STARKES STUDIUM.
PRIMA ZUKUNFT.

HOCHSCHULE HEILBRONN

TECHNIK WIRTSCHAFT INFORMATIK

Sicherheitstechnik, 7. Vorlesung (Safety Technology)

Campus Heilbronn

Campus Künzelsau
Reinhold-Würth-Hochschule

Campus Schwäbisch Hall

Fred Härtelt, Heilbronn

Beispiel: Dreamliner (Boeing 787)

Quellen: www.spiegel.de

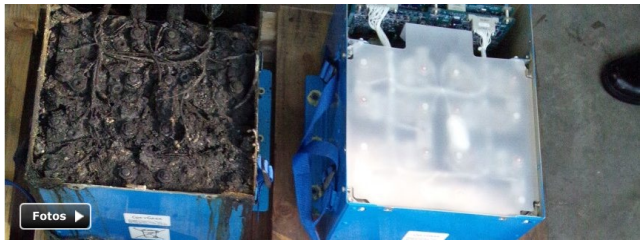
Boeing 787: US-Luftfahrtbehörde warnt vor Stromausfall im Dreamliner

Die US-Luftsicherheitsbehörde warnt: In Boeings Dreamliner kann im Flug der Strom ausfallen, das Flugzeug unkontrollierbar werden. Schuld ist ein Computerfehler.

- SW-Überlauf führt zu einem Stromausfall an Bord
- Überlauf des SW Zählers nach 248 Tagen
- Steuerungssystem kann (neben Entertainment-system, Klimaanlage und Licht auch betroffen sein
- Fehler wurde nach einen Labortest festgestellt
- Maßnahme: alle 120 Tage Neustart des Systems

Dreamliner-Pannen: Boeing wählte brandgefährliches Batteriematerial

Zwei Batteriebrände im Dreamliner bringen Boeing in Erklärungsnot. Der US-Luftfahrtkonzern hat für seinen neuen Jet ausgerechnet eine der feuergefährlichsten Akku-Sorten gewählt. Die Energiespeicher haben schon während der Entwicklung einen Großbrand verursacht.



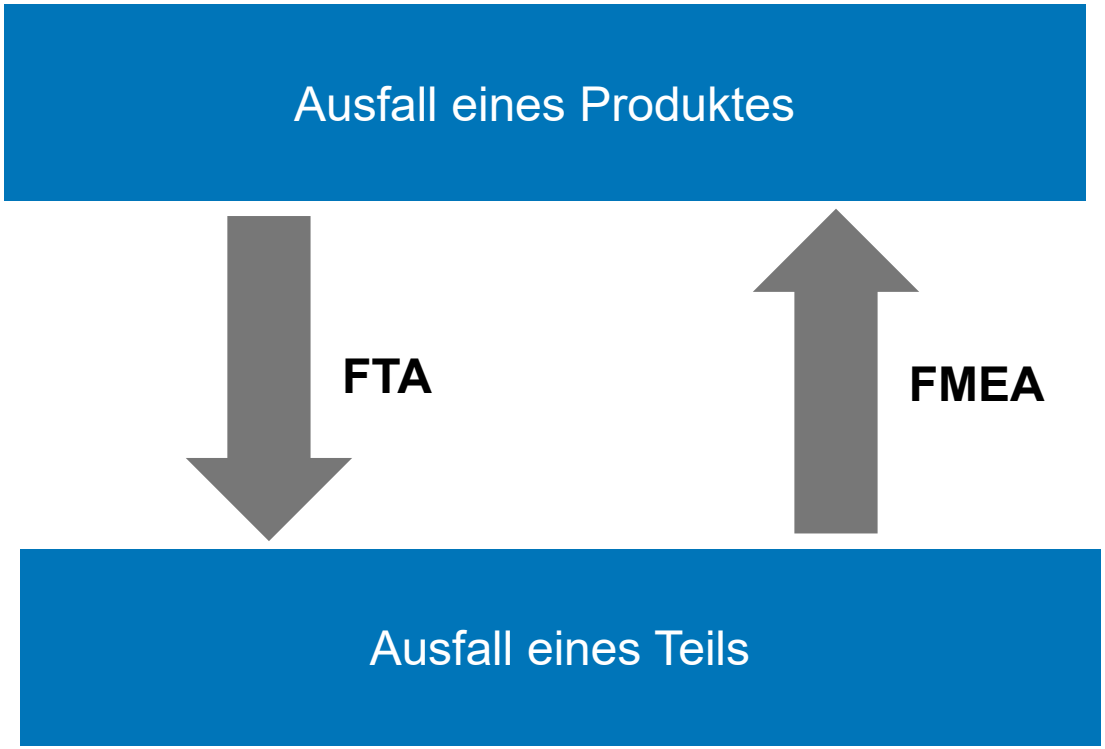
- Brand zweier Batterien (Lithium-Ionen Akkus)
- Neue Technologie anstelle Li-Cobalt / Li-Eisenph.
- „Thermal Runaway“ (Brand / Explosion)

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**

Sicherheitstechnik: Wiederholung

- FTA (Fehlerbaumanalyse)



Sicherheitstechnik: Wiederholung

- FTA (Fehlerbaumanalyse)

- Die FTA ist in drei wesentliche Arbeitsschritte unterteilt
  - Darstellung des Ursachen-Wirkungsgefüges (Fehlerbaum)
  - Ermittlung von Zuverlässigkeitskenngrößen für die Basisereignisse
  - Berechnung von Zuverlässigkeitskenngrößen

Sicherheitstechnik: Wiederholung

- FTA (Fehlerbaumanalyse)

