STARKES STUDIUM.
PRIMA ZUKUNFT.

HOCHSCHULE HEILBRONN

TECHNIK WIRTSCHAFT INFORMATIK

Sicherheitstechnik, 6. Vorlesung (Safety Technology)

Campus Heilbronn

Campus Künzelsau
Reinhold-Würth-Hochschule

Campus Schwäbisch Hall

Fred Härtelt, Heilbronn

Beispiel (2009): Toyota

Gaspedal-Panne: Toyota muss in den USA Milliardenstrafe zahlen

Die Rückrufaktion wegen defekter Gaspedale verfolgt Toyota noch immer. In den USA stimmte der japanische Autobauer jetzt einer Zahlung von 1,2 Milliarden Dollar zu. US-Justizminister Holder bezeichnete Toyotas Verhalten in der Pannenserie als "schändlich".

- Problematik:
  - „Selbstbeschleuniger“ (Auto beschleunigt durch klemmende Gaspedale oder rutschend Fußmatten) mit Todesfolge
  - Auswertung ergab (Quelle: NHTSA), dass jedoch die Vielzahl der Fälle auf Fehler des Fahrers zurückzuführen ist
  - Massive Glaubwürdigkeitsprobleme der Marke Toyota v.a. in den USA
  - **Gesamtkosten: 1,2 Milliarden US Dollar**

Quellen: www.spiegel.de, www.autobild.de

Sicherheitstechnik: zeitlicher Überblick

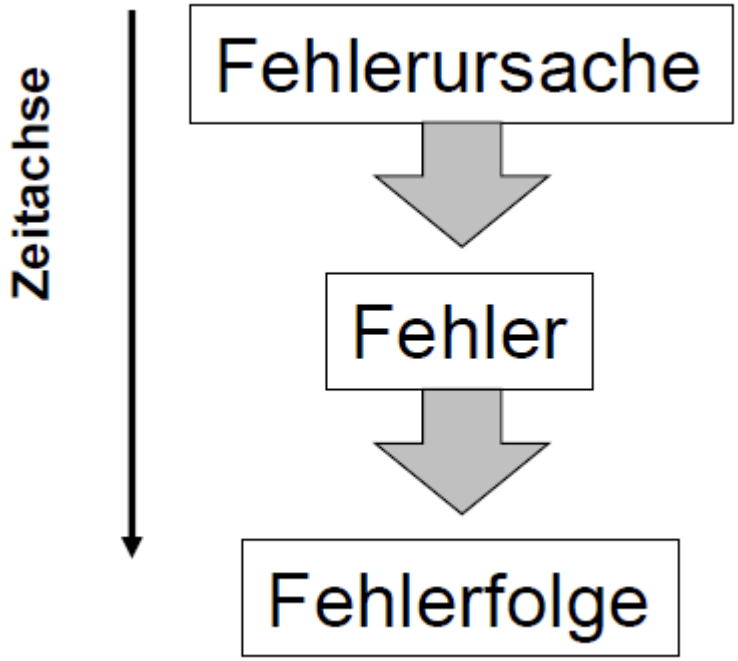
- 1. V: Definition Sicherheit, Normen und Vorschriften (14.03.2022)
- 2. V: Festlegung von Grenzen und Gefährdungen (21.03.2022)
- 3. V: Risikobeurteilung, -minimierung, Risikograph (28.03.2022)
- 4. V: Verteilungsfunktion, Ausfallraten, Fehlerbeherrschung (04.04.2022)
- 5. V: Fehlervermeidung, Fehlerentdeckung, 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: Fehlervermeidung & -entdeckung

- Fehlervermeidung erfolgt durch die Reduzierung von (Rest)-Fehlerraten
- Verschiedenste Analyseverfahren (FMEA, FTA, FMEDA) werden angewandt
- Standardisierte Prozesse können zur Fehlervermeidung beitragen
- Ziel ist es mit geeigneten Verfahren die Auftretenswahrscheinlichkeit zu reduzieren

Sicherheitstechnik: Wiederholung

- FMEA (Fehler- Möglichkeits- und Einfluss- Analyse)



Element	Ursache-Wirkungs-Analyse			derzeitiger Zustand					Veränderung		geänderter Zustand				
Funktionen / Q-Merkmale	potentielle Fehler	potentielle Folgen	potentielle Ursachen	Verhütung Prüfung	Auftreten	Bedeutung	Entdeckung	Risiko	Empfohlene Maßnahme	Verantwortung Termine, Ziele	getroffene Maßnahmen	Auftreten	Bedeutung	Entdeckung	Risiko neu
Funktion	Fehler 1	Folge 1	Ursache 1	V: P:											
			Ursache 2	V: P:											
		Folge 2	Ursache 1	V: P:											
			Ursache 2	V: P:											
	Fehler 2	Folge 1	Ursache 1	V: P:											
			Ursache 2	V: P:											
		Folge 2	Ursache 1	V: P:											
			Ursache 2	V: P:											

Sicherheitstechnik: Wiederholung

- FMEA (Fehler- Möglichkeits- und Einfluss- Analyse)

