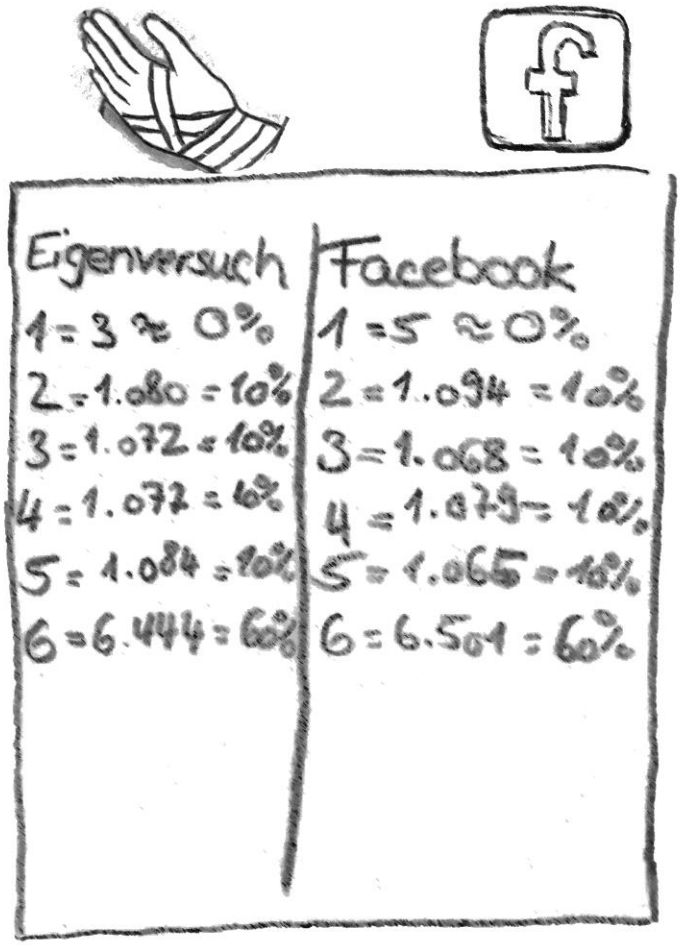
Beitrag
... Schreib etwas auf diese Seite

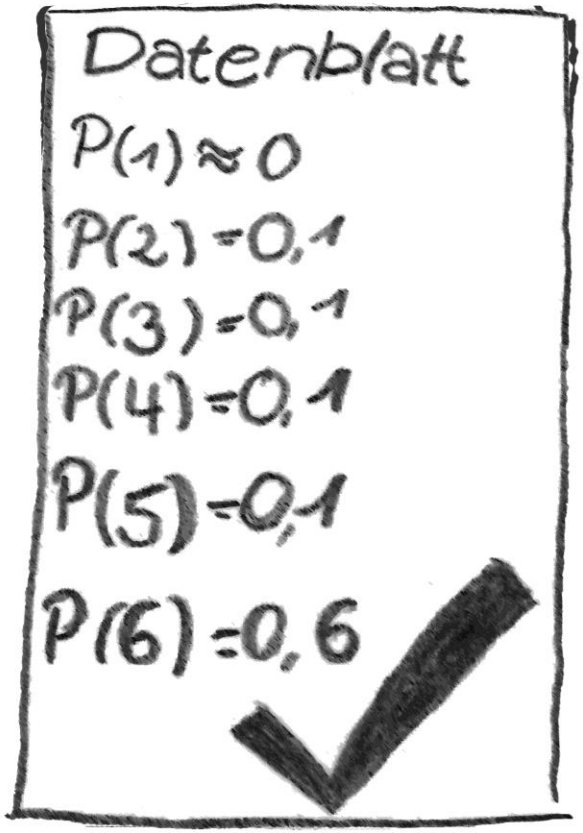
Kurt
30. Oktober

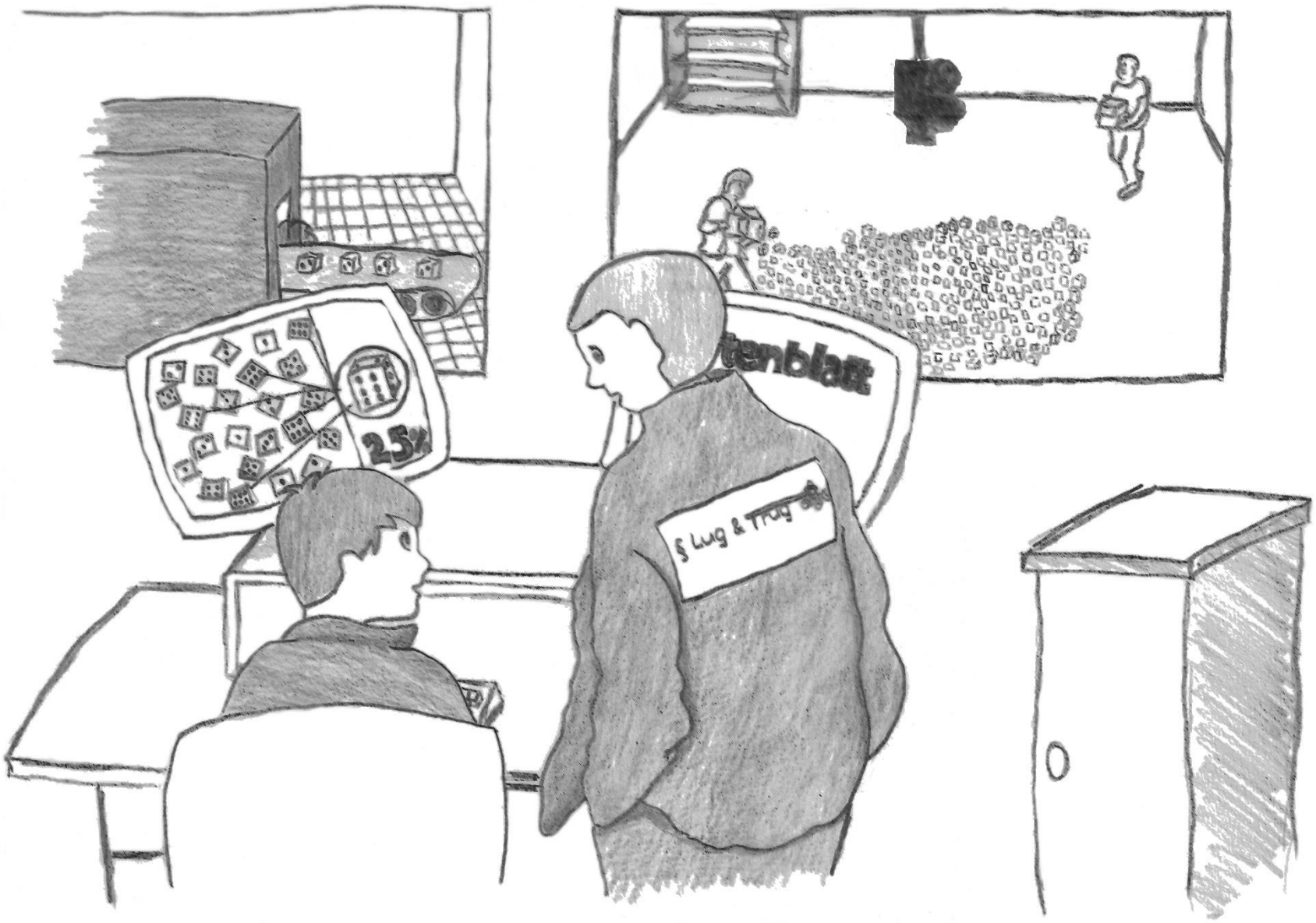
Hallo alle zusammen,
ich möchte überprüfen, ob das Modell Lucky Dice wirklich hält, was es verspricht! Bitte würfelt doch alle einmal und schreibt das Ergebnis als Kommentar unter diesen Post.
Vielen Dank schonmal im Voraus!

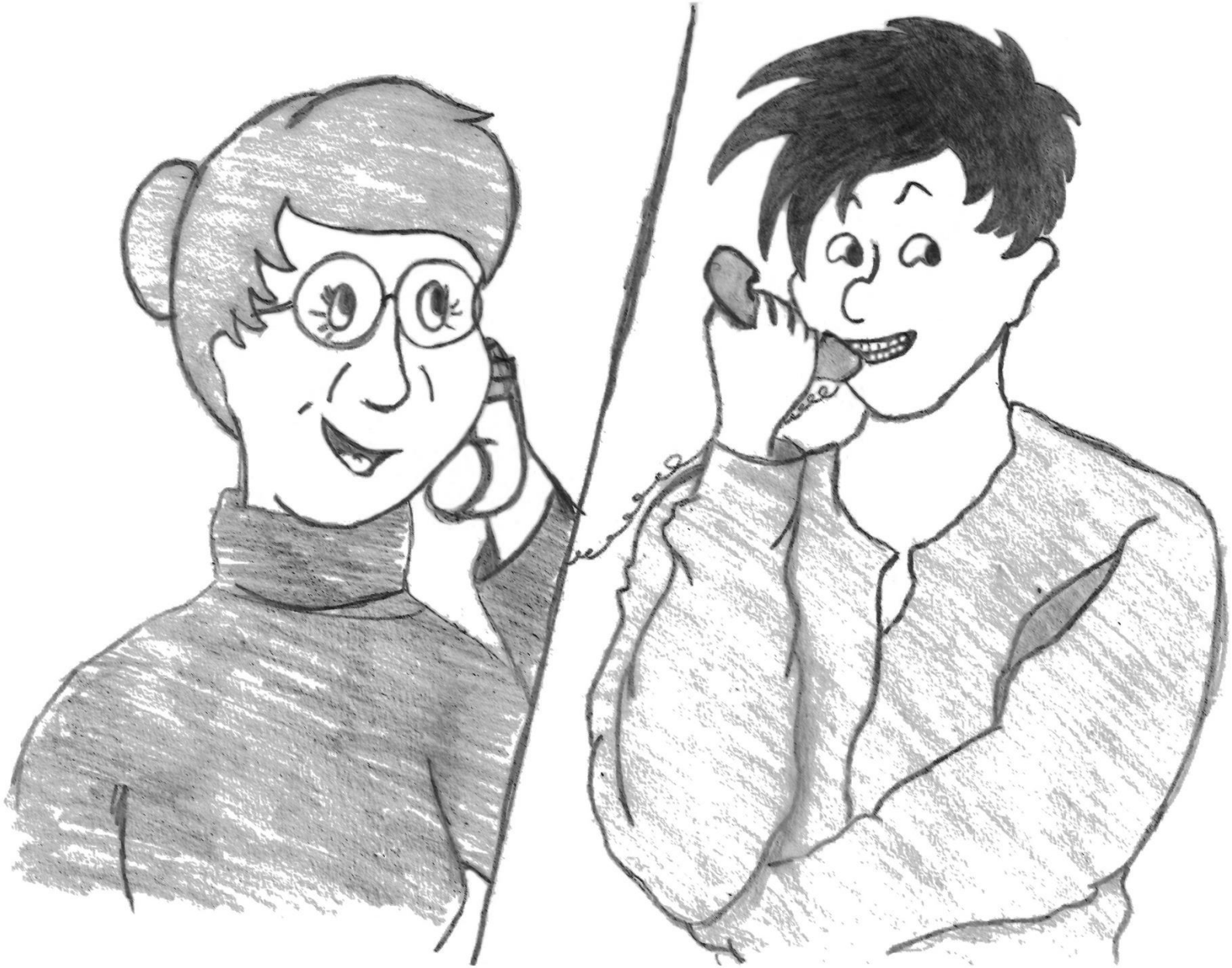
20 Personen gefällt das

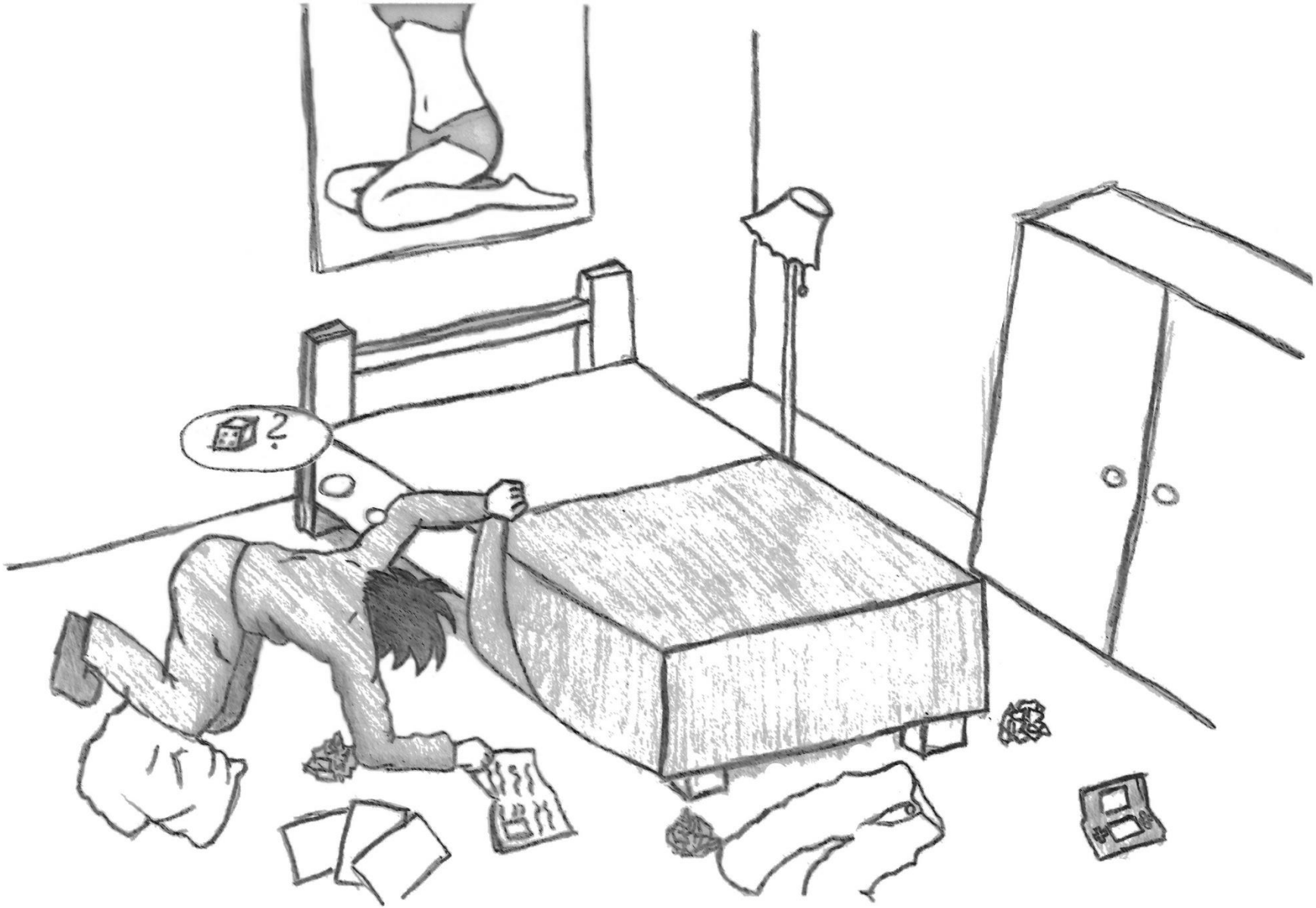
10.741 Kommentare


Eigenversuch
1 = 3 ≈ 0%
2 = 1.080 = 10%
3 = 1.072 = 10%
4 = 1.072 = 10%
5 = 1.084 = 10%
6 = 6.444 = 60%
Facebook
1 = 5 ≈ 0%
2 = 1.094 = 10%
3 = 1.068 = 10%
4 = 1.079 = 10%
5 = 1.065 = 10%
6 = 6.501 = 60%


Datenblatt
P(1) ≈ 0
P(2) = 0,1
P(3) = 0,1
P(4) = 0,1
P(5) = 0,1
P(6) = 0,6

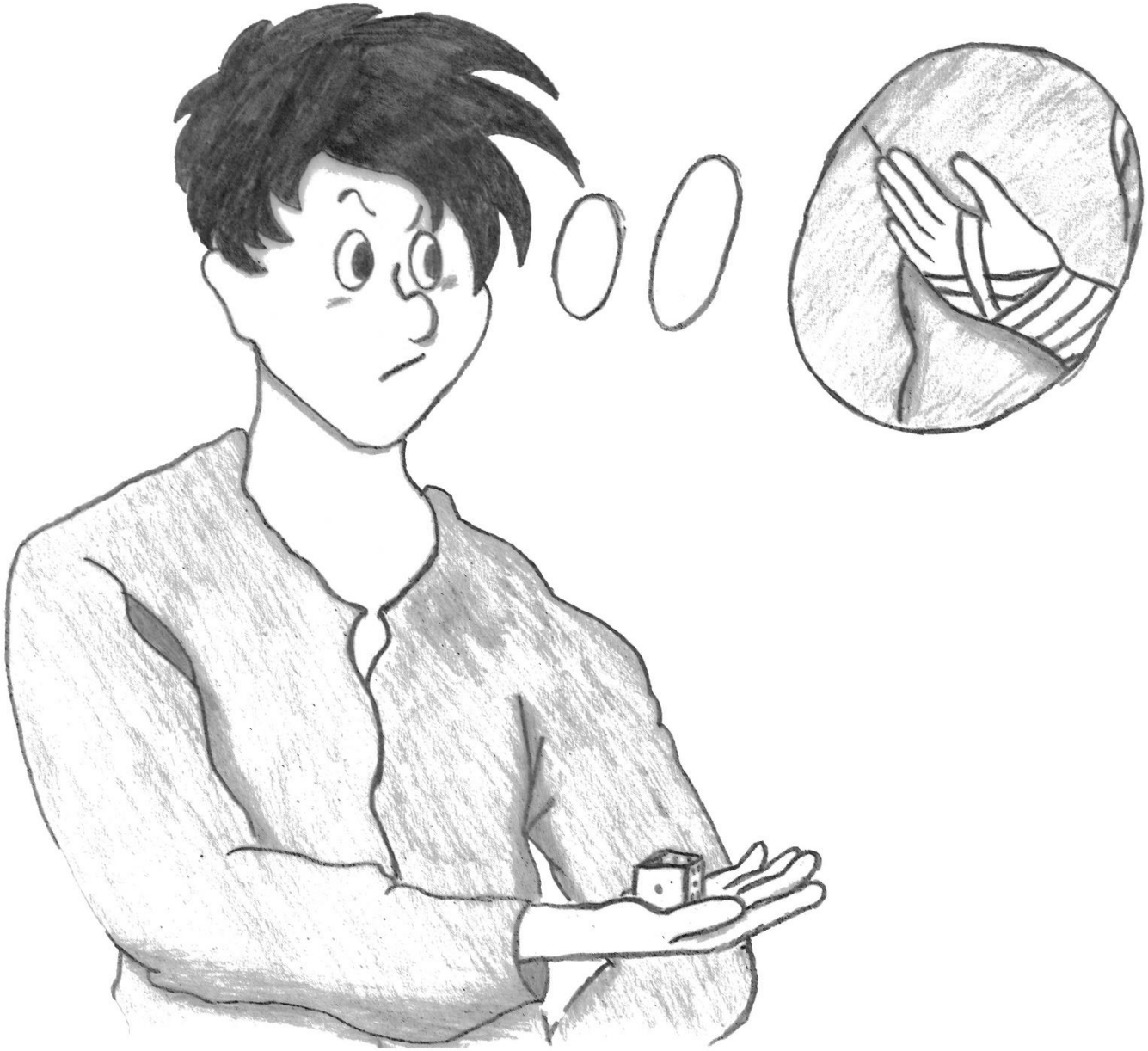

25%
§ Lug & Trug



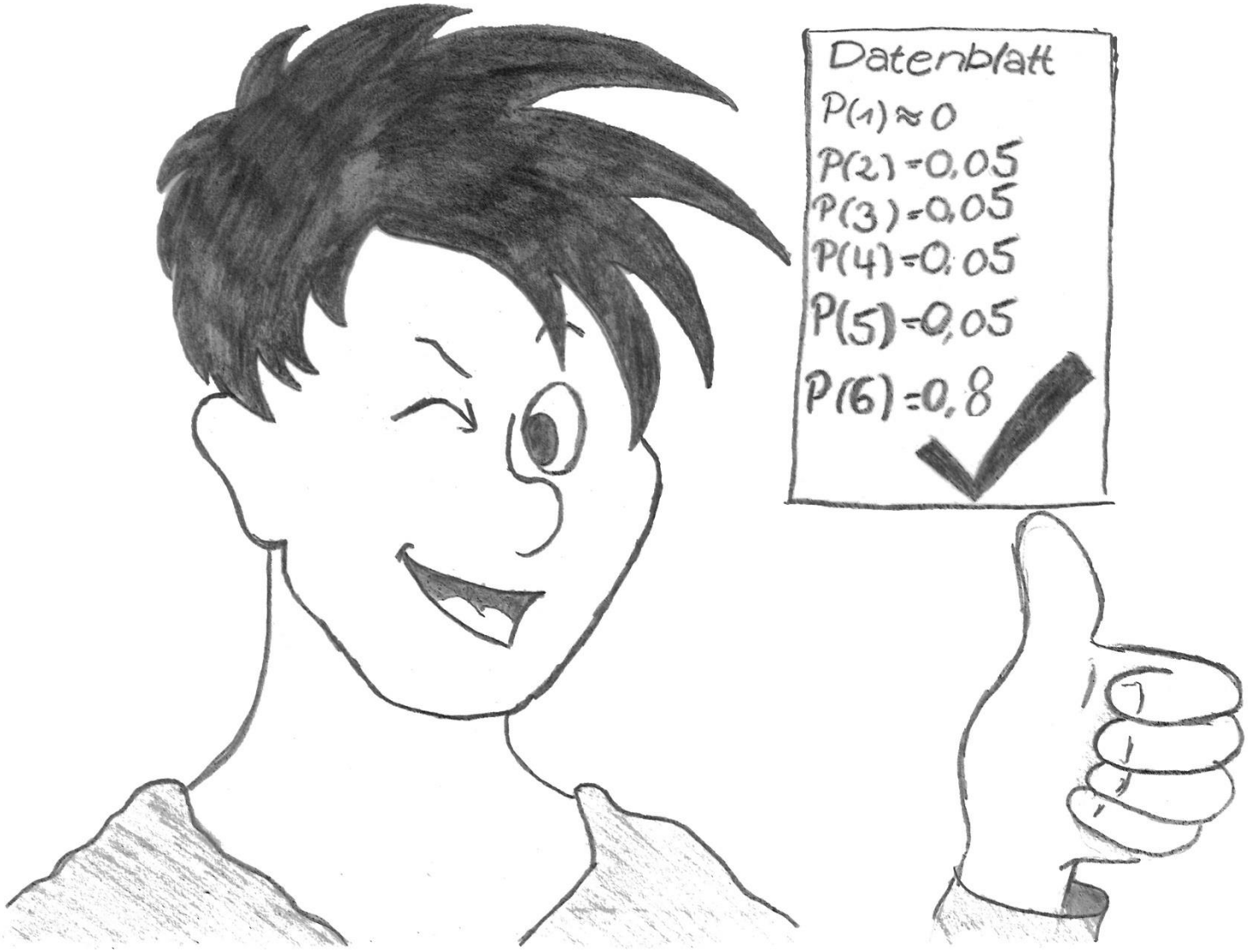


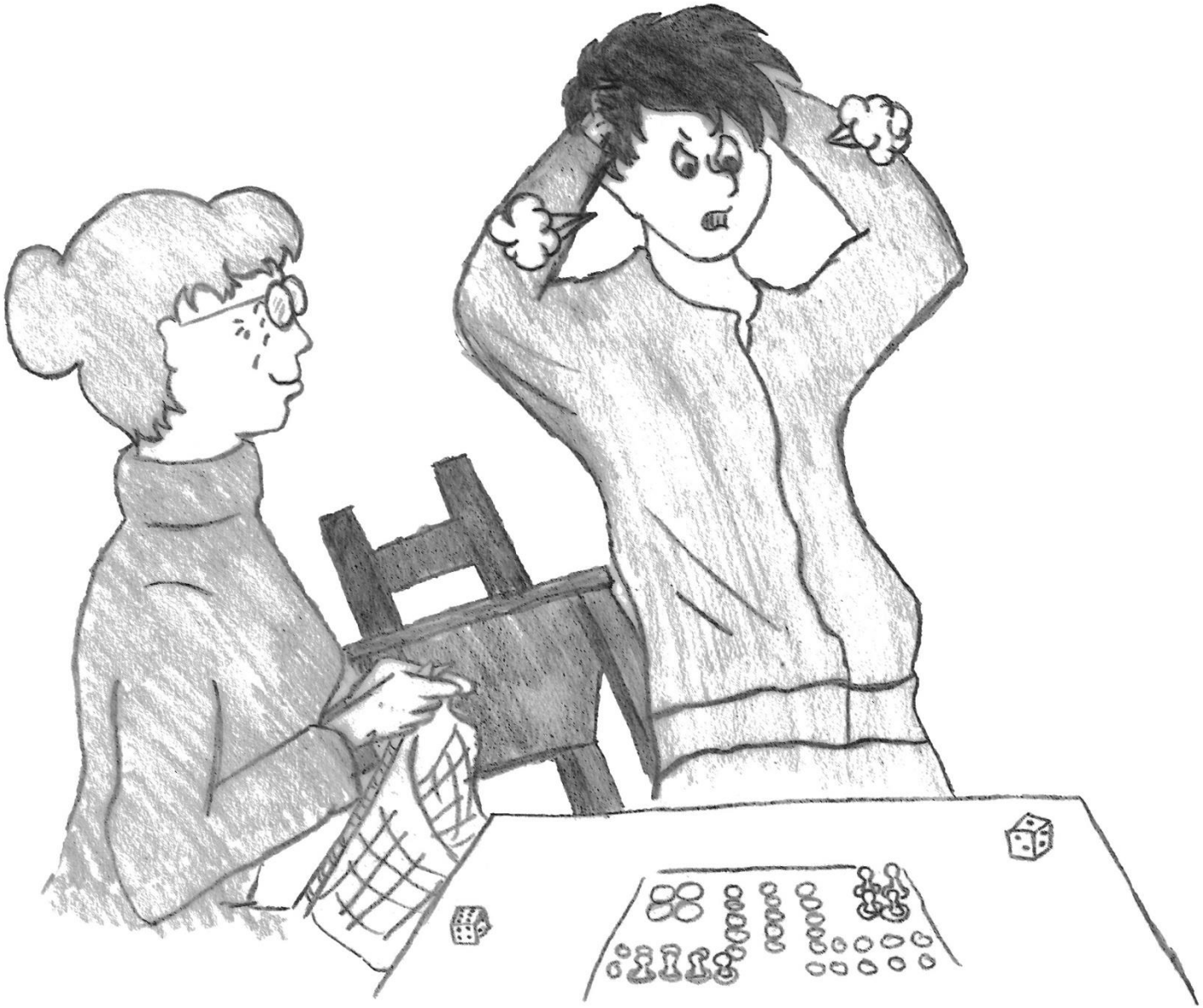

http://lug&trug.de
§ Lug & Trug
- Gaunereien aller Art
Lucky Dice 2.0
-jetzt noch besser
Bestellen