Boolesche Logik

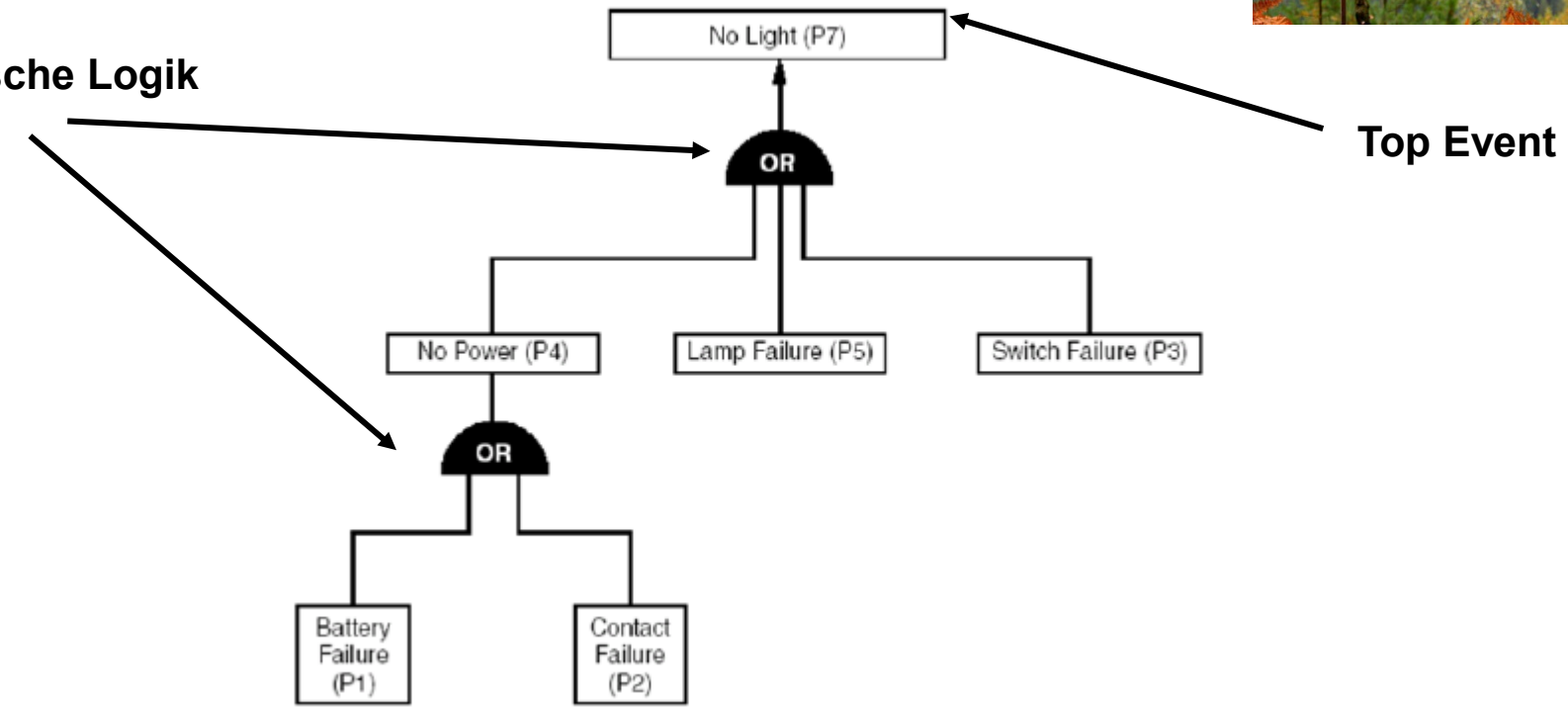
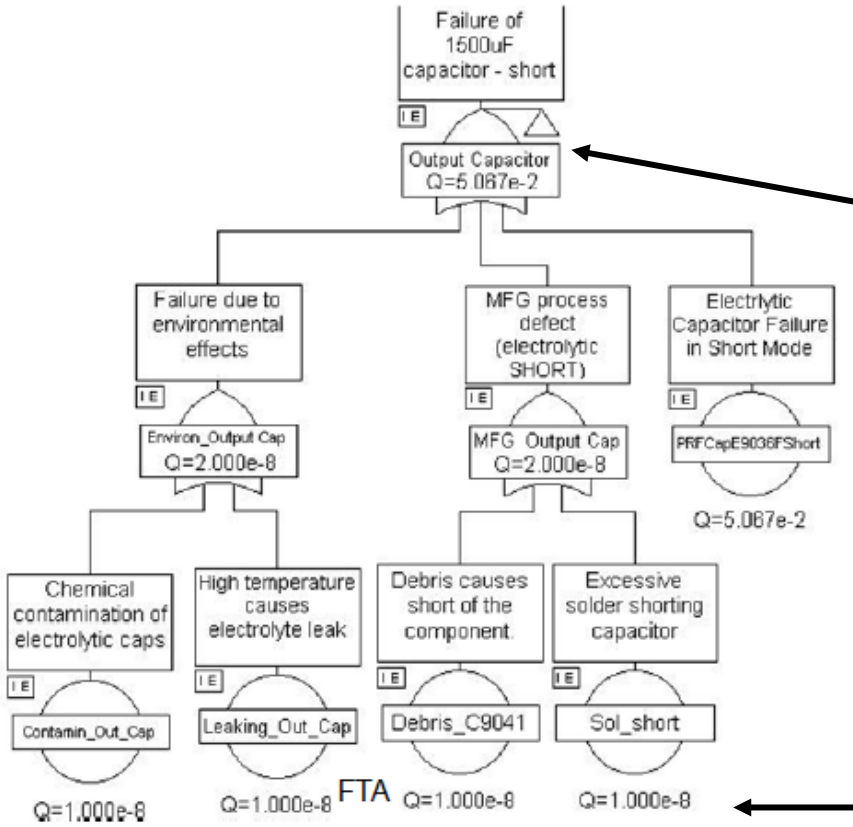


Figure 11.5 FTA of the vehicle headlamp.