	System-FMEA **Aufzug**	Konstr.-FMEA **Dichtungsring**	Prozess-FMEA **Loch bohren**
Funktionen / Q-Merkmale	• Last heben / senken (500 kg) • Last halten (2000 kg) • Kabine positionie-ren (+/- 1 cm)	• innen / aussen abdichten (Spez.) • beständig gegen Säure und Lauge (Spez.)	• Durchmesser bohren (5 h 7) • Tiefe bohren (9 +/- 0.1 mm) • Oberfläche ge-stalten (RZ 0.5)

Sicherheitstechnik: Wiederholung

- FMEA (Fehler- Möglichkeits- und Einfluss- Analyse)

Bedeutung (Auswirkung auf den Kunden)	Bewertung
Es ist unwahrscheinlich, dass der Fehler irgendeine wahrnehmbare Auswirkung auf das Verhalten des Produkts oder Systems haben könnte. Der Kunde wird den Fehler wahrscheinlich nicht bemerken.	1
Der Fehler ist unbedeutend und der Kunde wird nur geringfügig belästigt. Der Kund wird wahrscheinlich nur eine geringfügige Beeinträchtigung des Systems bemerken.	2–3
Mittelschwerer Fehler, der Unzufriedenheit bei einigen Kunden auslöst. Der Kunde wird die Beeinträchtigung bemerken und dadurch belästigt sein.	4–6
Schwerer Fehler, der den Kunden verärgert. Sicherheitsaspekte oder gesetzliche Überschreitungen sind aber nicht betroffen.	7–8
Äußerst schwerer Fehler, der zum „Liegenbleiben" führt oder möglicherweise die Sicherheit und/oder die Einhaltung gesetzlicher Vorschriften beeinträchtigt.	9–10

Wahrscheinlichkeit des Auftretens	Häufigkeit	Bewertung
Es ist unwahrscheinlich, dass ein Fehler auftritt.	→ 0	1
sehr gering: die Konstruktion entspricht generell früheren Entwürfen, für die verhältnismäßig geringe Fehlerzahlen gemeldet wurden.	1/20.000 1/10.000	2 3
gering: die Konstruktion entspricht generell früheren Entwürfen, bei denen gelegentlich, aber nicht in größerem Maße, Fehler auftraten.	1/2.000 1/1.000 1/200	4 5 6
mäßig: die Konstruktion entspricht generell Entwürfen, die in der Vergangenheit immer wieder Schwierigkeiten verursachten.	1/100 1/20	7 8
hoch: Es ist nahezu sicher, dass Fehler in größerem Umfang auftreten werden.	1/10 1/2	9 10

Wahrscheinlichkeit der Entdeckung	Bewertung
Hoch (größer 99,99 %); funktioneller Fehler, der nahezu sicher bei den nächsten Arbeitsgängen bemerkt wird.	1
Mittel (größer 99,7 %); offensichtlicher Fehler, der z. B. 100 % automatisch geprüft wird und den Kunden wahrscheinlich nicht erreichen wird.	2 bis 5
Gering (größer 98 %); leicht zu erkennender Fehler, der z. B. mit einer 100 % Funktionsprüfung kontrolliert wird.	6 bis 8
Sehr gering (mindestens 90 %); nicht leicht zu erkennendes Fehlermerkmal, das 100 % visuell oder manuell geprüft wird.	9
Unwahrscheinlich; verdeckter Fehler, der in der Fertigung oder Montage nicht erkannt wird, da das Merkmal nicht geprüft wird bzw. werden kann.	10

Risikoprioritätszahl (RPZ) = BxAxE

Sicherheitstechnik: Wiederholung

- FMEA (Fehler- Möglichkeits- und Einfluss- Analyse)

Fehlermöglichkeits- und -einflussanalyse

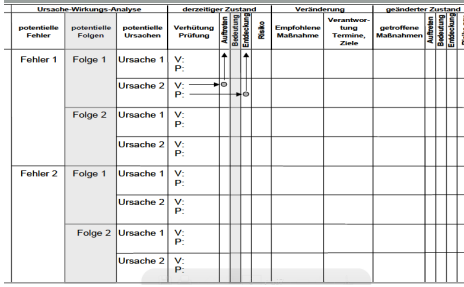
System-FMEA ☐ Konstruktions-FMEA ☒ Prozess-FMEA ☐

