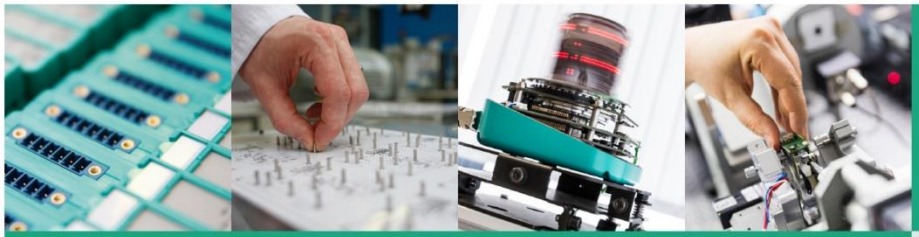


Your automation, our passion.

PEPPERL+FUCHS

Wann genau schalte ich denn ab?

Es ist mit vielem zu rechnen

Quelle: Pixabay

Es ist mit vielem zu rechnen

Es ist mit vielem zu rechnen

NOT MEASUREMENT SENSITIVE

MIL-HDBK-217F

2 DECEMBER 1991

SUPERSEDING
MIL-HDBK-217E, Notice 1
2 January 1990

THIS HANDBOOK IS FOR GUIDANCE ONLY - DO NOT CITE THIS DOCUMENT AS A REQUIREMENT

Ausfallraten raten?

Summary:

λ_{du} = 7,504 FIT	= (Σ Failure_Rate x %
λ_{dd} = 0,006 FIT	= (Σ Failure_Rate x %
λ_{s} = 25,03 FIT	= (Σ Failure_Rate x % distribu
$\lambda_{no\ effect}$ = 32,66 FIT	= (Σ Failure_Rate x % distribu
λtotal = 65,2 FIT	= (Σ Failure_Rate) of all comp
SFF (Safe failure fraction)	= {(total of safety and
	= (0,006+25,03)/(7,5(

Quelle: IEC 60812 CD Ed. 3

$\lambda_{DU} = 25{,}4375\ FIT$

$PFD(1yr) = 1{,}1149 \times 10^{-5}$
im Schaltjahr

Es ist mit vielem zu rechnen

DIN EN 61508-6 (VDE 0803-6):2011-02
EN 61508-6:2010

D.5 Schätzung von β unter Verwendung der Tabellen

- $S = X + Y$, um den Wert für β_{int} zu erhalten (der β-Faktor für unerkannte Ausfä
- $S_D = X(Z + 1) + Y$, um den Wert für $\beta_{D\,int}$ zu erhalten (β-Faktor für erkannte

Common Cause schätzen?

Tabelle D.3 – Werte für Z – Sensoren oder Stellg

Diagnose-deckungsgrad	Diagnose-Testintervall: Geringer als h	Zwischen 2 h und zwei Tagen	Zwischen zwei Tagen und einer Woche
[illegible]	2,0	1,5	1,0
≥ 90 %	1,5	1,0	0,5

Merkmal	Logik-Teilsystem X_{LS}	Logik-Teilsystem Y_{LS}	Sensoren und Stellglieder X_{SF}	Sensoren und Stellglieder Y_{SF}
Prozeduren/Bedienerschnittstelle				
Gibt es eine schriftliche [illegible]anweisung, die sicherstellt, dass alle Bauteilausfälle (oder Verschlechterungen) erkannt, deren Ursachen festgestellt und ähnliche Objekte im Hinblick auf mögliche ähnliche Ausfallursachen überprüft werden?		1,5	0,5	1,5
Sind Verfahren eingerichtet, die sicherstellen, dass die Instandhaltung (einschließlich Anpassung oder Kalibrierung) aller Teile der unabhängigen Kanäle zeitlich versetzt erfolgt und zusätzlich zu den manuellen Prüfungen, die der Instandhaltung folgen, zwischen der Beendigung der Instandhaltung eines Kanals und dem Start der Instandhaltung des nächsten Kanals ein einwandfreier Durchlauf des Diagnosetests erfolgt?	1,5	0,5	2,0	1,0

Tabelle D.4 – Berechnung von β_{int} oder $\beta_{D\,int}$

Bewertung (S oder S_D)	Entsprechender Wert von β_{int} oder $\beta_{D\,int}$ für: Logik-Teilsystem	Sensoren oder Stellglieder
120 oder darüber	0,5 %	1 %
70 bis 120	1 %	2 %
45 bis 70	2 %	5 %
kleiner als 45	5 %	10 %

