

STARKES STUDIUM.
PRIMA ZUKUNFT.



TECHNIK

WIRTSCHAFT

INFORMATIK

Sicherheitstechnik, 4. Vorlesung (Safety Technology)

Campus Heilbronn

Campus Künzelsau

Reinhold-Würth-Hochschule

Campus Schwäbisch Hall

Fred Härtelt, Heilbronn

Beispiel (1996): Absturz der Ariane 5

Raumfahrt: Abstürze durch Fehler

08.05.2009

Über 30 Jahre später, am 4. Juni 1996 um 9.34 Uhr morgens, drückte im Raumfahrtzentrum Kourou ein Mitarbeiter im Kontrollzentrum wieder einen roten Knopf – und zerstörte die Ariane 5 auf ihrem Jungfernflug. Die Rakete war nach 37 Sekunden Flug vom Kurs abgewichen und drohte auseinanderzubrechen. Auch ihre Trümmer stürzten anschließend in die Karibik.



► Problematik:

- Neue Hardware mit bestehender Software (Übernahme aus Ariane 4)
- Geschwindigkeit / Beschleunigung deutlich höher als bei Ariane 4
- Speicherüberlauf durch Umrechnung der höheren Geschwindigkeit (von einem 64 bit in einen 16 bit Wert), keine Tests

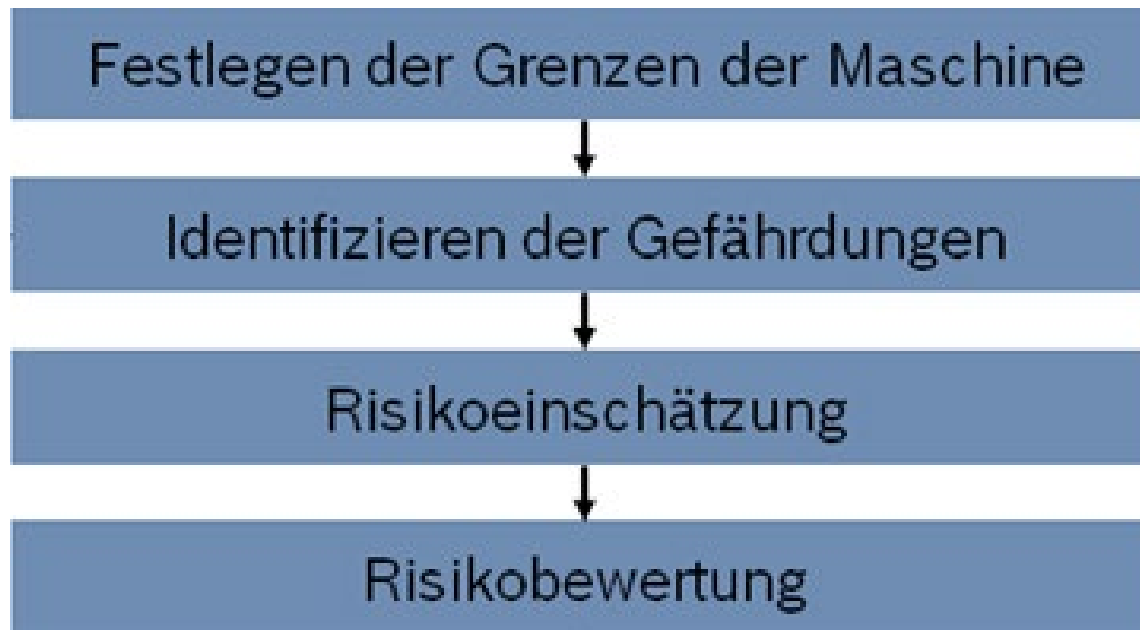


Quellen: www.wikipedia.de, www.chip.de

Sicherheitstechnik: zeitlicher Überblick

- ▶ 1. V: Definition Sicherheit, Normen und Vorschriften (14.03.2022)
- ▶ 2. V: Festlegung von Grenzen und Gefährdungen (21.03.2022)
- ▶ 3. V: Risikobeurteilung, -minimierung, Risikograph (28.03.2022)
- ▶ **4. V: Verteilungsfunktion, Ausfallraten, Fehlerbeherrschung (04.04.2022)**
- ▶ 5. V: Fehlervermeidung, Fehlerentdeckung, FMEA (11.04.2022)
- ▶ Keine Vorlesung am 18.04.2022 (Ostermontag)
- ▶ Keine Vorlesung am 25.04.2022
- ▶ 6. V: Redundanz, Strukturierungsmaßnahmen, FTA (02.05.2022)
- ▶ 7. V: Berechnung von Ausfallraten, FMEDA, Aufgabenstellung Belegarbeit, **Einteilung der Gruppen** (09.05.2022)
- ▶ 8. V: Prozess vs. Technik, Besonderheiten HW/SW, Zuverlässigkeit SW Entwicklungsprozess, Bsp. Belegarbeit, **Beginn der Gruppenarbeit** (16.05.2022)
- ▶ Rückfragen bezüglich Gruppenarbeit am 23.05., 30.05. und 13.06.2022 (WebEx)
- ▶ Abgabetermin der Gruppenarbeiten: **20.06.2022** (vor Beginn der Präsentationen)
- ▶ Präsentationstermine der Gruppen: **20.06.2022** (vorläufiger Stand)

Sicherheitstechnik: Wiederholung

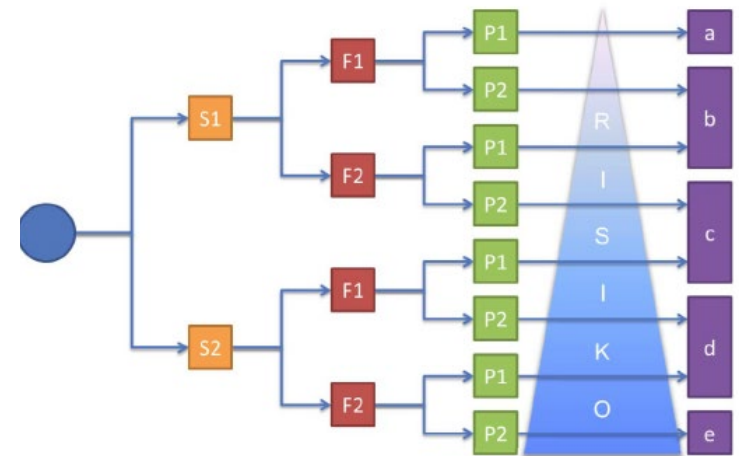


Sicherheitstechnik: Wiederholung

► 1. Berechnung des Performance Level (PL) mit einem Risikograph



S	Schwere der Verletzung
S1 – leicht (üblicherweise reversible Verletzung)	S2 – ernst (üblicherweise irreversible Verletzungen einschließlich Tod)
F	Häufigkeit und Dauer der Gefährdungsexposition
F1 – selten bis weniger häufig und/oder die Dauer der Gefährdungsexposition ist kurz (nicht häufiger als 2-Mal am Tag und insgesamt nicht länger als 15 min.)	F2 – häufig bis dauernd und/oder die Dauer der Gefährdungsexposition ist lang
P	Vermeidung der Gefährdung
P1 – möglich unter bestimmten Bedingungen	P2 – kaum möglich