Bestätigung durch betroffene Abteilung und/oder Lieferant	Name / Abteilung / Lieferant: *Firma S. Friedrich & Co.*	Name / Abteilung / Lieferant: *D. Meyer, Labor 46*							Teil-Benennung: *Fahrzeugtür, Fahrerseite* (1)		Teil-Nummer: *95DJ-2345-4AA*						
									Modell / System / Fertigung: *Auto 2000 - XYZ*		Datum: *23.01.95*						
									Erstellt durch (Name / Abt.): *A. Schmidt, Konstruktion 234-fg*		Überarbeitet Datum: *05.08.95*						
System-/ Konstruktions-komponente, Prozessablauf	Mögliche Fehler			Derzeitiger Zustand							Verbesserter Zustand						
	Art	Folgen	Ursachen	Kontroll-maßnahmen	Auftreten	Bedeutung	Entdeckung	RPZ	empfohlene Abstellmaß-nahmen	Verant-wortlich-keit	Kontroll-maßnahmen	Auftreten	Bedeutung	Entdeckung	RPZ		
Fahrzeugtür	*Korrosion im unteren Teil des Tür-außenblechs (innen)*	*Verkürzte Lebens-dauer der Tür führt zu*	*Nicht aus-reichend dicke Wachs-schicht spezifiziert*	*Fahrzeug-Dauerhaltbar-keitsprüfung T-118 T-109 T-301*	*4*	*7*	*7*	*196*	*zusätzlicher verschärfter Korrosionstest*	*A. Schmidt Abt. Konst. 234-fg*	*Testergebnisse (Test Nr. 1358) bestätigen bis-herige Wachs-dicke*	*2*	*7*	*2*	*28*		
Ein- und Aus-stieg für Fahr-zeug		*schlechtem Aussehen durch Rost*	*Nicht geeig-nete Wachs-art spezifi-ziert*	*physikalischer und chemischer Labortest Bericht Nr. 23G*	*2*	*7*	*2*	*28*	*keine*	—	—						
schützt Fahrer gegen Wetter-einfluss, Geräu-sche und seit-lichen Aufprall		*Wasser-eintritt*	*Wachs er-reicht nicht die vorge-sehene Stelle*	*Untersuchung an der Konstruktion*	*8*	*7*	*6*	*336*	*Prozess des Wachsein-bringens mit Prozess-FMEA untersuchen*	*FMEA-Team Leitung: Fertigung*	*Prozess-FMEA durchgeführt (Blatt Nr. 23 Pr)*	*3*	*7*	*2*	*42*		
dient als Be-festigung für Türbeschlag-teile		*Beeinträch-tigung der Funktion der Tür-innenteile*				(8)		(10)									
(2)	(3)	(4)	(5)	(6)	(7)		(9)		(11)	(12)	(13)			(14)			

Sicherheitstechnik: Übung 7

Element	Ursache-Wirkungs-Analyse			derzeitiger Zustand					Veränderung		geänderter Zustand				
Funktionen / Q-Merkmale	potentielle Fehler	potentielle Folgen	potentielle Ursachen	Verhütung Prüfung	Auftreten	Bedeutung	Entdeckung	Risiko	Empfohlene Maßnahme	Verantwortung Termine, Ziele	getroffene Maßnahmen	Auftreten	Bedeutung	Entdeckung	Risiko neu
Funktion	Fehler 1	Folge 1	Ursache 1	V: P:											
			Ursache 2	V: P:											
		Folge 2	Ursache 1	V: P:											
			Ursache 2	V: P:											
	Fehler 2	Folge 1	Ursache 1	V: P:											
			Ursache 2	V: P:											
		Folge 2	Ursache 1	V: P:											
			Ursache 2	V: P:											