ANMERKUNG 1 Die höchsten Werte von β in dieser Tabelle sind die

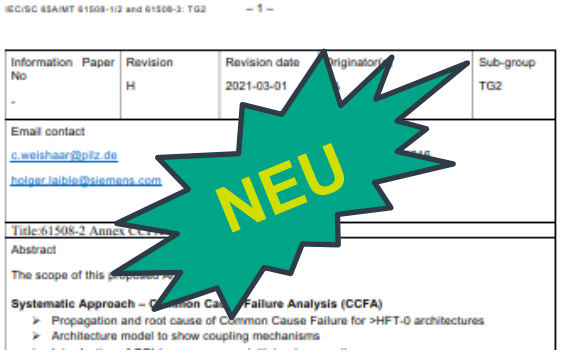
Tabelle D.5 – Berechnung von β für Redundanzsysteme

MooN		N = 2	N = 3	N = 4
M	1	β_{int}	0,5 β_{int}	0,3 β_{int}
	2	-	1,5 β_{int}	0,6 β_{int}
	3	-	-	1,75 β_{int}
	4			

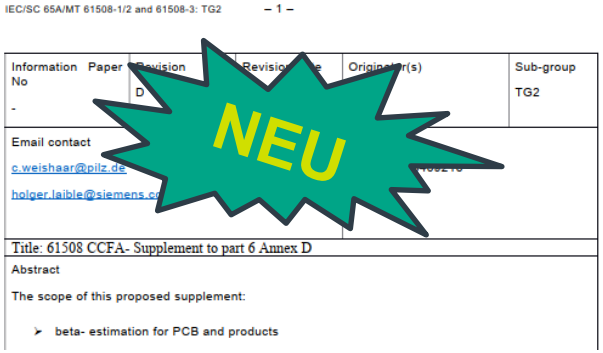
Quelle: DIN EN IEC 61508

Es ist mit vielem zu rechnen

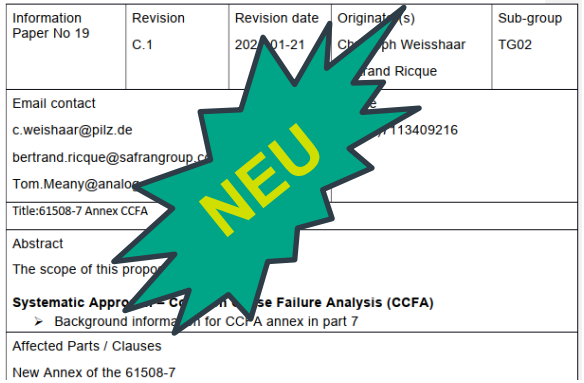
Common Cause schätzen?



Common Cause Initiator
Common Cause Coupling
7 Seiten



PCB / Products
Common Cause Impact
5 Seiten



Background Information
13 Seiten

10%? Markov?