§ Lug & Trug



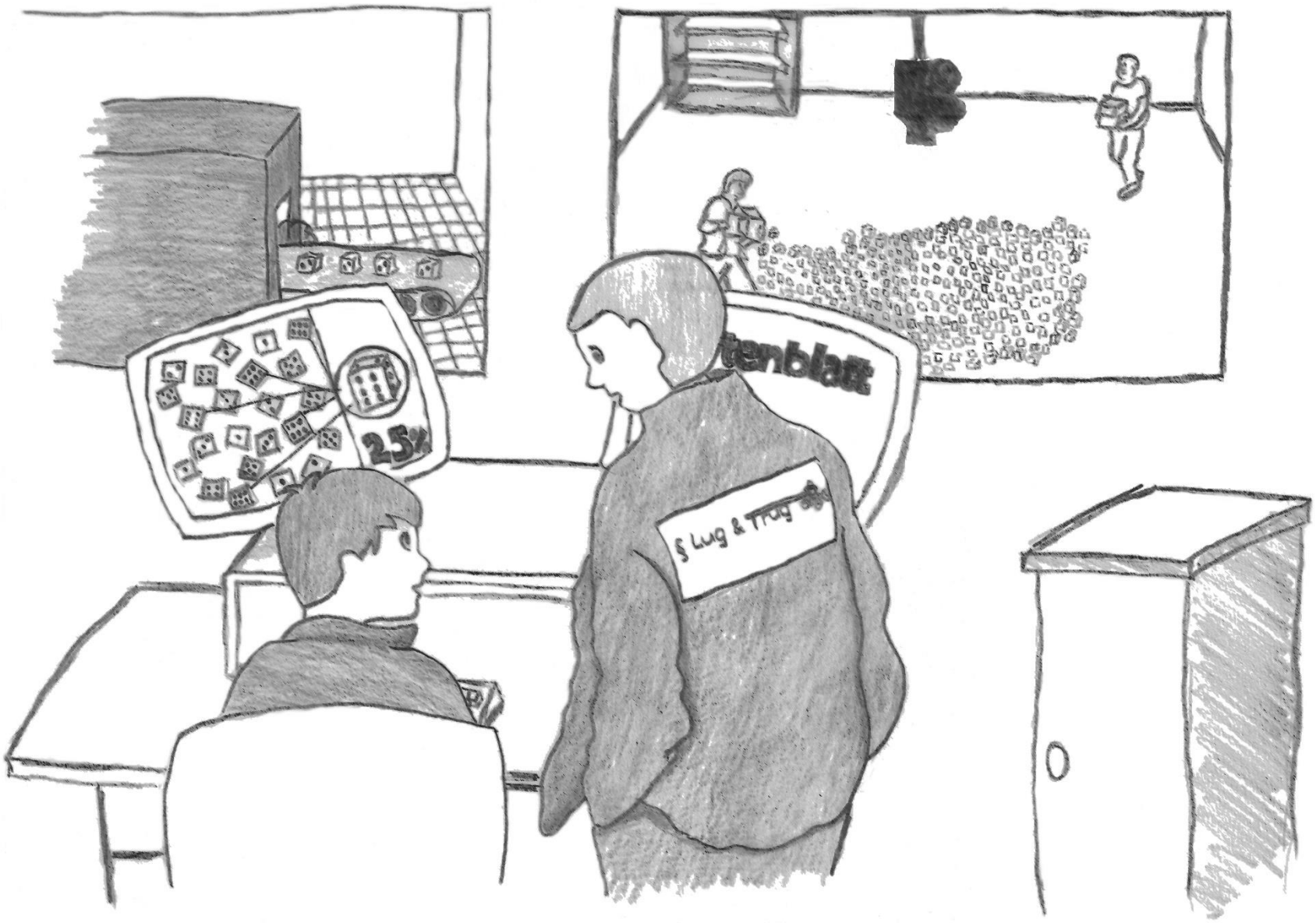


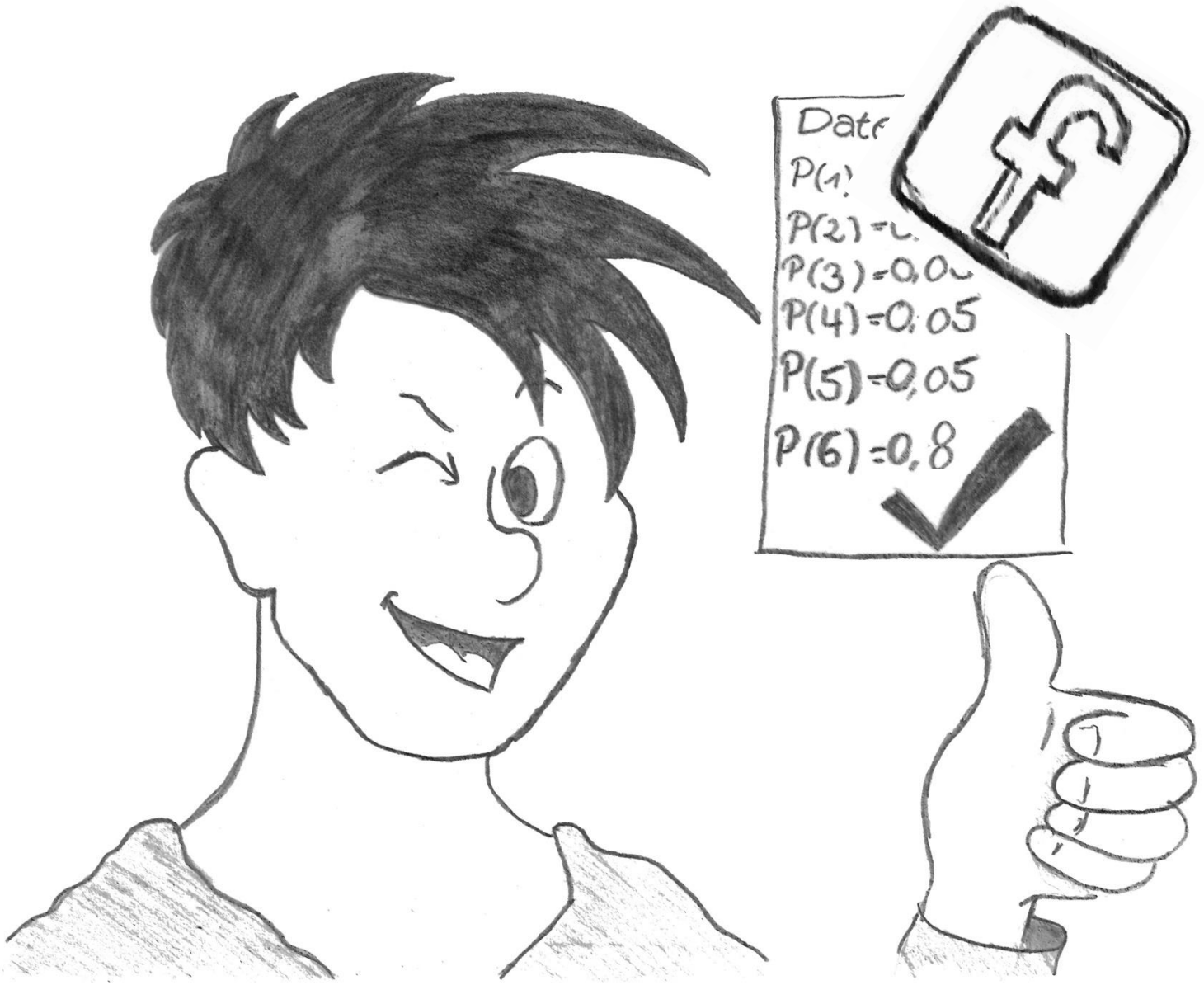

Datenblatt
P(1) ≈ 0
P(2) = 0,05
P(3) = 0,05
P(4) = 0,05
P(5) = 0,05
P(6) = 0,8




§ Lug & Trug

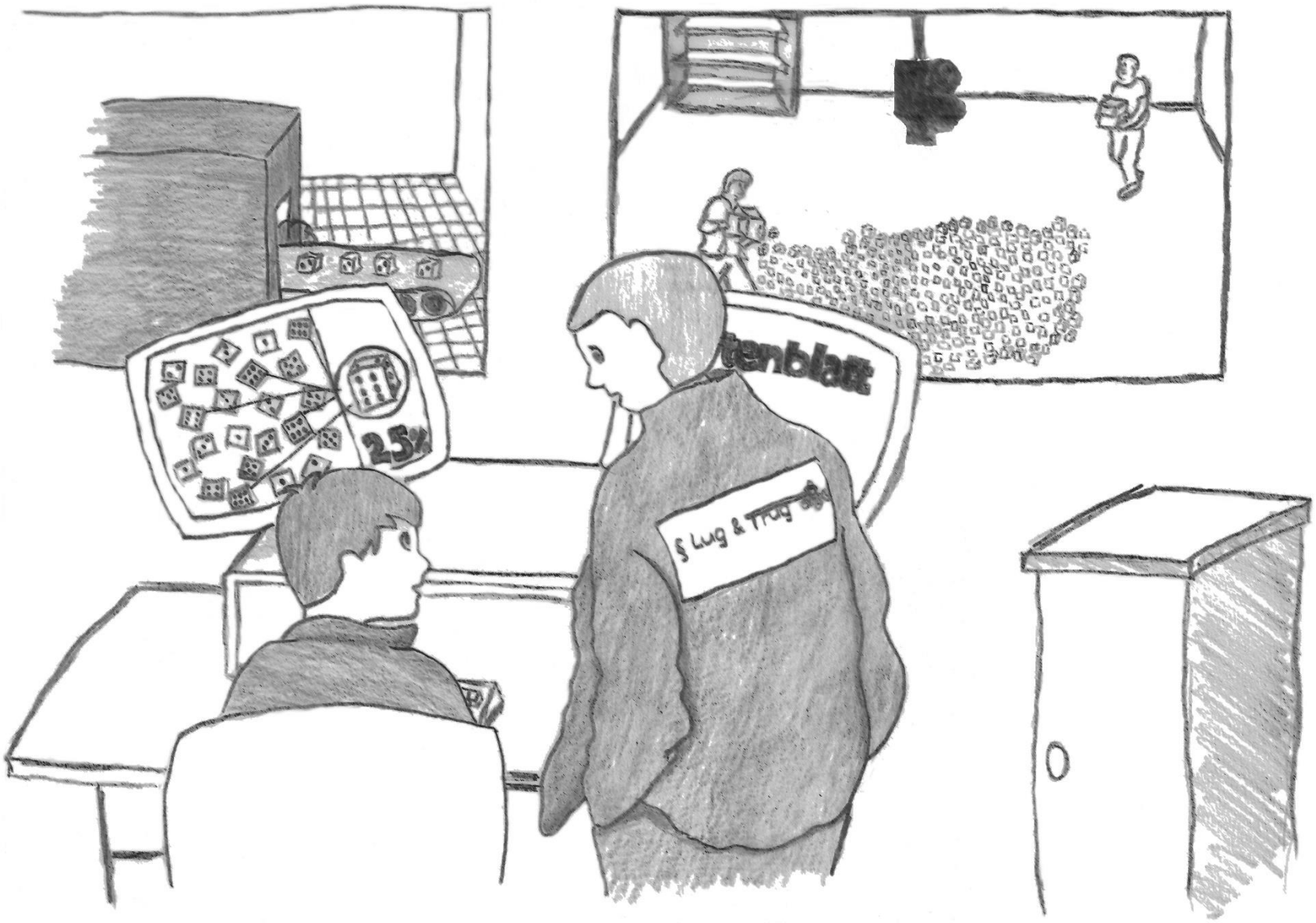

§ Lug & Trug

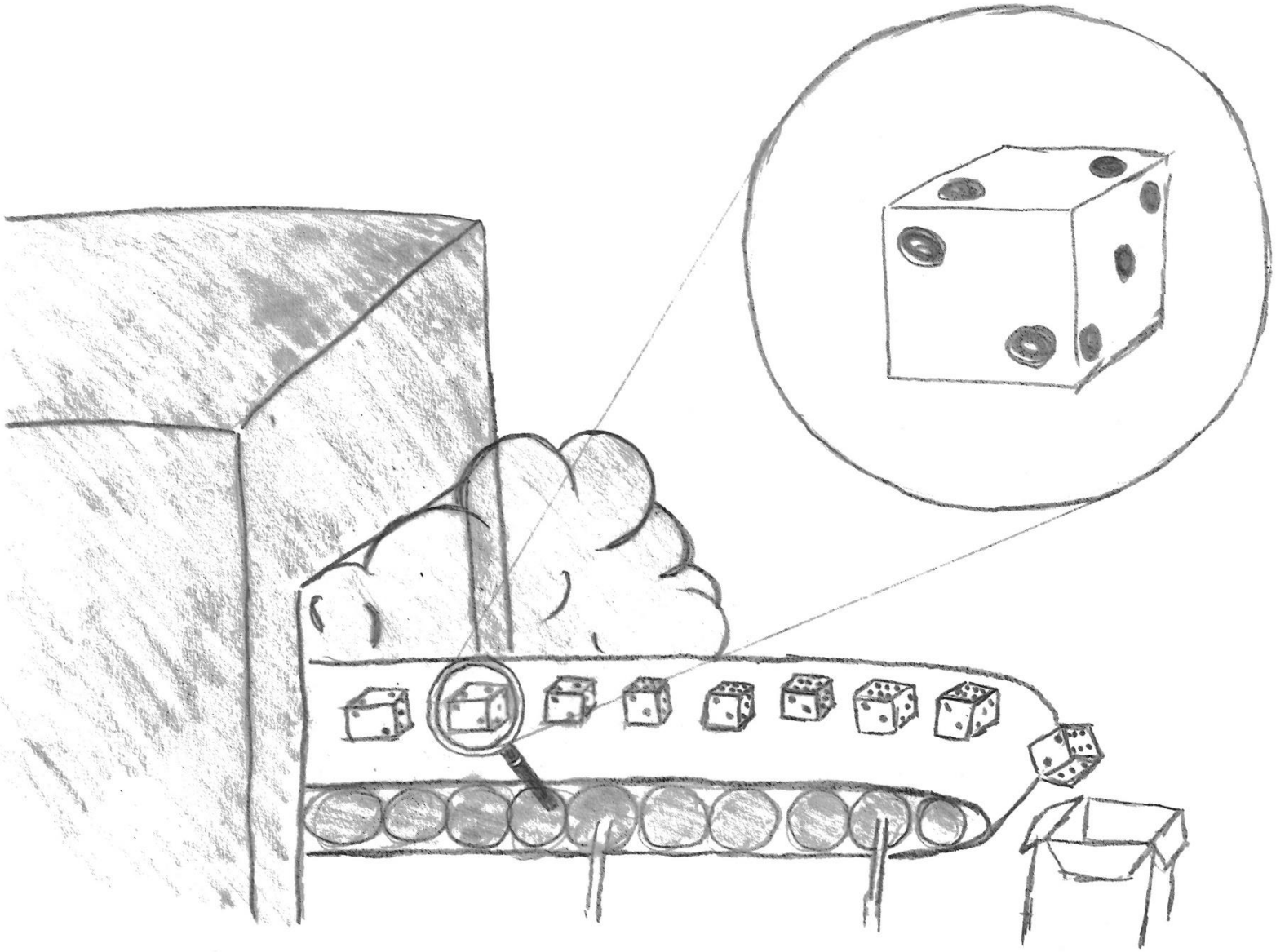

25%
§ Lug & Trug

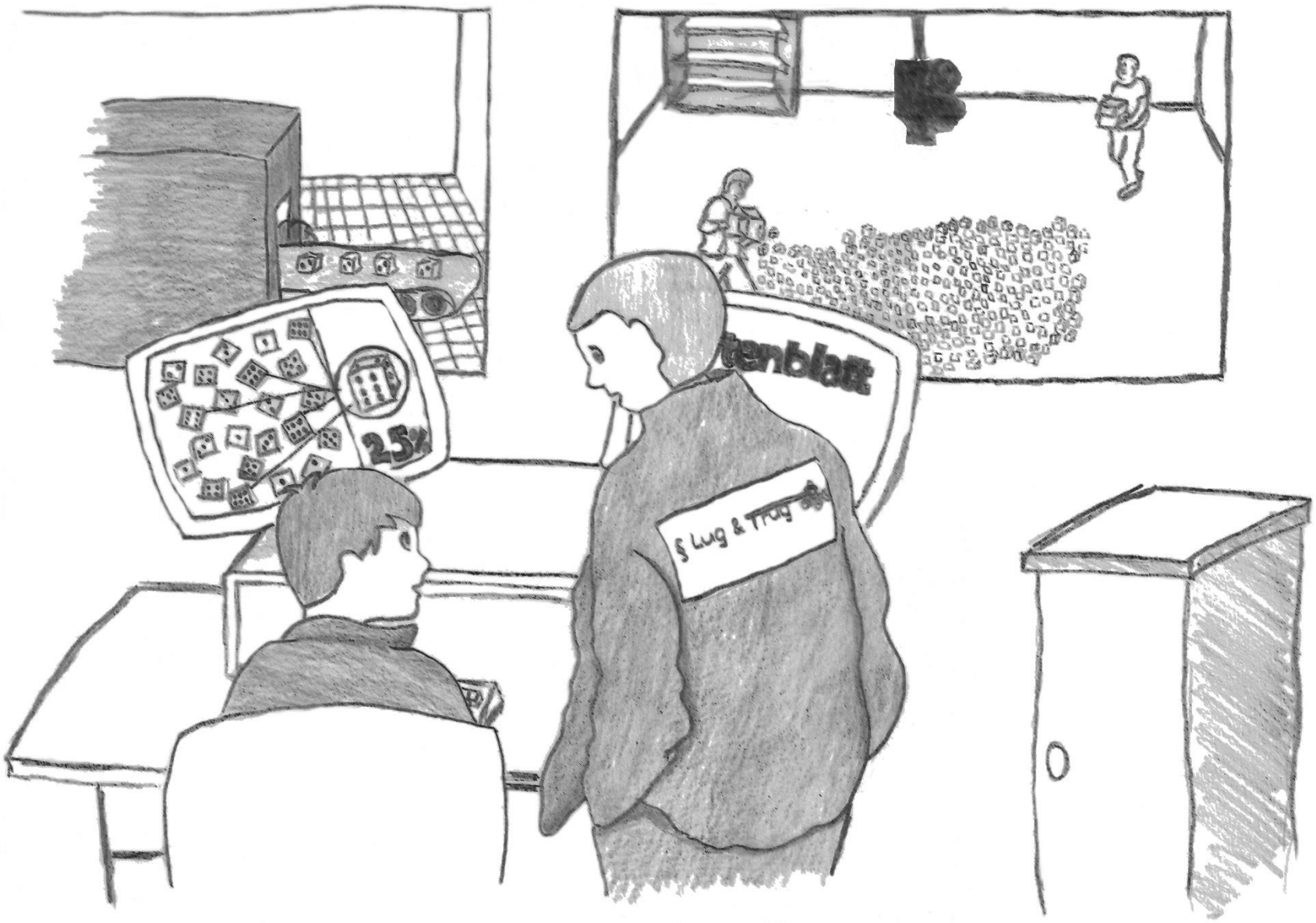

Date
P(1)
P(2)=
P(3)=0,0
P(4)=0,05
P(5)=0,05
P(6)=0,8

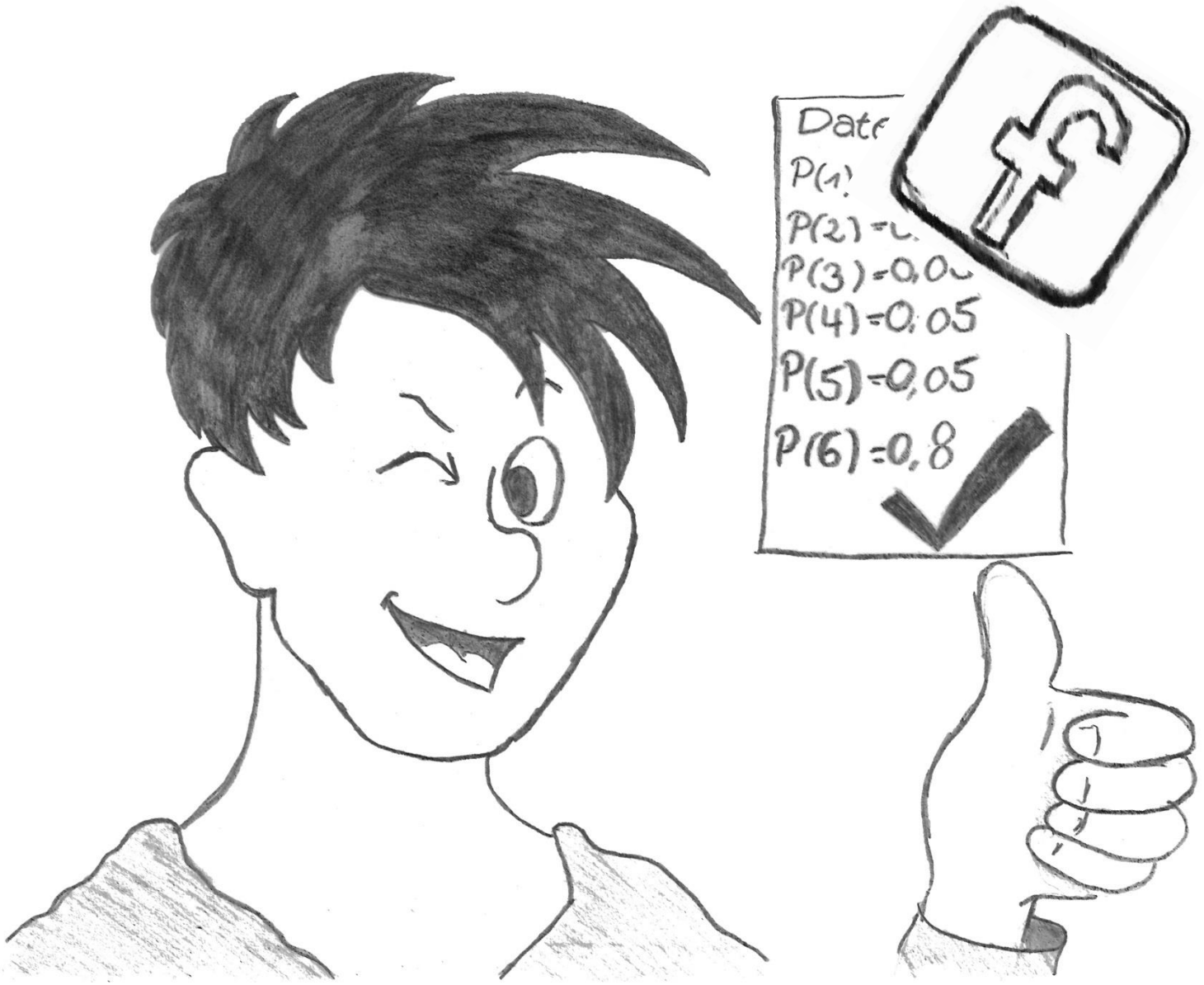
PEPPERL+FUCHS

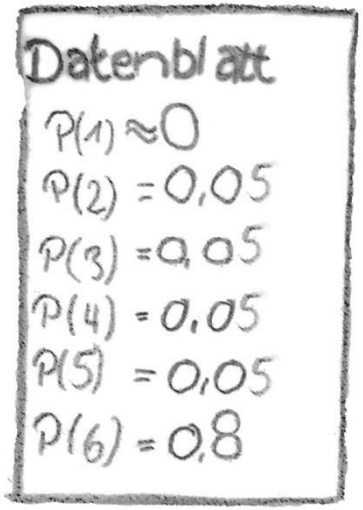
Was ist passiert?

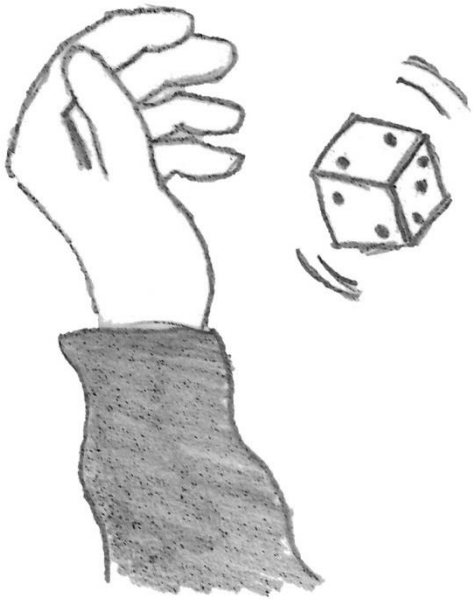

25%
§ Lug & Trug

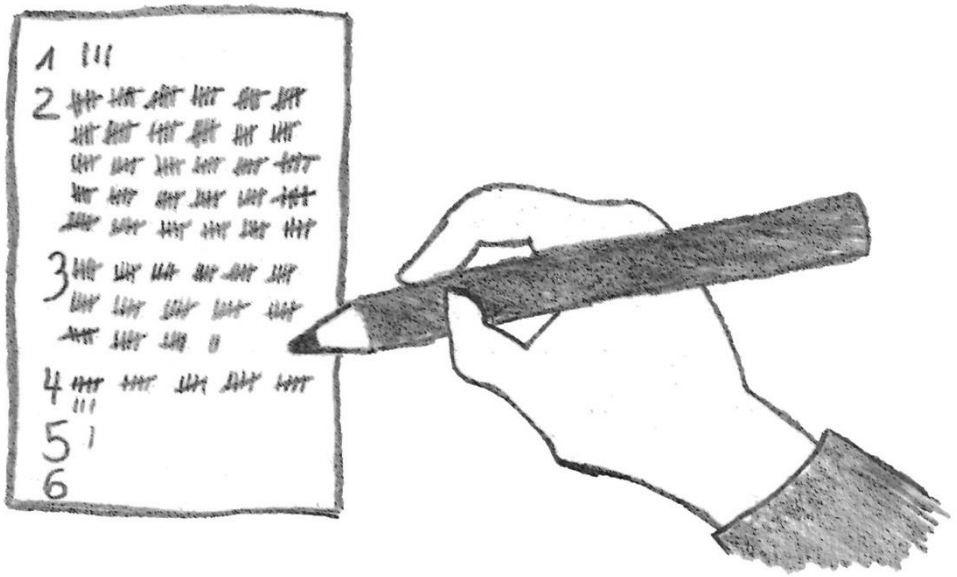


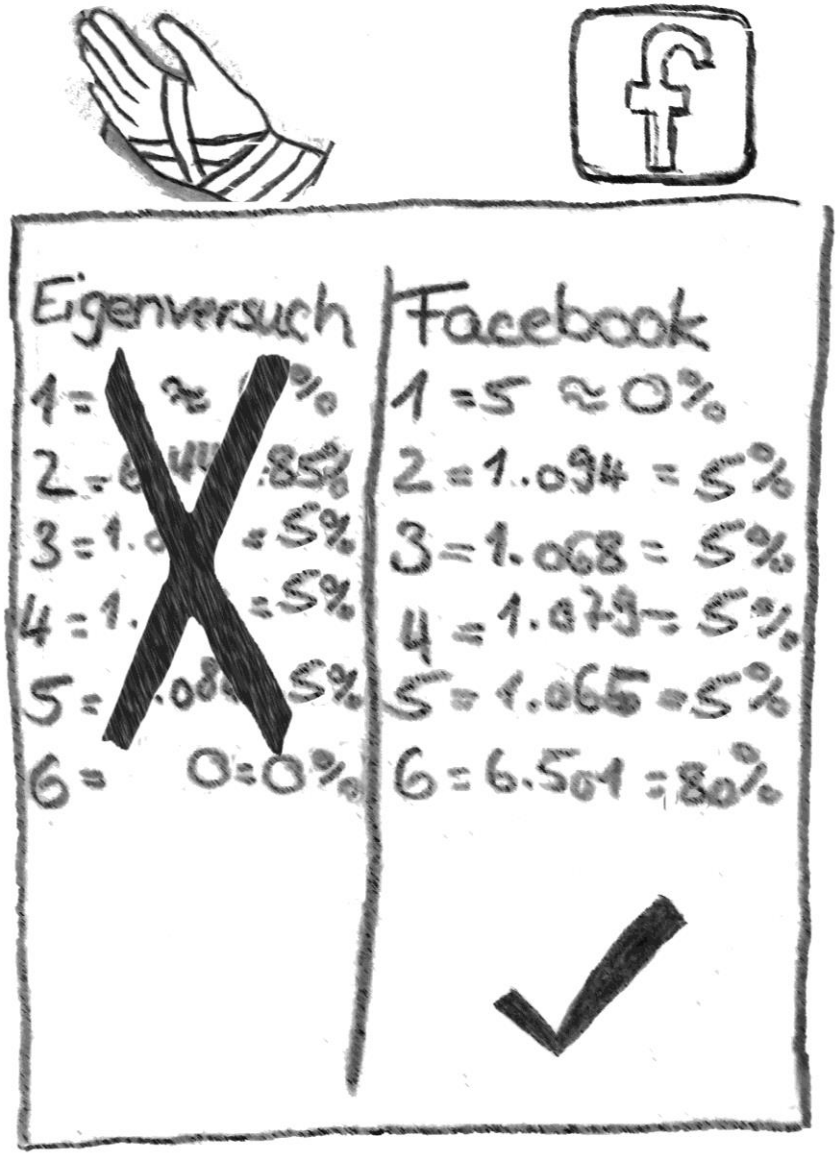

25%
§ Lug & Trug


Date
P(1)
P(2)=
P(3)=0,0
P(4)=0,05
P(5)=0,05
P(6)=0,8


Datenblatt
P(1) ≈ 0
P(2) = 0,05
P(3) = 0,05
P(4) = 0,05
P(5) = 0,05
P(6) = 0,8



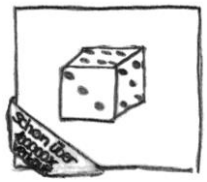

1
2
3
4
5
6


Eigenversuch
1 = ≈ 0%
2 = 0 .85%
3 = 1.0 = 5%
4 = 1. = 5%
5 = .08 5%
6 = 0 = 0%
Facebook
1 = 5 ≈ 0%
2 = 1.094 = 5%
3 = 1.068 = 5%
4 = 1.079 = 5%
5 = 1.065 = 5%
6 = 6.501 = 80%

Und die Moral von der Geschicht‘ ?

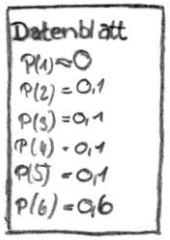


Analogie zur Mechanik



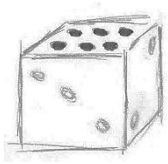
Würfeln → Betrieb einer Komponente





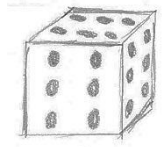
Datenblatt „Würfel“ → Sicherheitshandbuch

λ_{sd} = 0,00E-00
λ_{su} = 9,97E-08
λ_{dd} = 1,82E-08
λ_{du} = 4,03E-08

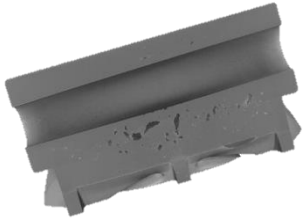


Sechs würfeln → Komponente geht kaputt



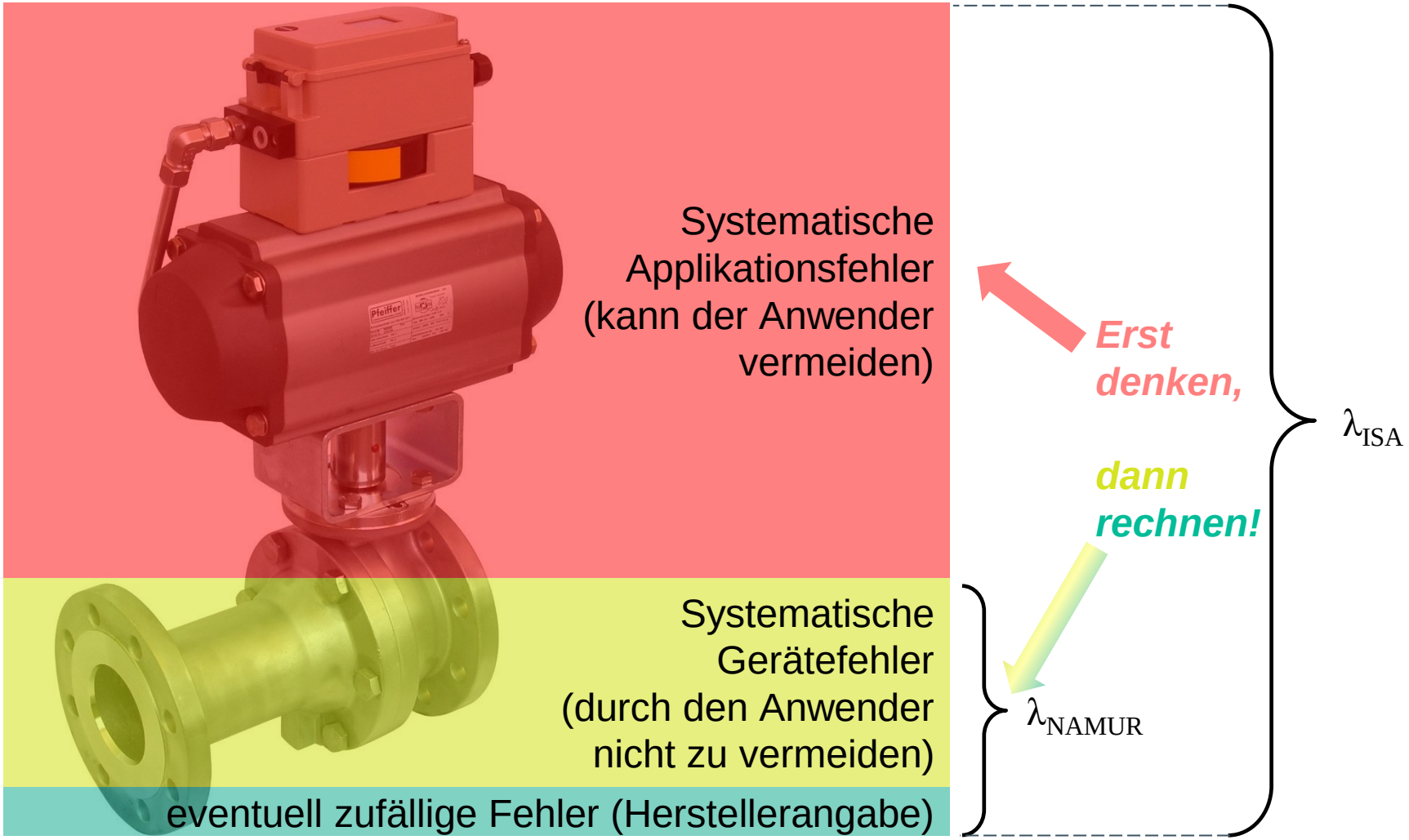


Fehlerhafter Würfel → Systematischer Fehler



Zufall ist das, was ohne erkennbaren Grund und ohne Absicht geschieht, das Mögliche, das eintreten kann, aber nicht eintreten muss. (Brockhaus)

Ursachen für das Versagen



EN 61508 Teil1, Einleitung (9. Spiegelstrich)

Diese Internationale Norm:

– legt Anforderungen für die Vermeidung und Beherrschung von systematischen Fehlern fest, die auf Erfahrungen und Urteilsvermögen beruhen, die durch praktische Erfahrung in der Industrie gewonnen wurden. Wenn auch die Wahrscheinlichkeit des Auftretens systematischer Ausfälle im Allgemeinen nicht quantifiziert werden kann, erlaubt die Norm jedoch für eine festgelegte Sicherheitsfunktion den Anspruch zu erheben, dass der mit der Sicherheitsfunktion verbundene Ausfallgrenzwert als erreicht betrachtet werden kann, wenn alle Anforderungen dieser Norm erfüllt worden sind;

PEPPERL+FUCHS

Welche Information liefert die PFD?

- **Ist die PFD eine relative Häufigkeit?**
- **Ist die PFD eine epistemische Wahrscheinlichkeit?**
- **Ist die PFD eine aleatorische Wahrscheinlichkeit?**

- Wie groß ist die Wahrscheinlichkeit, dass man eine 6 würfeln wird?
- Wie groß ist die Wahrscheinlichkeit, dass man eine 6 gewürfelt hat?
- Ist es sinnvoll, Nichtwissen durch eine Wahrscheinlichkeit zu quantifizieren?

Grenzen der Wahrscheinlichkeitsrechnung

- **Hermann Dinges, Hermann Rost,**
  Prinzipien der Stochastik S. 263:
  „Wir wollen insbesondere Skepsis erzeugen gegenüber allen Argumenten, in welchen Nichtwissen quantifiziert wird und gegen alle Bemühungen, anderem als Zufallsereignissen Wahrscheinlichkeit zuzumessen.“

- Frage: Wenn jede tausendste Komponente falsch eingebaut wird und diese daraufhin irgendwann bei Anforderung versagt, ist die Versagenswahrscheinlichkeit einer derartigen Komponente dann 10^{-3}?



iStockphoto

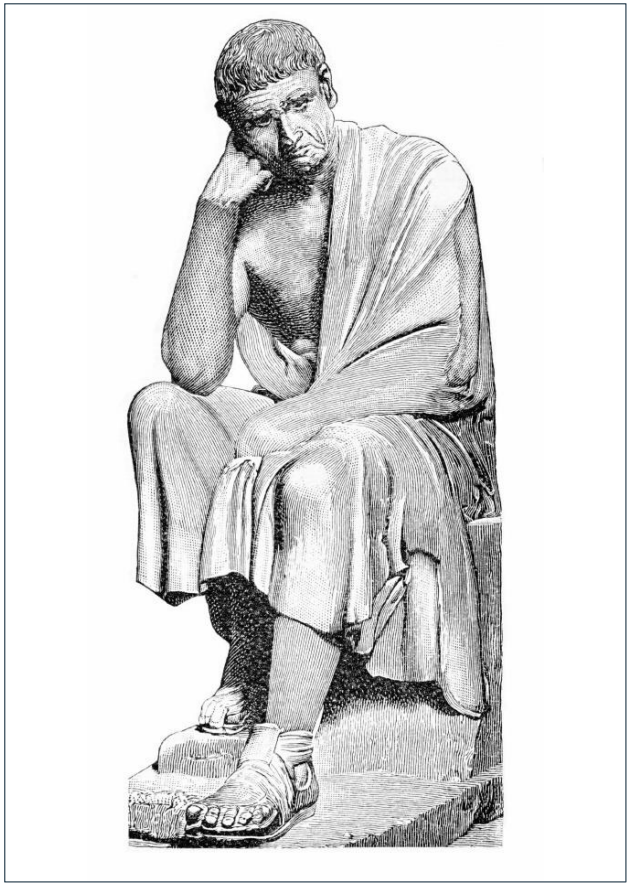
PEPPERL+FUCHS

Mathematische Modellierung versus Realität

- **Edmund Weitz, Konkrete Mathematik (nicht nur) für Informatiker, Seite 758:** „Man muss klar trennen zwischen der mathematischen Theorie einerseits und auf der anderen Seite der Interpretation ihrer Ergebnisse, die auf Modellbildung beruht. Die Wahrscheinlichkeitsrechnung liefert definitiv korrekte Resultate; nur haben diese mit der Welt außerhalb der Mathematik zunächst mal nichts zu tun. Wenn man Sie verwendet, um Aussagen über die Wirklichkeit zu machen, dann verlässt man den sicheren Hafen der Mathematik.“
- **Albert Einstein:** „Insofern sich die Sätze der Mathematik auf die Wirklichkeit beziehen, sind sie nicht sicher, und insofern sie sicher sind, beziehen sie sich nicht auf die Wirklichkeit.“
- **Wikipedia:** „Während über den mathematischen Umgang mit Wahrscheinlichkeiten weitgehend Einigkeit herrscht (siehe Wahrscheinlichkeitstheorie), besteht Uneinigkeit darüber, worauf die Rechenregeln der mathematischen Theorie angewendet werden dürfen.