Sicherheitstechnik: Lösung Übung 7

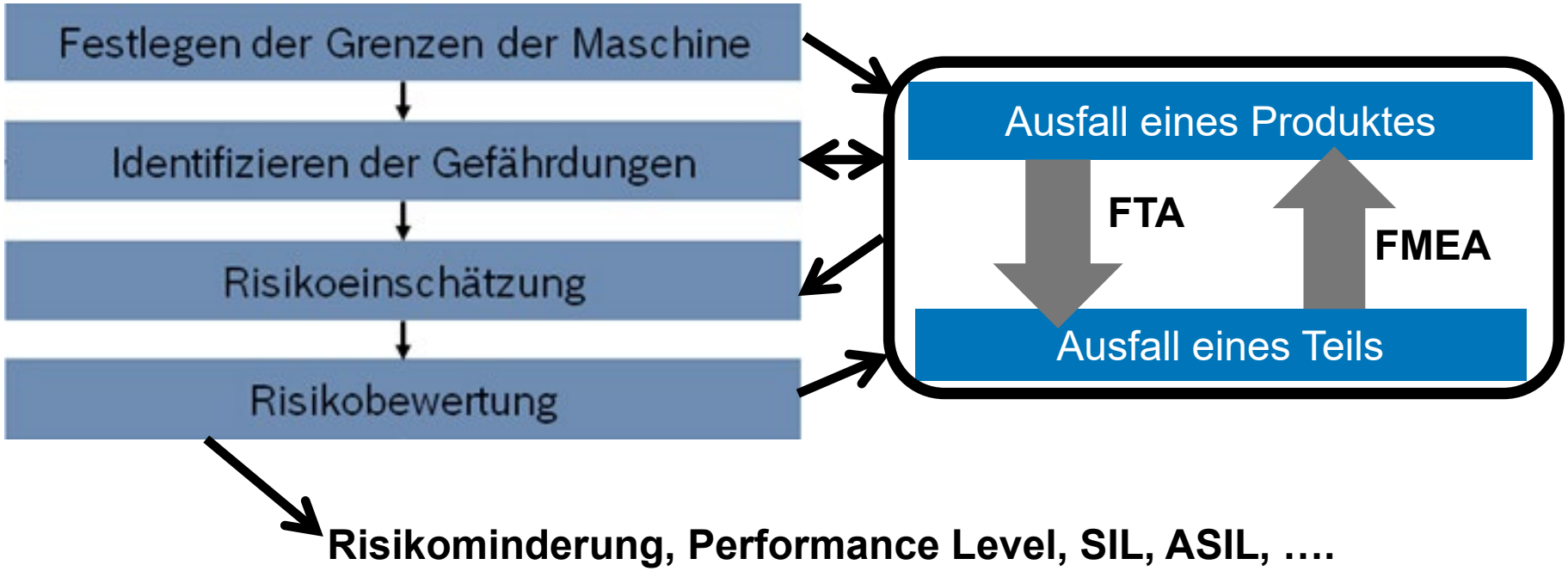


Fehler-Art	Fehler-auswirkung	Fehler-ursache	Kontroll-maßnahme	A	B	E	RPZ	Empfohlene Maßnahme	Getroffene Maßnahme	A	B	E	RPZ
Zweihand-schaltung defekt	Maschine funktioniert nicht	Steuerung ausgefallen	Regelmäßige Wartung	**2**	**8**	**2**	**32**	-	**-**				
Spaltvorgang wird nicht ausgelöst	Holz kann nicht gespalten werden	Verklemmung in der Maschine	Regelmäßige Wartung	**3**	**8**	**7**	**168**	Diagnose-abdeckung erhöhen	Tests, um Verklemmung zu erkennen	**2**	**8**	**2**	**32**
Holz fällt auf die Füße	Verletzung während Spaltvorgang	Sicherheitsabstand nicht eingehalten	Regelmäßige Wartung	**4**	**10**	**9**	**360**	Hinweis und Abdeckung	Abdeckung	**3**	**10**	**2**	**60**

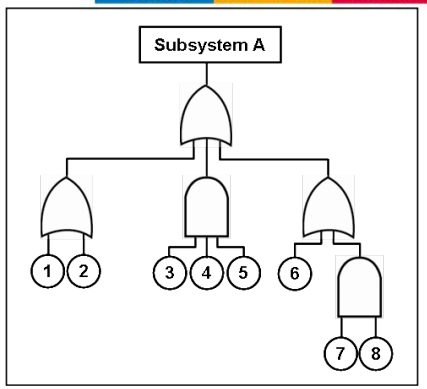
Redundanz

- = zusätzliche Vorhandensein funktional gleicher oder vergleichbarer Ressourcen eines technischen Systems, wenn diese bei einem störungsfreien Betrieb im Normalfall nicht benötigt werden (Definition wikipedia)
- Es gibt verschiedene Arten von Redundanz
- Funktionale Redundanz = sicherheitstechnische Systeme werden mehrfach parallel ausgelegt
- Räumliche Trennung von Sicherheitssystemen

Strukturierungsmaßnahmen



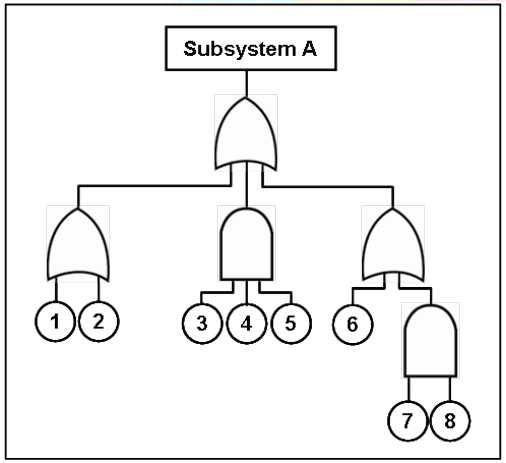
FTA: Fault Tree Analysis (Fehlerbaumanalyse)



- Was macht eine FTA?
  - ist eine systematische Methode der Systemanalyse
  - Untersucht ein System von oben nach unten
  - Bietet graphische Symbole zum leichteren Verständnis
  - nutzt mathematischen Werkzeuge
- Wann wird eine FTA genutzt?
  - Für die Untersuchung auf mögliche Fehler bezüglich ihrer
    - Modi und Ursachen;
    - auf ihren Beitrag zur System Unzuverlässigkeit