Eine Menge FMEDA

Quelle: Pixabay

Quelle: IEC 60812 Ed.3 CD

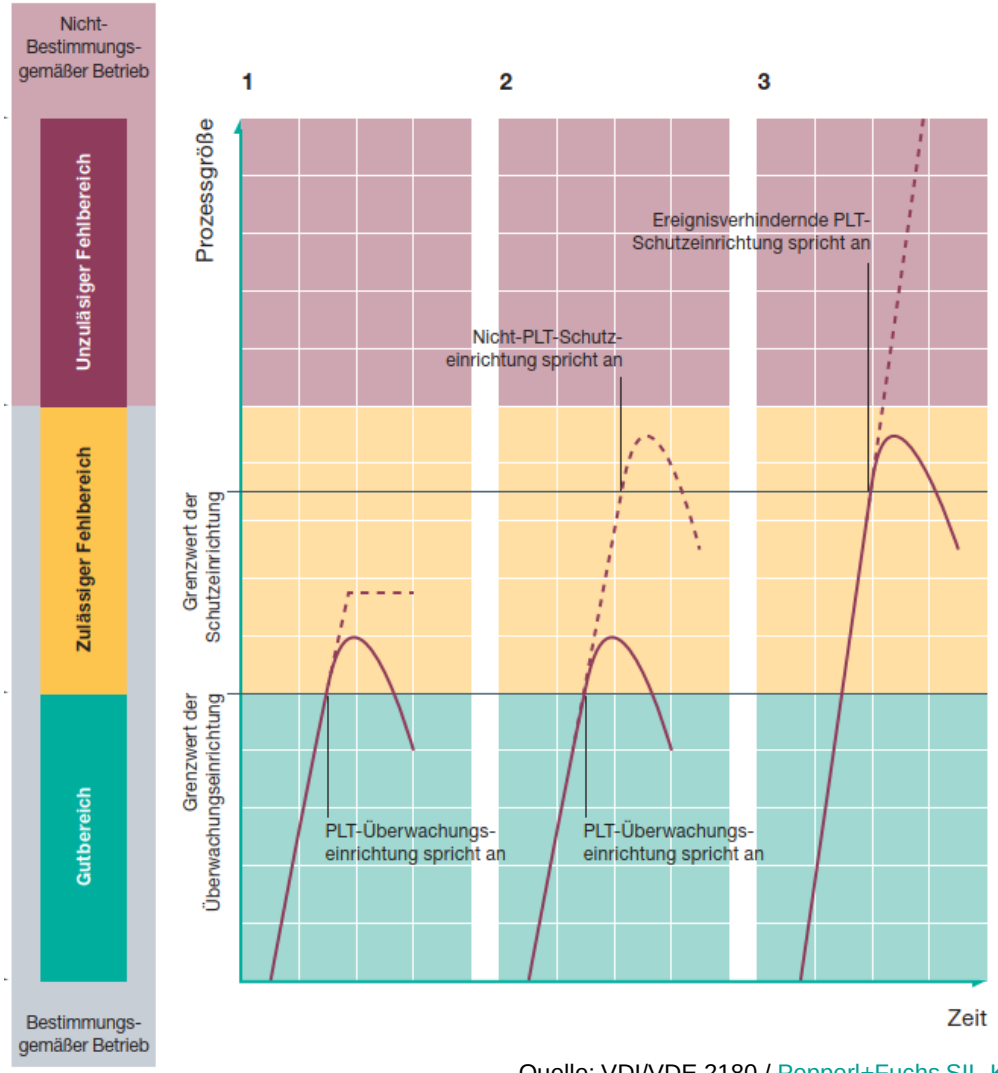
Name	Component	Function	Failure rate [FIT]	Failure Mode	Distribution	Effect
C2	Electrolytic Capacitor, aluminium electrolytic, non-solid electrolyte	Smoothing capacitor	5	Short	53%	F50 blows
				Open	35%	None in normal operation DC supply
				Electrolyte leak	10%	No effect on safety functi
				Decrease in capacitance	2%	Function still given
IC18	Regulator, power > 1 Watt, minor complexity	Voltage regulator used with R100 as current source	25	Stuck-hi	30%	No regulation -> out switching
				Stuck-lo	30%	Outputs de-energize
				Short	15%	No regulation -> ove the relays (diverse)

Quelle: Pixabay

Jeder Spannungsregler Weltweit fällt immer mit Ausfallrate 2,5 x 10^{-8} 1/h aus!