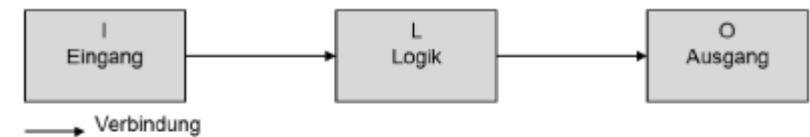
Sicherheitstechnik: Wiederholung

► Kategorien nach ISO 13849:

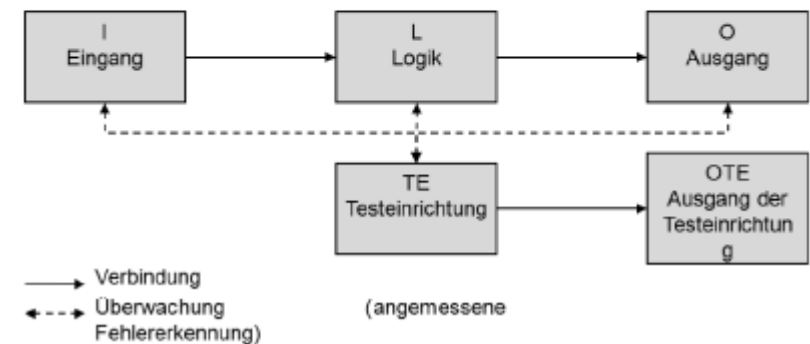


Merkmal	Kategorie				
	B	1	2	3	4
Gestaltung gemäß zutreffender Normen, zu erwartenden Einflüssen standhalten	X	X	X	X	X
Grundlegende Sicherheitsprinzipien	X	X	X	X	X
Bewährte Sicherheitsprinzipien		X	X	X	X
Bewährte Bauteile		X			
Mean Time to Dangerous Failure - MTTF _d	niedrig bis mittel	hoch	niedrig bis hoch	niedrig bis hoch	hoch
Fehlererkennung (Tests)			X	X	X
Einfehlersicherheit				X	X
Berücksichtigung von Fehlerakkumulation					X
Diagnosedeckungsgrad - DC _{avg}	kein	kein	niedrig bis mittel	niedrig bis mittel	hoch
Maßnahmen gegen Fehler gemeinsamer Ursache (CCF)			(X) bedingt	X	X
Hauptsächlich charakterisiert durch	Bauteilauswahl		Struktur		

Kategorie B und Kategorie 1



Kategorie 2



Sicherheitstechnik: Wiederholung

- Erreichung des Performance Level (PL) mit einem Risikograph

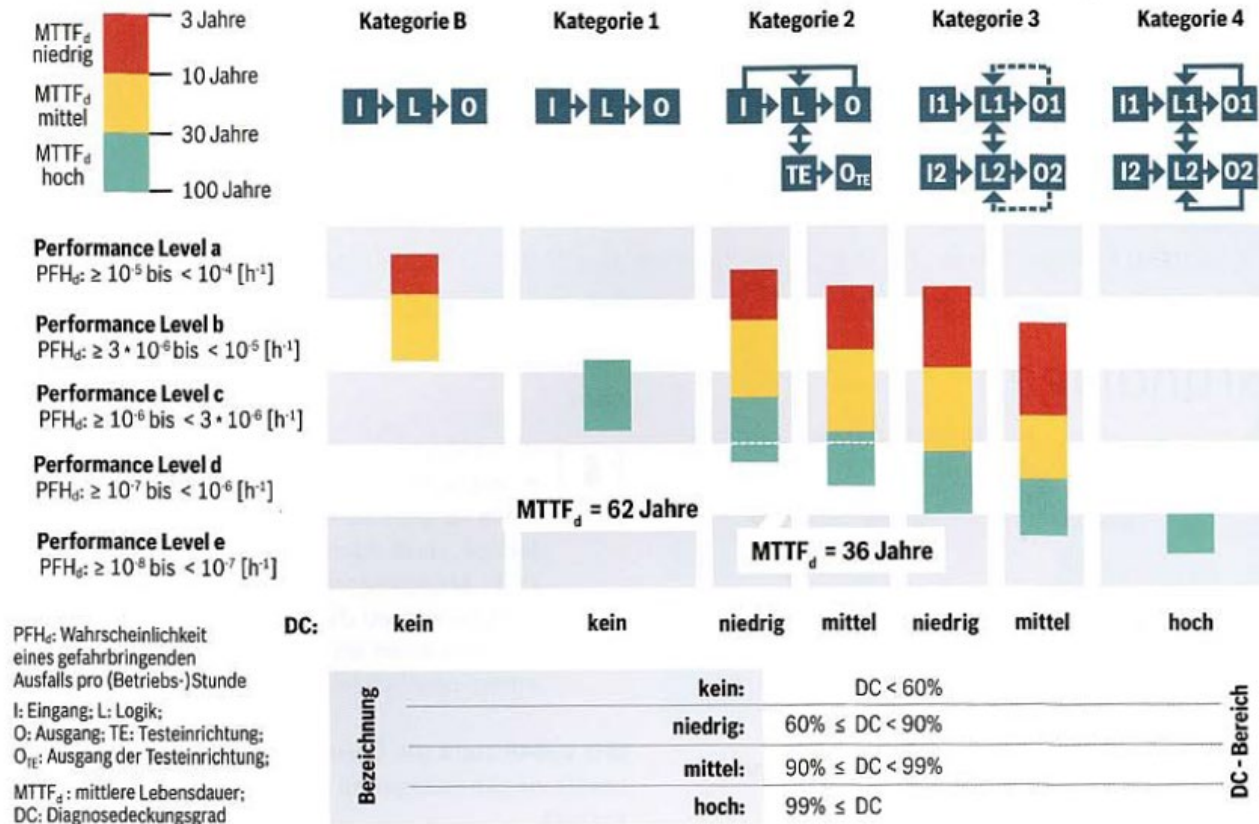
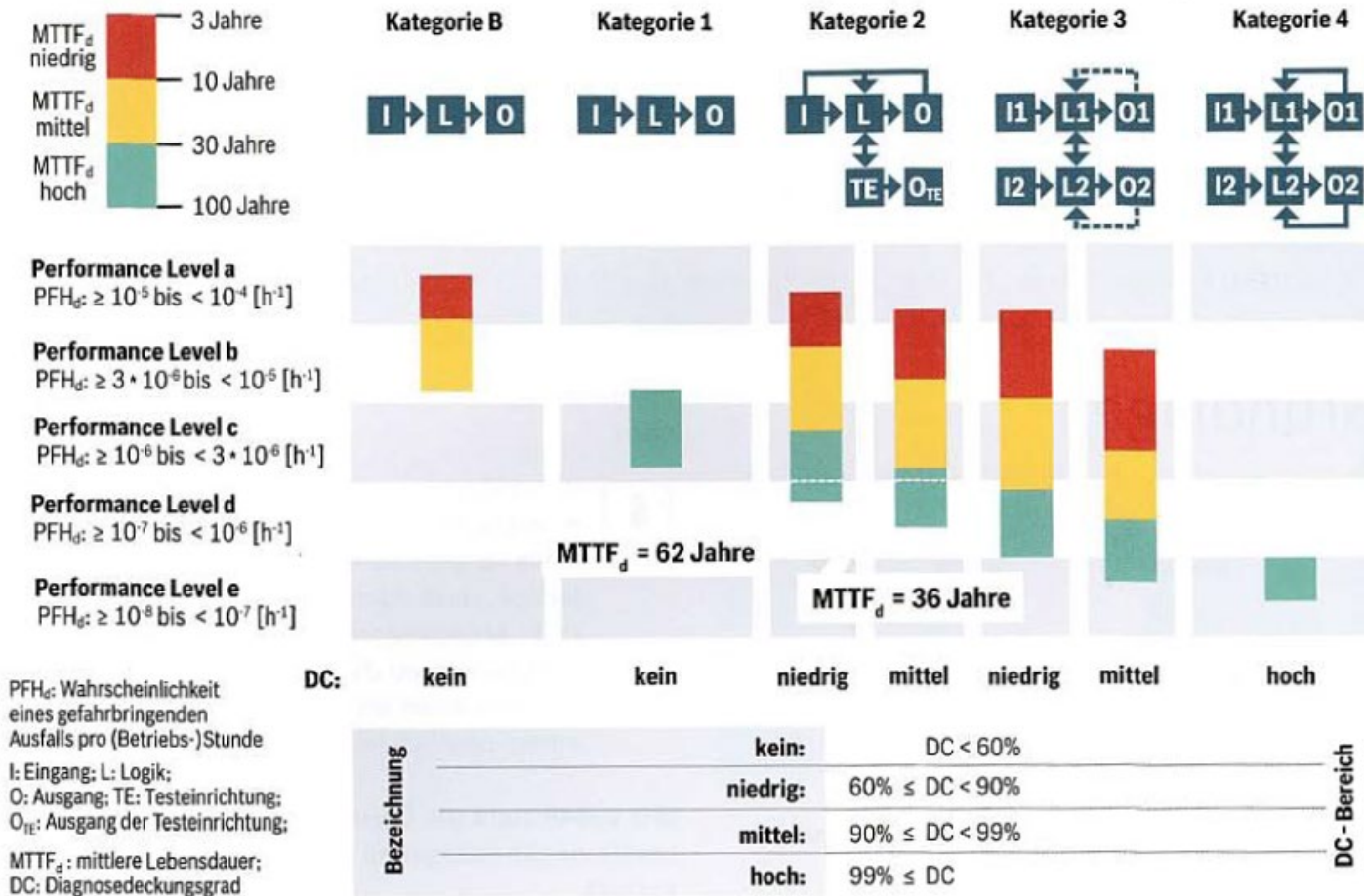