Sicherheitstechnik: Wiederholung

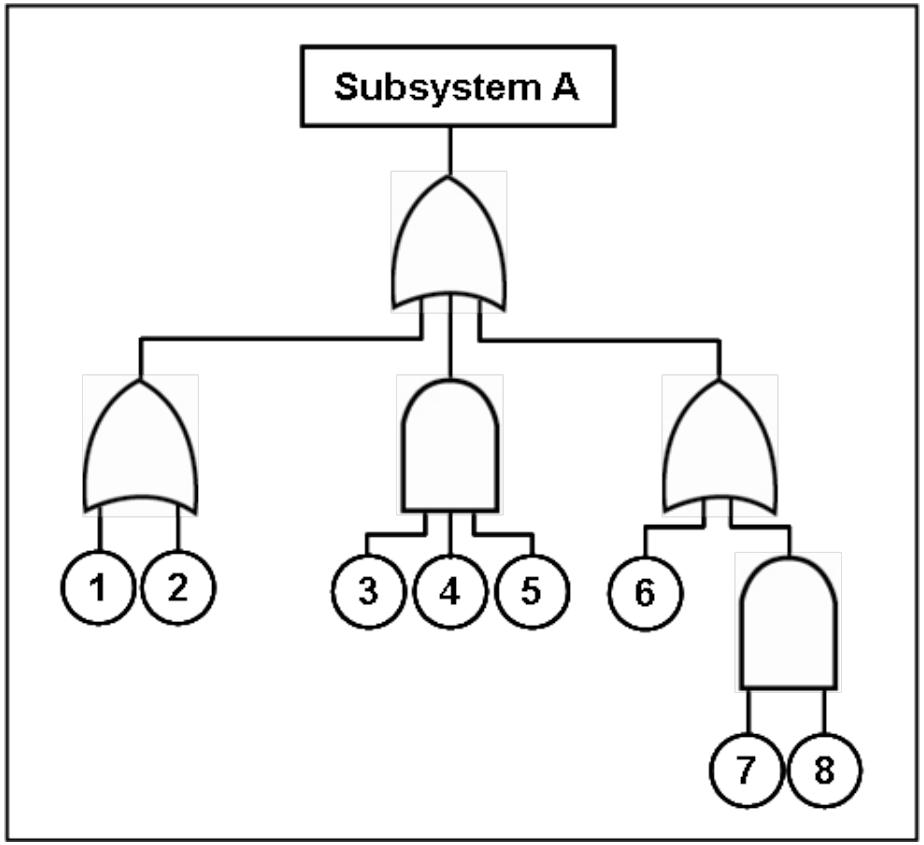
- FTA (Fehlerbaumanalyse)