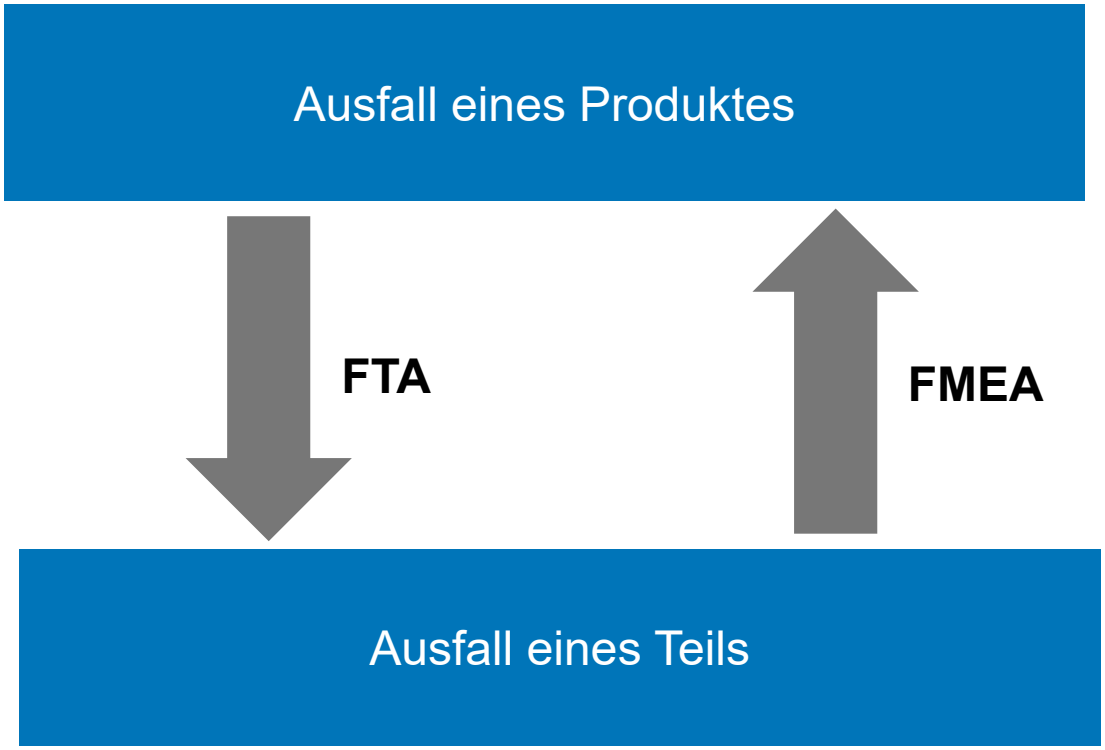
Quelle: warwick.ac.uk

FTA: Fault Tree Analysis (Fehlerbaumanalyse)



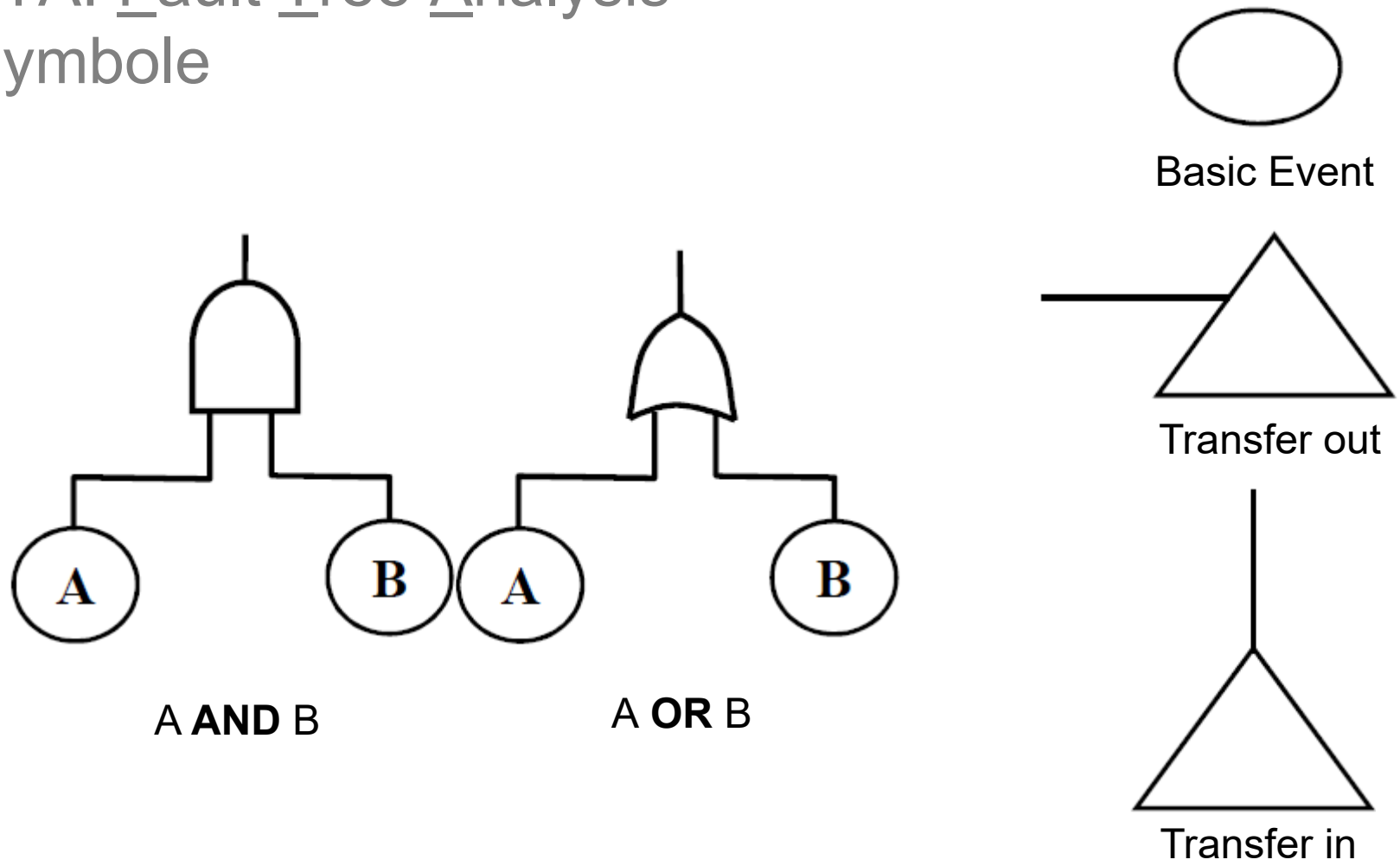
- Was ist eine FTA?
  - Es ist eine deduktive Risikoanalyse
  - Fehlverhalten werden mittels bool‘scher Algebra miteinander verknüpft
- Die FTA ist in drei wesentliche Arbeitsschritte unterteilt
  - Darstellung des Ursachen-Wirkungsgefüges (Fehlerbaum)
  - Ermittlung von Zuverlässigkeitskenngrößen für die Basisereignisse
  - Berechnung von Zuverlässigkeitskenngrößen