Abb. B-4.1: Beziehung zwischen Kategorien und PL

Sicherheitstechnik: Übung 5



Sicherheitstechnik: Lösung Übung 5

Angewandtes Diagramm nach DIN EN ISO 13849-1 zur Bestimmung des erforderlichen Performance-Level (PL).

Schwere der Verletzung (severity)

S1: leichte Verletzung

S2: Tod oder schwere Verletzung

Häufigkeit und Aufenthaltsdauer (frequency)

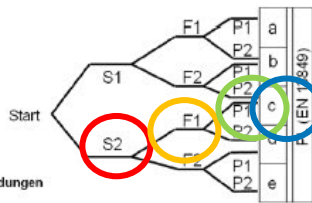
F1: selten bis öfter

F2: häufig bis dauernd

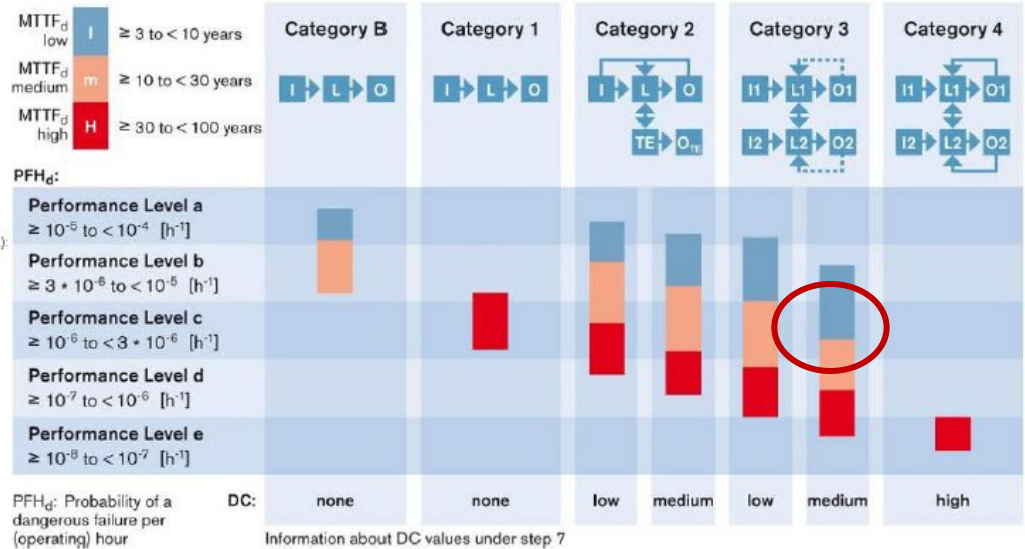
Möglichkeit zur Vermeidung von Gefährdungen (possibility of avoidance)

P1: möglich unter bestimmten Bedingungen

P2: kaum möglich



PL: Performance-Level



Gefährdung	Definierter Performance Level	Erreichter Performance Level
Verklemmung von Körperteilen während der Absenkung des Hubtischs	<p>S = 2</p> <p>F = 1</p> <p>P = 1</p> <p>PL = c</p>	<p>Kategorie = 3</p> <p>Diagnosedeckungsgrad = mittel</p> <p>PL = c</p>

Sicherheitstechnik

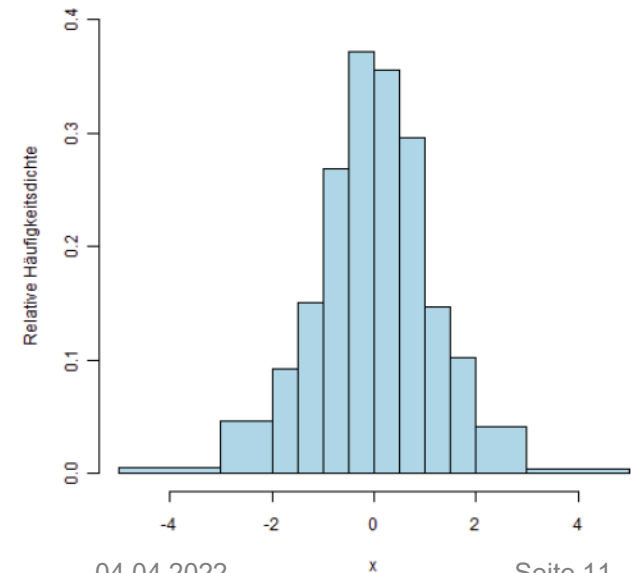
Inhalte

- ▶ Definition Sicherheit
- ▶ Aktuelle Normen und Vorschriften
- ▶ Methoden und Verfahren
 - ▶ Risikobeurteilung und –minderung, Risikograph
 - ▶ Verteilungsfunktionen, Ausfallraten, Fehlerbeherrschung und Vermeidung, Fehlerentdeckung, Redundanz
 - ▶ Strukturierungsmaßnahmen, FMEA, FTA, FMEDA u.a.
 - ▶ Unterscheidung Prozess vs. Technik
- ▶ Besonderheiten hinsichtlich Hardware und Software (Zuverlässigkeit SW Entwicklungsprozess)