Ergebnis

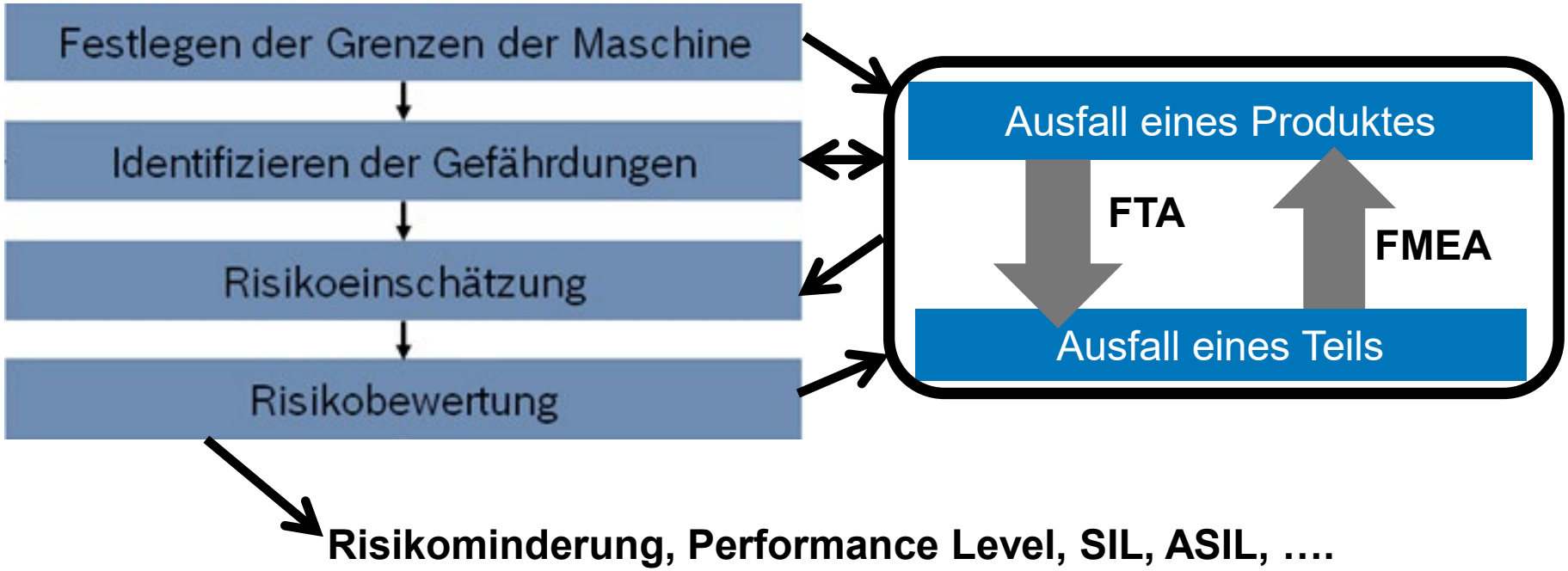
Fehlerrate

Sicherheitstechnik: Übung 9



Sicherheitstechnik: Lösung Übung 9

Sicherheitstechnik: Zusammenfassung



FMEDA
Failure Modes Effects and Diagnostic Analysis

- Was ist eine FMEDA?
  - Induktive Analyse
  - Typischerweise erfolgt die Analyse auf Bauteilebene
  - Zusammenfassende Auswertung zur Bewertung der sicheren und erkannten Ausfälle zu den gesamten Ausfällen (Safe Failure Fraction) und Diagnoseabdeckung (DC)
  - Wird typischerweise für hohe Sicherheitslevel (ISO 26262) angewandt

FTA vs. FMEDA

	FMEDA	FTA
Deduktiv (D) / Induktiv (I)	I	D
Quantitative Analyse möglich	Ja	Ja
Anwendbar bei Fehlerkombinationen	Nein	Ja
Anwendbar bei abhängigen Ereignissen	(bedingt)	Ja
Anwendbar bei sequentieller Abhängigkeit	Nein	Nein
Anwendbar bei komplexen Funktionen	(bedingt)	Ja