Mathematische Modellierung versus Realität

- **Stanislav Andreski, Hexenmeister der Sozialwissenschaften, Seite 145:**
  „Wogegen ich argumentiere, ist das seelenverderbte Tabu auf alles, was nicht quantifiziert werden kann, und **die abergläubische Ehrfurcht vor jedem Gekritzel, das wie Mathematik aussieht**.“



iStockphoto

Restrisiko


GUTEN TAG! ICH BIN DIE STATIS-TISCHE WAHR-SCHEINLICHKEIT.
UND ICH BIN DAS RESTRISIKO.
KO
KO



Außergewöhnliche Möglichkeiten für die Umsetzung einer PLT-Sicherheitseinrichtung –

die experimentellsten Umsetzungsversuche die uns begegnet sind

Persönliche Vorstellung

Malika Mast

Geschäftsführerin RAMSYS GmbH

- FS Eng im Arbeitsgebiet Explosion Protection

  Id.-Nr.: 0328/2019 (TÜV Süd)

- FS Eng für Maschinen

  # 14527/17 (TÜV Rheinland)

- FSCEA (Functional Safety Certified Engineer Application)

  A031_01255/18 (TÜV Nord)



Kontaktdaten:

Hervester Straße 36

46286 Dorsten

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

m.mast@ramsys.org

www.ramsys.org

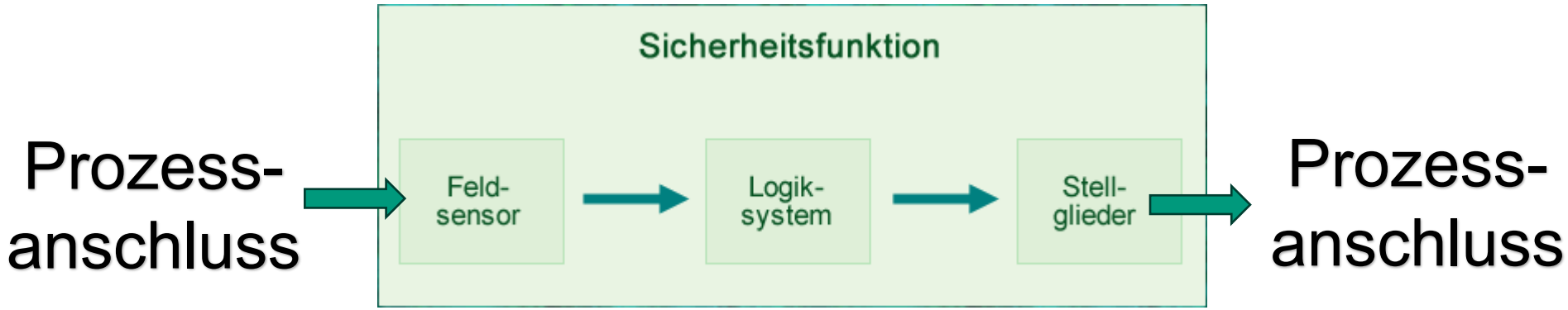
Agenda

- Intention des Vortrages
- Limitierende Faktoren bei einer PLT-Sicherheitseinrichtung
- Praxisbeispiele
- Zusammenfassung

I. Intention des Vortrages

Intention des Vortrages

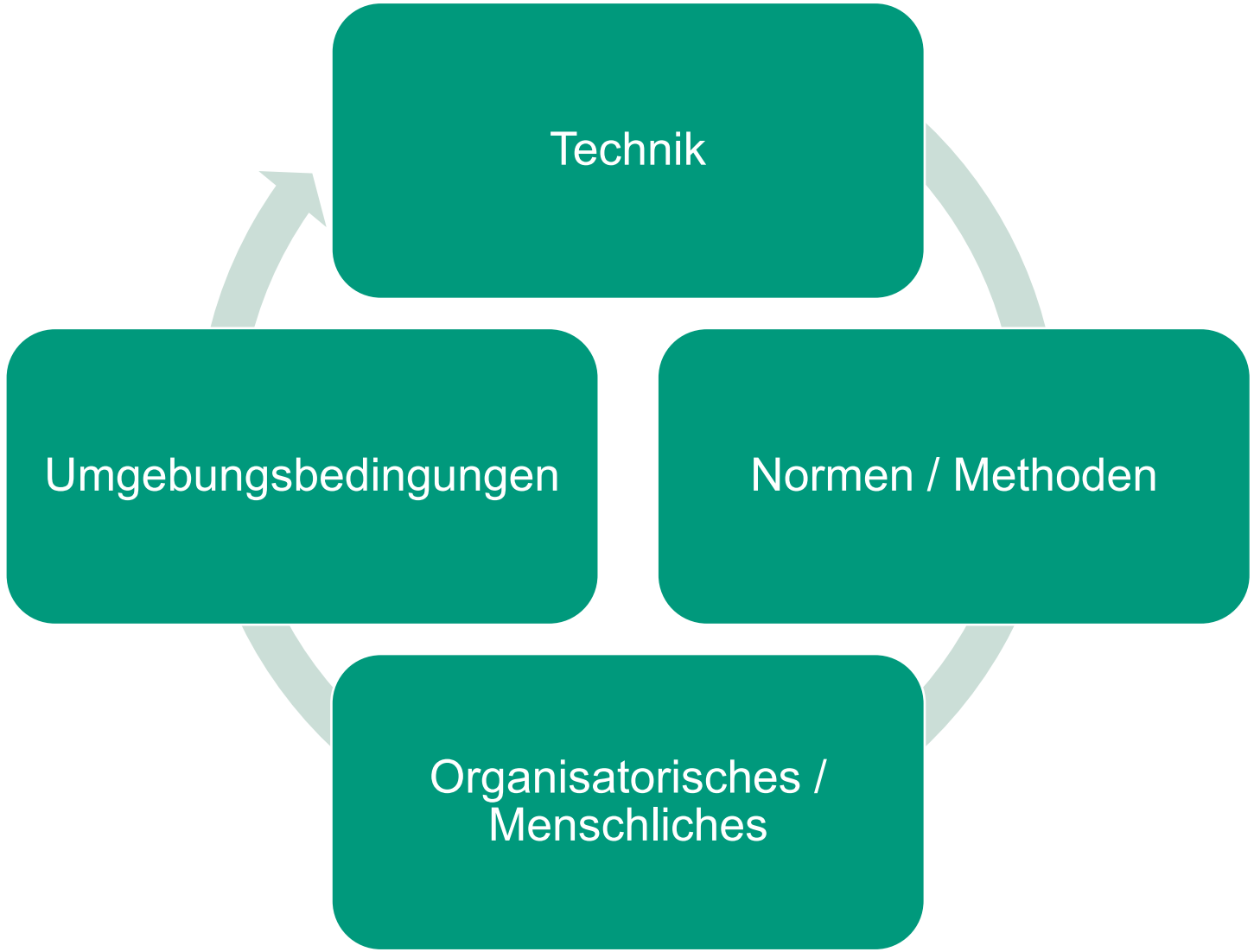
- Der Ablauf einer PLT-Sicherheitseinrichtung ist allgemein bekannt



- Bei der Umsetzung gibt es verschiedenste Möglichkeiten diesen Aufbau anzuwenden
- Ich möchte Ihnen heute einfach mal ein paar Beispiele aus der Praxis zeigen und zur Diskussion anregen

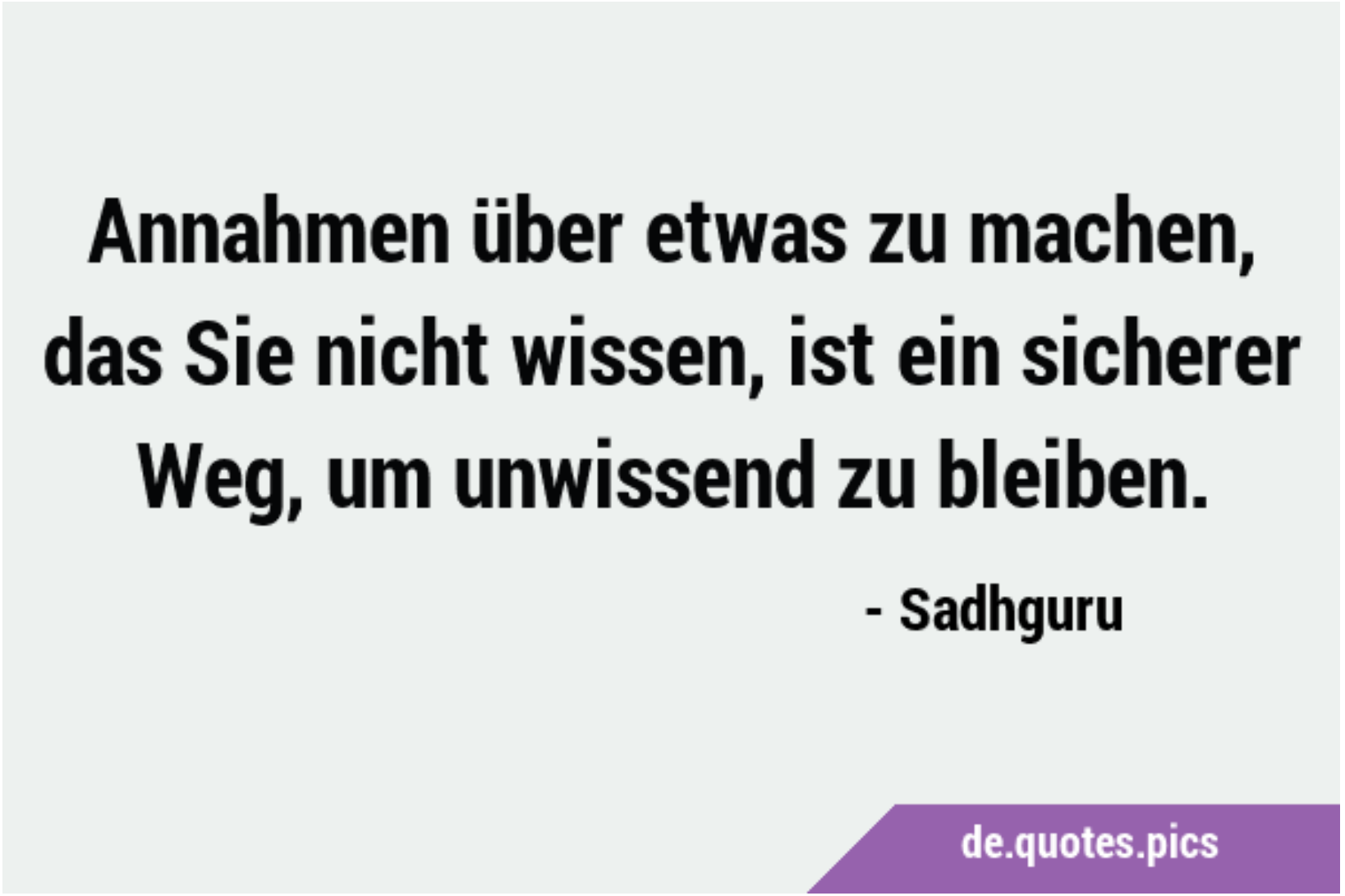
II. Limitierende Faktoren bei einer PLT-Sicherheitseinrichtung

Limitierende Faktoren bei einer PLT-Sicherheitseinrichtung



Limitierende Faktoren bei einer PLT-Sicherheitseinrichtung

RAMSYS
DAS machen Ingenieure



III. Praxisbeispiele

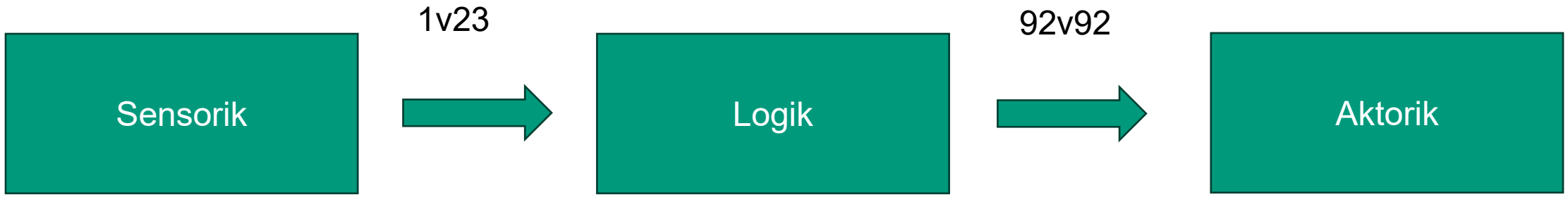
Praxisbeispiel: 1

RAMSYS
DAS machen Ingenieure

- Generell besteht keine Nummerische Begrenzung in der Norm
- Gerade bei Bestandsanlagen, bei denen Nachträglich eine Risikobeurteilung durchgeführt wird, kommt es zu Kuriosen Fällen
- Sätze wie:
  - Wir sind hier eh Redundanz, schreib einfach mal SIL-3 auf.
  - Wir haben hier ja eh noch Ventile oder Transmitter. Nimm die mal alle mit auf. Mehr kann ja nicht schaden.
- Führen gerne zu folgendem Beispiel

Praxisbeispiel: 1

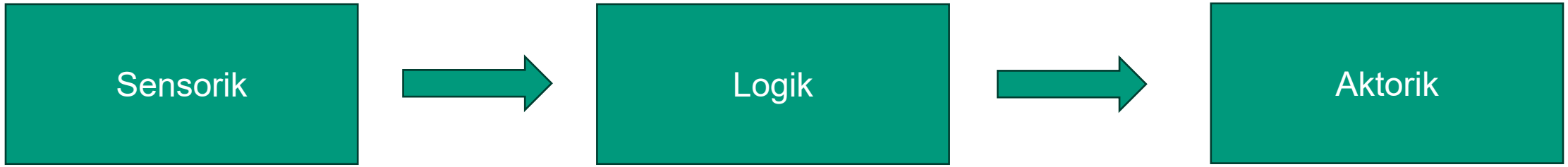
- Der bisher größte Kreis der uns begegnet ist.



- Ist eine solche Verschaltung sinnvoll?

Praxisbeispiel: 2

- Wir steigern uns jetzt langsam, aber bleiben erstmal bei der einfachen Darstellung



- Gerade sind wir nach oben / unten gegangen (Anzahl der Sensoren / Aktoren)
- Es gibt aber auch noch eine Zweite Richtung. Die Frage die man sich stellen kann. Wie sind die Pfeile zwischen Sensorik → Logik und Logik → Aktorik begrenzt?
- Bei Änderungen an der Anlage kann es vorkommen, dass Systeme / Schränke ausgetauscht werden bzw. eine SSPS hinzugefügt wird. In diesem Fall ist die Schaltung zeitlich sehr gewachsen.

Praxisbeispiel: 3

- Ein Beispiel was vielleicht mehrere von Ihnen schon gesehen haben



Praxisbeispiel: 4

- Als letztes Beispiel: Der etwas andere Aktor

Sensorik → Logik →



Aufgaben:
Mit einem Gaswarngerät vor Ort gucken gehen,
Wie Schlimm die Lage wirklich ist.

Was denken Sie darüber?

Praxisbeispiel: 4

- Als letztes Beispiel: Der etwas andere Aktor

- Welche Zuverlässigkeit hat ein Mensch, den Sie in eine Ex-Zone im Gefahrenfall schicken?

- Wiederkehrende Prüfungen?
  - Kontrolluntersuchung beim Arzt?
  - Jährliche Messung der 100m Sprintzeit?



Praxisbeispiel 5

Warum Prüfen?

Sensorkreis

Messstelle	L001
Hersteller	Endress + Hauser
Geräteart	Liquiphant
Gerätetyp	FTL81
PFD	1,10E-03

Messstelle	L001
Hersteller	Pepperl + Fuchs
Geräteart	Schaltverstärker
Gerätetyp	HiC 2841
PFD	1,04E-02

Messstelle	L001
Hersteller	HIMA
Geräteart	Digitaleingangskarte
Gerätetyp	X-DI-3201
PFD	2,41E-04

Logik

Gerät	CPU
Hersteller	Hima
Gerätetyp	X-CPU31
PFD	1,99E-04

Aktorkreis

Messstelle	V001
Hersteller	HIMA
Geräteart	Digitalausgangskarte
Gerätetyp	X-DO-3201
PFD	3,16E-04

Messstelle	V001
Hersteller	Pepperl + Fuchs
Geräteart	Ventilsteuerbaustein
Gerätetyp	HiC 2873
PFD	0,00E+00

Messstelle	V001
Hersteller	Samson
Geräteart	Magnetventil
Gerätetyp	3967-1
PFD	2,92E-02

Messstelle	V001
Hersteller	Samson
Geräteart	Pneum. Antrieb
Gerätetyp	3277
PFD	7,01E-03

Messstelle	V001
Hersteller	Samson
Geräteart	Hubventil
Gerätetyp	3241
PFD	4,49E-02

Praxisbeispiel 5

RAMSYS
DAS machen Ingenieure

Warum Prüfen?

Sensorik

Kanal A				PFD												Architektur				
Messstelle	Hersteller	Geräteart	Gerätetyp	λ_{DU} [FIT]	Prüfintervall T_0 PTC0	[Monate]	Prüfintervall T_1 PTC1	[Monate]	Prüfintervall T_2 PTC2	[Monate]	$\lambda_{0,A}$ [FIT] PTC0	$\lambda_{1,A}$ [FIT] PTC1	$\lambda_{2,A}$ [FIT] PTC2	ß	PFD_{avg}	Typ	SFF	HFT	Struktur	SC
L001	Endress + Hauser	Liquiphant	FTL81	3,00	0%	0	0%	0	100%	1000	0	0	3,00		1,10E-03	B	99,60%	0	1v1	3
L001	Pepperl + Fuchs	Schaltverstärker	HiC 2841	28,5	0%	0	0%	0	100%	1000	0	0	28,5		1,04E-02	A	83,00%	0	1v1	2
L001	HIMA	Digitaleingangskarte	X-DI-3201	5,51	0%	0	0%	0	100%	120	0	0	5,51		2,41E-04	B	99,64%	0	1v1	3
												PFD			1,17E-02		**SIL-Eignung der Architektur**			2

SSPS-CPU

			PFD					Architektur				
Gerät	Hersteller	Gerätetyp	λ_{DU} [FIT]	TI [a]	Struktur	ß	PFD_{avg}	Typ	SFF	Betriebs-bewährt	HFT	SC
CPU	Hima	X-CPU31	4,55	10	1v1		1,99E-04	B	99,76%		0	3
PFD							1,99E-04					3

Aktorik

Kanal A				PFD												Architektur				
Messstelle	Hersteller	Geräteart	Gerätetyp	λ_{DU} [FIT]	Prüfintervall T_0 PTC0	[Monate]	Prüfintervall T_1 PTC1	[Monate]	Prüfintervall T_2 PTC2	[Monate]	$\lambda_{0,A}$ [FIT] PTC0	$\lambda_{1,A}$ [FIT] PTC1	$\lambda_{2,A}$ [FIT] PTC2	ß	PFD_{avg}	Typ	SFF	HFT	Struktur	SC
V001	HIMA	Digitalausgangskarte	X-DO-3201	7,21	0%	0	0%	0	100%	120	0	0	7,21		3,16E-04	B	99,62%	0	1v1	3
V001	Pepperl + Fuchs	Ventilsteuerbaustein	HiC 2873	0,00	0%	0	0%	0	100%	1000	0	0	0,00		0,00E+00	A	100,00%	0	1v1	3
V001	Samson	Magnetventil	3967-1	80,00	0%	0	0%	0	100%	1000	0	0	80,00		2,92E-02	A		0	1v1	2
V001	Samson	Pneum. Antrieb	3277	19,20	0%	0	0%	0	100%	1000	0	0	19,20		7,01E-03	A	94,00%	0	1v1	2
V001	Samson	Hubventil	3241	123,00	0%	0	0%	0	100%	1000	0	0	123,00		4,49E-02	A	78,00%	0	1v1	2
												PFD			8,14E-02		**SIL-Eignung der Architektur**			2

Praxisbeispiel 5

- **Warum Prüfen?**
- Einen solch „einfachen“ Aufbau mit entsprechend geeigneten Geräten kann ich in der Theorie sehr weit ausreizen.

Ergebnis

Teil	PFD_{avg}	SIL_{PFD}	SIL_{HFT}	SIL
Sensor	1,17E-02		2	
CPU	1,99E-04		3	
Aktor	8,14E-02		2	
Ergebnis SIF	9,34E-02	1	2	1
Vorgabe erfüllt				**JA**

- → Dieses Ergebnis ist mit einem Austausch alle 1000 Monate (ca. 83 Jahre) gerechnet und ich erreiche immer noch einen SIL-1

Praxisbeispiel 5

- **Warur**
- Einen der Theori

Ergebnis

Teil
Sensor
CPU
Aktor
Ergebnis S
Vorgabe erfüllt

- → Die chnet und ic



IV. Zusammenfassung

Zusammenfassung

- Es ist gut das man diverse Freiheiten hat bei der Umsetzung einer PLT-Sicherheitseinrichtung
- Es sollte nie der Ingenieursmäßige Sachverstand vergessen werden
- Sollten Anlagen sicher sein, ja unbedingt! Aber es muss auch noch möglich sein, diese zu betreiben
- Der Faktor Mensch bleibt unberechenbar und ist keine Zuverlässige PLT-Sicherheitseinrichtung nach DIN EN 61508 / 61511

Eigene Erfahrungen

- Was sind Ihre Erfahrungen? Welche Beispiele kennen Sie?







Haben Sie Fragen?

RAMSYS
DAS machen Ingenieure

Vielen Dank für Ihre Aufmerksamkeit

Malika Mast Dipl. Ing / Geschäftsführerin

E-Mail: M.Mast@ramsys.org

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

Mobil: 0171 / 3037392

FLUIDE SIL-MECHANIK

DUMDUMDUM DUDU DUMMDUMM
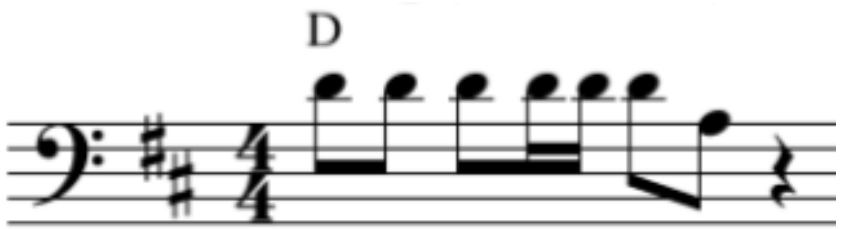
rösberg
Process Automation & IT Solutions



Marco Knödler
Co-Lead Large Capital Projects &
Subject Matter Expert Functional Safety

DUMDUM DUMDUDU DUMDUMM

rösberg
Process Automation & IT Solutions





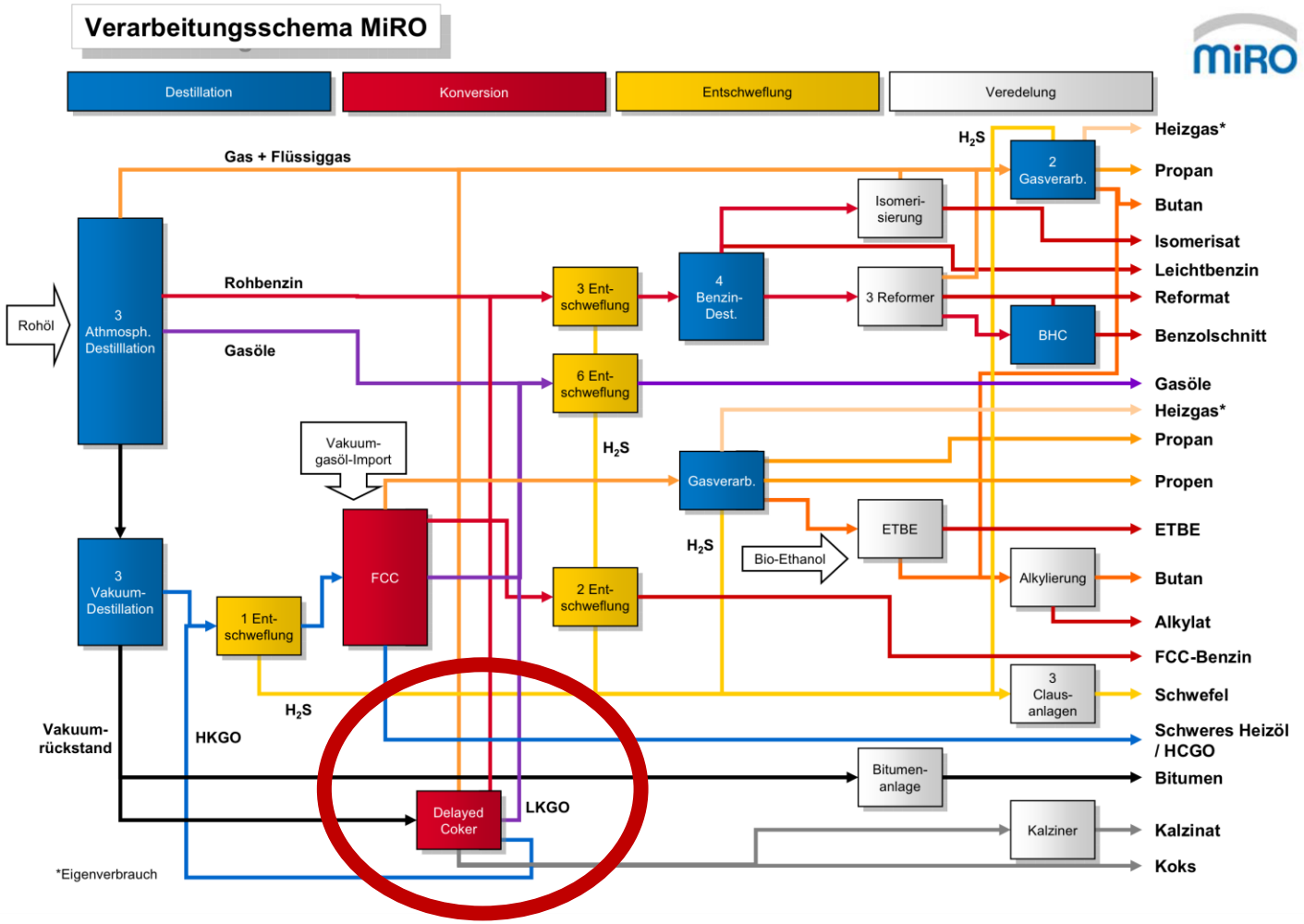
https://youtu.be/R5sO9dhPK8g?si=OUuEdymWgDXwrhP6



https://m.facebook.com/story.php?story_fbid=pfbid02ZEDfsw6yRZpA5btYeqF9SHHXFbDDgBL8cNJ27oSw9aEBpkZhWCQ9dR36KzJxBNFAl&id=100064776456173

PRAXISBEISPIEL AUS DEM DELAYED COKING PROZESS

rösberg
Process Automation & IT Solutions

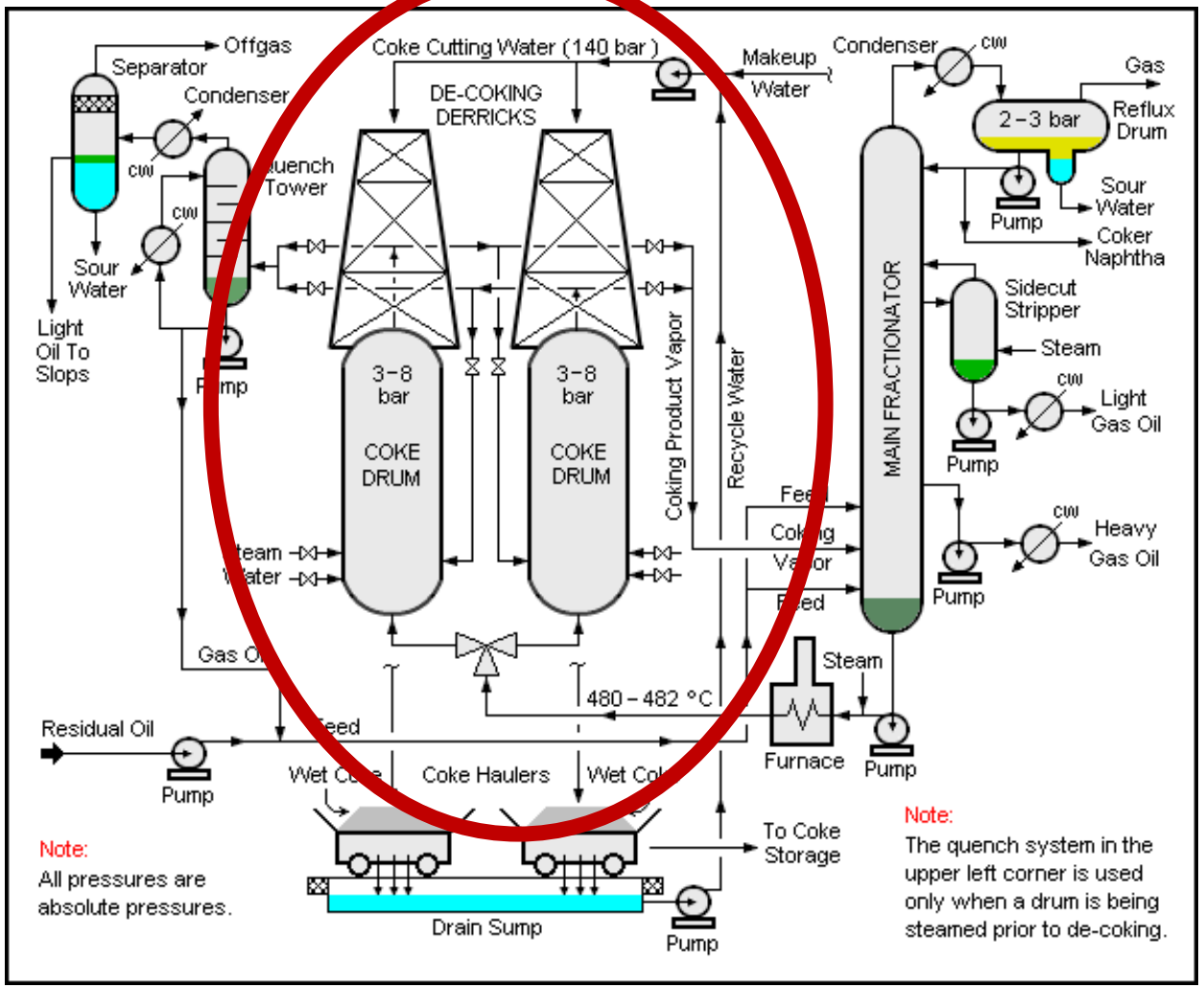


https://refiningcommunity.com/wp-content/presentations/Cologne-Germany-2008/DCU/Delayed-Coking-at-MiRO-Refinery-Esser-Schaefer-MiRO-DCU-Cologne-Germany-2008.pdf

PRAXISBEISPIEL AUS DEM DELAYED COKING PROZESS

rösberg
Process Automation & IT Solutions

In 1913, William Merriam Burton, working as a chemist for the Standard Oil of Indiana refinery at Whiting, Indiana, was granted a patent[8] for the Burton thermal cracking process that he had developed. […]
In 1929, based on the Burton thermal cracking process, Standard Oil of Indiana built the first delayed coker. It required very arduous manual decoking.[7]