FTA vs. FMEA



Quelle: warwick.ac.uk

FTA: Fault Tree Analysis Symbole



Quelle: warwick.ac.uk

FTA: Fault Tree Analysis (Fehlerbaumanalyse)

Top Event:

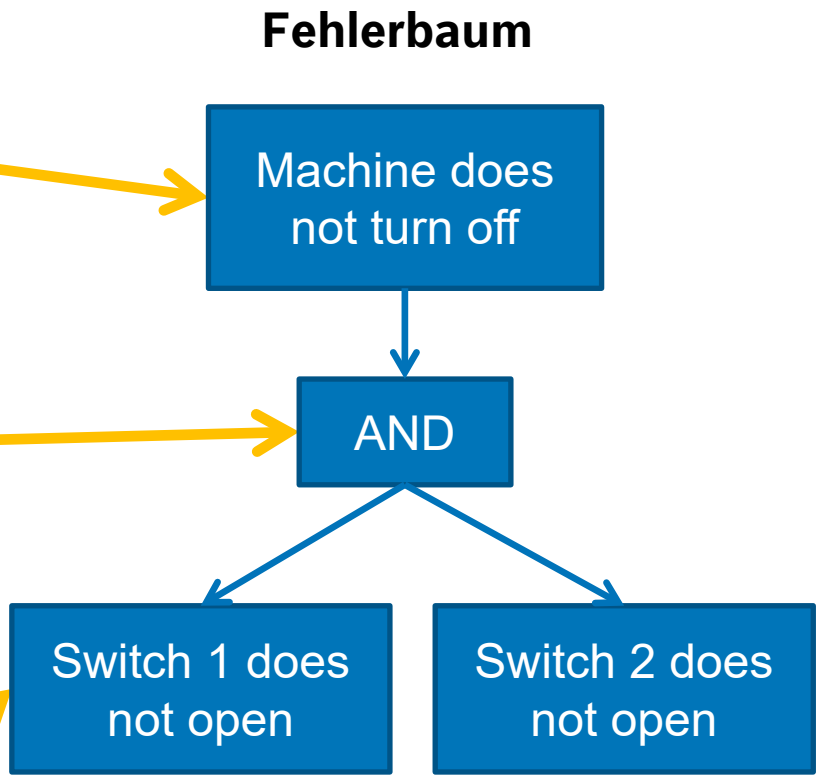
for jeden Fehler wird ein “Top Event” definiert

Boolesche Logik:

AND = Reihenschaltung

OR = Parallelschaltung

Fehler



FTA: Fault Tree Analysis (Fehlerbaumanalyse)

1) Fehlerbaum anlegen (Darstellung des Ursachen-Wirkungsgefüges)
2) Zuverlässigkeitskenngrößen für die Basisereignisse bestimmen
   - Parameter können bestimmt werden via
     - Tests
     - Betriebs- und Felderfahrungen
     - Verwendung von Zuverlässigkeitskenngrößen auf der höchstmöglichen sinnvollen Ebene mit geringster Granularität.
3) Berechnung der Wahrscheinlichkeiten

   AND = Die Gesamtwahrscheinlichkeit ist das Produkt aller Einzelwahrscheinlichkeiten