Verteilungsfunktion

- ▶ Hintergrund Verteilungsfunktion (siehe Mathematik 3 Vorlesung -> Kategorie von Messfehlern)
- ▶ Normalverteilung als eine beispielhafte Verteilungsfunktion (weitere: Hypergeometrische Verteilung, Binominalverteilung, Poissonverteilung, ...)
- ▶ Die Abweichung kann zu einer Fehlerfortpflanzung führen

$$p(x) = \frac{1}{\sigma \sqrt{2\pi}} \exp\left(-\frac{(x - \mu)^2}{2\sigma^2}\right)$$



Verteilungsfunktion

► Bedeutung

- Aufgrund der Fehlerfortpflanzung und den Einfluss auf die Fehlerraten (Vererbung von Fehlern -> siehe auch Gaußsches Fehlerfortpflanzungsgesetz).

$$\sigma_y = \sqrt{\left(\frac{\partial y}{\partial x_1} \cdot \sigma_1\right)^2 + \left(\frac{\partial y}{\partial x_2} \cdot \sigma_2\right)^2 + \dots + \left(\frac{\partial y}{\partial x_n} \cdot \sigma_n\right)^2}$$

- Dies hat Auswirkung auf die Absicherung von Fehlern und wie man diese verhindern kann (Einfachfehler, Mehrfachfehler, ...).

Fehlerraten

- ▶ = Fehlerquote
- ▶ der relative Anteil von fehlerhaften Elementen im Verhältnis zur Gesamtheit
- ▶ relative Häufigkeit, mit der ein Fehler bei einem Produkt, einer Dienstleistung, einem Produktionsprozess oder der Arbeitsqualität auftaucht
- ▶ Wird vor allem im Qualitätsmanagement verwendet
- ▶ Einheit: z.B. Maß, Prozent, ppm, ...
- ▶ Wird in verschiedensten Handbüchern referenziert

Fehlerraten

► Bsp. Siemensnorm:

			Komplexität in Bit / Complexity in bits										$\theta_{vj,1}$ in °C	
			512 ¹⁾ 16K	32K 64K	128K 256K	512K 1M	2M 4M	8M 16M	32M 64M	128M 256M	512M 1G	2G 4G		
			λ_{ref} in FIT											
Bipolar	RAM, FIFO	statisch <i>static</i>	50	60	-	-	-	-	-	-	-	-	75	
	PROM		60	80	-	-	-	-	-	-	-	-		
MOS, CMOS, BICMOS	RAM	dynamisch <i>dynamic</i>	50	30	20	10	10	15	20	25		-	55	
			-	-	-	-	-	-	-	-	70	(100)	70	
	RAM, FIFO	statisch langsam >=30ns <i>static slow</i> ²⁾	15	10	10	10	10	30	50	-	-	-	55	
		statisch schnell <30ns <i>static fast</i> ²⁾	30	25	15	25	40	55	90	-	-	-	70	
	ROM mask		50	30	15	15	15	15	25	-	-	-	55	
	EPROM, OTPROM UV-löschbar <i>UV eraseable</i>		30	30	20	20	20	20	40	-	-	-		
	FLASH		-	-	30	30	40	50	70	(100)	-	-		
			-	-	-	-	-	-	-	-	(200)	-		70
	EEPROM, EAROM		30	30	30	50	-	-	-	-	-	-		55

Fehlerraten

► Bsp.: Birolini

Table 3.4 Indicative values for failure modes of electronic components (%)

Component		Shorts	Opens	Drift	Functional
Digital bipolar ICs		50* ^Δ	30*	—	20
Digital MOS ICs		20 ^Δ	60*	—	20
Linear ICs		—	25 ⁺	—	75 ⁺⁺
Bipolar transistors		85	15	—	—
Field effect transistors (FET)		80	15	5	—
Diodes (Si)	general purpose	80	20	—	—
	Zener	70	20	10	—
Thyristors		20	20	50	10 [◇]
Optoelectronic devices		10	50	40	—
Resistors, fixed (film)		—	40	60	—
Resistors, variable (Cermet)		—	70	20	10 [#]
Capacitors	foil	15	80	5	—
	ceramic	70	10	20	—
	Ta (solid)	80	15	5	—
	Al (wet)	30	30	40	—
Coils		20	70	5	5
Relays		20	—	—	80 [†]
Quartz crystals		—	80	20	—

* input and output half each; ^Δ short to V_{CC} or to GND half each; ⁺ no output;
⁺⁺ improper output; [◇] fail to off; [#] localized wearout; [†] fail to trip / spurious trip $\approx 3/2$

Fehlerbeherrschung

- ▶ Verschiedene Möglichkeiten (z.B. durch die Vermeidung von Einzel- und Mehrfachfehlern) werden angewendet in der Hardware und Software
- ▶ Hardware: z.B. Redundanz (2 Kanäle)
- ▶ Software: z.B. Überwachungsfunktionen
- ▶ Verschiedene Analyseverfahren: FMEA, FTA, FMEDA
- ▶ Weitere Möglichkeiten bestehen in der Anwendung von standardisierten Prozessen

ISO 26262: Gefahren- und Risikoanalyse

		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	ASIL A
	E4	QM	ASIL A	ASIL B
S2	E1	QM	QM	QM
	E2	QM	QM	ASIL A
	E3	QM	ASIL A	ASIL B
	E4	ASIL A	ASIL B	ASIL C
S3	E1	QM	QM	ASIL A
	E2	QM	ASIL A	ASIL B
	E3	ASIL A	ASIL B	ASIL C
	E4	ASIL B	ASIL C	ASIL D

S: Estimation of potential severity

Class	SO	S1	S2	S3
Description	No injuries	Light and moderate injuries	Severe and life threatening injuries (survival probable)	Life threatening injuries (survival uncertain), fatal injuries

E: Estimation of probability of exposure in driving and operating situation

Class	E1	E2	E3	E4
Description	Very low probability	Low probability	Medium probability	High probability

C: Estimation of controllability

Class	CO	C1	C2	C3
Description	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable

Übung 11



		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	ASIL A
	E4	QM	ASIL A	ASIL B
S2	E1	QM	QM	QM
	E2	QM	QM	ASIL A
	E3	QM	ASIL A	ASIL B
	E4	ASIL A	ASIL B	ASIL C
S3	E1	QM	QM	ASIL A
	E2	QM	ASIL A	ASIL B
	E3	ASIL A	ASIL B	ASIL C
	E4	ASIL B	ASIL C	ASIL D

S: Estimation of potential severity

Class	SO	S1	S2	S3
Description	No injuries	Light and moderate injuries	Severe and life threatening injuries (survival uncertain), fatal injuries	Life threatening injuries (survival uncertain), fatal injuries

E: Estimation of probability of exposure in driving and operating situation

Class	E1	E2	E3	E4
Description	Very low probability	Low probability	Medium probability	High probability

C: Estimation of controllability

Class	C0	C1	C2	C3
Description	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable

Lösung Übung 11

		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	ASIL A
	E4	QM	ASIL A	ASIL B
S2	E1	QM	QM	QM
	E2	QM	QM	ASIL A
	E3	QM	ASIL A	ASIL B
	E4	ASIL A	ASIL B	ASIL C
S3	E1	QM	QM	ASIL A
	E2	QM	ASIL A	ASIL B
	E3	ASIL A	ASIL B	ASIL C
	E4	ASIL B	ASIL C	ASIL D

S: Estimation of potential severity

Class	S0	S1	S2	S3
Description	No injuries	Light and moderate injuries	Severe and life threatening injuries (survival probable)	Life threatening injuries (survival uncertain), fatal injuries

E: Estimation of probability of exposure in driving and operating situation

Class	E1	E2	E3	E4
Description	Very low probability	Low probability	Medium probability	High probability

C: Estimation of controllability

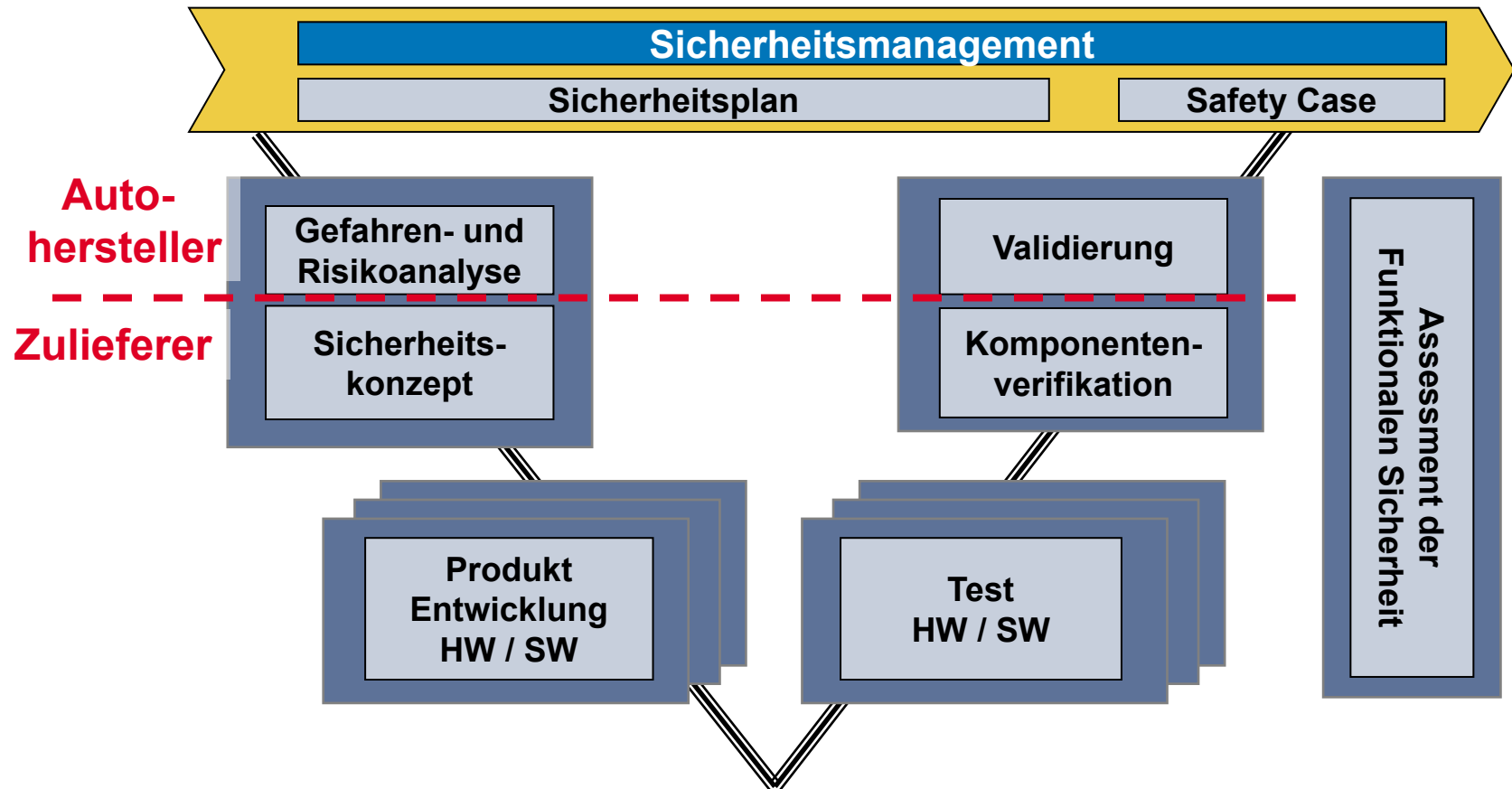
Class	C0	C1	C2	C3
Description	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable

Gefährdung	Fahrzeug während der Fahrt	Fahrzeug in Stillstand
Ungewollte Beschleunigung des Fahrzeugs	<p>S = 3</p> <p>E = 2</p> <p>C = 3</p> <p>ASIL = B</p>	<p>S = 3</p> <p>E = 3</p> <p>C = 2</p> <p>ASIL = B</p>