FMEDA
Failure Modes Effects and Diagnostic Analysis

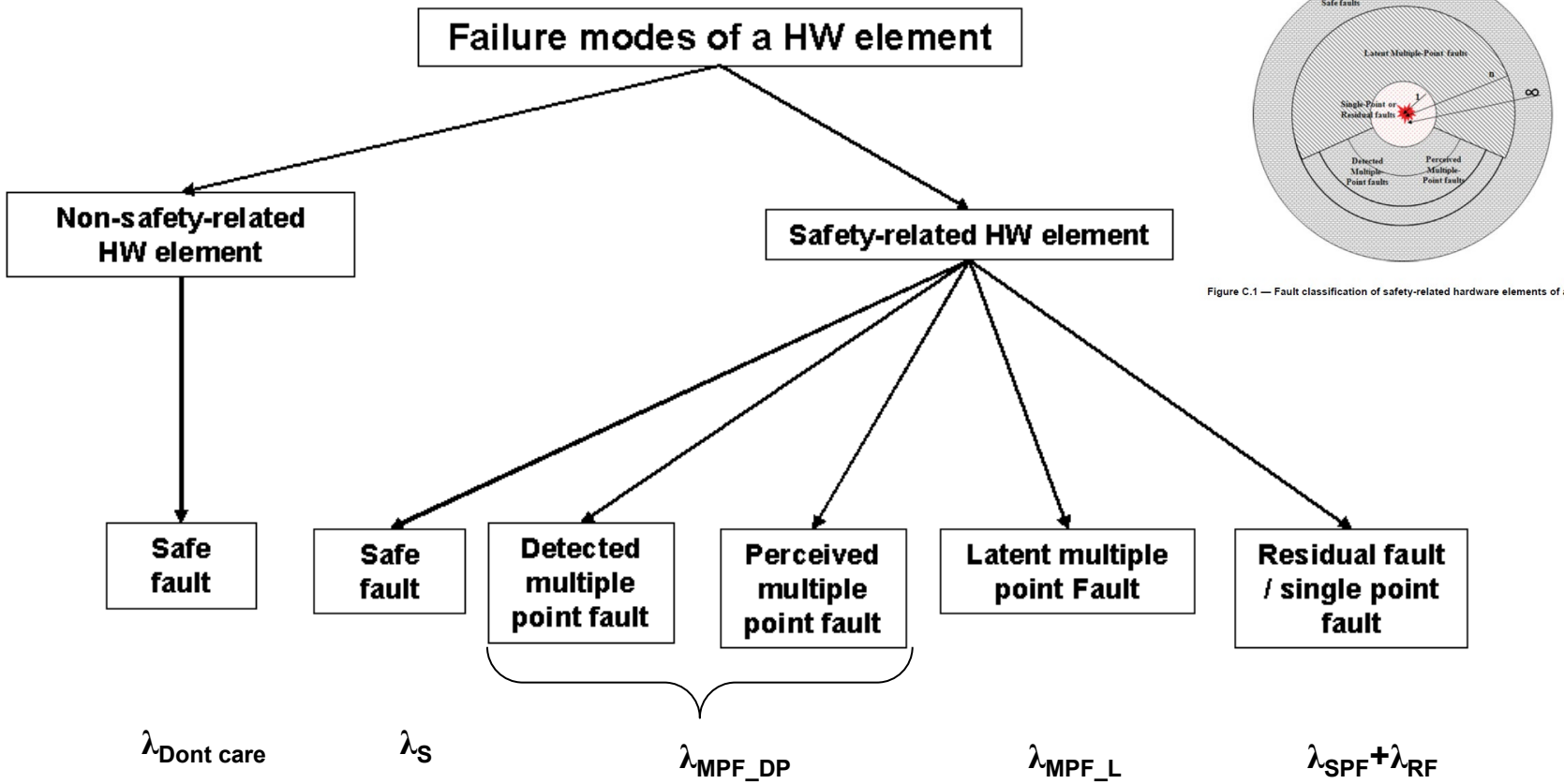


Figure C.1 — Fault classification of safety-related hardware elements of an item

FMEDA
Failure Modes Effects and Diagnostic Analysis

- **Safe fault (λ_S)**: Fehler, deren Auftreten die Wahrscheinlichkeit der Verletzung eines Sicherheitsziels nicht wesentlich erhöhen
- **Multiple point fault (λ_{MPF})**: ein Fehler von mehreren unabhängigen Fehlern, die in Kombination zu einem Versagen an mehren Punkten führt
  - wird wahrgenommen, wird detektiert (λ_{MPF_P} and λ_{MPF_D})
  - latent (λ_{MPF_L})
- **Single point fault (λ_{SPF})**: Fehler in einem Element, die nicht von einem Sicherheitsmechanismus abgedeckt wird und dessen Fehler direkt zu der Verletzung einer Sicherheitsziels führt
- **Residual fault (λ_{RF})**: Restfehlerrate eines Single point faults, die zu der Verletzung eines Sicherheitsziels in einem Hardware-Element führt, in dem der Teil der Fehler nicht durch die bestehenden Sicherheitsmechanismen abgedeckt wird
- **Don’t care fault ($\lambda_{Dont\ care}$)**: wird für die Analyse nicht berücksichtigt. Vorher ist eine Unterscheidung zwischen Safe fault und Don’t care fault durchzuführen

FMEDA
Failure Modes Effects and Diagnostic Analysis

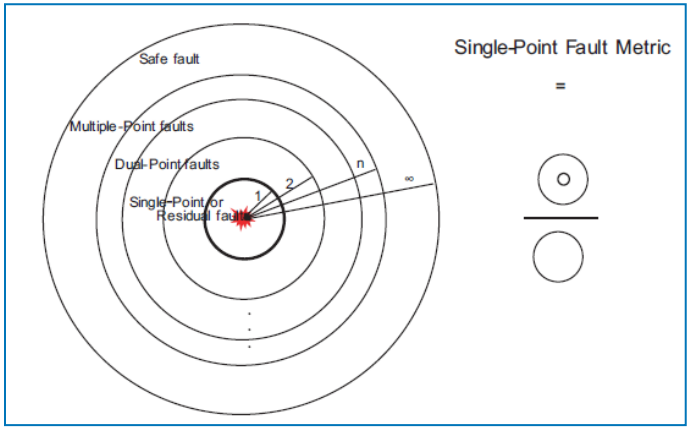
- Validierung der Hardware Metriken (ISO 26262-5, Sektion 8)

  1) Single-point fault Metrik
     - Ziel: > 99% (ASIL D)

  2) Multiple-fault Metrik
     - Ziel: > 90% (ASIL D)

- Identifizierung von kritischen Elementen

$$1-\frac{\sum_{SR,HW}(\lambda_{SPF}+\lambda_{RF})}{\sum_{SR,HW}\lambda}=\frac{\sum_{SR,HW}(\lambda_{MPF}+\lambda_{S})}{\sum_{SR,HW}\lambda}$$



$$1-\frac{\sum_{SR,HW}(\lambda_{MPF,latent})}{\sum_{SR,HW}(\lambda-\lambda_{SPF}-\lambda_{RF})}=\frac{\sum_{SR,HW}(\lambda_{MPF,perceived\ or\ detected}+\lambda_{S})}{\sum_{SR,HW}(\lambda-\lambda_{SPF}-\lambda_{RF})}$$

FMEDA
Failure Modes Effects and Diagnostic Analysis

Vorbereitung einer FMEDA (Organisation, Team, Dokumente)

1. Identifikation von relevanten Modulen / Teilen
2. Bestimmung der Fehlerraten
3. Bestimmung der Fehlermodi
4. Festlegung der Fehlerauswirkungen
5. Sortierung in Fehlerklassen
6. Entwicklung und Festlegung der Sicherheitsmechanismen
7. Bestimmung der „Failure Mode Coverage“
8. Kalkulation der Hardwaremetriken
9. Auswahl und Definition der Maßnahmen
10. Dokumentation und Präsentation

FMEDA:
Vorbereitung einer FMEDA

- Aufgaben, Sicherheitsziele (Einstufung, worst case, sicherer Zustand) und weitere Informationen sind zu definieren (Anforderungsliste, Blockdiagramme, Schaltpläne)
- Auswahl, welche Methoden anderweitig noch verwendet werden (FMEA, FTA, …)
- FMEDA Team zusammenstellen (Moderator, HW Experten, zusätzliche Mitglieder)
- Standards und typische Normen müssen bekannt / vorhanden sein (z.B. für Fehlerraten: SN 29500 or IEC 62380)

FMEDA: 1. Identifikation von relevanten Modulen / Teilen

- Metriken werden für jedes Sicherheitsziel berechnet
- Ob ein HW Element "sicherheitsrelevant" ist, ist vom Sicherheitsziel abhängig (ein HW Element kann "sicherheitsrelevant" für ein Sicherheitsziel, für ein anderes nicht)
  - 1) ein Fehler in diesem HW-Element kann zu einer Verletzung der Sicherheitsziels führen ODER
  - 2) eine HW-Element ist Teil eines Sicherheitsmechanismus, der die Verletzung eines Sicherheitsziel zu verhindern sollte ODER
  - 3) das HW Element einen (deutlichen) Einfluss auf den Pfad hat, der für die Sicherheit relevant ist

FMEDA:
2. Bestimmung der Fehlerraten

- Einheit: FIT (Failure in Time) = 10^-9 pro Stunde
- Quellen:
  - Industrie Standards (SN29500 / IEC62380)
  - Felddaten
  - Expertenentscheidung (basierend auf Daten / Testerfahrung)
- Nur eine Quelle sollte verwendet werden
- Bei Benutzung von Industrie Standards:
  - Ausfallraten für Komponententypen der referenzierten Schaltungsblöcke sollten genommen werden
  - Einflussfaktoren müssen berücksichtigt werden (z.B. Temperatur, Vibrationen)