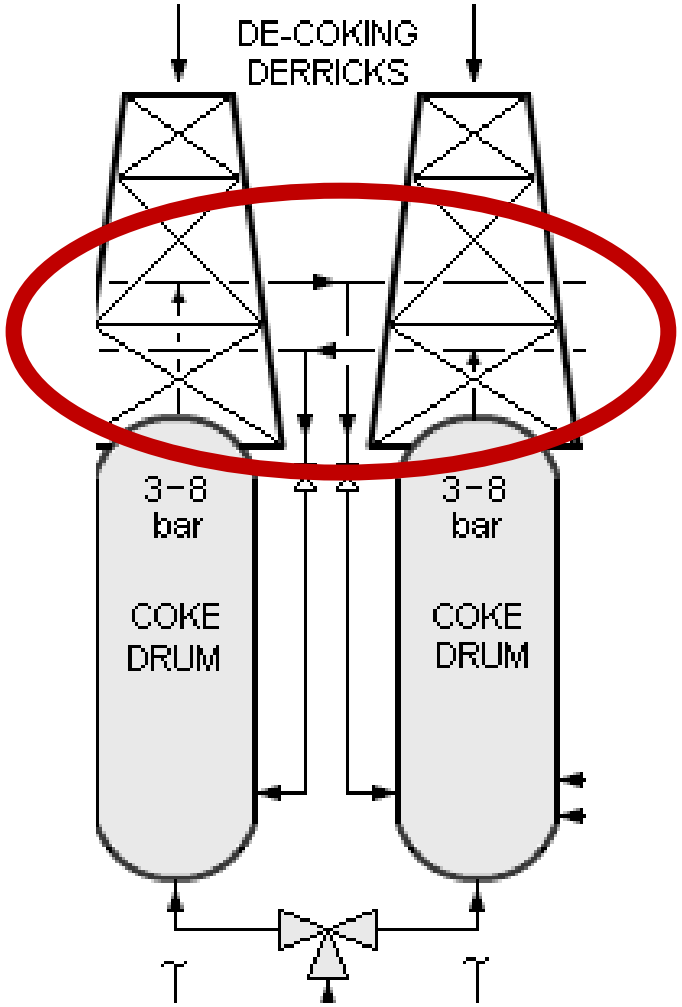
https://en.wikipedia.org/wiki/Delayed_coker#Schematic_flow_diagram_and_description

DE-COKING X DE-HEADING

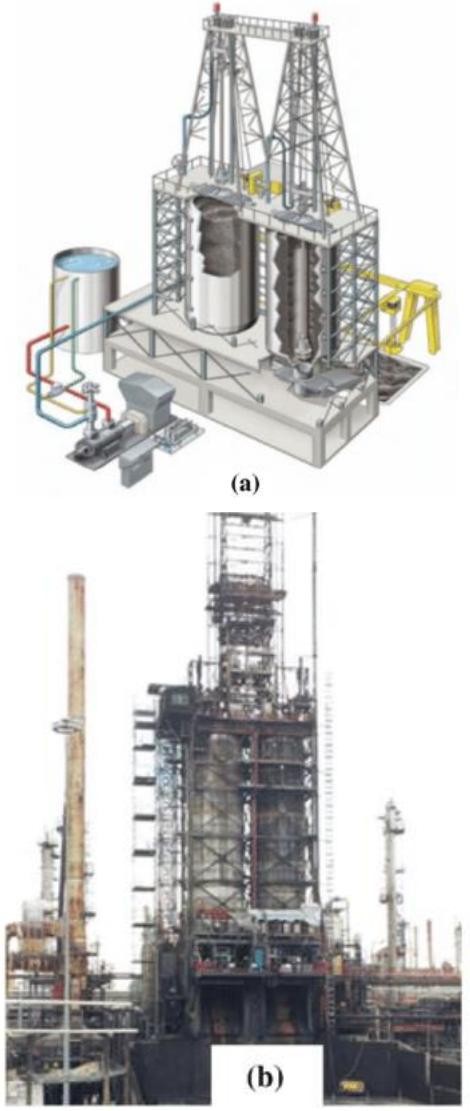
rösberg
Process Automation & IT Solutions

Drums werden paarweise in einem Zyklus von üblich 24-36h betrieben - Nach Reaktionsphase muss über „Coke Cutting“ der feste Petrokoks entfernt werden. Damit verbunden ist auch das zyklische, betriebliche De-Heading.
„Best practice“ (state of the art): Absperrarmaturen

https://www.google.com/search?q=delayed+coking+operation+deheading



https://en.wikipedia.org/wiki/Delayed_coker#Schematic_flow_diagram_and_description



https://www.researchgate.net/figure/Delayed-coker-operation-schematic-a-and-delayed-coker-b_fig2_269775838

EVOLUTION DES DE-HEADING

rösberg
Process Automation & IT Solutions

Chain-Hoist and Trolley are used to move the flange plate

Drill stem guide assembly manually positioned with chain hoist

Old Top Head Operations

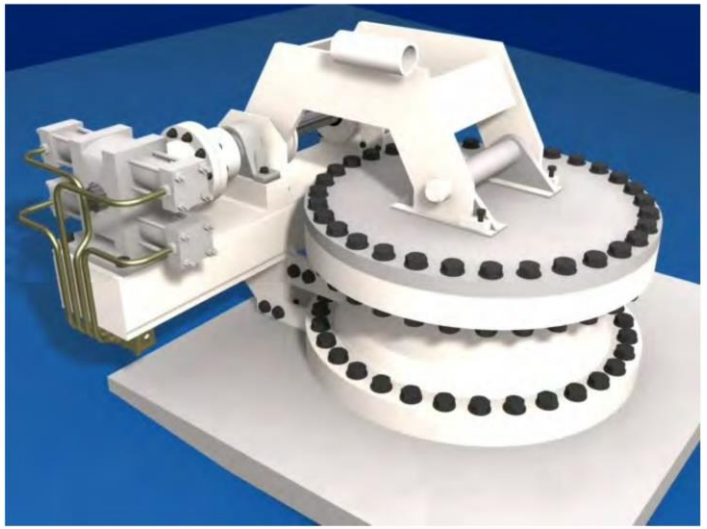


Unbolting the top head

Top Head Safety

Evolution of Facilities:

(4) Swing-Back Hydraulic Top Head*





* Foster-Wheeler & Tesco Design

https://refiningcommunity.com/wp-content/uploads/2017/07/Delayed-Coker-Coke-Drum-Top-Head-Safety-Moloney-ExxonMobil-DCU-Rio-de-Janiero-2014.pdf

EVOLUTION DES DE-HEADING

rösberg
Process Automation & IT Solutions

https://www.zjtechnologies.de/fileadmin/user_upload/downloads/Delayed_Coking_Top_Unheading.pdf

Delayed Coking Top Unheading

The DC Top Unheading device design is based on our well proven and multiple used Double Disc Through Conduit Type Gate Valve.
Its properties were increased for the higher demand for pressure and frequent tightening performance in the delayed Coker application.



Was ist die Sicherheitsfunktion des/der Unheading Devices?

- Prozess läuft bei bis zu 7 bar, 500 Grad C in ca. 30m hohen Reaktoren („Drums“) mit ca. 9m Durchmesser
- „kompakte Designs“ mit 36“ Flansch werben mit „nur“ 6,5m Länge und Gewichten ab 7 Tonnen
- Kräfte bei (dicht) Schließen im 3-4-stelligen kN-Bereich

REALITY FICTION

rösberg
Process Automation & IT Solutions

BP starts new Whiting Coker



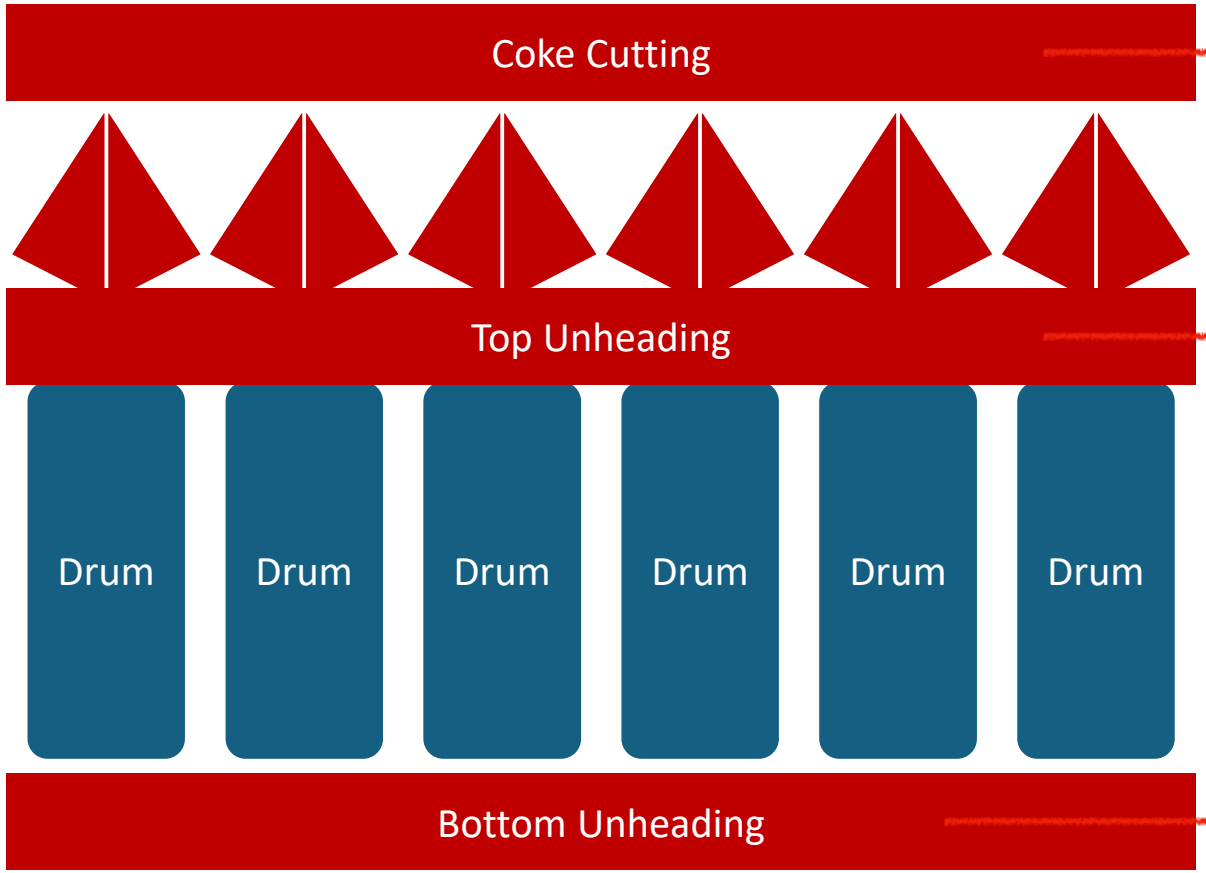
This is a work of fiction. Names,
characters, business, events and
incidents are the products of the
author's imagination. Any resemblance to actual persons
or actual events is purely coincidental.

https://chicago.suntimes.com/2023/5/18/23729343/bp-refinery-hit-40-million-fine-agrees-spend-200-million-pollution-control

https://www.bp.com/en/global/corporate/news-and-insights/press-releases/bp-completes-commissioning-of-whiting-refinery-units.html

REALITY FICTION - GESAMTSYSTEM

rösberg
Process Automation & IT Solutions





REALITY FICTION – UNHEADING ACTUATION & CONTROL

rösberg
Process Automation & IT Solutions

https://www.zjtechnologies.de/fileadmin/user_upload/downloads/Delayed_Coking_Top_Unheading.pdf

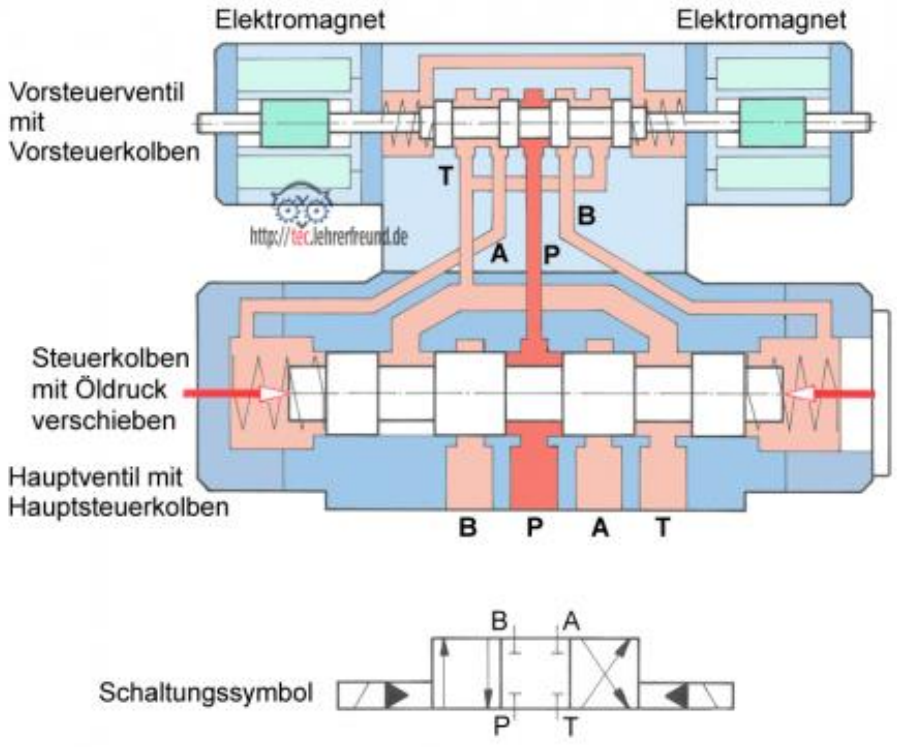
Delayed Coking Top Unheading

The DC Top Unheading device design is based on our well proven and multiple used Double Disc Through Conduit Type Gate Valve.
Its properties were increased for the higher demand for pressure and frequent tightening performance in the delayed Coker application.



- Kräfte bei (dicht) Schließen im 3-4-stelligen kN-Bereich
- Zylinder-Hub ca 1m

-> Vorsteuerventile

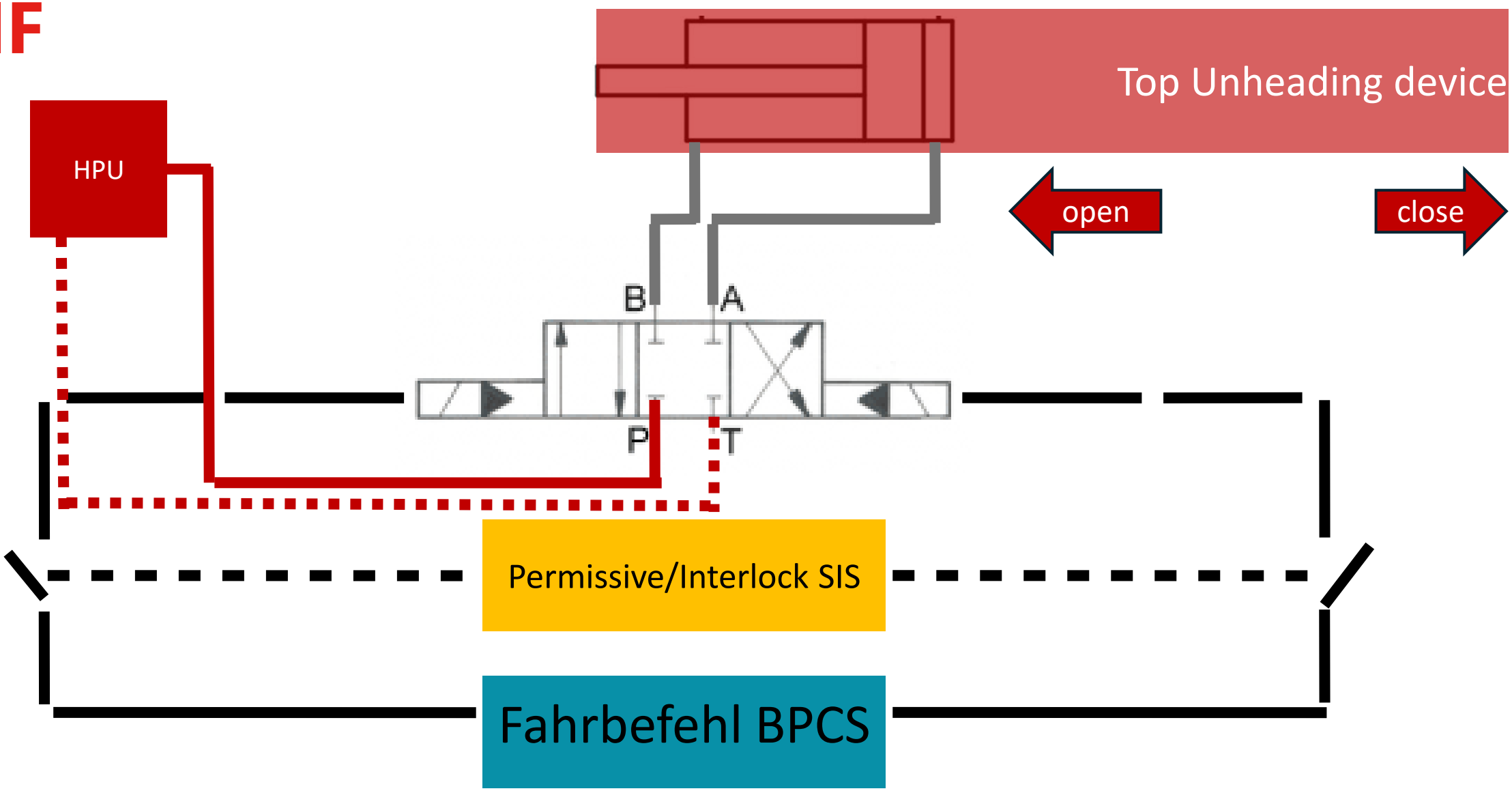


https://www.lehrerfreund.de/technik/1s/Hydraulische-Antriebe-9-Wie-funktioniert-ein-vorgesteuertes-Wegeventil/3802



https://www.blacinc.com/hpcu

REALITY FICTION - REALISIERTE SIF



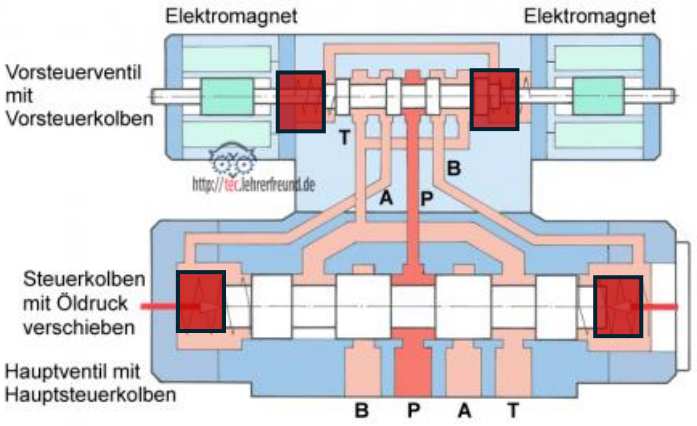
DUMDUM DUMDUDU DUMDUMM

rösberg
Process Automation & IT Solutions



Top Unheading device

open



HPU

In der Fluidmechanik ist der Übergang von flüssigem Wasser zu festem Eis und umgekehrt eine wichtige Eigenschaft, bekannt als die Anomalie des Wassers:



https://www.timeanddate.de/wetter/usa/chicago/rueckblick?month=12&year=2013

#SYSTEMATISCH RICHTIG

STATT ZUFÄLLIG FALSCH



DANKE FÜR EURE AUFMERKSAMKEIT - SICHERES ARBEITEN!

rösberg
Process Automation & IT Solutions



MARCO KNÖDLER

Co-Lead Large Capital Projects &
Subject Matter Expert Functional Safety

- VDI/VDE GMA Fa 2.12, 2.18, 3.22
- DKE 914.0.7, 11
- CEN/TC69/WG1
- NAMUR AK 4.5

SIL-Sprechstunde 2025 – außergewöhnliche Beispiele – Klassifikation von Sicherheitsfunktionen

Außergewöhnliche Beispiele können auch neue Arten von Sicherheitsfunktionen umfassen. Diese können sehr vielfältig sein.

Um hier nicht den Wald vor lauter Bäumen zu verlieren, ist eine Begriffsklärung notwendig.

Hierzu können wir versuchen, Sicherheitsfunktionen zu klassifizieren. Ich werde einige Vorschläge machen. Dazu stelle ich auch Beispiele aus anderen Gebieten als die Verfahrenstechnik vor.



Agenda:

1. **Beispiele für Sicherheitsfunktionen**
2. **Klassifikation von Sicherheitsfunktionen**
3. **Meine Fragen an Sie**



Ingo Rolle, im September 2025
ingorolle@outlook.de

Beispiele für Sicherheitsfunktionen

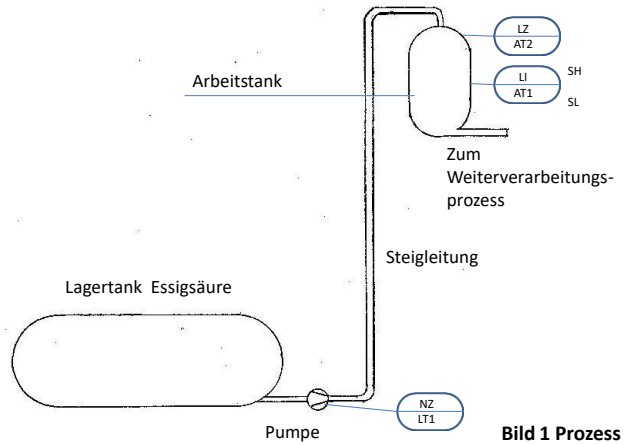
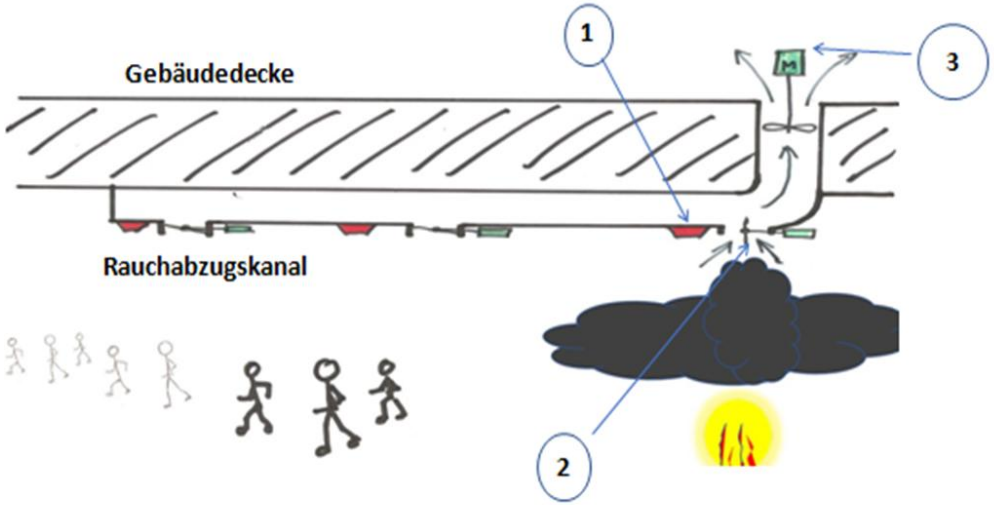


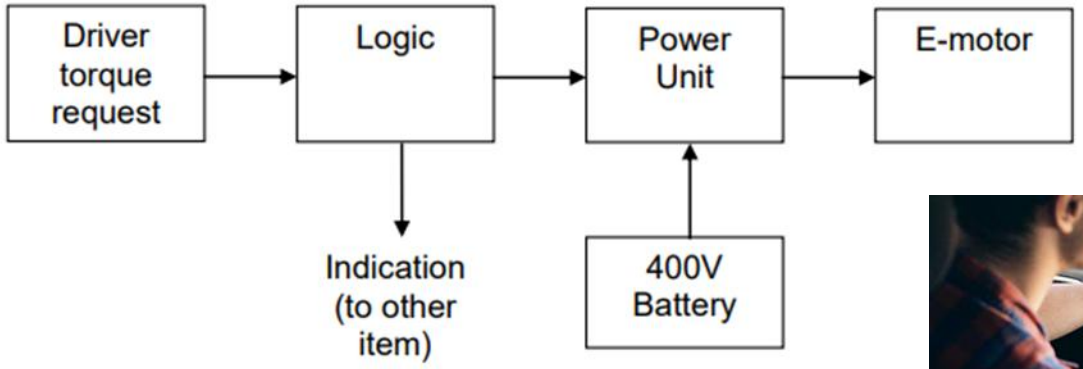
Bild 1 Prozess

„ Erreicht der Flüssigkeitsspiegel im Arbeitstank den Melder LZ AT2, ist die Pumpe NZLT1 abzuschalten“



Maschinelle Entrauchung eines Gebäudes mit Menschenansammlungen und eingeschränkten Fluchtmöglichkeiten

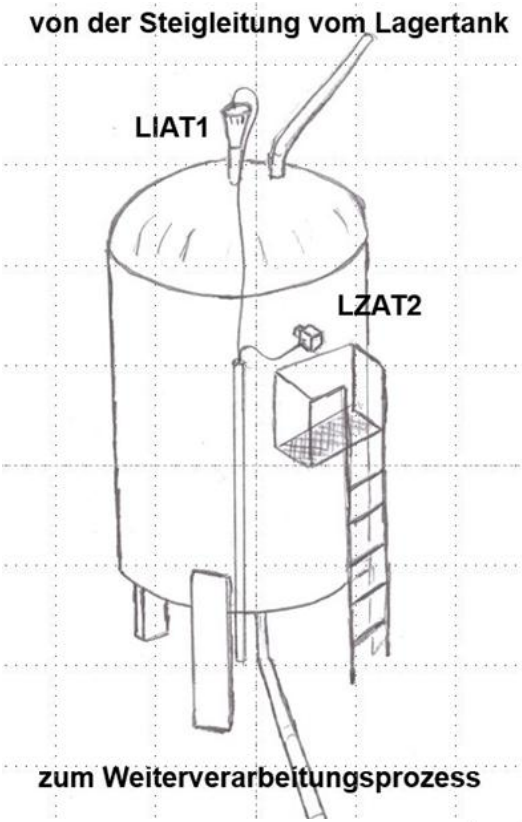
“Bei Entstehung von Rauch ist dieser abzusaugen, um die Zeit, während der die Menschen fliehen können, zu verlängern.”





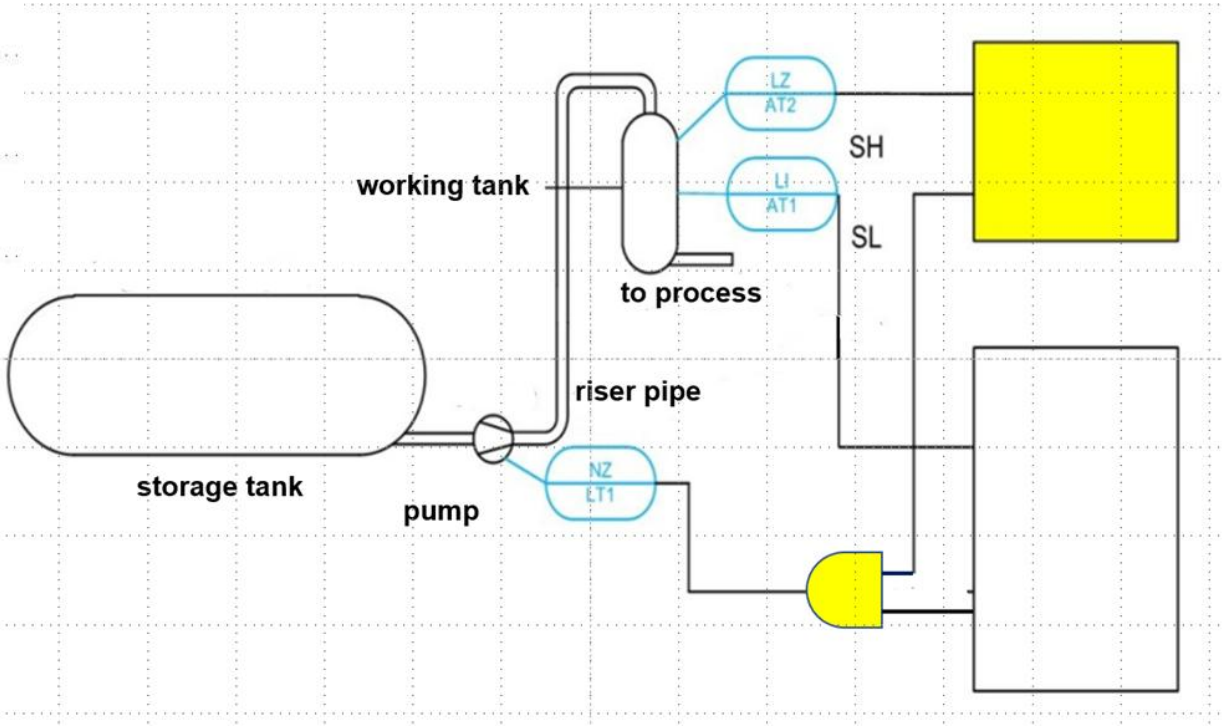
„Unbeabsichtigtes Beschleunigen ist zu vermeiden“
„Unbeabsichtigtes Verzögern ist zu vermeiden“

Beispiele für Sicherheitsfunktionen - Überlaufschutz



In einer Lebensmittelfabrik wird 60%ige Essigsäure verarbeitet. Sie wird in einem Lagertank vorgehalten, von dort in einen im 4. Stockwerk gelegenem Arbeitstank gepumpt und aus diesem für die Weiterverarbeitung entnommen. Im Arbeitstank wird der Füllstand mit Hilfe von LIAT1 kontinuierlich gemessen. Diese Messeinrichtung verwendet das kapazitive Messprinzip.

Ist vom Weiterverarbeitungsprozess so viel Essigsäure aus dem Arbeitstank entnommen worden, dass die Minimummarke bei LIAT1SL unterschritten wird, so wird über eine SPS die Pumpe NZLT1 eingeschaltet. Wird die Maximummarke bei LIAT1SH erreicht, so wird die Pumpe wieder ausgeschaltet.

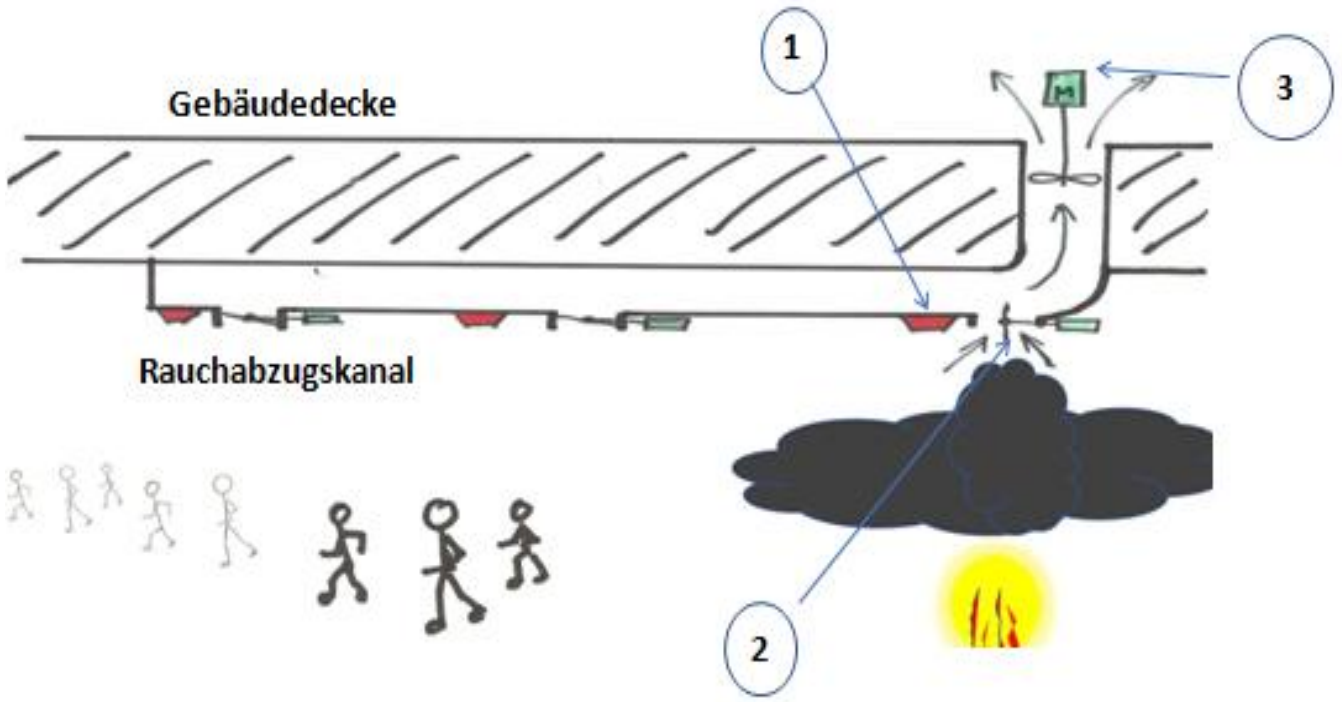


Sicherheitsfunktion:

„ Erreicht der Flüssigkeitsspiegel im Arbeitstank den Melder LZ AT2, ist die Pumpe NZLT1 abzuschalten“

Ingo Rolle, im September 2025

Beispiele für Sicherheitsfunktionen – maschinelle Entrauchung



Maschinelle Entrauchung eines Gebäudes mit Menschenansammlungen und eingeschränkten Fluchtmöglichkeiten

“Bei Entstehung von Rauch ist dieser abzusaugen, um die Zeit, während der die Menschen fliehen können, zu verlängern.”