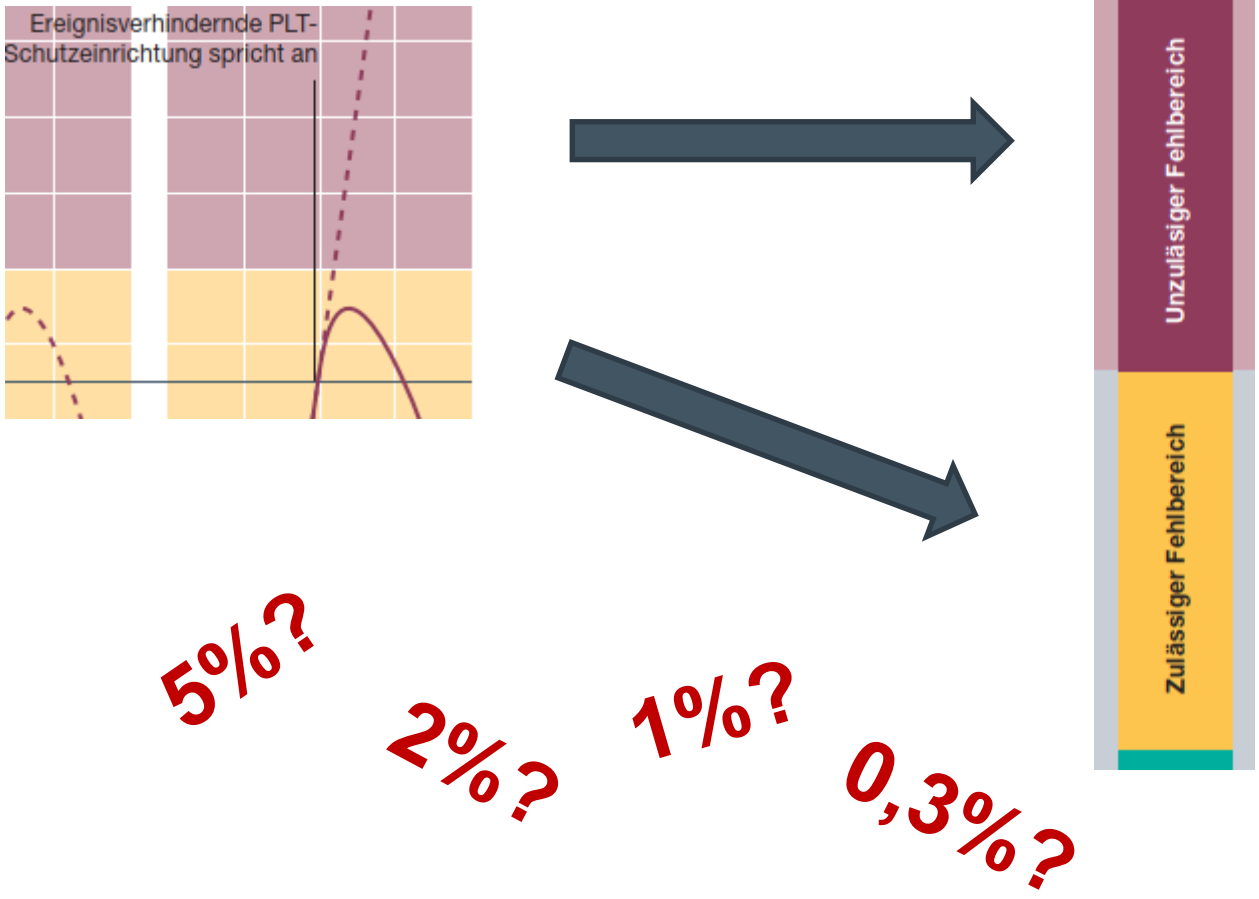
Da kommen total exakte Werte raus!

Wann schalte ich ab?



Quelle: VDI/VDE 2180 / Pepperl+Fuchs SIL-Kompendium

Wie nahe gehe ich denn an die Grenze?



Messtoleranz für den Grenzwert wird wichtig!

Wo liegt der Unterschied in Ausfallraten?

Quelle: exida FMEDA Tool

Name	Component	Qty	Function	Failure Mode	Effect	Lb	Pct_Lb	Distribution
R1	Resistor - Metal film --- No further functionality specified	1		Short circuit	-	2,0E-10	100,0%	10,0%
		1		Open circuit	-	2,0E-10	100,0%	60,0%
		1		Reduced value up to 0.5x	-	2,0E-10	100,0%	15,0%
		1		Increased value up to 2x	-	2,0E-10	100,0%	15,0%
		1		---	-	2,0E-10	100,0%	0,0%
		1		---	-	2,0E-10	100,0%	0,0%
C5	Capacitor (non-electrolytic) - Ceramic NDK / LDC (COG, NPO) --- No further functionality specified	1		Short circuit	-	1,0E-09	100,0%	50,0%
		1		Open circuit	-	1,0E-09	100,0%	30,0%
		1		Reduced value up to 0.5x	-	1,0E-09	100,0%	10,0%
		1		Increased value up to 2x	-	1,0E-09	100,0%	10,0%
		1		---	-	1,0E-09	100,0%	0,0%
		1		---	-	1,0E-09	100,0%	0,0%

0,06 FIT

0,2 FIT

Bei 5% war Drift kein Problem, jetzt gefahrbringend.

Vertraue keiner Statistik…

Name	Component	Qty	Function	Failure Mode	Effect	Lb	Pct_Lb	Distribution
R1	Resistor - Metal film --- No further functionality specified	1		Short circuit	-	2,0E-10	100,0%	10,0%
		1		Open circuit	-	2,0E-10	100,0%	60,0%
		1		Reduced value up to 0.5x	-	2,0E-10	100,0%	15,0%
		1		Increased value up to 2x	-	2,0E-10	100,0%	15,0%
		1		---	-	2,0E-10	100,0%	0,0%
		1		---	-	2,0E-10	100,0%	0,0%
C5	Capacitor (non-electrolytic) - Ceramic NDK / LDC (COG, NPO) --- No further functionality specified	1		Short circuit	-	1,0E-09	100,0%	50,0%
		1		Open circuit	-	1,0E-09	100,0%	30,0%
		1		Reduced value up to 0.5x	-	1,0E-09	100,0%	10,0%
		1		Increased value up to 2x	-	1,0E-09	100,0%	10,0%
		1		---	-	1,0E-09	100,0%	0,0%
		1		---	-	1,0E-09	100,0%	0,0%

Der Unterschied liegt meist nur in Drift-Fehlern.