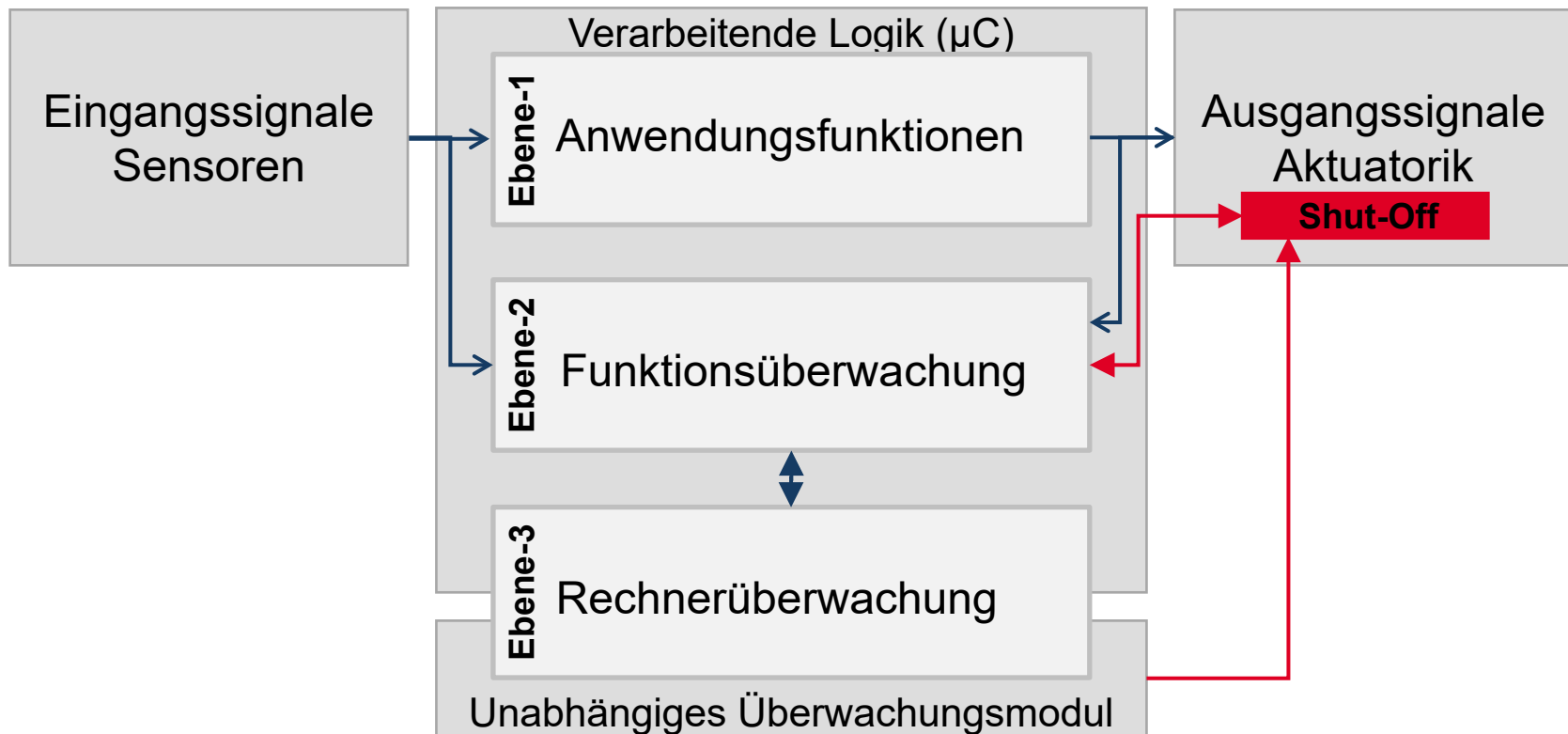
ISO 26262: Beispiele für Gefährdungen

Beispiel

ISO 26262: Verantwortlichkeiten



ISO 26262: Sicherheitskonzept (3-Ebenen Modell)



Quelle: Andreas Heyl

ISO 26262: Sicherheitskonzept



Schema zur Absicherung einer Wirkkette

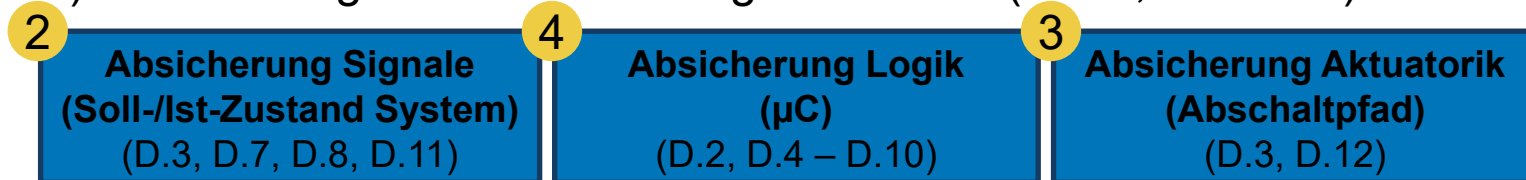
1) Bestimmung Sicherheitsziel und Sicherheitsanforderungen

Sicherheitsziel Fehlertoleranzzeit Sicherer Zustand ASIL

2) Definition Sicherheitsfunktion, z.B. Überwachung von Parametern

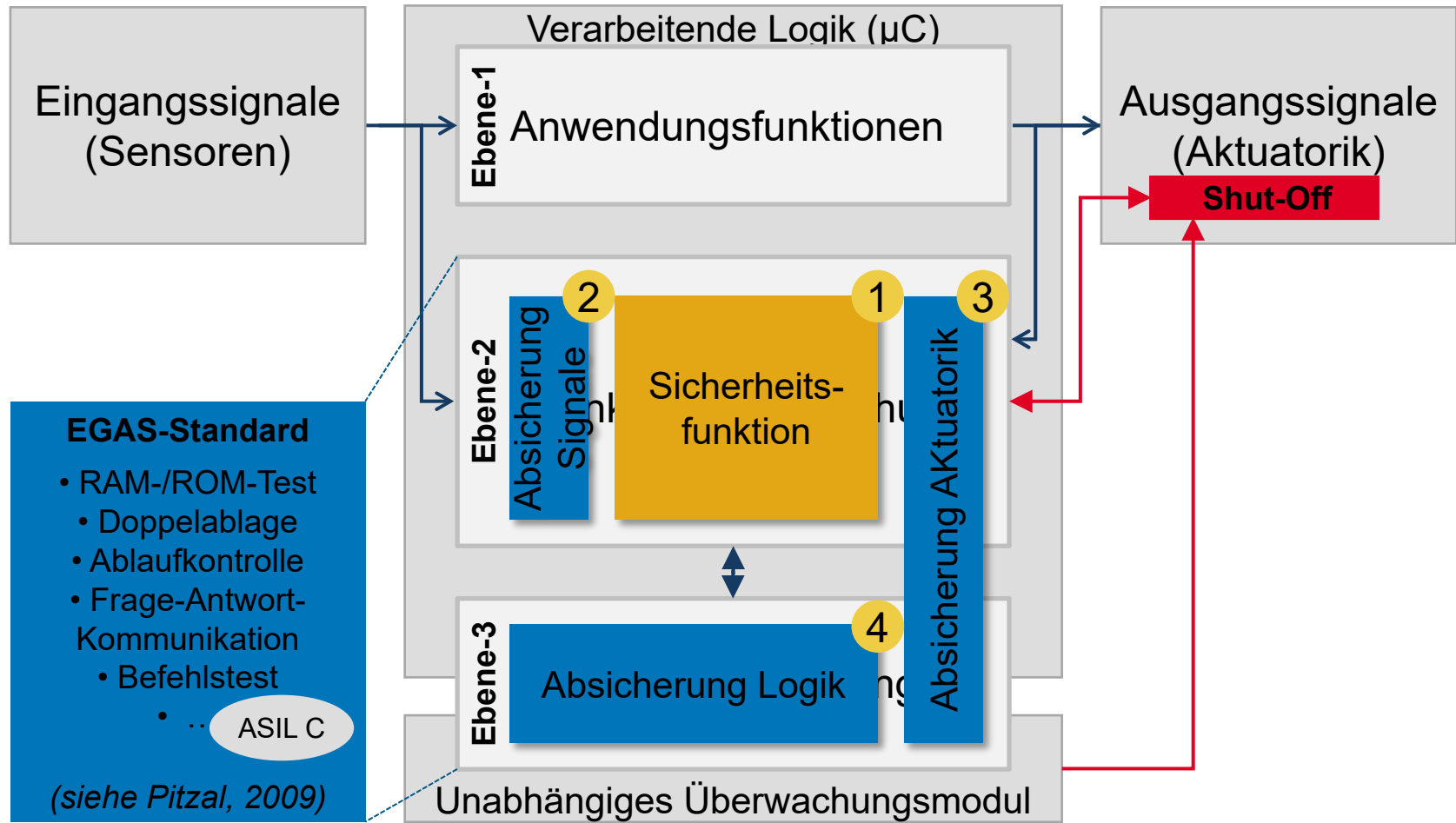


3) Absicherung Sicherheitskette gemäß ASIL (Teil 5, Annex D)