Ein typisches Szenario:

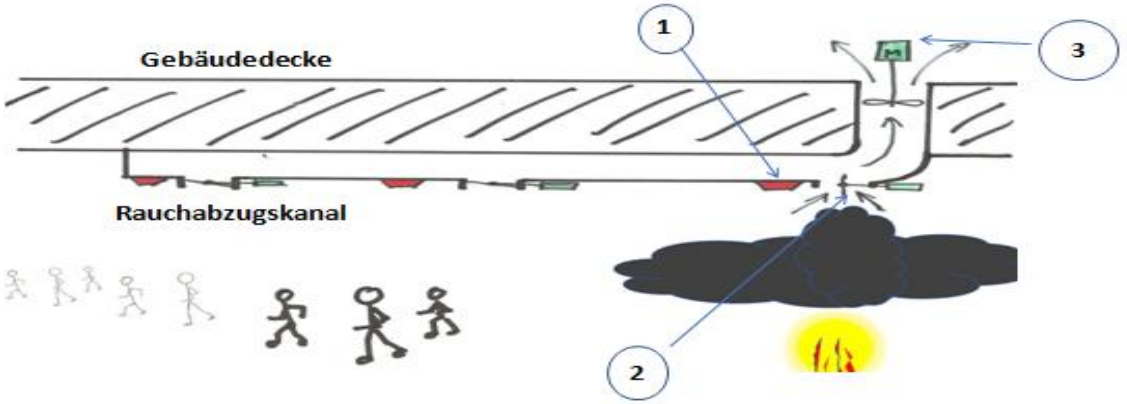
Der Rauchdetektor 1 stellt fest, dass sich an dieser Stelle Rauch entwickelt.

Daraufhin öffnet ein elektromotorisch angetriebener Schieber die Öffnung im Rauchabzugskanal 2.

Der Ventilator 3 startet und beginnt mit der Rauchabsaugung.

Bei Eintreffen der Feuerwehr muss es die Steuerung ihr ermöglichen, die Kontrolle über die weiteren Aktionen zu übernehmen

Beispiele für Sicherheitsfunktionen – maschinelle Entrauchung



Das System muss hierbei Verriegelungsbedingungen beachten und Entscheidungen treffen:

Es dürfen nur diejenigen Öffnungen im Abzugskanal geöffnet werden, unter denen Rauch festgestellt wurde, und auch hiervon nur eine maximale Anzahl, andernfalls würde die Förderleistung des Ventilators nicht ausreichen.

Startet der Ventilator, ohne dass Abzugsöffnungen geöffnet sind, wird er den Abzugskanal durch Unterdruck zerstören.

Als Spannungsversorgung wird das öffentliche Netz genutzt. Da Szenarien denkbar sind, in denen ein Brand ausbricht und gleichzeitig die öffentliche Stromversorgung gestört ist, muss das System hiergegen tolerant sein. Als Redundanz wird eine Einspeisung aus einer anderen Stelle des öffentlichen Netzes und eine Notstromversorgung aus Batterien vorgesehen.

Idee zu diesem Beispiel: Klaus Wagner/HIMA

Beispiele für Sicherheitsfunktionen – Drehmomentanforderung

Unbeabsichtigtes Beschleunigen ist zu vermeiden

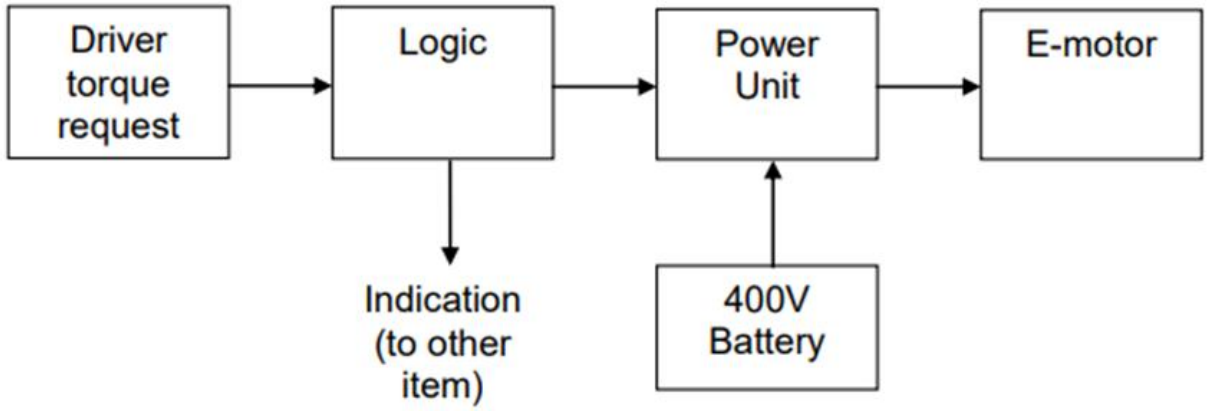
Unbeabsichtigtes Verzögern ist zu vermeiden

Hierbei wird die kontinuierliche Regelaufgabe der Drehmomenterzeugung als betriebliche Funktion aufgefasst und die Abweichungen werden sicherheitsgerichtet überwacht. Dann haben wir eine Anforderungsfunktionen.

Ebenfalls vorstellbar wäre die Spezifikation einer kontinuierlichen Sicherheitsfunktion:

Das Drehmoment an den Rädern muss der Stellung des (Gas)pedals folgen.

(Es hängt also viel von der Spezifikation ab)





Ingo Rolle, im März 2025. Das Beispiel ist von Dr. Alexander Rudolph.

Klassifizierung von Sicherheitsfunktionen nach der Betriebsart

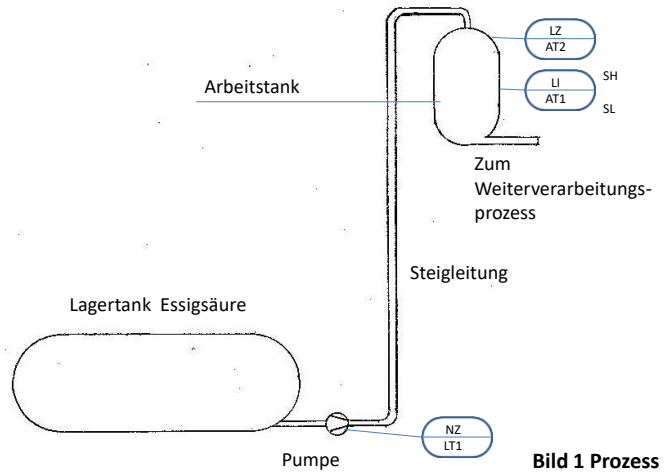


Bild 1 Prozess

Betriebsart mit niedriger Anforderungsrate

Betriebsart mit hoher Anforderungsrate (mehr als 1 x pro Jahr ??)

kontinuierliche Betriebsart

„Erreicht der Flüssigkeitsspiegel im Arbeitstank den Melder LZ AT2, ist die Pumpe NZLT1 abzuschalten“

Unbeabsichtigtes Beschleunigen ist zu vermeiden
Unbeabsichtigtes Verzögern ist zu vermeiden

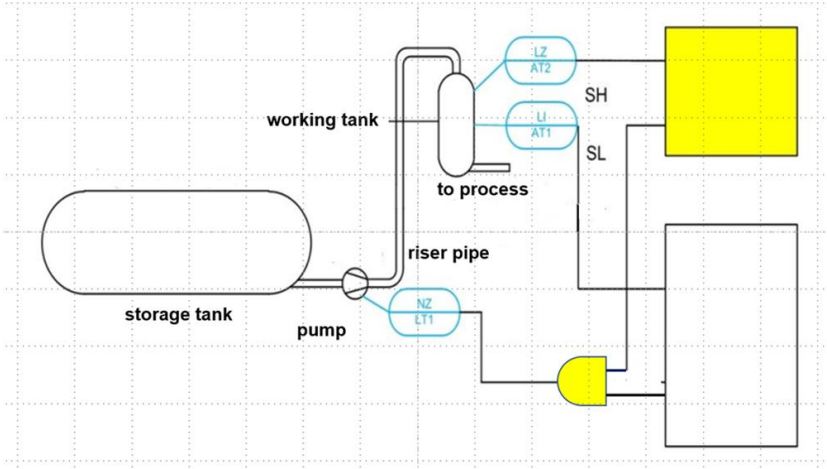
Das Drehmoment an den Rädern muss der Stellung des (Gas)pedals folgen.



Ingo Rolle, im September 2025

Klassifizierung sichere Konstruktion - Schutzmaßnahmen

Erreicht der Flüssigkeitsspiegel im Arbeitstank den Melder LZ AT2, ist die Pumpe NZLT1 abzuschalten



Definition: Eine Schutzmaßnahme liegt vor, wenn das System (Prozess + BPCS) auch ohne diese seine Funktion erbringen kann. Bei einer sicheren Konstruktion ist dies nicht möglich.

Schutzeinrichtung

sichere Konstruktion

Bei dieser Definition ist eine Schutzmaßnahme gleichbedeutend mit einem Anforderungssystem = „Demand System“.

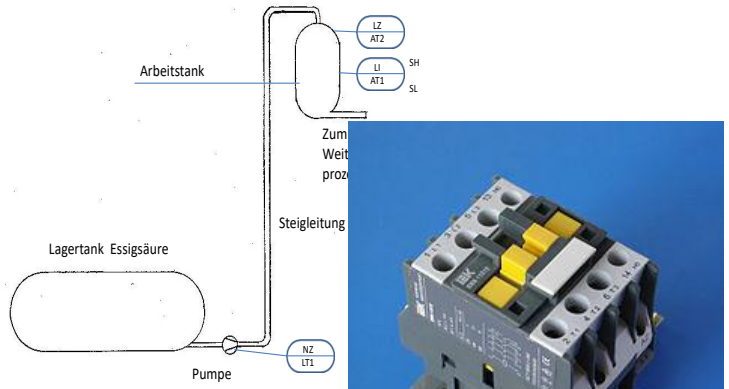
Unbeabsichtigtes Beschleunigen ist zu vermeiden
Unbeabsichtigtes Verzögern ist zu vermeiden

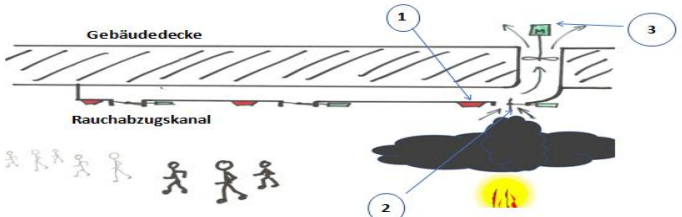
Das Drehmoment an den Rädern muss der Stellung des (Gas)pedals folgen.



Ingo Rolle, im September 2025

Klassifizierung von Sicherheitsfunktionen – Verhalten eines Anforderungssystems bei Auftreten einer Anforderung (de-energize to trip oder energize to trip)







Kann die EUC (Prozess) bei Auftreten einer Anforderung mit Hilfe einer sicheren einfachen Abschaltmaßnahme in den sicheren Zustand versetzt werden ?

Der Begriff „sichere einfache Abschaltmaßnahme“ bedarf einer Klärung. Jede Zustandsänderung benötigt Energie. Kommt diese Energie aus einem Energiespeicher, dem wir vertrauen, und vertrauen wir auch der Art der Energiewandlung und finden diese Dinge einfach, sprechen wir von „sicher und einfach“. Die Beurteilung ist also auch etwas subjektiv.

Der sichere Zustand ist erreicht, wenn das Schütz für die Pumpe abgefallen ist. Die Energie, um in diesen Zustand zu gelangen, wird dem Energiespeicher „Feder an den Schützkontakten“ entnommen. Diesem Speicher vertrauen wir. Die Energiewandlung geschieht, indem die gespeicherte Energie der Feder in Bewegungsenergie beim Öffnen der Kontakte umgewandelt wird. Das finden wir einfach und vertrauenswürdig. „de-energize to trip“

Der sichere Zustand im Falle der Anforderung dieser Sicherheitsfunktion ist die Entrauchung an der richtigen Stelle. Die Leistung, die hierfür erforderlich ist, ist sehr hoch und muss einem Energiespeicher entnommen werden, dem wir nicht vertrauen (z.B. Netzversorgung) oder nicht einfach ist (Akkumulatoren und Notstromdiesel). Gleiches gilt für die Energiewandlung. „energize to trip“

Ingo Rolle, im September 2025 Bilder aus Wikipedia

Klassifizierung von Sicherheitsfunktionen – Verhalten eines Anforderungssystems bei Auftreten einer Anforderung

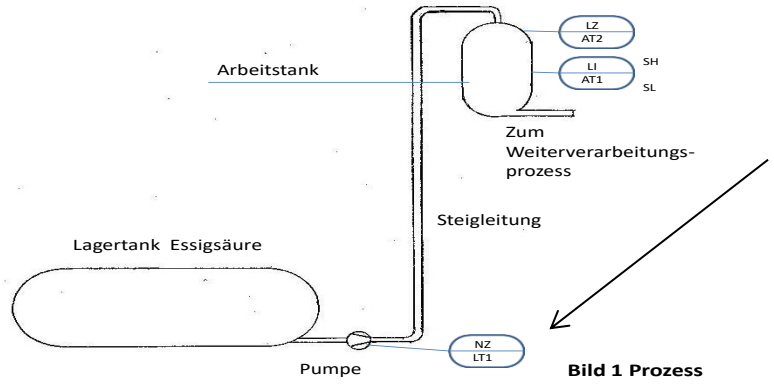
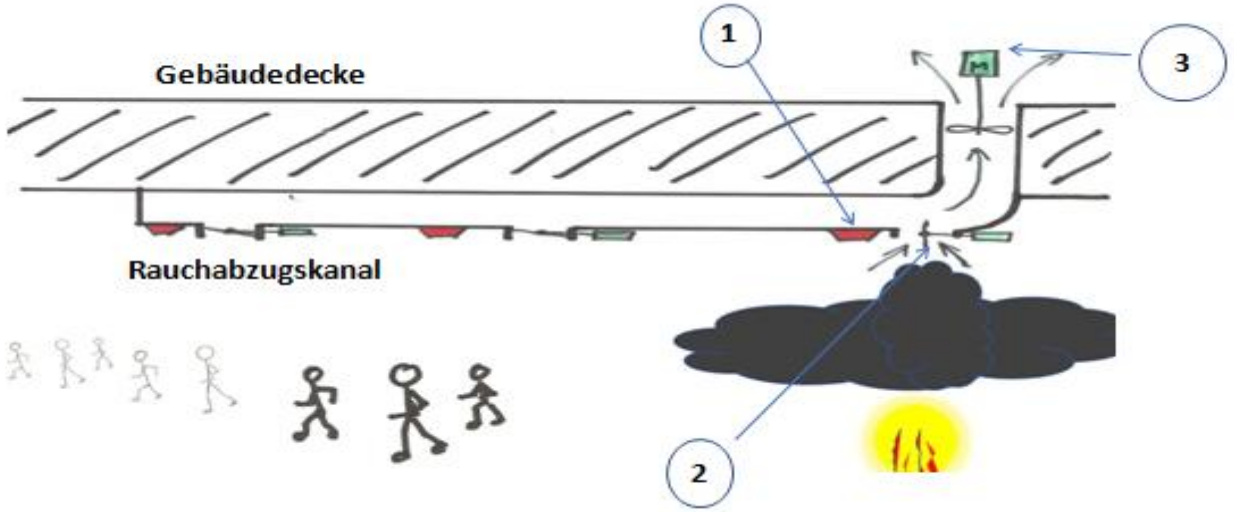


Bild 1 Prozess

Kann der sichere Zustand lange und ohne zusätzliche Energiezufuhr anhalten?

Das ist hier der Fall. Dieses ist ein typisches Szenario der chemischen Industrie oder des Maschinenbaues. Eine Schutzmaßnahmen versetzt den Prozess (EUC) durch eine einfache, sichere Abschaltmaßnahme in den sicheren Zustand, und dieser ist stabil. Zu seiner Aufrechterhaltung wird keine dauernde Leistung benötigt.

Im zweiten Beispiel ist das System von vornherein so ausgelegt, dass der sichere Zustand nur ca. 10 min anhält. Ständige Energiezufuhr ist erforderlich.



Ingo Rolle, im September 2025

Klassifizierung von Sicherheitsfunktionen - Verhalten des Systems bei Erkennen eines (internen) Ausfalls

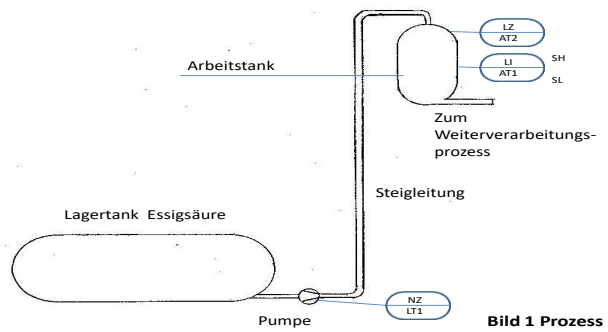
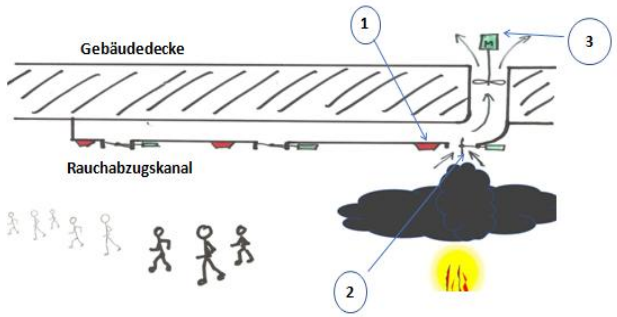


Bild 1 Prozess





Diese Sicherheitsfunktion kennt „sichere Ausfälle“. Sie versetzen den Prozess (EUC) mit Hilfe einer einfachen, sicheren Abschaltmaßnahme in einen sicheren Zustand, der ohne Leistungszufuhr anhält. Man nennt dies auch „fail safe“.

Fail-safe-Systeme sind in der Praxis weit verbreitet, meist als High-Demand im Maschinenbau oder Low-Demand in der chemischen Verfahrenstechnik. Ein sicherer Ausfall bedeutet bei ihnen das Ausführen des Aktionsteils der Sicherheitsfunktion. Dies hat die gleiche Wirkung wie ein Fehlalarm, englisch „nuisance trip“.

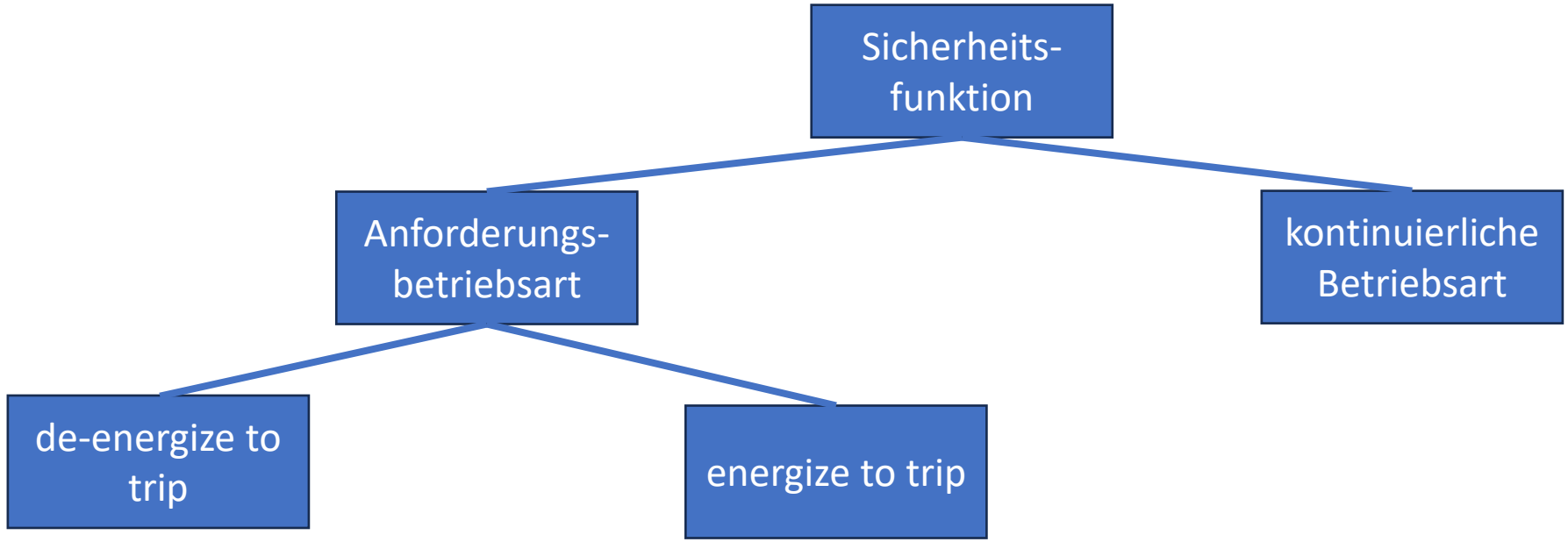
In einem Kanal dieser Systeme gibt es keine „sicheren Ausfälle“, weil einfache, sichere Abschaltmaßnahmen nicht möglich sind oder ein sicherer Zustand, der andauernd und ohne Leistungszufuhr aufrechterhalten werden kann, nicht existiert.
Wenn der andere Kanal oder ein Diagnosemechanismus einen Ausfall erkennt, sind Rückfallmechanismen notwendig („Degradationsstrategien“, z.B. anderer Kanal). Das System büßt einen Teil seiner Sicherheitseigenschaften ein (nämlich die Redundanz, es „degradiert“). Man nennt dies auch „fail operational“.
Die Degradationsstrategie wird beispielsweise fortgeführt durch:

- **Erreichung eines sicheren Zustands ohne Leistungszufuhr (Warnung an den Fahrer, rechts ranfahren und anhalten) oder**

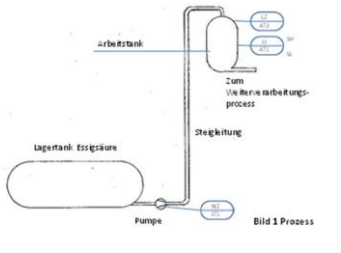
- **Instandsetzung des Systems (in die Werkstatt fahren, Service anfordern).**

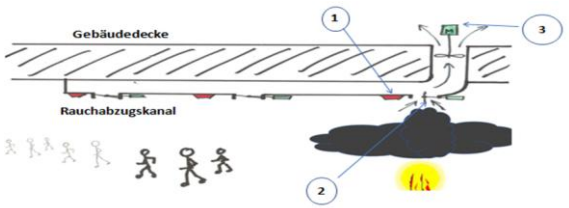
Ingo Rolle, im September 2025

Klassifizierung von Sicherheitsfunktionen – Versuch einer Taxonomie



typische Degradations-strategie	**fail-safe**	**fail-operational mit individueller Folgestrategie**	**fail-operational mit individueller Folgestrategie**

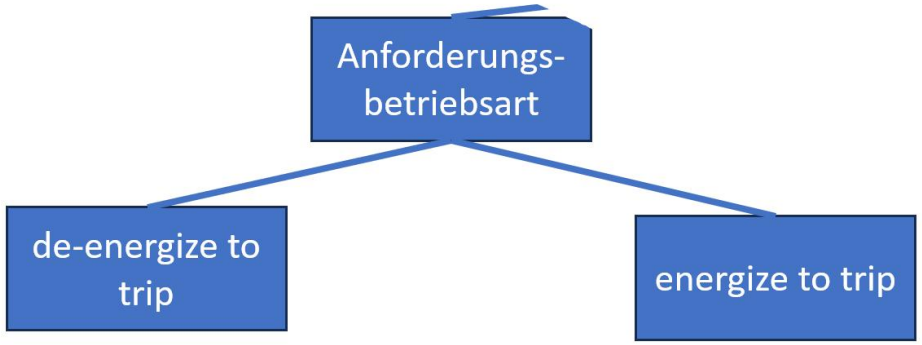




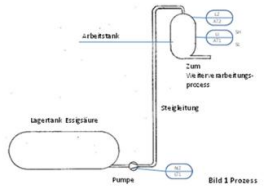


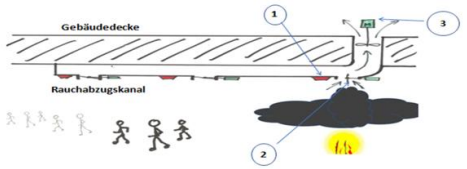
Ingo Rolle, Januar 2025

Klassifizierung von Sicherheitsfunktionen – Versuch einer Taxonomie



typische Degradations-strategie	fail-safe	fail-operational mit individueller Folgestrategie	fail-operational mit individueller Folgestrategie







Rolle, Januar 2025

Bemerkung: Energize to trip-Systeme fallen gewöhnlich genau im Fall der Anforderung aus. Damit die Sicherheitsfunktion trotzdem noch erbracht werden kann, muss eine Degradationsstrategie vom Typ „fail operational“ implementiert werden.

SIL-Sprechstunde 2025 – neue Typen von Sicherheitsfunktionen – meine Fragen an Sie

Sind die hier behandelten Sicherheitsfunktionen im Anwendungsbereich der IEC 61508 oder einer abgeleiteten Norm? Nach meiner Meinung ja.

– lässt einen weiten Bereich von Prinzipien, Verfahren und Maßnahmen zu, um funktionale Sicherheit für sicherheitsbezogene E/E/PE-Systeme zu erreichen, verwendet aber nicht ausdrücklich das Fail-Safe-Konzept. „Fail-Safe"-Konzepte und „inhärent sichere" Prinzipien können jedoch anwendbar sein, und der Einsatz solcher Konzepte ist zulässig, vorausgesetzt, dass die Anforderungen der zutreffenden Abschnitte in der Norm erfüllt werden.

d) gilt diese Norm für alle Typen sicherheitsbezogener E/E/PE-Systeme, einschließlich Schutzsysteme und Leit- oder Steuerungssysteme,

aus Einleitung und Anwendungsbereich der DIN EN 61508-1(VDE 0803-1):2011

Ist es klug, sie nach IEC 61508 zu behandeln? (Das Anwenden von Normen ist freiwillig.) Meine Meinung:

Es hat den Vorteil einer stärkeren Vereinheitlichung. Allerdings werden wir einige Methoden aus unserem Standard-Werkzeugkasten nicht mehr anwenden können. Hier muss Neuland betreten werden.



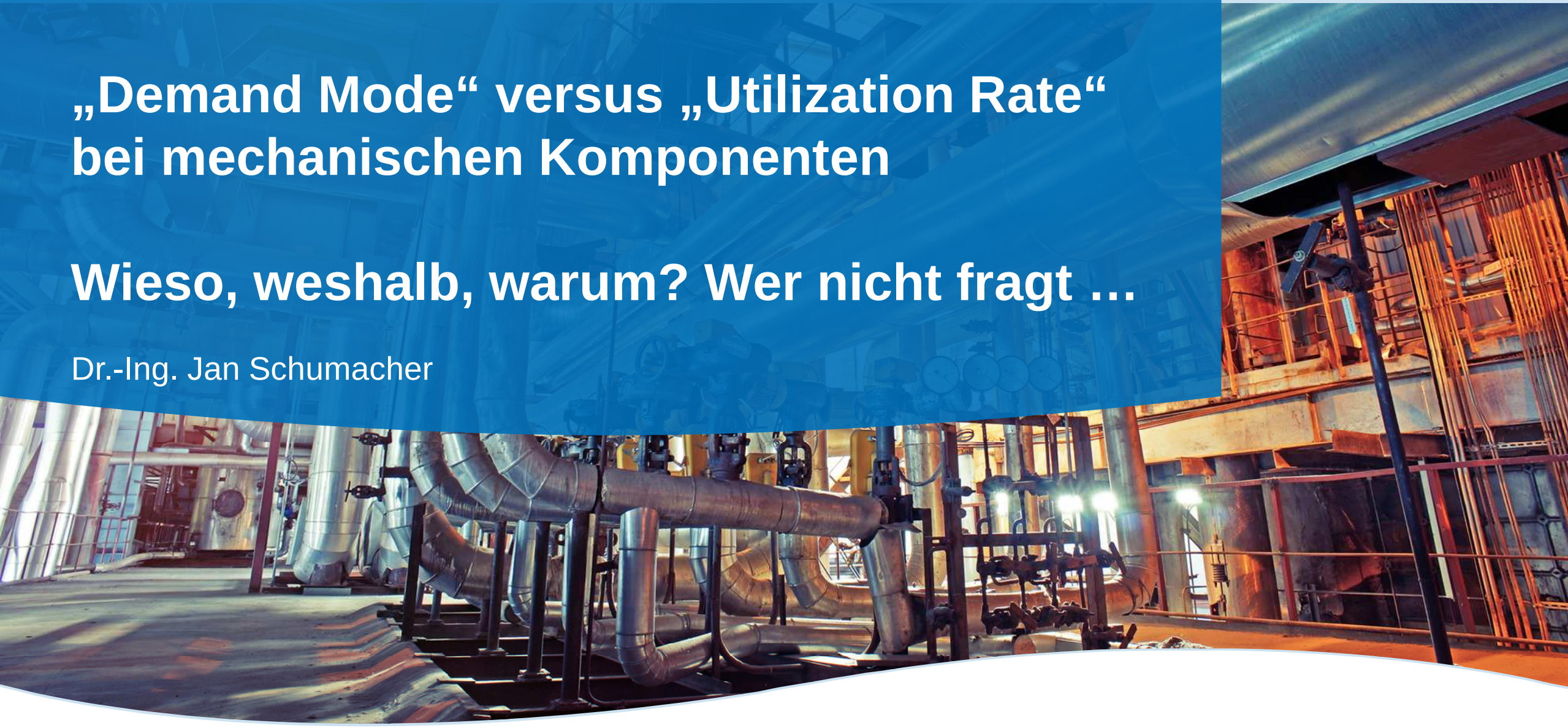
?

Ingo Rolle, im September 2025, Bild aus Pixabay

„Demand Mode“ versus „Utilization Rate“ bei mechanischen Komponenten

Wieso, weshalb, warum? Wer nicht fragt …

Dr.-Ing. Jan Schumacher



TÜVRheinland®
Genau. Richtig.

Grundlegendes zu mechanischen Komponenten

Mechanische Komponenten haben in der Regel …

… eine Jahrzehnte lang bewährte Funktionsweise.

… Jahrzehnte lang bewährte Werkstoffe.

… ein vorhersehbares Ausfallverhalten.

… direkten Kontakt zum Betriebsmedium.

… keine internen Redundanzen.

… keine integrierten Diagnosemöglichkeiten.

… nur wenige sichere Fehler.

… eine niedrige Anforderungsrate der Sicherheitsfunktion, aber eine häufige Anforderung der Betriebsfunktion.