		Komplexität in Bit / *Complexity in bits*										$\vartheta_{vj,t}$
		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										in °C
Bipolar	RAM, FIFO statisch *static*	50	60	-	-	-	-	-	-	-	-	75
	PROM	60	80	-	-	-	-	-	-	-	-	
MOS, CMOS, BICMOS	RAM dynamisch *dynamic*	50	30	20	10	10	15	20	25		-	55
		-	-	-	-	-	-	-	-	70	(100)	70
	RAM, FIFO statisch langsam >30ns *static slow* [2]	15	10	10	10	10	30	50	-	-	-	55
	statisch schnell <30ns *static fast* [2]	30	25	15	25	40	55	90	-	-	-	70
	ROM *mask*	50	30	15	15	15	15	25	-	-	-	55
	EPROM, OTPROM UV-löschbar *UV eraseable*	30	30	20	20	20	20	40	-	-	-	
	FLASH	-	-	30	30	40	50	70	(100)	-	-	
		-	-	-	-	-	-	-	-	(200)	-	70
	EEPROM, EAROM	30	30	30	50	-	-	-	-	-	-	55

Quelle: SN 29500-2:2010-09

FMEDA:
3. Bestimmung der Fehlermodi

- Jedes Hardwareelement hat einen spezifischen Failure-Mode

- Quellen:
  - Handbücher (IEC 62380, Birolini)
  - Experteneinschätzung
  - Tabelle D1 (ISO 26262-5, Annex D)
  - Anforderung Hersteller

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		20Δ	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 ≈ 3/2

Quelle: Birolini, Alessandro (Reliability Engineering)

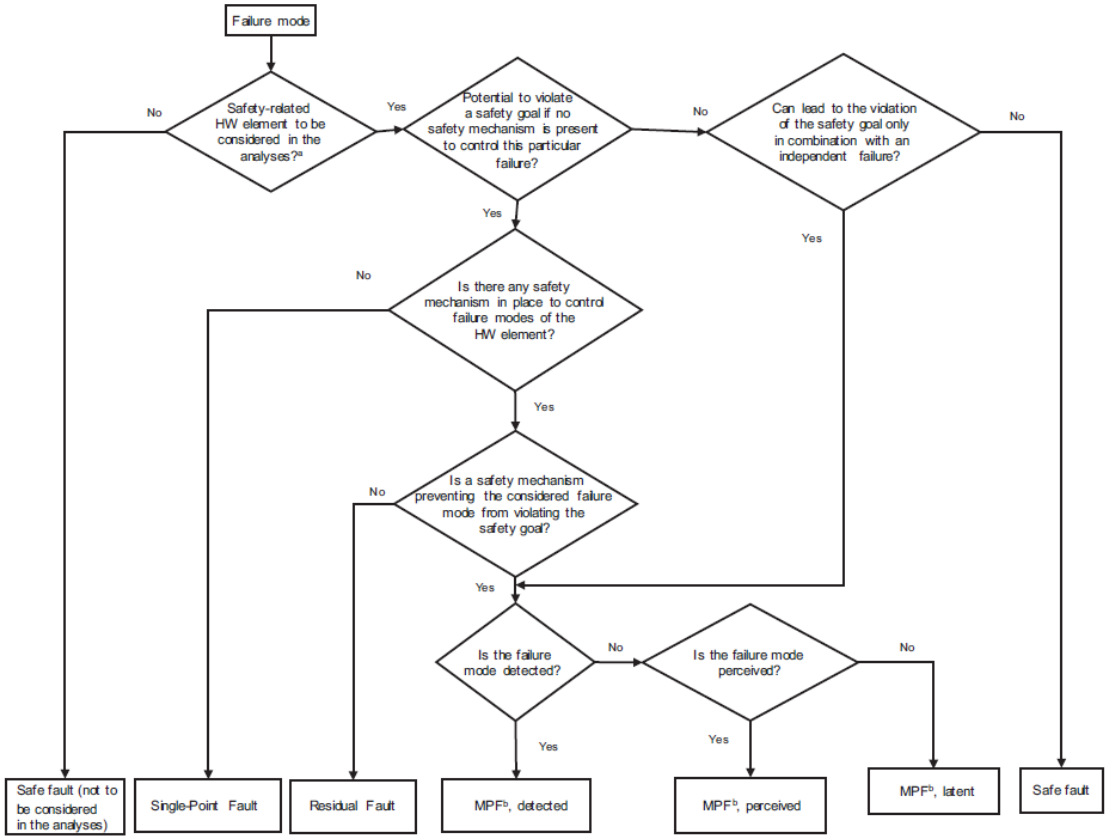
FMEDA:
4. Festlegung der Fehlerauswirkungen

- Ursache, Fehler und Versagen (Ergebnis) sind zu definieren (wie FMEA)

- Bsp. (Motorsteuerung):
  - Ursache: Widerstand unterbrochen
  - Fehler: Strom zu hoch am Einlassventil
    -> Druck auf Rädern zu hoch
  - Versagen: Sicherheitsziel