   OR = Die Gesamtwahrscheinlichkeit ist die Summe aller Einzelwahrscheinlichkeiten

FTA: Fault Tree Analysis (Fehlerbaumanalyse): Beispiel 1

Top Event

Boolesche Logik

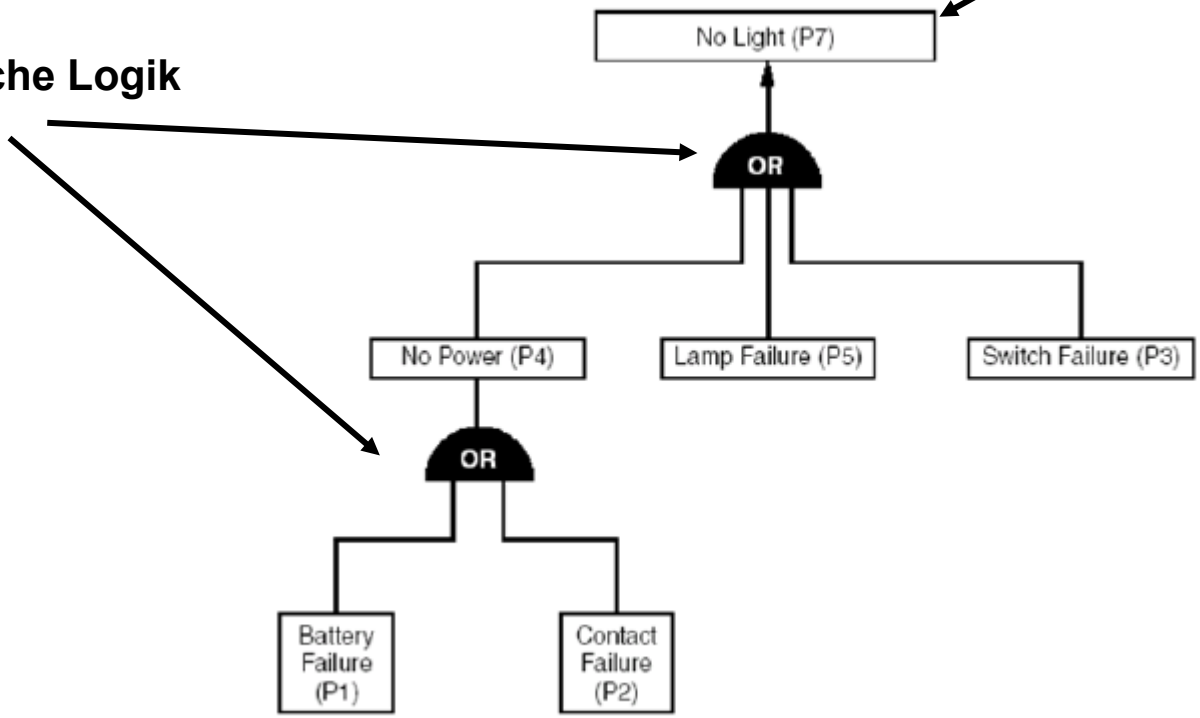
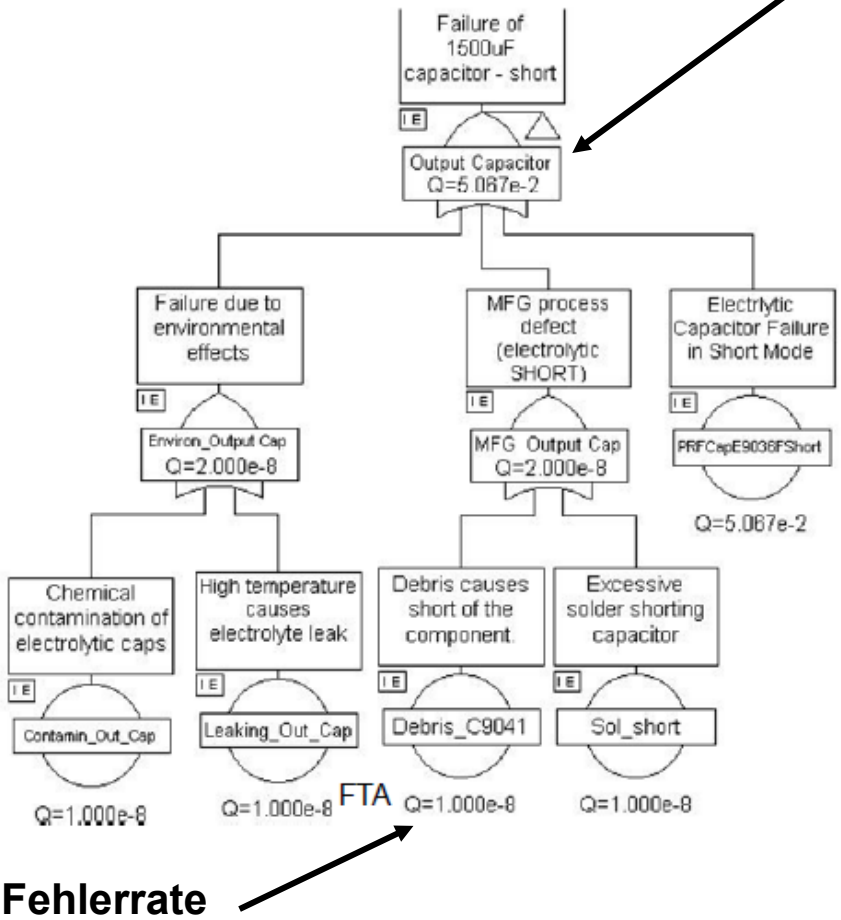


Figure 11.5 FTA of the vehicle headlamp.