Übliche sicherheitstechnische Kennwerte:

HFT = 0 / 1oo1

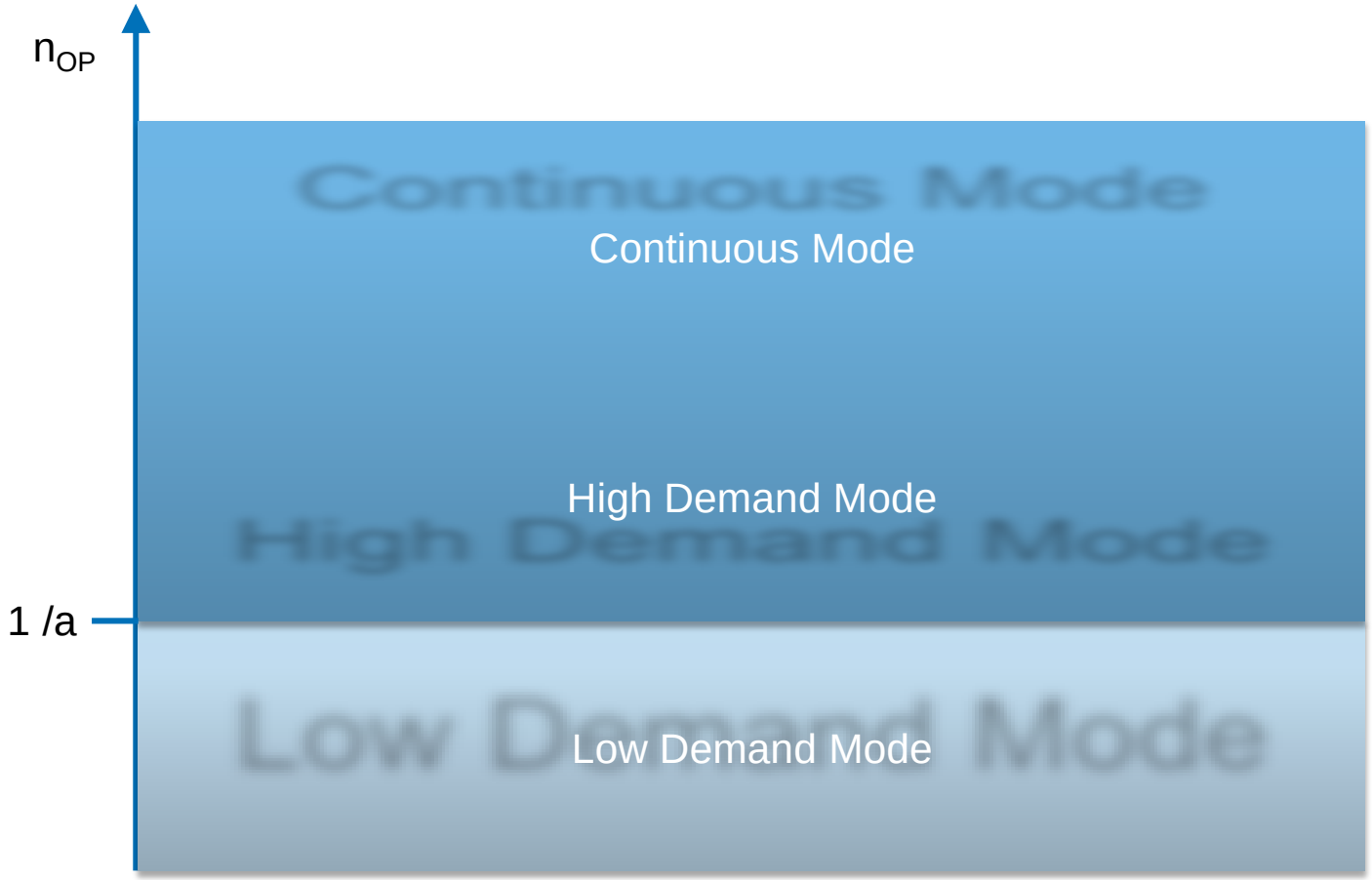
Typ A Element

SFF < 60 %

DC = 0 %

TÜVRheinland®
Genau. Richtig.

Wie oft wird die Sicherheitsfunktion angefordert?



TÜVRheinland®
Genau. Richtig.

DIN EN 61508-4

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

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

ANMERKUNG Das sicherheitsbezogene E/E/PE-System, das die Sicherheitsfunktion ausführt, hat normalerweise keinen Einfluss auf die EUC oder das EUC-Leit- oder Steuerungssystem, bis eine Anforderung auftritt. Wenn das sicherheitsbezogene E/E/PE-System ausfällt, so dass es nicht die Sicherheitsfunktion ausführen kann, dann kann es jedoch die EUC veranlassen, in einen sicheren Zustand zu wechseln (siehe IEC 61508-2, 7.4.6[NA2)]).

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

– **Betriebsart mit kontinuierlicher Anforderung (en: continuous mode):** wobei die Sicherheitsfunktion die EUC in einem sicheren Zustand als Teil des normalen Betriebs hält

TÜVRheinland®
Genau. Richtig.

Ist damit alles geklärt?

TÜVRheinland®
Genau. Richtig.

Was passiert,
wenn ich Elemente sowohl für Sicherheits- als auch für Betriebsfunktionen einsetze?

TÜVRheinland®
Genau. Richtig.

Wie kann ich Alterungs- und Verschleißeffekte berücksichtigen?

TÜVRheinland®
Genau. Richtig.

EN 17955:2024 „Functional Safety of safety-related automated valves“

3.9
utilization rate
total movements of the mechanical compliant item per year

Note 1 to entry: This includes but is not limited to movements due to demand of the safety function plus movements due to testing (automatic online diagnostic tests or manual tests) plus operations requested by the EUC control system.

Note 2 to entry: EN 61508-2 defines different modes of operation, which only consider the number of demands of the safety function per year. However, for mechanical compliant items the primary fault mechanism largely depends on the overall number of movements of the compliant item (including testing, demands by the EUC control system, etc.), rather than depending on the number of movements due to a demand on the safety function only. Therefore, this document defines a utilization rate in addition to the mode of operation to correctly consider different fault mechanisms like ageing, wear and fatigue.

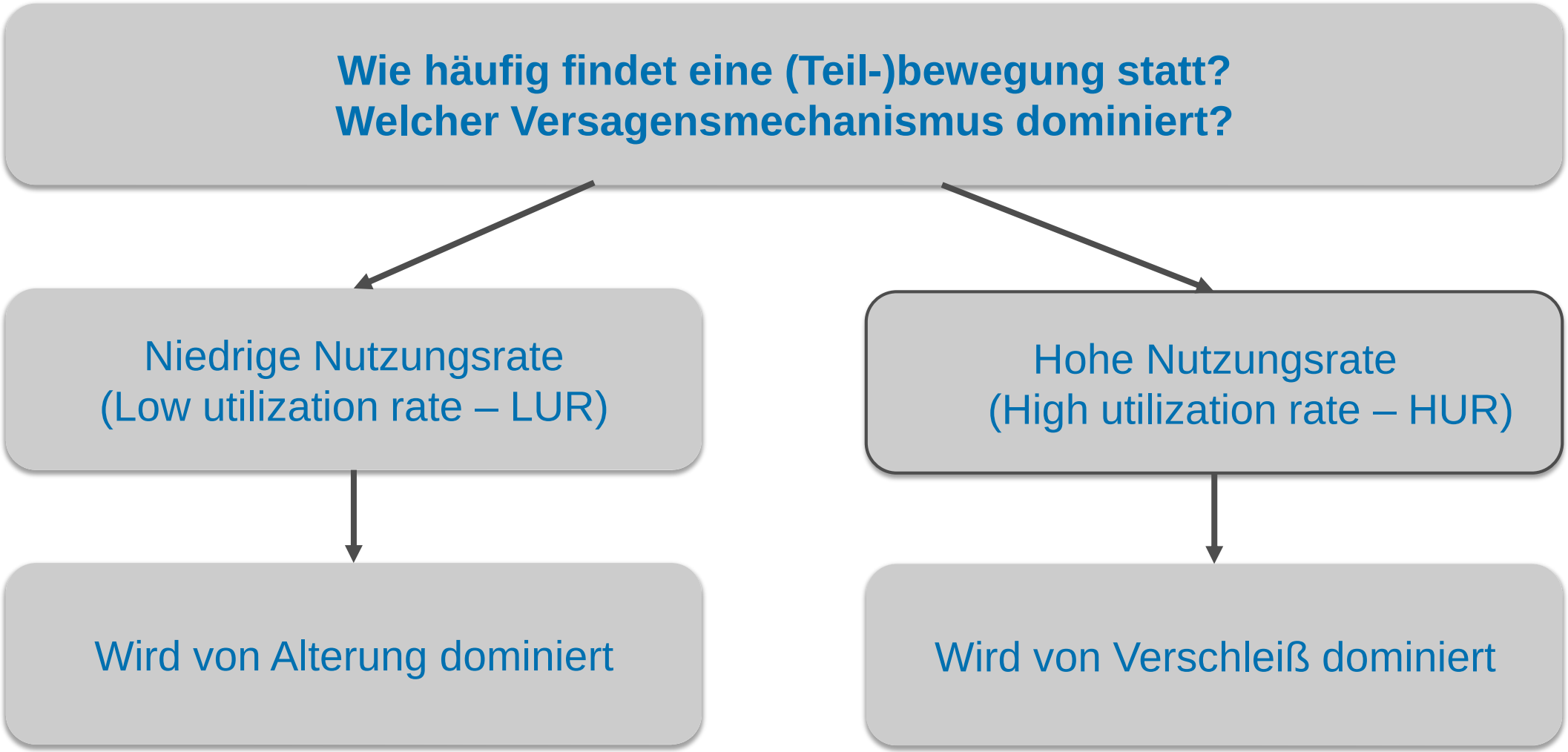
Note 3 to entry: The utilization rate of different compliant items in a safety-related function or a final element can differ, e.g. if some but not all compliant items are tested by a full stroke test or if some of the compliant items are used for basic process control as well.

Note 4 to entry: A partial stroke is considered as a movement and is therefore considered in the utilization rate.

Note 5 to entry: Since ageing effects depend more on the number of movements than on the distance of travel, the number of movements is decisive rather than the percentage of the stroke travelled or the absolute length of the stroke.

TÜVRheinland®
Genau. Richtig.

Definition der Nutzungsrate



TÜVRheinland®
Genau. Richtig.

Quantifizierung der Nutzungsrate

Table 6 — Number of operations per year and utilization rate

Total movements per year	**< 1**	**1 ... 500**	**> 500**
Assessment necessary?	No (optionally possible)	Obligatory	No (optionally possible)
Utilization rate	Low or optional assessment shows that “high” is more appropriate	Low or high depending on assessment result	High or optional assessment shows that “low” is more appropriate

TÜVRheinland®
Genau. Richtig.

Low Demand Mode
&
Low Utilization Rate

TÜVRheinland®
Genau. Richtig.

High Demand Mode
&
High Utilization Rate

TÜVRheinland®
Genau. Richtig.

Low Demand Mode
&
High Utilization Rate

TÜVRheinland®
Genau. Richtig.

High Demand Mode
&
Low Utilization Rate

TÜVRheinland®
Genau. Richtig.

Zusammenfassung

- EN 17955 spezifiziert die Anforderungen für mechanische Bauteile
- Beim Erarbeiten der Norm wurde die *Utilization Rate (Nutzungsrate)* neu definiert
- Durch Kenntnis und Beachtung der tatsächlichen Nutzungsrate können systematische Fehler vermieden werden

TÜVRheinland®
Genau. Richtig.

Vielen Dank für Ihre Aufmerksamkeit

Dr.-Ing. Jan Schumacher

jan.schumacher@de.tuv.com

Tel.: +49 221 806 5290

Mobile: +49 172 458 4674

LEGAL DISCLAIMER

Dieses Dokument ist Eigentum von TÜV Rheinland. Es dient nur zu vertraulichen Informationszwecken für den Empfänger. Weder dieses Dokument noch irgendwelche Informationen oder Daten, die darin enthalten sind, dürfen ohne vorherige schriftliche Zustimmung von TÜV Rheinland zu anderen Zwecken verwendet oder vervielfältigt oder ganz oder teilweise an Dritte weitergegeben werden. Dieses Dokument ist nicht ohne eine mündliche Erklärung (Präsentation) des Inhalts vollständig.

TÜV Rheinland AG

TÜVRheinland®
Genau. Richtig.

Funktionale Sicherheit ohne Schnickschnack

GMA FA 2.18 - "Engineering von sicherheitsgerichteten Systemen„

VDI/VDE 2180

Blatt 5 „Basiskonzept zur Umsetzung der Funktionalen Sicherheit“

Das hier haben wir schon…

VDI/VDE 2180 Blatt 1-4

VDI/VDE 2180 – Blatt 1-4
Funktionale Sicherheit in der Prozessindustrie



Blatt 1
Einführung
Begriffe
Konzeption

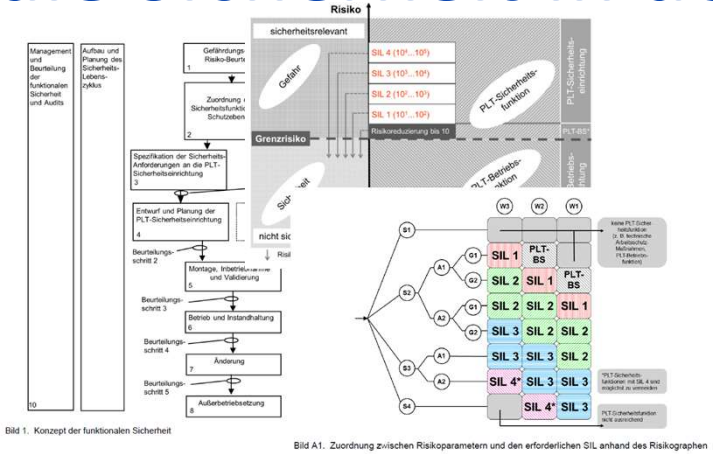


Bild 1. Konzept der funktionalen Sicherheit

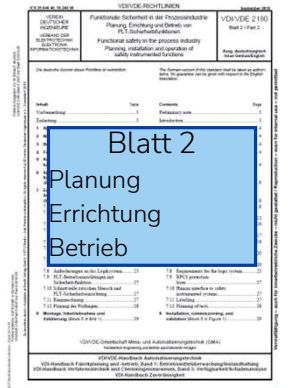
Bild A1. Zuordnung zwischen Risikoparametern und den erforderlichen SIL anhand des Risikographen



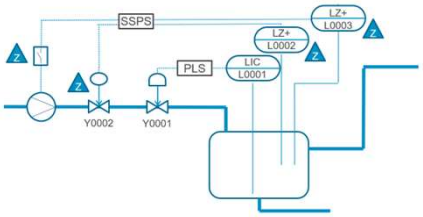
Blatt 3
PFD-Berechnung

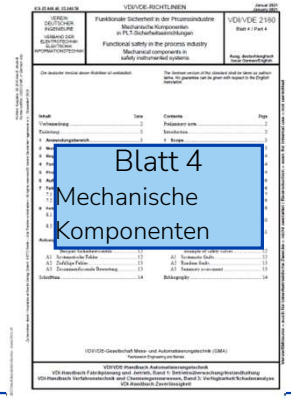
Formeln basierend auf der Kanalausfallrate λ_{DU}

$PFD_{1oo1} \approx \frac{1}{2}\lambda_{DU}T_1$	(3)
$PFD_{1oo2} \approx \frac{1}{3}\lambda_{DU}^2T_1^2 + \beta\cdot\frac{1}{2}\lambda_{DU}T_1$	(4)
$PFD_{1oo3} \approx \frac{1}{4}\lambda_{DU}^3T_1^3 + \frac{1}{2}\beta\cdot\frac{1}{2}\lambda_{DU}T_1$	(5)
$PFD_{2oo2} \approx \lambda_{DU}T_1$	(6)
$PFD_{2oo3} \approx \lambda_{DU}^2T_1^2 + \frac{3}{2}\beta\cdot\frac{1}{2}\lambda_{DU}T_1$	(7)

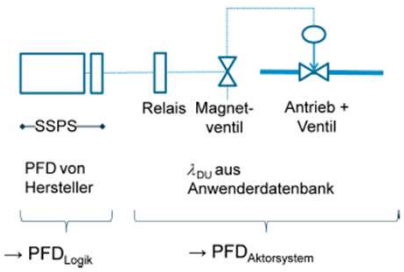


Blatt 2
Planung
Errichtung
Betrieb





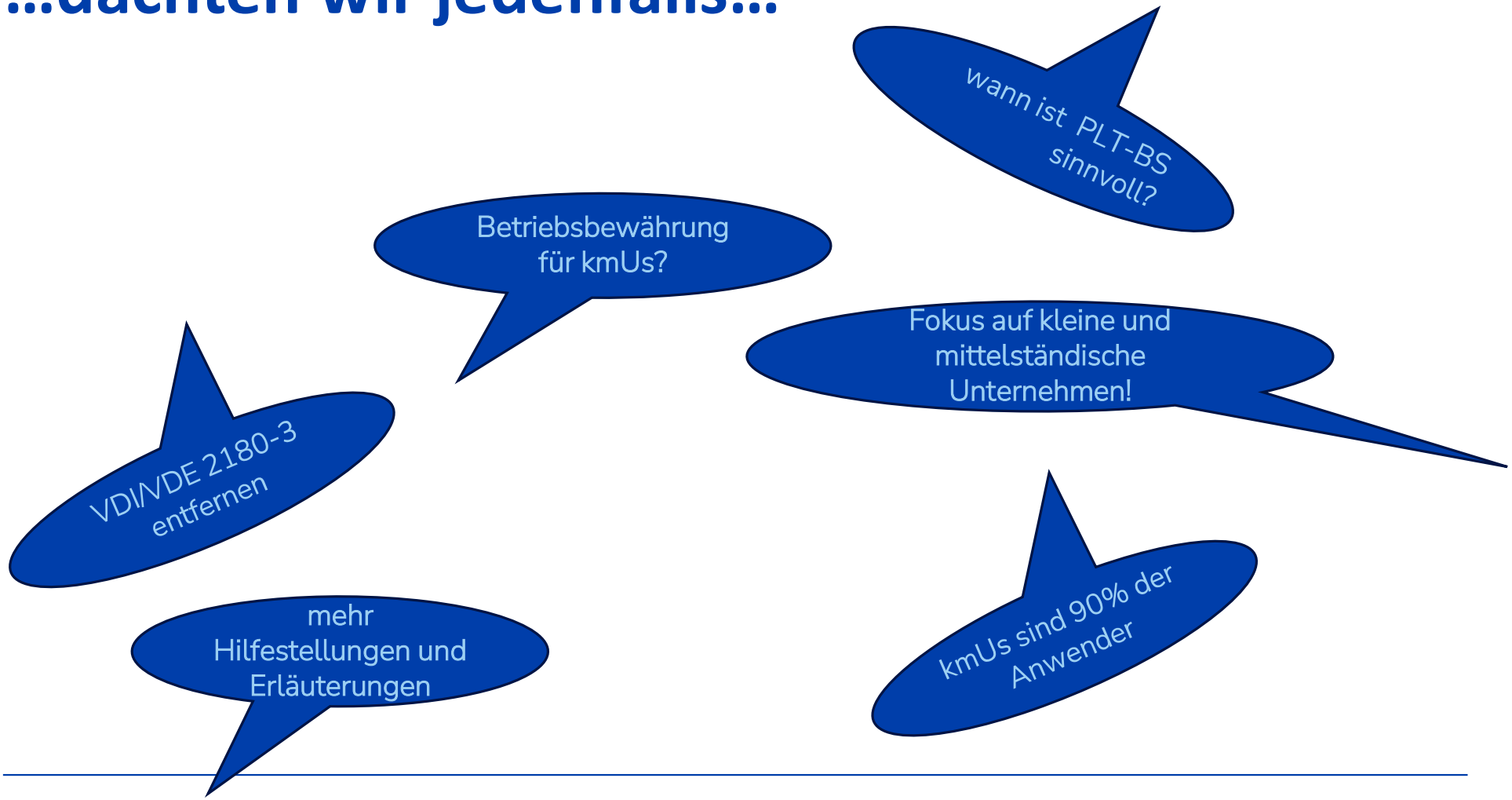
Blatt 4
Mechanische Komponenten



Damit ist alles gesagt.

VDI/VDE 2180 Blatt 1-4

…dachten wir jedenfalls…



Fokus auf Unternehmen mit begrenzten Ressourcen für Funktionale Sicherheit

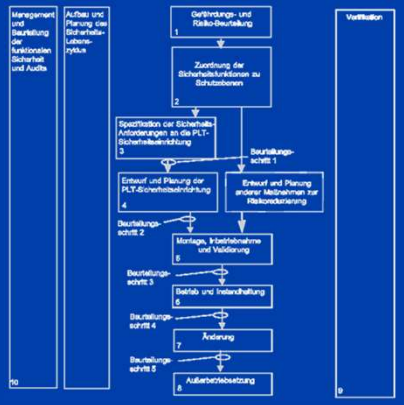
VDI/VDE 2180 Blatt 5

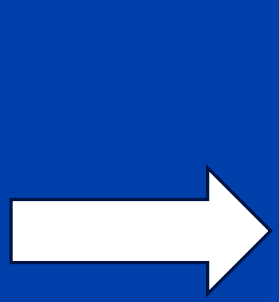
Gregor, das ist doch ´n alter Hut…



Gregor, das ist doch ´n alter Hut…

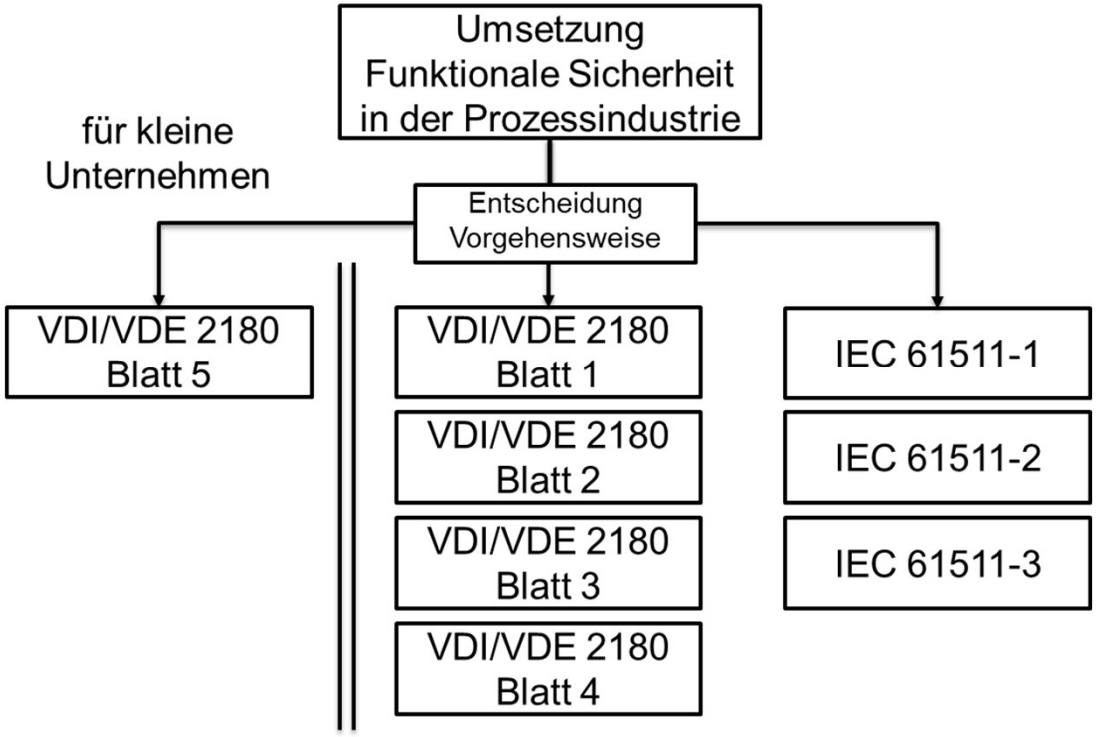
Ja, es gibt viel…
…und vieles davon kommt offensichtlich nicht an.



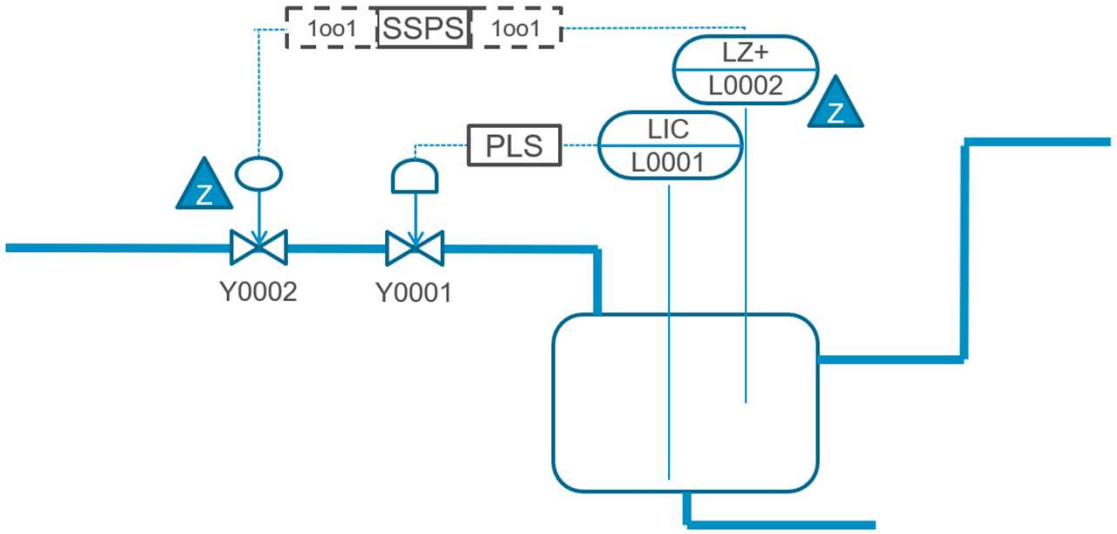




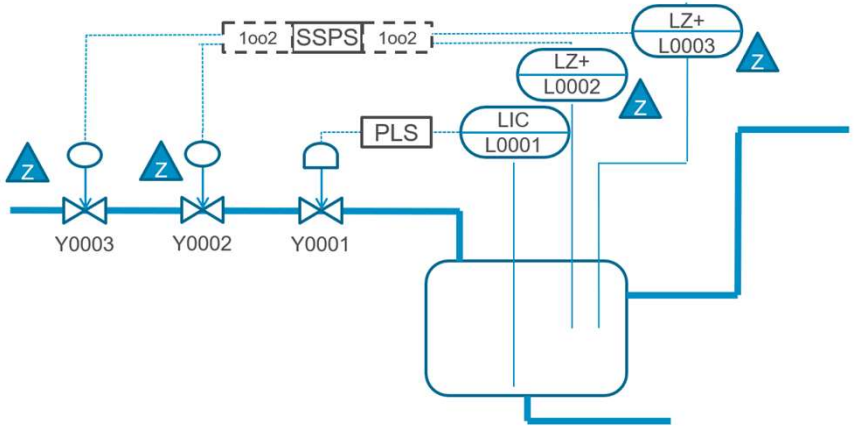
Ganzheitlicher Ansatz!

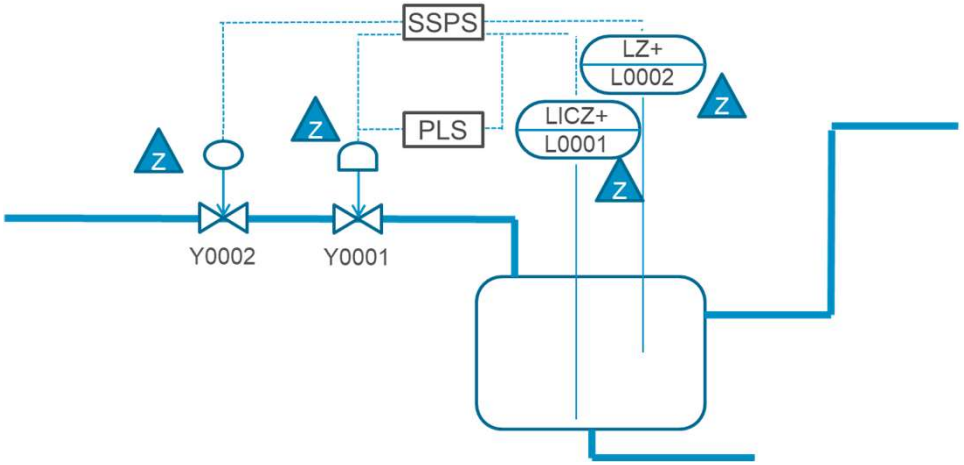


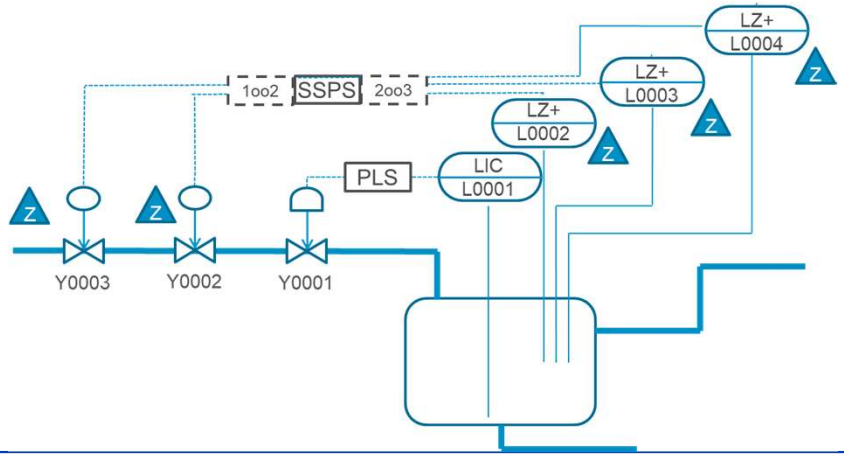
einfache Regeln – SIL 2



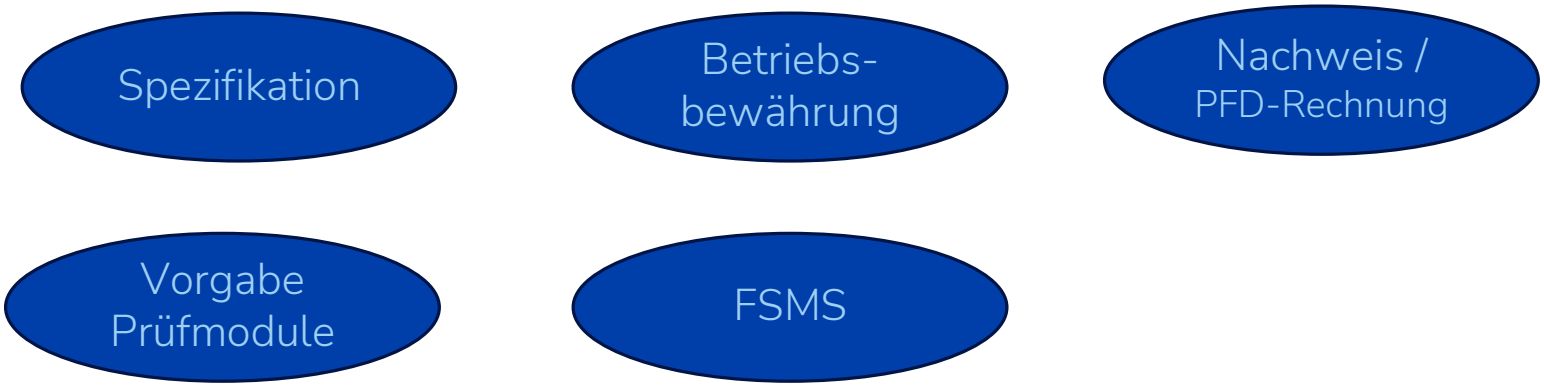
einfache Regeln – SIL 3







einfache Regeln



Inhalt Functional Safety Management System

Anhang A Functional Safety Management System

Bei der Realisierung des Functional Management Systems müssen die Anforderungen der 0 beachtet werden. Folgende Fragestellungen können dabei unterstützen:

- Wer führt die Sicherheitsbetrachtung durch und ist für die Spezifikation der Sicherheitseinrichtungen verantwortlich? Welche Werkzeuge (z.B. Risikomatrix, Risikograph) werden dafür eingesetzt und wie sind diese kalibriert?
- Wer führt die Planung (einschl. Erstellung von Prüfvorschriften und Betriebsanweisungen) und Realisierung neuer Sicherheitseinrichtungen durch?
- Wie ist das Konzept für die Geräteauswahl und die Betriebsbewährung? Welche Standard- Feldgeräte bzw SSPS werden eingesetzt?
- Wer führt die Erstinbetriebnahme und Validierung durch?
- Wer führt die Instandhaltung durch (Reparatur, Wartung, Gerätetausch)
- Wie ist der aktuelle Zustand aller Komponenten dokumentiert, sodass bei Problemen ein Zurücksetzen auf den Sollzustand möglich ist?
- Wie sind die Komponenten der Sicherheitseinrichtungen vor Ort, in der Planungsdokumentation, in der as built Dokumentation gekennzeichnet?
- Wer führt die regelmäßigen Prüfungen durch?
- Wie erfolgt die Überwachung/Plausibilitätskontrolle der Sicherheitseinrichtungen zwischen den Prüfungen?
- Wie werden die Prüfergebnisse ausgewertet und etwaige Schwachstellen ermittelt?
- Wie erfolgt die Dokumentation (z.B. Spezifikation, as built Unterlagen, Prüfungsunterlagen, Reparatur- und Wartungsberichte) und wo wird diese vorgehalten?
- Wie wird das Auslösen der Sicherheitsfunktion dokumentiert, sodass etwaige Schwachstellen im Sicher

Safety Requirement Specification

Anhang B Sicherheitsspezifikation / Safety Requirement Specification

Die Sicherheitsspezifikation ist für jede Sicherheitsfunktion auszufüllen. Bitte beachten, dass es sich hier um eine beispielhafte Darstellung handelt und Inhalte mehrerer Sicherheitsfunktionen zusammengefasst werden können.