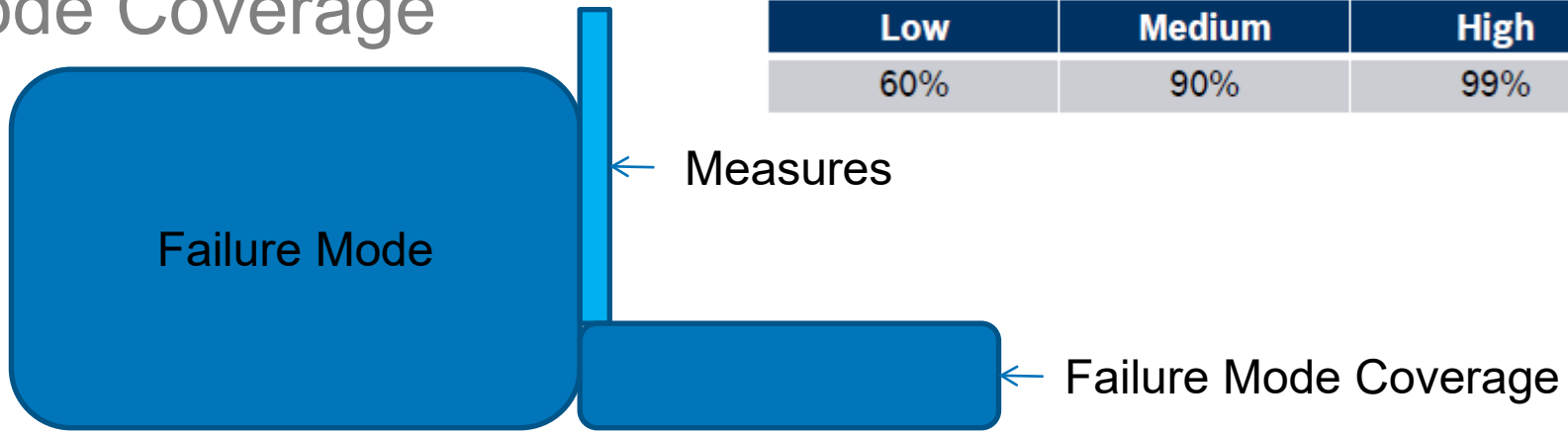
FMEDA: 5. Sortierung in Fehlerklassen / 6. Festlegung Fehlermechanismus

- Auswahl der Fehlerklasse,
  (Single Point Fault,
  Residual Fault,
  Multiple Fault, …)



FMEDA: 7. Bestimmung der „Failure Mode Coverage“

Low	Medium	High
60%	90%	99%



- Fehler erkannt oder unter Kontrolle
  - Fehler erkannt: mittels Warnung (Information für Bediener und Abschalten des Systems)
  - Fehler kontrolliert: kein kritischer Einfluss
  - Quellen: Experteneinschätzung, ISO 26262 Annex D, detaillierte Analyse, Kombination verschiedener Maßnahmen
  - Fehlerreaktionszeit muss beachtet werden

FMEDA:
8. Kalkulation der Hardwaremetriken

- Hardware Metriken = Sicherheit messbar machen
  - Relative Metriken = Messung der Architektur (SPFM, LFM)
  - Absolute Metriken = Messung des Restrisikos (PMHF)

- Gesamtmetriken werden durch die Addition der “Failure Modes” pro Sicherheitsziel bestimmt

FMEDA: 9. Auswahl und Definition der Maßnahmen + 10. Dokumentation und Präsentation

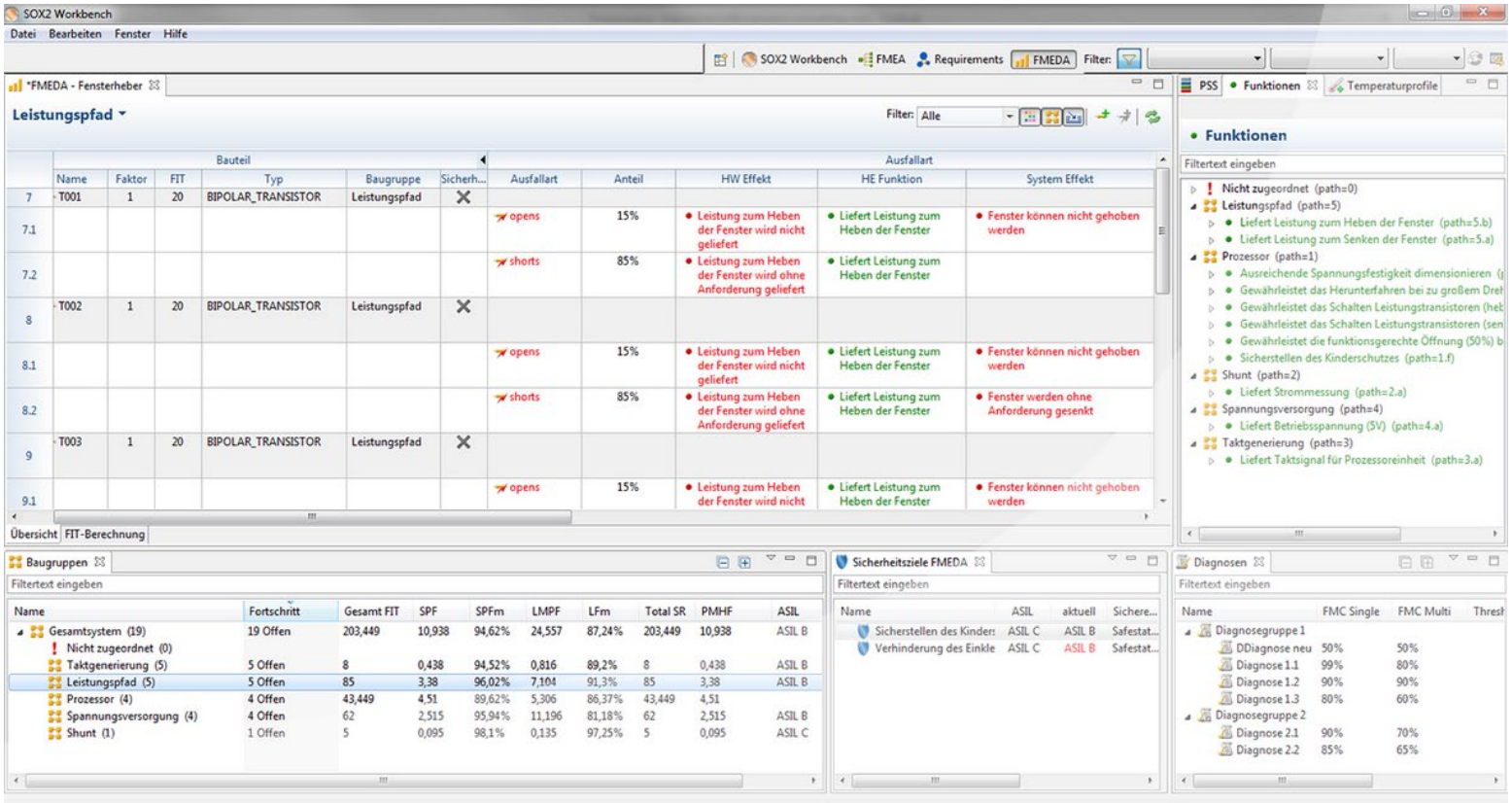
- Für jeden Funktionsblock müssen Modi gefunden werden, welche den grössten Einfluss auf die Verletzung des Sicherheitsziels haben
- Wie kann der Einfluss reduziert werden?
  - Diagnoseabdeckung erhöhen (neuer Sicherheitsmechnismus, Designupdate, Ausführung von Tests, …)
  - Reduzierung der Fehlerraten (Überprüfung HW Spezifikas)
  - Update der Architektur (Robustness der Funktionalität)
- Anschließend Dokumentation, Präsentation (analog Vorgehen wie z.B. bei FMEA)