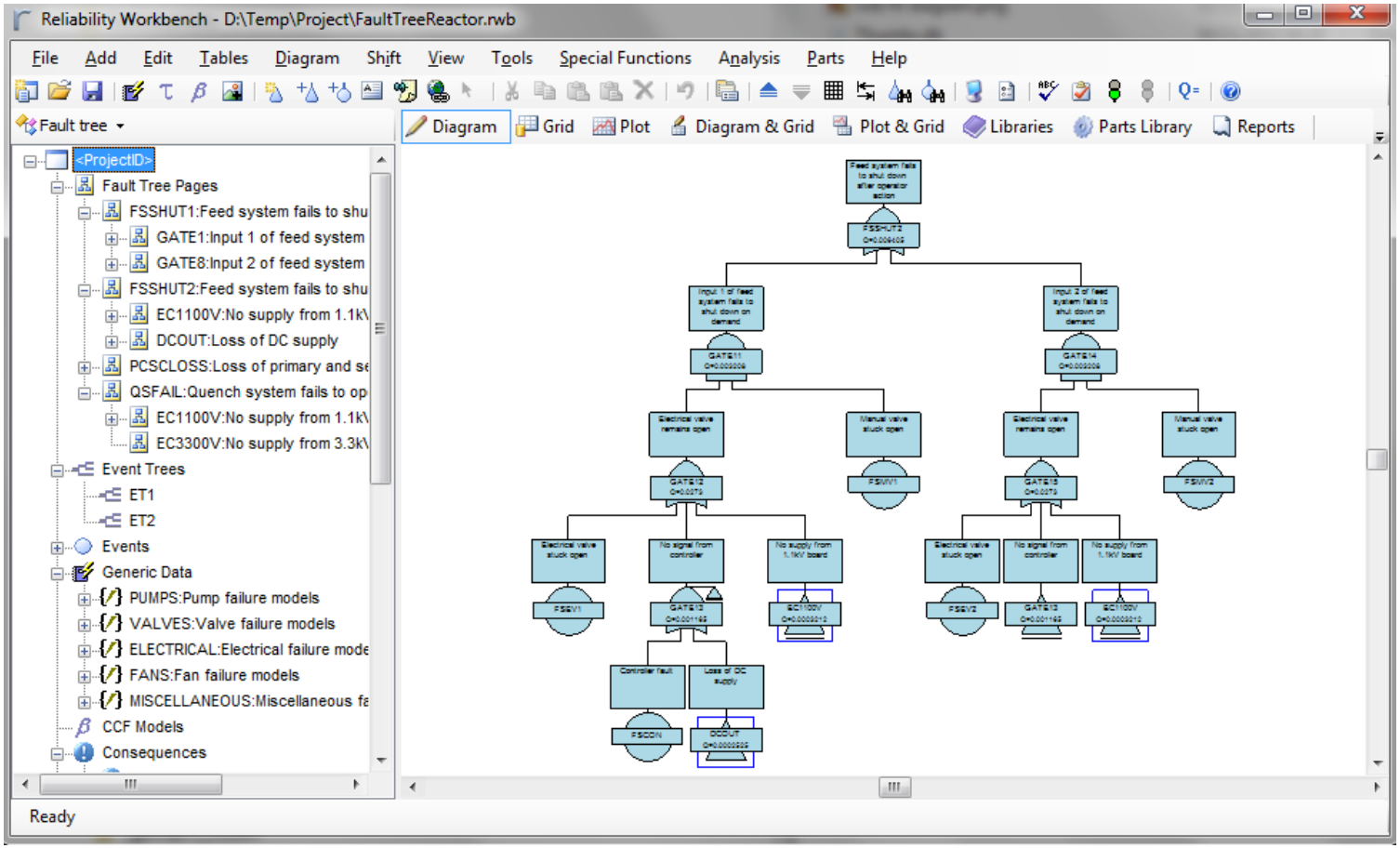
FTA: Fault Tree Analysis (Fehlerbaumanalyse): Beispiel 2

Ergebnis

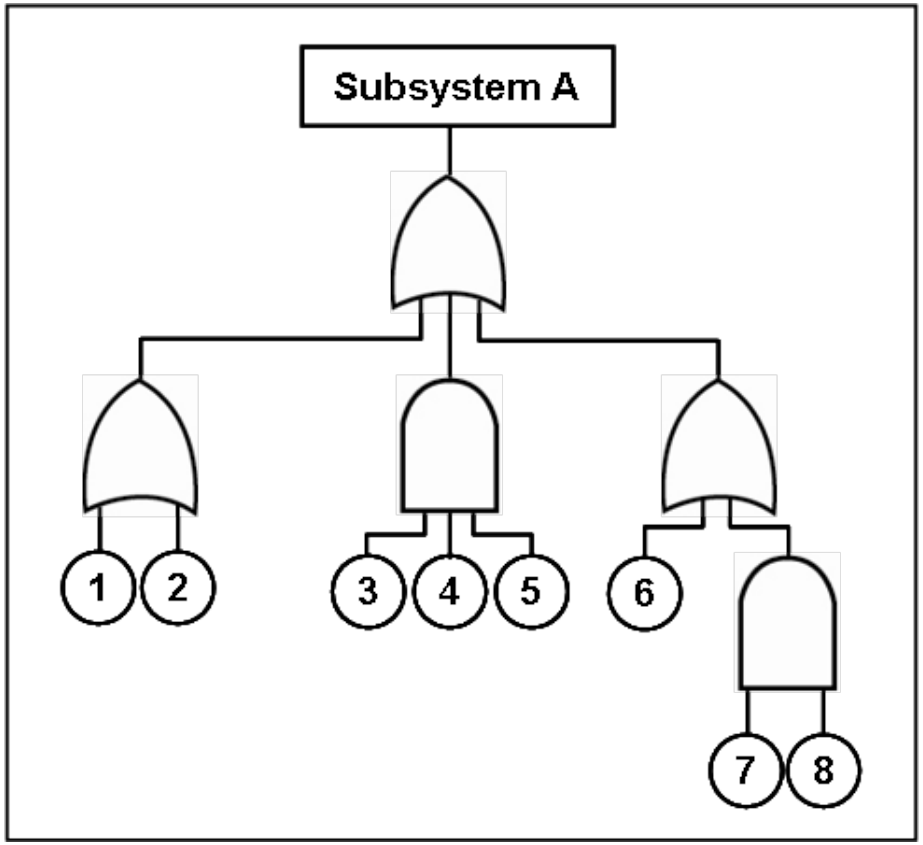


Fehlerrate

FTA: Fault Tree Analysis (Fehlerbaumanalyse)
Tool: FaultTree+ (Isograph)



Sicherheitstechnik: Übung 8



Sicherheitstechnik: Lösung Übung 8