Quelle: Andreas Heyl

ISO 26262: Sicherheitskonzept

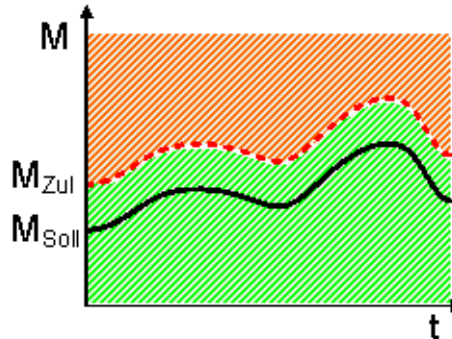


Quelle: Andreas Heyl

ISO 26262: Motorsteuerung

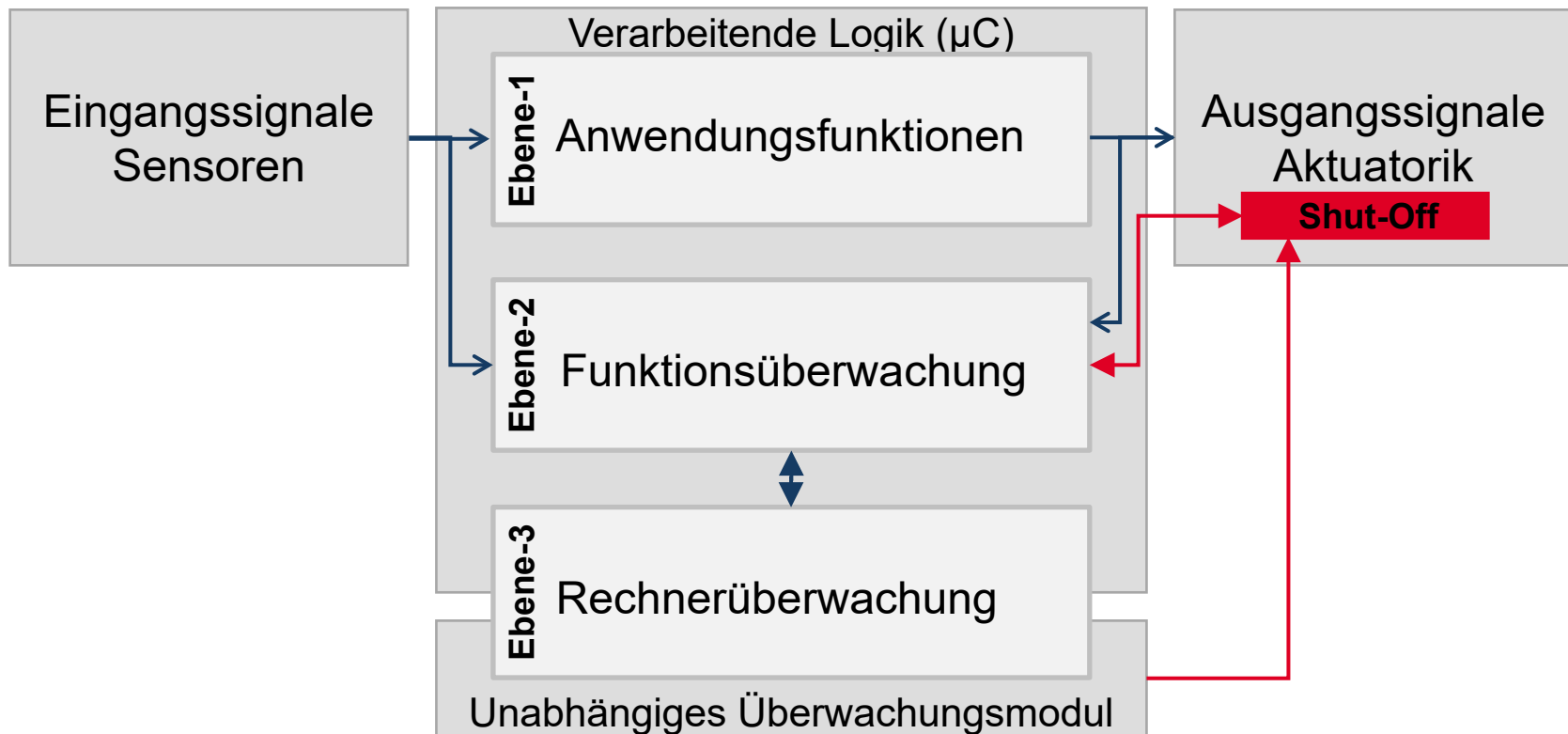


Sicherheitsziel	Vermeidung ungewollter Beschleunigung	ASIL B
Sicherer Zustand	Motor "Aus" bzw. Einspritzmengenbegrenzung	500ms
Sicherheitsanforderung	"Das gestellte Drehmoment muss kontinuierlich auf Grenzwertüberschreitung überwacht werden."	

1	Sicherheitsfunktion	$M_{Ist}(t) \leq M_{zul}(t) = f(M_{Soll}(t))$	
2	Abzusichernde Signale	M_{Soll} : Pedal, CAN, Drehzahl, ... M_{Ist} : Luft-, Kraftstoffmasse, Zündung, ...	
3	Abschaltpfad	Deaktivierung momentenrelevanter Endstufen (fail silent)	