FMEDA
Failure Modes Effects and Diagnostic: Beispiel

Cells Reviewed	Component Name	Description	Failure rate / FIT	Safety-related component to be considered in the calculations?	Failure Mode	Failure rate distribution	Failure effect (see FTA)	Failure Path	Failure mode that has the potential to violate the safety goal in absence of safety mechanisms ?	Safety mechanism(s) allowing to prevent the failure mode from violating the safety goal ?	Failure mode coverage wrt. violation of safety goal	Residual- or Single-Point Fault failure rate / FIT	Failure mode that may lead to the violation of safety goal in combination with an independent failure of another component ?	Detection means ? Safety mechanism(s) allowing to prevent the failure mode from being latent ?	Failure mode coverage wrt. Latent failures	Latent Multiple-Point Fault failure rate / FIT
reviewed	R3	Resistor	3	Yes	open	30			x		0	0,900			0	
reviewed					closed	10					0	0,000			0	
reviewed					drift 0,5	30					0	0,000			0	
reviewed					drift 2	30			x		0	0,900			0	
reviewed	R13	Resistor	2	Yes	open	90			x		0	1,800			0	
reviewed					closed	10			x		0	0,200			0	
reviewed	R23	Resistor	2	Yes	open	90					0	0,000			0	
reviewed					closed	10			x		0	0,200			0	
reviewed	C13	Capacitor	2	Yes	open	20			x		0	0,400			0	
reviewed					closed	80					0	0,000			0	
reviewed	C23	Capacitor	2	No	open	20					0	0,000			0	
reviewed					closed	80					0	0,000			0	
reviewed	WD	ASIC	20	Yes	Out stuck at 1	50					0	0,000	x		0	10,00
reviewed					Out stuck at 0	50					0	0,000			0	
reviewed	T71	IC	5,00	Yes	open circuit	50					0	0,000			0	
reviewed					short circuit	50			x	SM1	90	0,250	x	SM1_L	80	0,45
reviewed	R71	Resistor	2	Yes	open	90					0	0,000			0	
reviewed					closed	10					0	0,000	x		0	0,20
reviewed	R72	Resistor	2	Yes	open	90					0	0,000			0	
reviewed					closed	10					0	0,000	x		0	0,20
reviewed	R73	Resistor	2	No	open	90					0	0,000			0	
reviewed					closed	10					0	0,000			0	
reviewed	R74	Resistor	2	Yes	open	90					0	0,000	x		0	1,80
reviewed					closed	10					0	0,000	x		0	0,20
reviewed	I71	Resistor	5	No	open	70					0	0,000			0	
reviewed					closed	20					0	0,000			0	
reviewed	C71	Capacitor	2	Yes	open	20					0	0,000	x		0	0,40
reviewed					closed	80					0	0,000			0	
reviewed	R81	Resistor	2	No	open	90					0	0,000			0	
reviewed					closed	10					0	0,000			0	
reviewed	L1	LED	10	No	open	90					0	0,000			0	
reviewed					closed	10					0	0,000			0	
reviewed	µC	IC	100	Yes	all	50			x	SM4	90	5,000	x	SM4_L	100	0,00
reviewed					all	50					0	0,000			0	

FMEDA
Failure Modes Effects and Diagnostic Analysis

- Tools: Safety Office, Medini, Excel basierte Tools, …



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)

Belegarbeit: Aufgabenstellung

- 3er oder 4er Gruppe
- Selbstgewähltes Beispiel
- Aufgabenstellung
- Präsentation im Plenum am **20.06.2022** per WebEx
- FMEA Formblatt, FTA Tool
- **Rückmeldung spätestens bis zum 16.05.2022 über Gruppenzusammensetzung und ausgewähltes Beispiel**
- **Abgabetermin: 20.06.2022 (Belegarbeit und Präsentationsunterlage)**
- **Kontakt: fred.haertelt@hs-heilbronn.de**