Und: fast immer eine gefährliche, eine sichere Richtung – halber Wert!

Prima! Nur 0,13 FIT

Etwas nachgedacht…

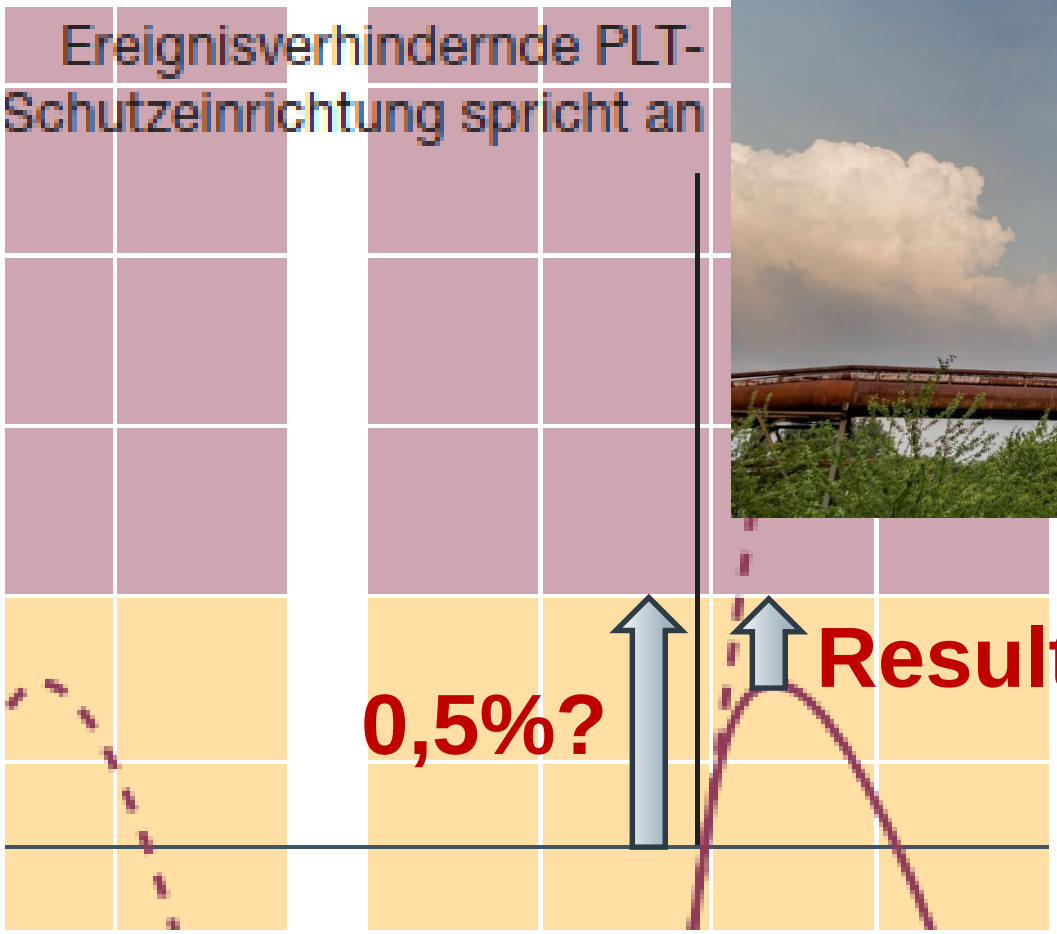
Angabe mit kleinen Messtoleranzen ist kein Problem und wird auf Anfrage gemacht. Resultate sind nicht schlecht.

Aber nur wenn Erfahrungswerte das Ergebnis bestätigen!

source of uncertainty	HW	SW	AI
systematic failures	✓	✓	✓
„random" failures	λ	– –	λ_{AI}

Quelle: VDE-AR-E 2842-61

Etwas nachgedacht…



Resultat: 0,x% ?