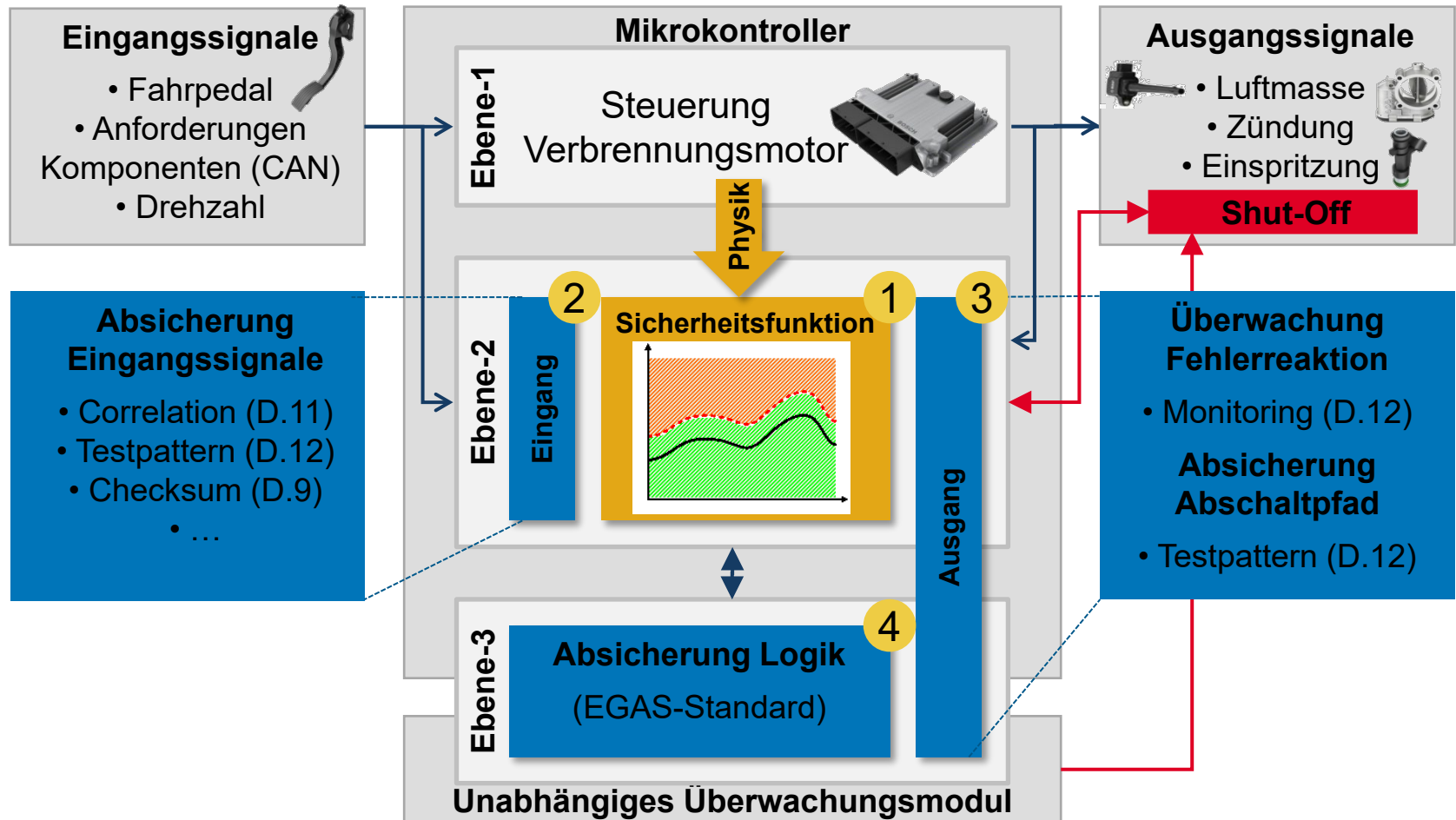
Quelle: Andreas Heyl

ISO 26262: Sicherheitskonzept (3-Ebenen Modell)



Quelle: Andreas Heyl

ISO 26262: Motorsteuerung

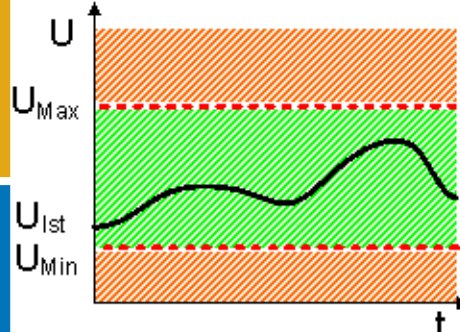


Quelle: Andreas Heyl

ISO 26262: Batteriesteuerung

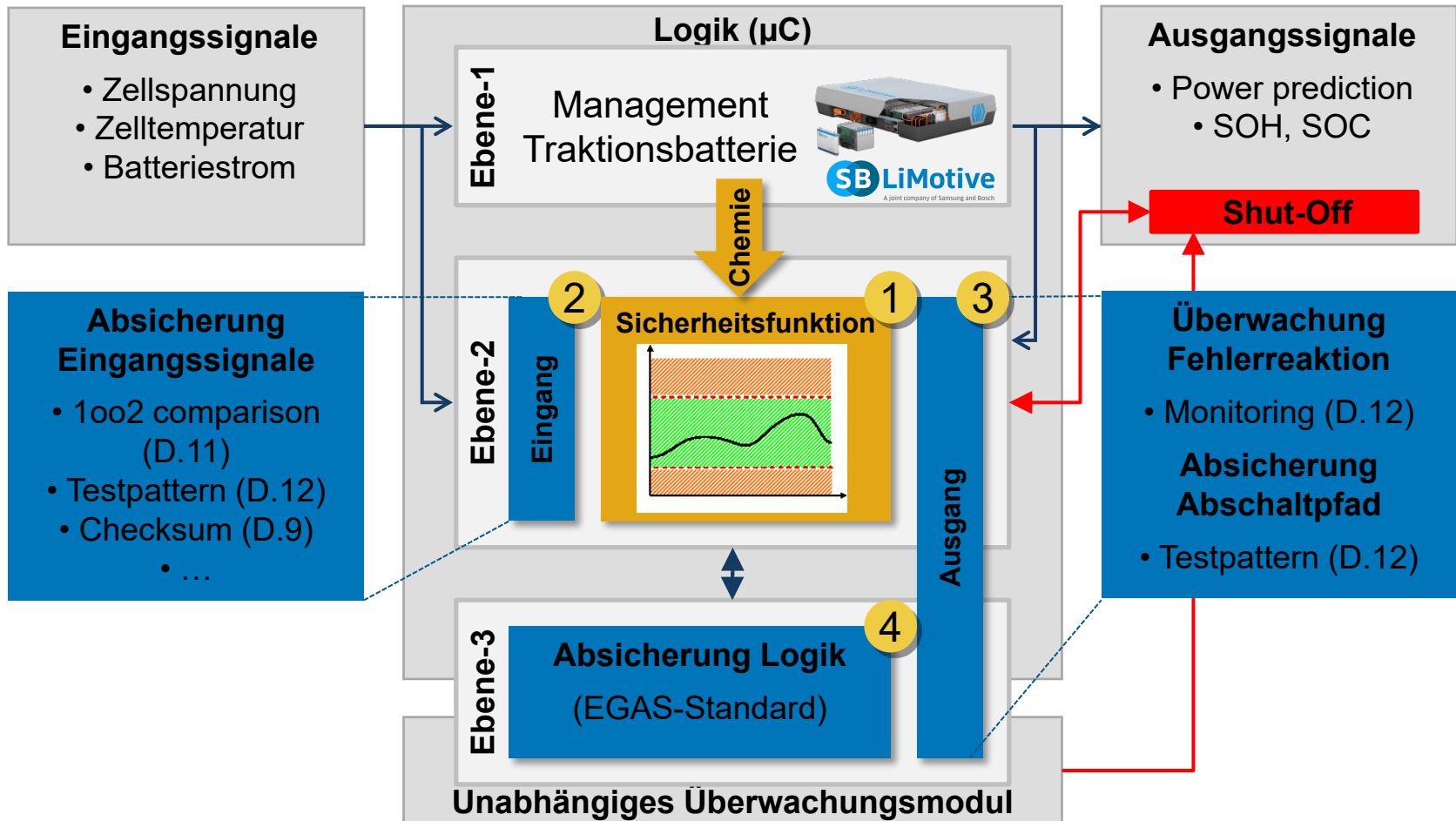


Sicherheitsziel	<i>Vermeidung Überhitzung der Batterie</i>	ASIL C
Sicherer Zustand	<i>Galvanische Trennung HV-Stromkreis</i>	1 – 30s
Sicherheitsanforderung	<i>“Die Batterieparameter müssen kontinuierlich auf Grenzwertüber- und -unterschreitung überwacht werden.” (<=> Thermal Runaway)</i>	

1	Sicherheitsfunktion	$U_{Zelle,min} \leq U_{Zelle} \leq U_{Zelle,max}$ $T_{Zelle} \leq T_{Zelle,max}$ $I_{Pack} \leq I_{pack,max}$	
2	Abzusichernde Signale	Zell-, Packspannungen Zelltemperaturen Batteriestrom	
3	Abschaltpfad	<i>Trennen beider Hauptschütze (fail-silent)</i>	

Quelle: Andreas Heyl

ISO 26262: Batteriesteuerung



Quelle: Andreas Heyl