SIF-ID	Anlage/Werk	
Kurzbeschreibung		
Gefahren- und Riskoanalyse		
Wird die Sicherheitsfunktion voraussichtlich seltener als 1x pro Jahr benötigt?	Ja – sonst kann Blatt 5 nicht angewendet werden	
Welche Sensoren sollen mit welcher Sicherheitssteuerung mit welchen Aktoren verwendet werden?		
Was ist die Grenze zum sicheren Betrieb und warum?		
Wie soll der sichere Zustand nach Auslösung der SIF sein?		
Gibt es mögliche Prozesszustände, die die SIF nicht in einen sicheren Zustand führen?		
Kann die SIF einen unsicheren		

Eignung von Geräten für Prozess

Anhang C Prüfung der Eignung von Geräten für den Prozess

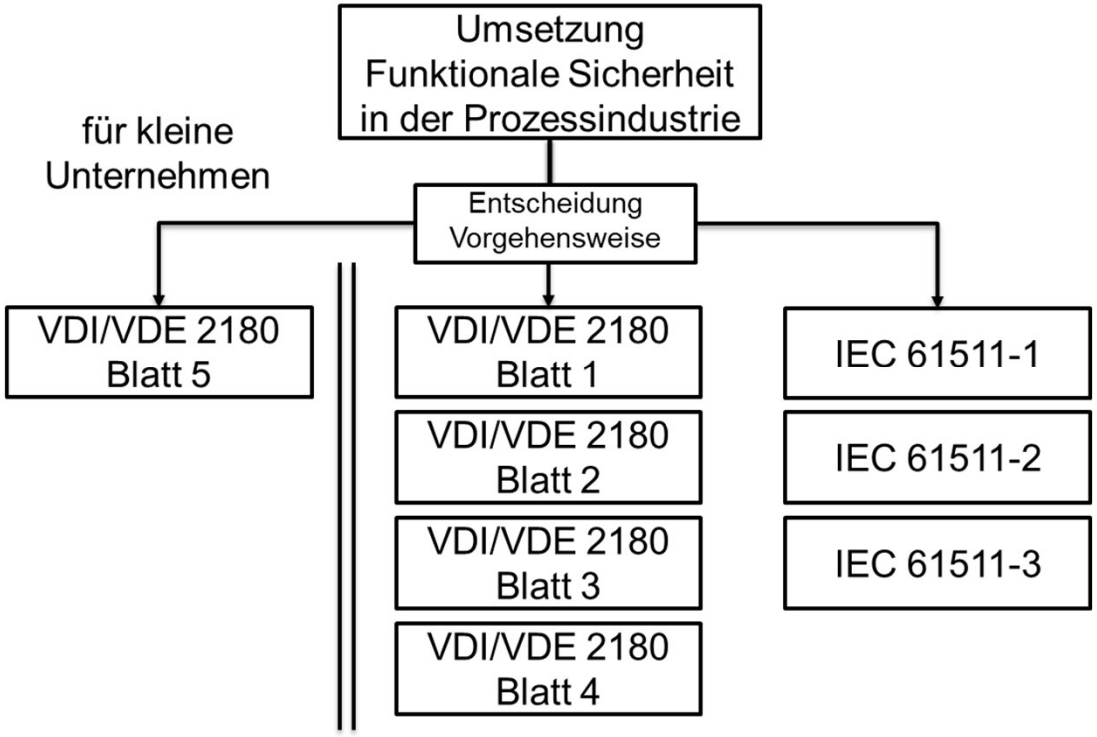
Geräte müssen für den Einsatz geeignet sein. Dabei ist auf folgende Punkte zu achten:

- Ist das gewählte Messprinzip für die gestellte Aufgabe geeignet?
- Ist der Messbereich so gewählt, dass eine hinreichende Auflösung sichergestellt ist und die Messunsicherheit genügend gering ist?
- Sind die Umgebungsbedingungen für den vorgesehenen Montageort geeignet (Temperatur, Feuchtigkeit, EMV, Sonneneinstrahlung, Korrosionseinflüsse, etc.)?
- Sind Montageort/Montageart für das Messprinzip geeignet? (z.B. Einlaufstrecken bei Blendenmessungen, Ausschluß von Feuchtigkeit bzw. Blasen in Impulsleitungen, Eliminierung von Vibration, mechanischer Spannung)
- Ist eine einfacher Austausch möglich ? (Zugänglichkeit, Absperreinrichtungen, etc.)

Unterschied Blatt 1-4 zu Blatt 5

- Betriebseinrichtungen mit Sicherheitsfunktion (PLT-BS) sind ausgeschlossen und werden grundsätzlich in SIL2 realisiert.
- SIL1 wird grundsätzlich in SIL2 realisiert.
- Variable Prüffristen oder Prüffristverlängerung nicht Teil von Blatt 5
  Prüfintervall von 1 Jahr angesetzt
- Auslösen einer Sicherheitseinrichtung, die zur Funktion Energie benötigt (z.B. motorgetriebene Ventile) nicht betrachtet (energize to trip)
- keine Betriebsbewährung von Geräten beschrieben - entweder anderen Firmen bzgl. Betriebsbewährung anschließen
  oder Geräte einsetzen, die nach IEC61508 entwickelt sind.
- PFD-Nachweis ist generisch und nur unter fixen Rahmenbedingungen zulässig – dafür entfällt die spezifische Berechnung für jede PLT-Sicherheitsfunktion

Deshalb: nicht springen



…und wenn ich jetzt doch mal eine Sonderlösung benötige ?

VDI/VDE 2180 Blatt 5

Blatt 5 hat Fokus auf kleine und mittelständische Unternehmen.

Wie klein muss mein Unternehmen sein, damit ich Blatt 5 anwenden darf ?

VDI/VDE 2180 Blatt 5

…und wann isses jetzt endlich fertig?

Publikation Gründruck voraussichtlich November 2025

VDI/VDE 2180 Blatt 5

„Sind Fehlerraten eine Quantifizierung von Geiz, Unwissen und Faulheit?“

Oder

Sind Fehlerraten eine Quantifizierung von Kostendruck, Erkenntnisaufwand und Terminnot

Christian Demski

Aug. 2025

General Business

IEC 61511 / 08 DEFINITIONS

3.2.81
systematic failure
failure related to a pre-existing fault, which consistently occurs under particular conditions, and which can only be eliminated by removing the fault by a modification of the design, manufacturing process, operating procedures, documentation or other relevant factors

Note 1 to entry: The cause of systematic failures of the software may be known as "bugs".

Note 2 to entry: Corrective maintenance without modification would usually not eliminate the failure cause which involves the failure under particular conditions.

Note 3 to entry: A systematic failure can be reproduced by deliberately applying the same conditions, although not all reproducible failures are systematic.

Note 4 to entry: Examples of faults leading to systematic failure include human error that originates in:

- the SRS;
- the design, manufacture, installation, operation or maintenance of the hardware;
- the design or implementation of software (including application program).

Note 5 to entry: Similar devices designed, installed, operated, implemented or maintained likely to contain the same faults. Therefore they are subject to common cause failures conditions occur.

Systematic Failure:
Fault & Condition, can be reproduced, can be eliminated.

3.2.59
random hardware failure
failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of a total equipment comprising many components occur at predictable rates but at unpredictable (i.e., random) times.

Note 2 to entry: Two major differences distinguish the random hardware failures and the systematic failures:

- a random hardware failure involves only the system itself while a systematic failure involves both the system itself (a fault) and a particular condition (see 3.2.81). Then a random hardware failure is characterized by a single reliability parameter (i.e., the failure rate) while a systematic failure is characterized by two reliability parameters (i.e., the probability of the pre-existing fault and the hazard rate of the particular condition).
- a systematic failure can be eliminated after being detected while random hardware failures cannot.

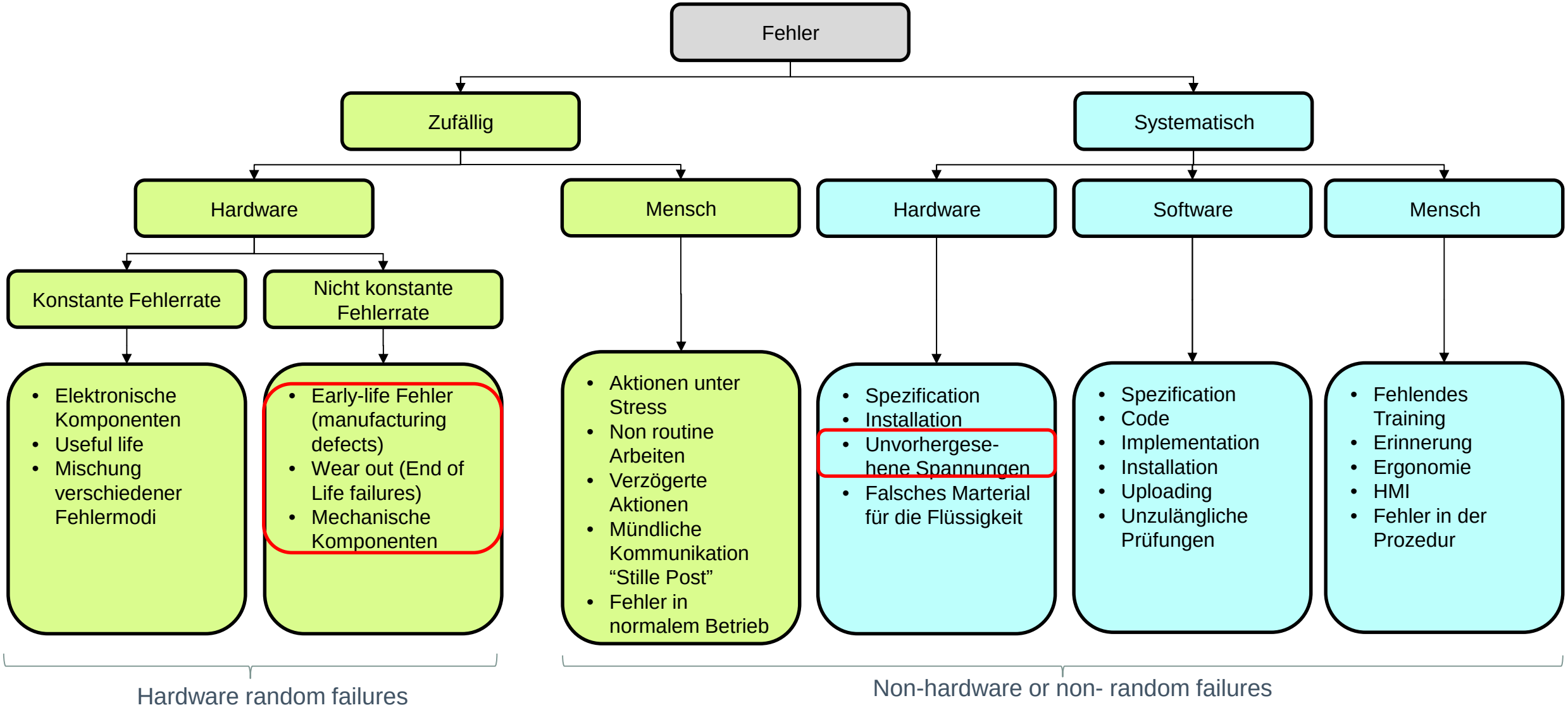
This implies that the reliability parameters of random hardware failures can be estimated from field feedback while it is very difficult to do the same for systematic failures. A qualitative approach is preferred for systematic failures.

[SOURCE: IEC 61508-4:2010, 3.6.5, modified – The notes have been changed]

Random Failure:
Fault, can occur at random times, cannot be eliminated

Source: IEC 61511 ed. 2 2016

DEFINITION ISO TR 12489



Source: ISO TR 12489 (2013) slightly wording changes have been made

DEFINITION IN THE NAMUR.SMART NE 93

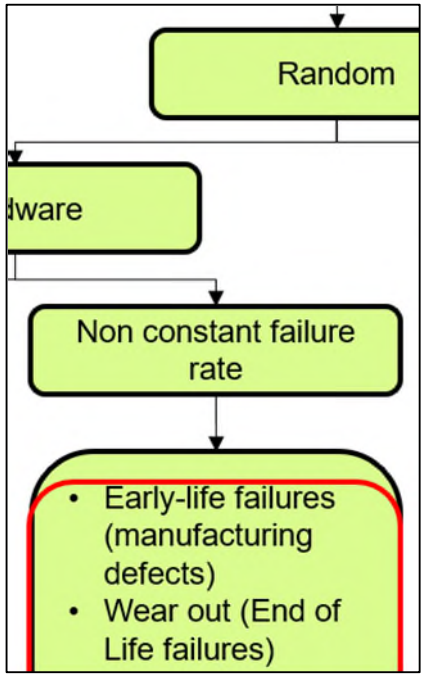
Fehlerbilder/Ursache		Fehlerursache		
Deutsch	Englisch	Zufällig*	Systematisch Engineering	Systematisch Betrieb
Interner Gerätefehler (nicht durch Medium verursacht)	Internal device fault (not caused by product)	x		
Alterung / Verschleiß	Wear out	x		
Leitungsbruch/ Leitungsschluss	Open circuit/ short circuit	x		
Signal eingefroren	Frozen signal, stuck-at	x		
Sonstiger zufälliger Fehler/ohne Befund	Other random fault	x		
Zu hohe Messungenauigkeit, Signaldrift (Elektronikfehler)	Bad accuracy of measurement, signal drift (electronic fault)	x		
Kontakt schaltet nicht / klemmt	Contact does not switch	x		
EMV	EMC		x	
Planungsfehler	Design error		x	
Montagefehler	Installation fault		x	
Produkteinflüsse	Influence of product		x	
Umwelteinflüsse	Influence of environment		x	
Applikationssoftwarefehler/Parametrierfehler	Application programming error / Paramatrization error		x	
Konstruktionsfehler	Constructional fault		x	
Sonstiger systematischer Fehler Engineering	Other systematic fault engineering		x	
Korrosion	Corrosion			x
Bedienungsfehler	Operating error (Human Error)			x
Unbefugter Eingriff / Manipulation	Unauthorized access / sabotage			x
Nicht entfernte Überbrückung	Unremoved bypass			x
Fehlerhafte Prüfanweisung	Incorrect test procedure			x
Zu hohe Messungenauigkeit, Signaldrift (Umwelteinfluss/Betrieb)	Bad accuracy of measurement, signal drift (environmental influences)			x
Undichtigkeit im Durchgang	Internal leakage			x
Undichtigkeit nach Aussen	External leakage			x
Blockieren der Mechanik	Mechanical blockage			x
Sonstiger systematischer Fehler Instandhaltung	Other systematic fault maintenance			x
Mechanische Beschädigung	Mechanical damage			x
* Konvention: Alles was nicht systematisch Betrieb/Engineering ist				

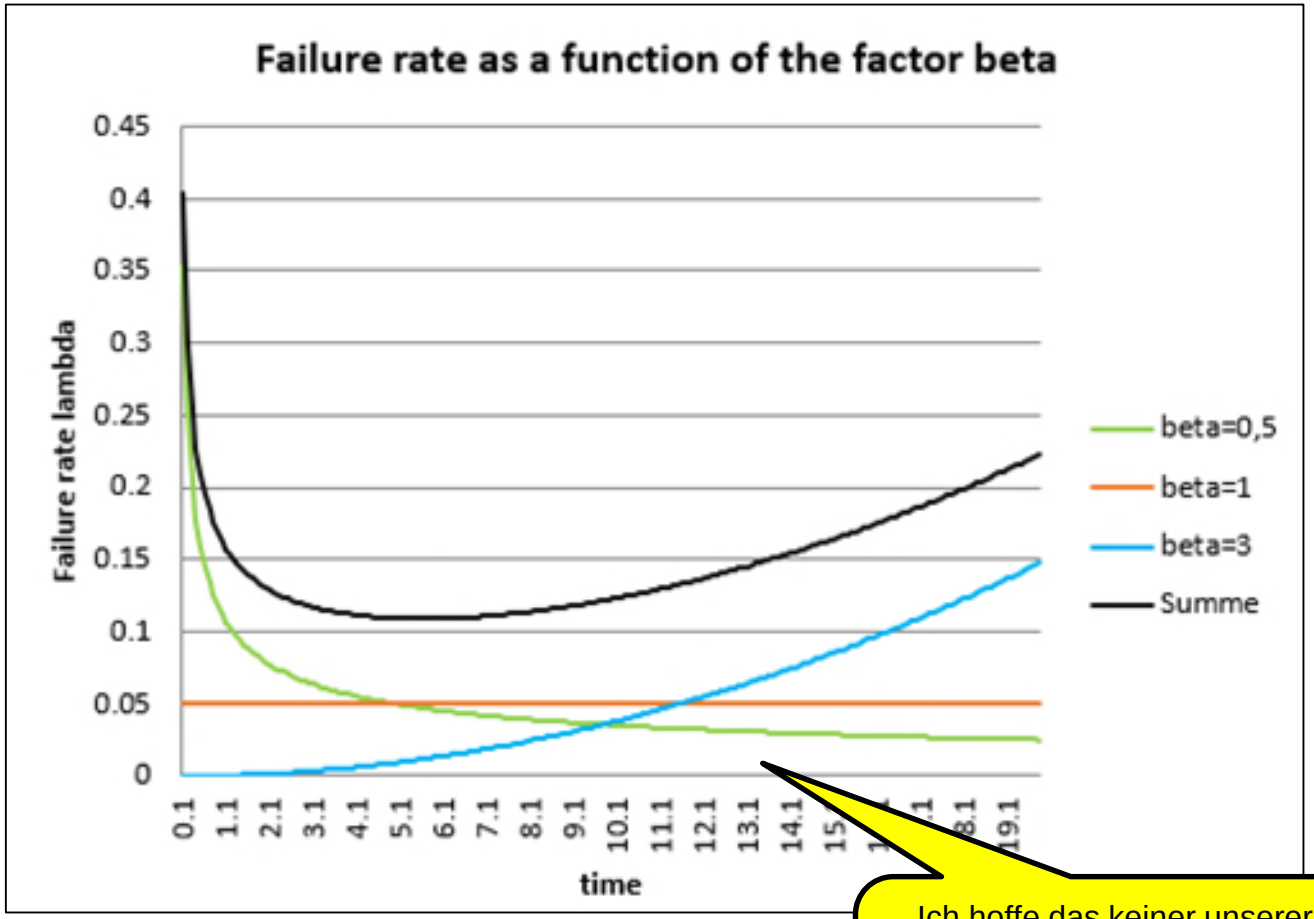
The good thing is both approaches agree that wear out cannot be predicted…

Mixture of reason & effect

Source: NAMUR.smart Training [V1.74] Aug.2023

AT LEAST BOTH AGREE…..





- Early failures, beta<1 caused by:
  - Failure in construction
  - Failure in Design
  - Failure in a Programming
  - Failure in installation
- Late failures, beta>1 caused by:
  - aging
  - Wear out
- Constant failure rate beta=1 caused by:
  - Random failures in the electronic

	Fehlerursache
Englisch	random
Internal device fault (not caused by product)	x
Wear out	x
Open circuit/ short circuit	x

Ich hoffe das keiner unserer Kollegen für die Zuverlässigkeit mitbekommt, dass wir alle “Wear out” Effkte als zufällig klassifizieren….

SYSTEMATISCHE UND ZUFÄLLIGE FEHLER

Special thanks to Dr. Jörg Isenberg
auma Solutions for a world in motion
Integrity Safety auma SIL Level

Gibt es zufällige Fehler in der Mechanik?

Example: gebrochener Schaft

- Dimensionierung, Produktion, Qualitätskontrolle,… der Hersteller vom Antrieb ist frei von Fehlerquellen
- Eingangskontrollen vom Antriebsersteller: Sichtprüf

Random failure? **Systematic failure?**



Neue Root Cause:

- Röntgenmessungen als Teil der Eingangskontrolle ergaben Einschlüsse im Stangenmaterial

Random failure? **Systematic failure?**

Systematische und Zufällige Fehler

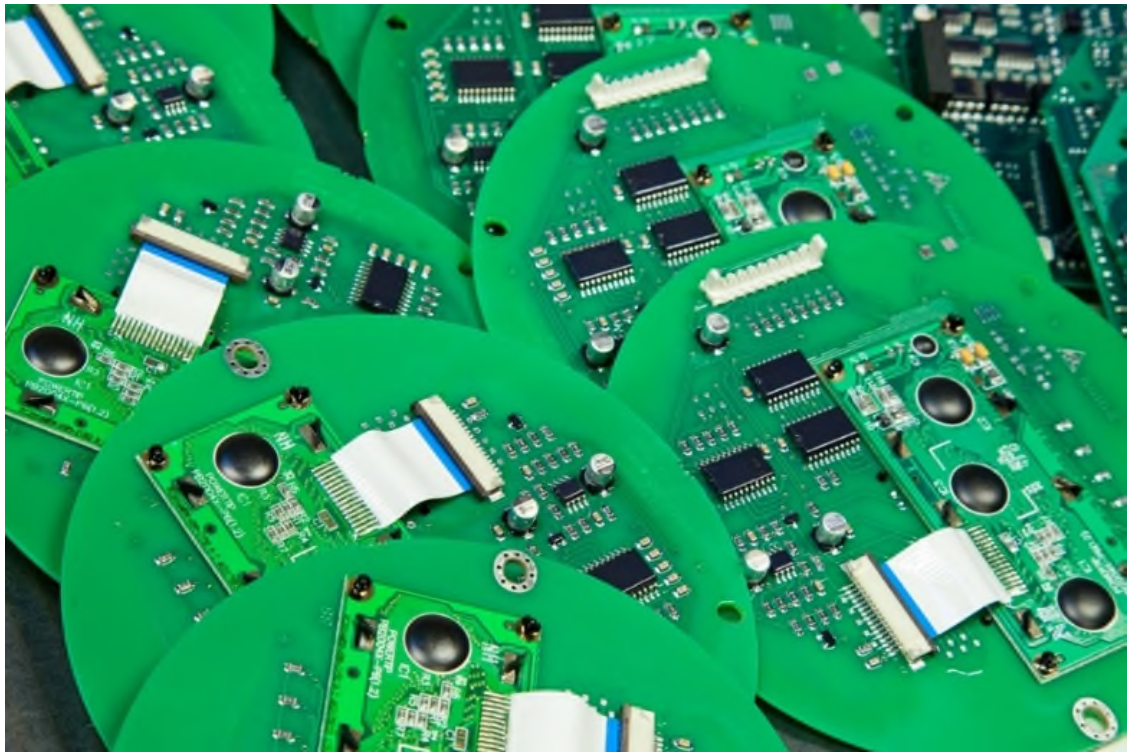
Special thanks to Dr. Jörg Isenberg
auma Solutions for a world in motion
Integrity Safety auma SIL Level

Existieren zufällige Fehler in Elektronik: (quantenmechanische Effekte mal Ausgenommen) **?**

Beispiel: Fehlerhafte („burned“) Transistoren in Antriebsreglern

- Richtig dimensioniert, keine Felhler in der Antriebsproduktion…

Random failure? Systematic failure?



Neue Root Cause:

- Röntgenuntersuchung unter dem Elektronenmikoskop ergabern die Isolationsschicht war zu gering bzw. war kontaminiert.

Random failure? Systematic failure?

Systematische und Zufällige Fehler

Gibt es zufällige Fehler in der Mechanik?

Beispiel:

- Wir hatten einen Fehler an einem Drucktransmitter der driftete. Keine sinifikante Korrosion zu erkennen, die Dianose der Elektronik ergab keinen Fehler.

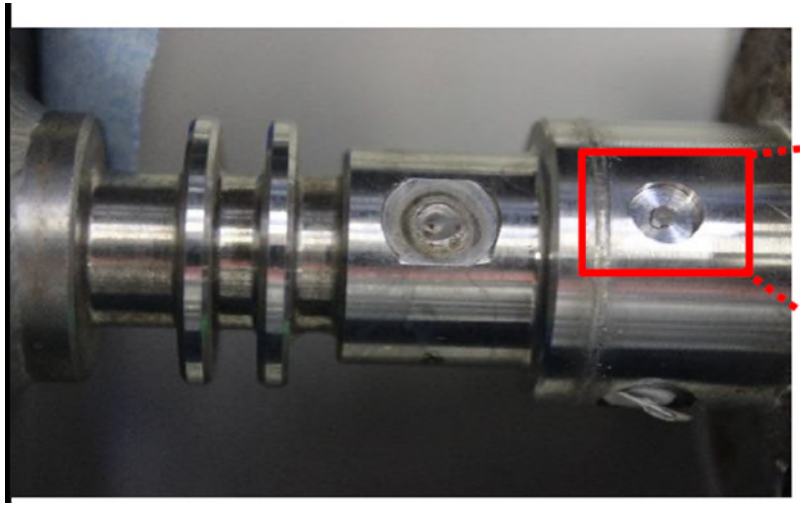
  Random failure? Systematic failure?

- Nach einiger Zeit ist schon wieder ein Drucktransmitter über mehrere Tage in eine Richtung gedriftet.

  Random failure? Systematic failure?

- Die Füllung des Öls wurde in der internen Kapillare wurde korrekt durchgeführt; aber durch unsere korrosive Umgebung wurde die Füllöffnung angegrifffen.

  Random failure? Systematic failure?



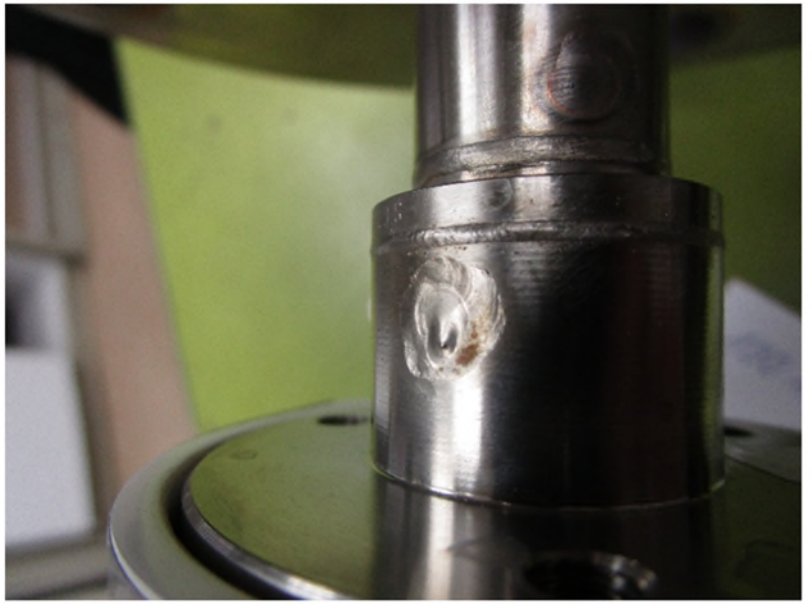


Abbildung 6: Verschweißter Einfüllstutzen

SYSTEMATISCHE UND ZUFÄLLIGE FEHLER

Gibt es zufällige Fehler an Sensoren?

Beispiel: Der Drucktransmitter hatte einen zu roßen Druck angezeigt. Es wurde kein Fehler in der Installation und der Elektronik im Werkstatt gefunden.

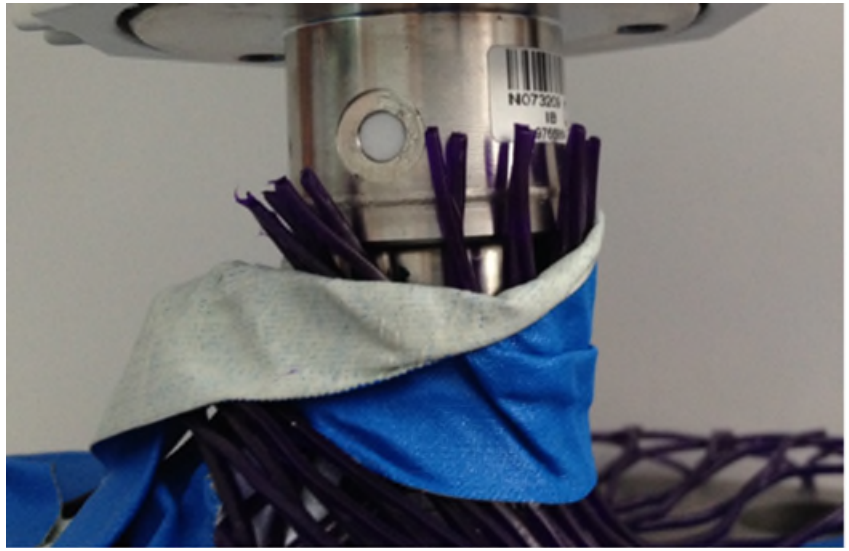
Random failure? Systematic failure?

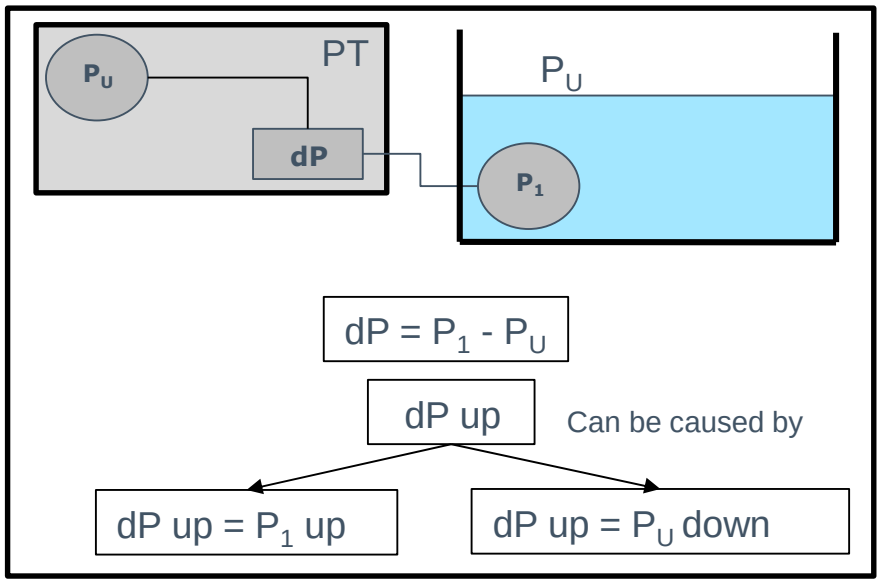
- Der gleiche Fehler trat nach einigen Monaten wieder auf.

Random failure? Systematic failure?

- Der Drucktransmitter ist eigentlich ein Differenzdrucktransmitter
- Der atmospäriche Druck ist das “zweite Bein”; es wird innerhalb des Transmittergehäuses gemessen.
- Der Luftfilter war zu dicht. Damit hatte der P_U im Transmitter mit der P_U oberhalb der Flüssigkeit nicht mehr viel zu tun.

Random failure? Systematic failure?





Definition von Christian

Zufällige Fehlerraten sind Quantifizierung von Geiz, Unwissen und Faulheit.

Oder in ein wenig netteren Worten

Vielleicht ja auch quantenmechanisce Effekte, wir können sie nur nicht erklären…..

Alle Fehler sind systematisch.
Jeder Fehler hat einen Grund.

Wir akzeptieren Fehler, wenn es nicht sinnvoll ist, alle Fehler zu identifizieren oder zu vermeiden. Das gilt für alle Phasen des Lebenszykus.

Also, solange diese Fehler selten und zufällig verteilt auftreten, können wir auch den probabelistischen Weg wählen, um diese übrigbleibenden Fehler zu kontrollieren.

„Failure rates generate business not safety“
From Dr. Gregor Schmitt-Pauksztat

Wie viel sind wir bereit für die Vermeidung von Fehler zu investieren?

- Ventile:
  - Wollen wir Ventile verwenden wie für die Kernkraftwerke?
    - ✓ Drei abgießen, zwei zerstörned prüfen, und dann 100% Röntenprüfungen am 3…

      Die Kosten pro Ventil steigen um das neunfache
- Sensoren:
  - Wollen wir in Zukunft alle elektronischen Komponenten mit Rasterelektronenmikoskop und Röntgengeräten untersuchen, um zu identifizieren dass alle elektronischen Komponenten innerhalb und ausserhalb in ihrer Toleranzen sind?