Wann schalte ich denn ab?

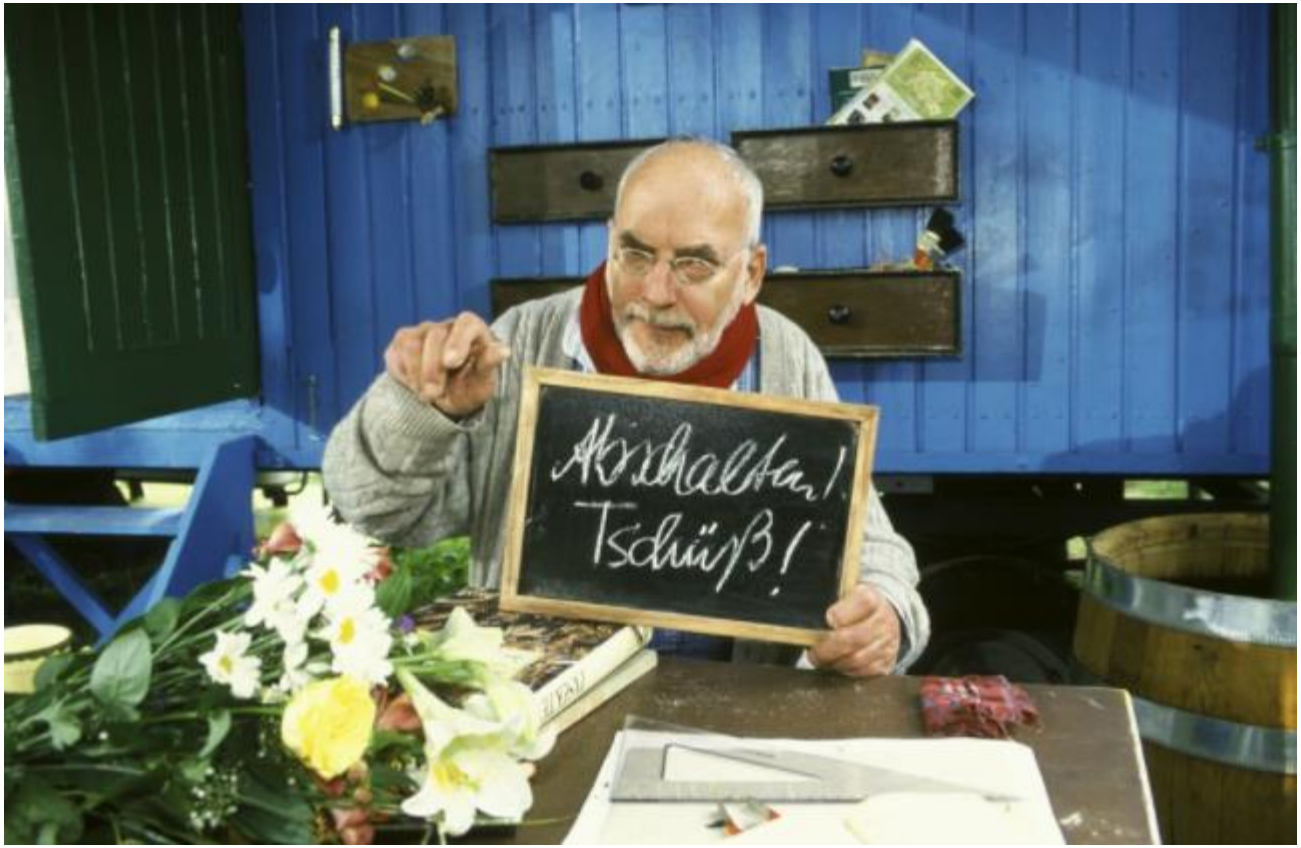


Foto: ZDF/Christiane Pausch

PEPPERL+FUCHS

About the presenter

Dipl. Ing. Michael Kindermann

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

THE END…

Michael Kindermann

mkindermann@de.pepperl-fuchs.com

Pepperl+Fuchs Inc.
Twinsburg · Ohio · USA
Tel. +1 330 425 3555
E-Mail: sales@us.pepperl-fuchs.com

Pepperl+Fuchs GmbH
Mannheim · Germany
Tel. +49 621 776 0
E-Mail: info@de.pepperl-fuchs.com

Pepperl+Fuchs PTE Ltd.
Singapore
Tel. +65 677 99091
E-Mail: sales@sg.pepperl-fuchs.com