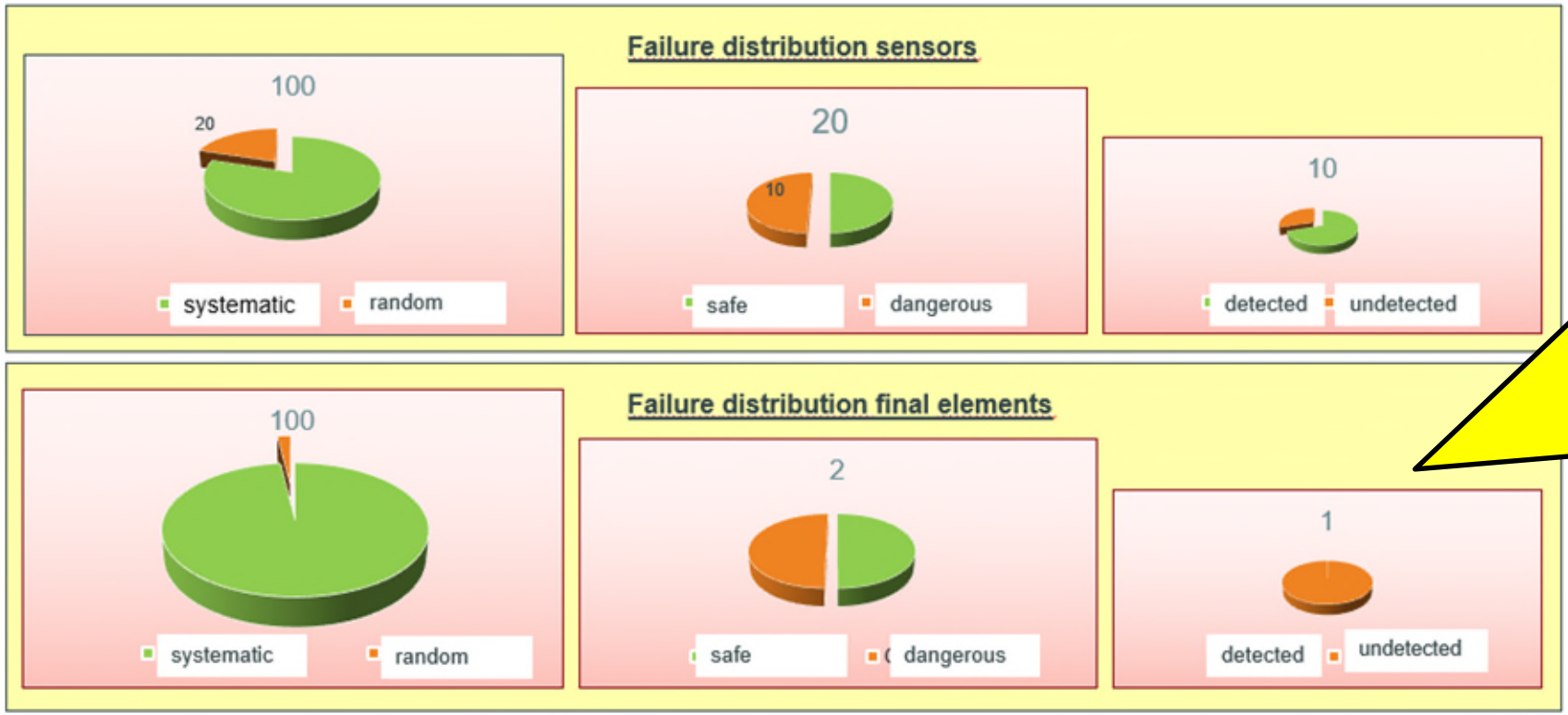
    Die Kosten eines Sensors würden sich versechsfachen.
- Instandhaltung:
  - Wir können Fehler vermeiden, wenn wir ein drittes Augenpaar dazunehmen, um alle Maintenance Aktivitäten zu überwachen.
    - ✓ Die Kosten würden sich zumindest verdoppeln.

- •
- •
- •

You get the point.

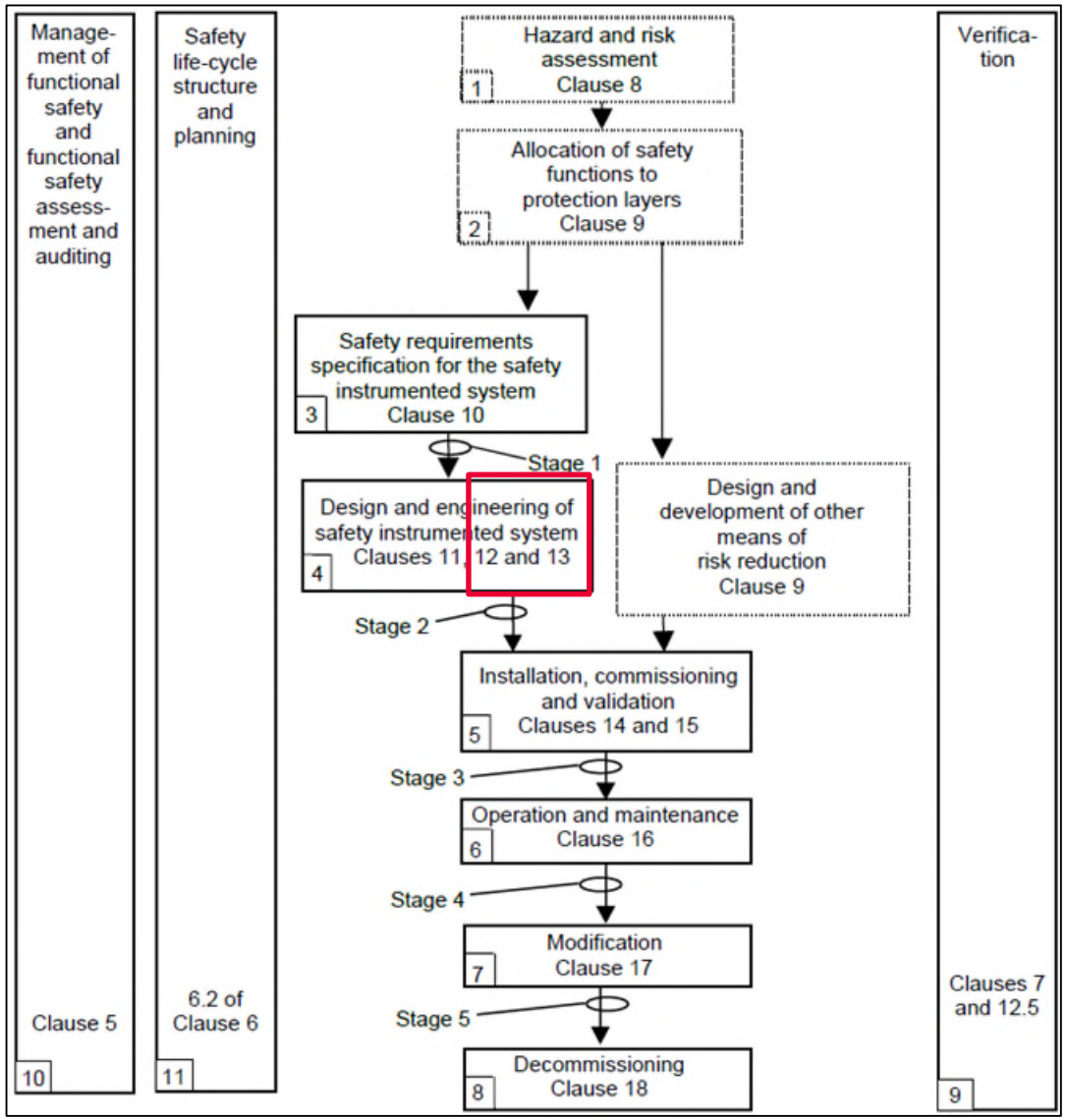
Warum haben wir also zufällige Fehler….

- Wir akzeptieren, dass wir nicht 100% zuverlässige Prozesse haben
- Wir akzeptieren, dass wir Fehler machen bei der:
  - Auswahl
  - Installation
  - Konfiguration…..
- Wir akzeptieren statistische Prozesse in der Qualitätskontrolle für die Geräte die wir verwenden

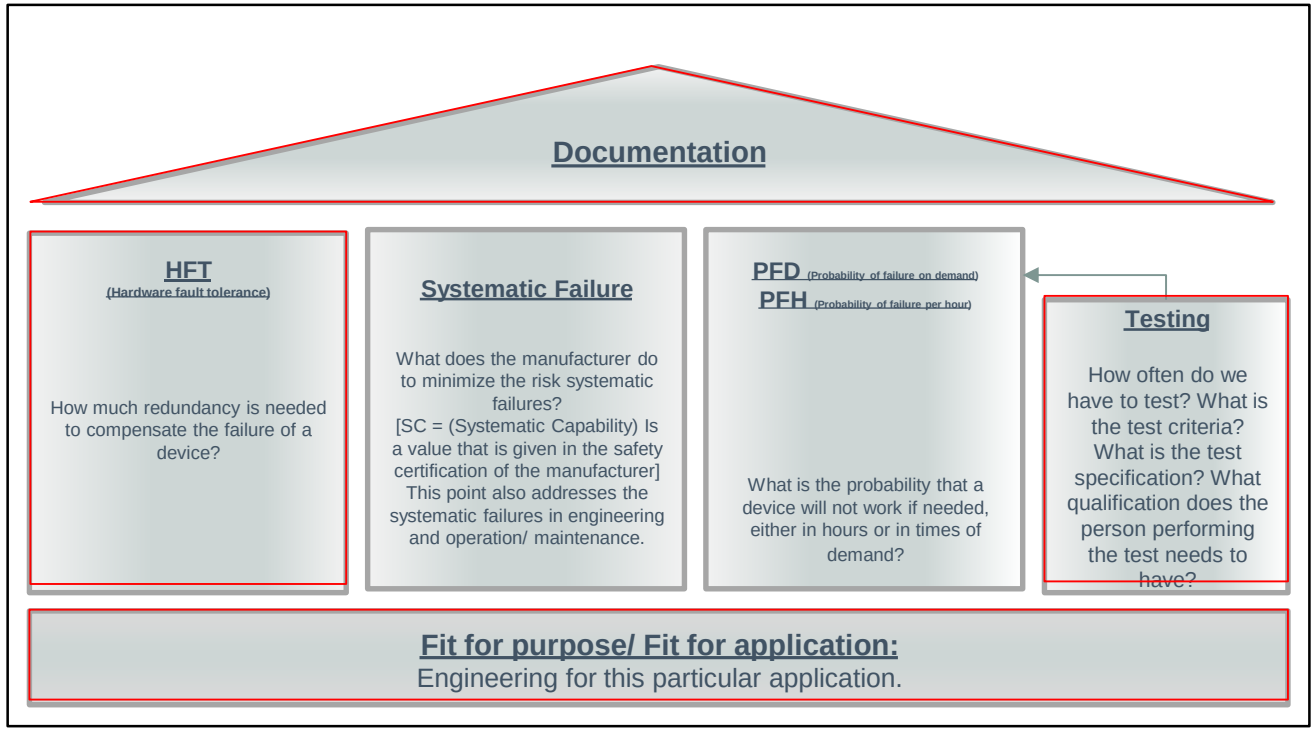


Die Fehlerraten die wir für mechanische Komponenten verweden können auch höher sein, auch wenn der Grund für den Fehler gefunde wurde, weil wir nicht willig sind alle notwendingen Maßnamen zu ergreifen, um die Fehler zu vermeiden.

REMEMBER….



- **The main task of the functional safety life cycle is to reduce systematic failures during the life cycle.**
- Only in the small red box we care about the PFD calculation and random failures.



Einige Erkenntnisse zur Diskussion….

Einige Erkenntnisse:

- Vermeidung von Fehlern soweit möglich.
- Kontrollieren, dass die übrigbleibenden Fehler selten und zufällig sind
- Diese übrigbleibenden Fehler mit probabelistischen Mitteln unter Kontrolle halten.

- Wir können „systematische Fehler“ nicht aus der Statistik entfernen, wenn wir sie in Zukunft nicht sicher vermeinden.
- Wir müssen akzeptieren, dass Fehler die theoretisch systematisch sind, zufällig auftreten, da wir sie nicht kontrollierern können oder wollen.
- Wir müssen aber sicherstellen, dass die Fehler **selten** und **zufällig verteilt** sind.
- Wir müsssen dann aber auch die Fehlerraten hinnehmen, die wir nicht kontrollieren können oder wollen.

Einige Fragen;

- Gibt es neben der Vermeidung von systematischen Fehlern und dem Kontrollieren von zufälligen Fehlern noch andere Kategorien von Fehlern und andere Methoden diese zu kontrollieren?
- **Sollten wir systematische Fehler von den Fehlerraten ausschließen, auch wenn wir sie in der Zukunft nicht vermeiden?**
- Verifizieren wir eigentlich die Fehlerraten regelmäßig?

DFFERENT PATH….

1

We have “0” **random** dangerous undetected failures → We do not need any PFD calculation → We have to avoid failures at all cost (Is this realistic?)

Do we want to pay for this?

3

Try to avoid systematic failures by the processes → Take measures in the filed and consider all of the failures being part of the things that fall through the cracks → Ensure they follow a random pattern and are seldom → Limit the use of the random management to a maximum interval for testing.

A mixture of random and systematic approach.

2

We take all failures into the random dangerous undetected bucket → We do not need to put that much effort into avoiding failures (Is this realistic?) → We come up with test frequencies that are very short → The safety function is not designed well…

Who wants to manage the process safety risk with this?

IF YOU HAVE QUESTIONS

- If you have questions or you would like to have discussions, please contact me.



Christian Demski
Dow Deutschland Anlagengesellschaft mbH
IEA SIS Expertise Area Leader
Technical Expertise & Solutions
Cdemski@dow.com
+494146913814
Postfach 1120
Stade 21677

Vielen Dank an Johannes Schmidt für die deutlich diplomatischere Version des Vortragstitels.

SIL Sprechstunde 2025

Fred Stay –HIMA consulting

HIMA CONSULTING

HIMA SMART SAFETY.

#safetygoesdigital



Wer ich bin



Fred Stay
Director Safety Consulting Europe
HIMA Paul Hildebrandt GmbH
Albert-Bassermann-Straße 28 I 68782 Brühl
Phone +49 6202 5770-130
Cell +49 1624250759 | f.stay@hima.com

58 Jahre alt, glücklich verheiratet, 3 wunderbare Kinder

Praktische Erfahrungen (3+ Jahrzehnte) in
..Process Automation
..Functional Safety in process industry

- FS Expert (TÜV Rheinland, # 275/16 SIS)
  Über 30 Jahre Erfahrung auf dem Gebiet der Funktionalen Sicherheit
- Themenschwerpunkte:
  - Management der Funktionale Sicherheit
  - Durchführung und Unterstützung von Gefahren- und Risikoanalysen
  - FS-Assessments und Audits
  - SIL-Verifizierungen
  - Spezifikation und Auslegung von Sicherheitssystemen
- Trainer für den Functional Safety Engineer Kurs (TÜV Rheinland)

Märchenstunde

Es war einmal…
ein Standard

..der war einigen Menschen fremd und unangenehm….

…daher begann man, sonderbare Dinge über ihn zu erzählen und ihn zu vermeiden oder zu umgehen…



© HIMA Paul Hildebrandt GmbH 2025

Wahre Märchen..selbst erlebt

- Beispiel Betreiber (Forschungsanlage):
  Sicherheitsspezifikationen für 2 Anlagenteile (HW+SW) – Bedingung: Begriff SIL darf nicht erwähnt werden
  Grund: SIL ruft die Behörde auf den Plan und schränkt Flexibilität ein

- Beispiel Errichter: Gefahren- und Risikoanalyse Thermoprozessanlage startet mit Z-Funktionen im Design (erfahrungsbasiert) und endet mit „keine SIL-Anforderung, Umsetzung in PLS möglich“
  Grund: akute SIL-Allergie ;-), Realisierung eines SIS wird umgangen, um vermeintlichen Aufwand zu vermeiden

- Beispiel Hersteller: Analysegerät zur Messung Brennstoffgehalt
  Betreiber benötigt SIL-Qualität. Keine Mitwirkung des Herstellers bei Nachweis
  Grund: „SIL Firlefanz“

In allen Fällen war der Reifegrad des Wissens der beteiligten Parteien hinsichtlich FuSi gering

© HIMA Paul Hildebrandt GmbH 2025

Funktionale Sicherheit im Explosionsschutz

© HIMA Paul Hildebrandt GmbH 2025

Explosionsschutz und FuSi

es gibt viele Überschneidungen und Gemeinsamkeiten

In Prozessanlagen und deren Umgebung besteht das Risiko diverser Explosionstypen:



Risikoanalysen von Produktionsanlagen in Ex-Bereichen

Quelle: Vortrag TÜV SÜD Tag des Explosionsschutzes Dorian Marx, München, 23-Okt-2024

Und nur wenig Gründe um unterschiedliche Wege beim Design und Betrieb der Ex-Einrichtung zu gehen

© HIMA Paul Hildebrandt GmbH 2025

FuSi vs TRGS725 Methodik?

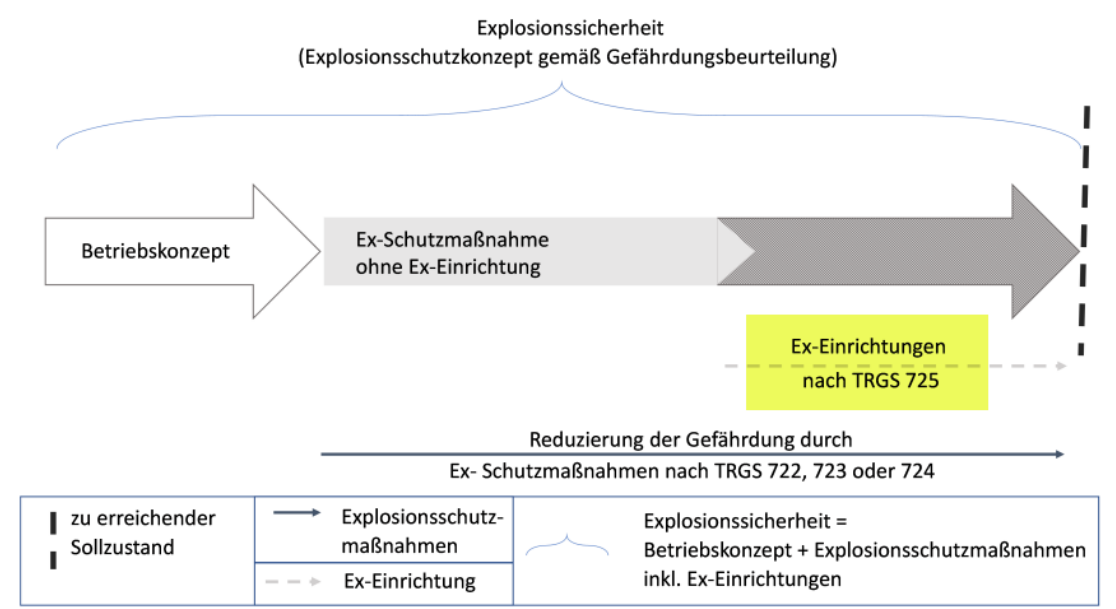
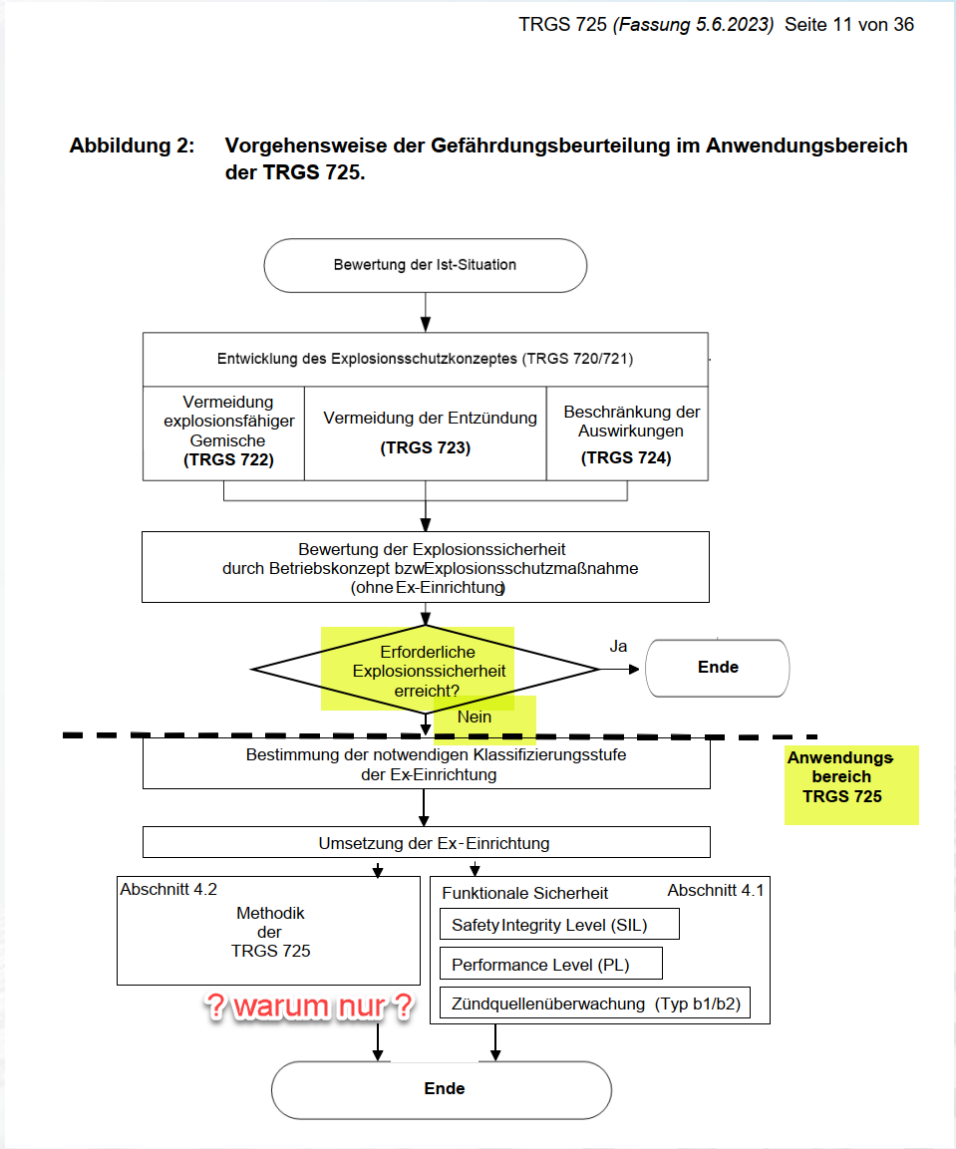


Abbildung 1: Explosionsschutzkonzept.



Der Aufbau des Explosionsschutzkonzepts und die Vorgehensweise der Gefährdungsbeurteilung sind absolut nachvollziehbar.
ABER: Warum schafft man für die Ex-Einrichtung eine Parallelwelt, wenn es schon einen anerkannten STAND DER TECHNIK für FuSi seit mehr als 20 Jahren gibt?
International hat die TRGS keine Bedeutung, die IEC 61508/61511 sowie ISO13849 jedoch schon.

SPS als Gaswarneinrichtungen_FBRCI-18.pdf

© HIMA Paul Hildebrandt GmbH 2025

Gemeinsame Grundprinzipien

Aktives **Safety Management**, welches folgendes beinhaltet:

- Lebenszyklusansatz
- Gefährdungs-/Risikoanalyse
- Wiederholungsprüfungen
- Klassifizierungsstufen
- Hohe/Niedrige Anforderungsrate
- Auch die Einbeziehung des Betriebskonzepts ist den FuSi-Fachkundigen bei der Risikoanalyse wohlbekannt.

Vermeidung zufälliger Fehler:

- Redundanzen und Mindestanforderungen an Fehlertoleranz/Verfügbarkeit

Vermeidung Fehler gemeinsamer Ursache

Vermeidung systematischer Fehler

- Betriebsbewährung inkl. Forderung nach dessen Nachweis durch den Anwender
- Kompetenz der Beteiligten
- Verifikation und Validierung
- Dokumentation
- Beurteilung durch Fachkraft
- Zugriffskontrolle
- Management of Change

© HIMA Paul Hildebrandt GmbH 2025

Ähnliche Lösungsansätze

4.2.3 Technische Ausführung von Ex-Einrichtungen zur Erfüllung der Klassifizierungs-stufen K2 oder K3

(1) Für einfache Funktionseinheiten in Ex-Einrichtungen mit erhöhter Zuverlässigkeit (hoch oder dauerhaft sichergestellt) gelten die Anforderung von Abschnitt 4.2.2 analog.

Beispiel: Ex-Einrichtung der Klassifizierungsstufe K2 mit betriebsbewährten Komponenten



Abbildung 10: Ex-Einrichtung in der Klassifizierungsstufe K2 - Reihenschaltung der Funktionseinheiten Sensor (K2), Verarbeitung (K2) und Aktor (K2).

Diese Aussage gehe ich noch einigermaßen mit (Vgl. mit SIL: Typ A Geräte betriebsbewährt)

© HIMA Paul Hildebrandt GmbH 2025

Unterschiedliche Auffassungen

(2) Komplexe Funktionseinheiten der Klassifizierungsstufen K2 und K3 können nur verwendet werden, wenn diese durch den Hersteller oder durch den Arbeitgeber hinsichtlich ihrer Zuverlässigkeit bewertet sind. Informationen zur Bewertung der Signalverarbeitung können Anhang 2 entnommen werden, Hinweise zur Betriebsbewährung von Sensoren und Aktoren finden sich in Anhang 3.

Diese Aussage gehe ich nicht mit (Vgl. zu SIL: Typ B Geräte betriebsbewährt)
Wie soll ein Arbeitgeber komplexe Geräte wie z.B. nicht-sichere SPS oder PLS bewerten?
Anhang 2 macht hier schwache Aussagen mit Anforderungen, an denen die meisten Betreiber scheitern werden

© HIMA Paul Hildebrandt GmbH 2025

Unterschiedliche Auffassungen

(3) Wird bei komplexen Ex-Einrichtungen die geforderte Zuverlässigkeit durch die Ex-Einrichtung in Gänze oder in Teilen nicht unmittelbar erreicht, kann die Zuverlässigkeit durch zusätzliche Ex-Einrichtungen, wie beispielsweise vollständige oder teilweise Redundanz, erhöht werden (s. Abbildung 11).

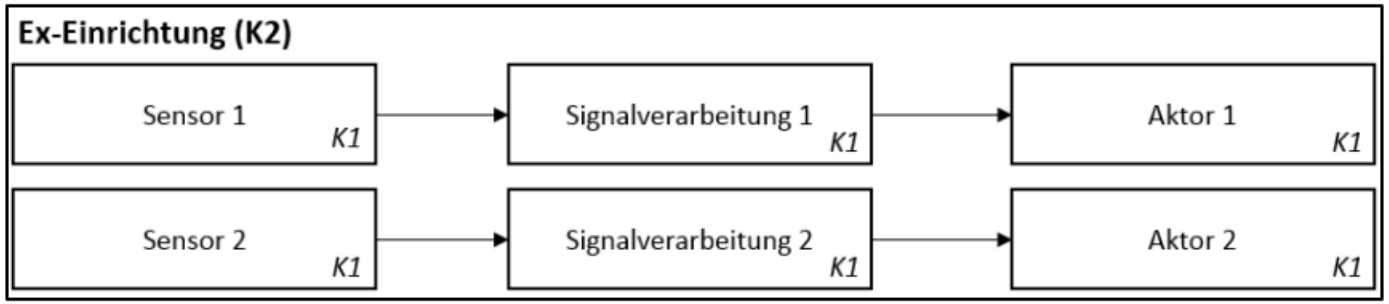


Abbildung 11: Zwei Ex-Einrichtungen der Klassifizierungsstufe K1 (unabhängige Redundanz) und einer resultierenden Klassifizierungsstufe 2.

K1= ausreichende Zuverlässigkeit der Ex-Einrichtung

Hier wird von komplexen Einrichtungen geredet, im Beispiel dann das Ganze dann aber mit Geräten „ausreichender Zuverlässigkeit (K1)“ umgesetzt. Es wird einzig auf Redundanz gesetzt.
Vgl. zu SIL: bei homogener Redundanz wird hier die systematische Eignung auch der SW gefordert, diese ist wichtig, um Common Mode/Common Cause Failure zu vermeiden. Hersteller von Geräten mit SIL-Eignung berücksichtigen dies schon im Design.
Wie soll diese Überlegungen ein Arbeitgeber im Nachhinein leisten?

© HIMA Paul Hildebrandt GmbH 2025

Unterschiedliche Auffassungen

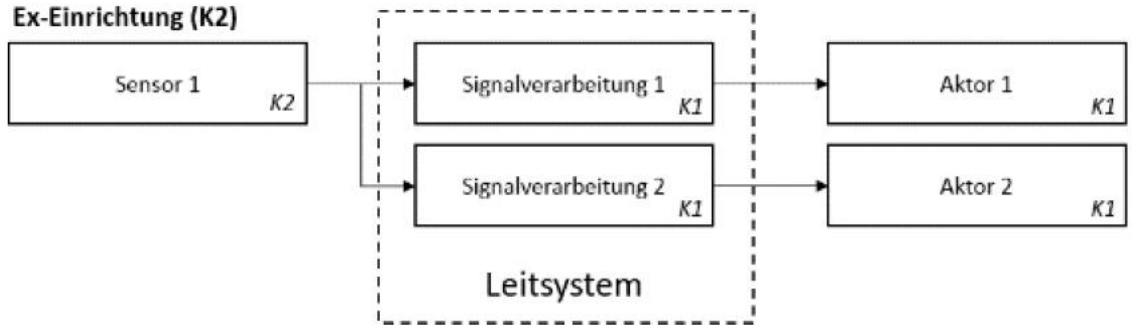


Abbildung 15: Ex-Einrichtung mit Klassifizierungsstufe K2 (bei Realisierung in einem gemeinsamen Prozessleitsystem unter Berücksichtigung von Abschnitt 4.2.3 Absatz 6).

Es gibt Betreiber, die über Werksnormen hier schon einen Riegel vorgeschoben haben → K2 nicht im PLS sondern in SSPS

Sieht man hier nur die Investitionskosten?
..und nicht den Aufwand, der über den ganze Lebenszyklus hinweg mit diesen ganzen Maßnahmen entsteht? (wenn man diese denn wirklich gewissenhaft verfolgt)

4.2.3 Technische Ausführung von Ex-Einrichtungen zur Erfüllung der Klassifizierungsstufen K2 oder K3

(6) Bei der Umsetzung einer Ex-Einrichtung mit der Klassifizierungsstufe K2 in einem Prozessleitsystem (PLS) muss das Leitsystem nicht redundant ausgeführt sein (s.a. Abbildung 17 bis 17), wenn die Gefährdungsbeurteilung nach Abschnitt 3.2 unter Verwendung der TRGS 720 bis TRGS 724 ergeben hat, dass

1. die Wahrscheinlichkeit eines Ausfalls gemeinsamer Komponenten als ausreichend selten eingestuft wurde,
2. eine Explosion nicht unmittelbar durch einen undefinierten Zustand des PLS ausgelöst werden kann (das bedeutet, dass das Fehlverhalten des PLS eine Explosion nicht kausal nach sich zieht),
3. der sichere Zustand bei zentralem Ausfall des PLS in ausreichend kurzer Zeit durch technische oder organisatorische Eingriffe wiederherzustellen ist und
4. betriebsmäßige Zündquellen (Zündquellen im Normalbetrieb) nach dem Stand der Technik ausgeschlossen sind.

(7) Zusätzlich zu den Anforderungen nach Anhang 2 Absatz 7 muss für das PLS hierzu in der Gefährdungsbeurteilung festgestellt worden sein, dass

1. ein zentraler Ausfall des PLS entsprechend 4.2.2. Absatz 4 bewertet und die dort beschriebenen Maßnahmen zur Entdeckung umzusetzen sind,
2. der Ausfall gemeinsam genutzter Komponenten des PLS erkannt wird und Korrekturmaßnahmen ergriffen werden und
3. ein unbeabsichtigtes Ändern der Ex-Einrichtungen nach dem Stand der Technik verhindert wird.

© HIMA Paul Hildebrandt GmbH 2025

Unterschiedliche Auffassungen

Es ist fraglich, ob mit den Maßnahmen dieser Methodik eine dem SIL oder PL gleichwertige Gefährdungsreduzierung erwirkt wird.

Es ist fraglich, ob der Aufwand für den Nachweis der Konformität über den Lifecycle hinweg geringer ausfällt.

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

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

1 SIL, Safety Integrity Level

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

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

4 Zündquellenüberwachung

5 Betriebseinrichtung mit Sicherheitsfunktion

© HIMA Paul Hildebrandt GmbH 2025

Wer hat Angst vor dem bösen SIL?

Funktionale Sicherheit gem. IEC61508 oder ISO13849 ist weltweit anerkannt und reflektiert den Stand der Technik…

Sie hilft dabei Risiken gezielt zu reduzieren und legt die dafür notwendige Qualität der technischen und organisatorischen Maßnahmen (über SIL oder PL) fest.

Betreiber können dabei auf konforme Produkte und Services zurückgreifen.
Der Nachweis der Konformität und der Betrieb der Ex-Einrichtung wird dadurch wesentlich unterstützt.



Persönl. Fazit: TRGS 725 Methodik greift die Prinzipien der FuSi gem. IEC61508 und IEC61511 auf, bleibt dabei jedoch schwammig und verlagert die Verantwortung der Eignung, der Fehleraufdeckung und den Erhalt der Integrität auf den Betreiber.

© HIMA Paul Hildebrandt GmbH 2025

Diskussion



Braucht es den 2. Weg über die Methodik der TRGS 725 zur Umsetzung von Ex-Einrichtungen?

Fred Stay
Director Safety Consulting Europe
HIMA Paul Hildebrandt GmbH
Albert-Bassermann-Straße 28 I 68782 Brühl
Phone +49 6202 5770-130
Cell +49 1624250759 | f.stay@hima.com