

Betriebssicherheit

Kapitel 6: Fehlerbaumanalyse

Derk Rembold, 2020

Inhalt

- Anwendung
- Bildzeichen
- Vorgehen bei der Analyse
- Bewertung

Fehlerbaumanalyse (Fault Tree Analysis, FTA)

Einsatzgebiete

- Erstmaliger Einsatz bei Raketenentwicklung
- Luftfahrtindustrie
- Kernenergieindustrie mit Formalisierung
- Chemische Industrie
- Robotik
- Software-Industrie

Anwendung der Fehlerbaumanalyse

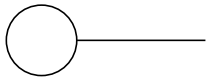
Werkzeug zur logischen Verknüpfung zwischen **Komponenten** und **Teilsystemausfällen**.

Ziele sind:

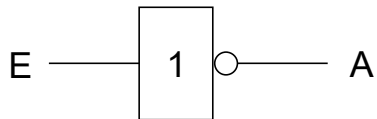
- Identifikation der Kombination von Ausfällen, die zum unerwünschten Ergebnis führen.
- Ermittlung der Zuverlässigkeit eines Systems aus den Zuverlässigkeitsgrößen des Systems (quantitativ).

Bildzeichen

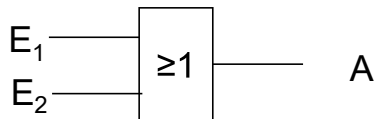
Standardeingang



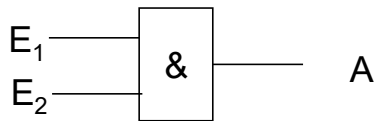
Nicht-Verknüpfung



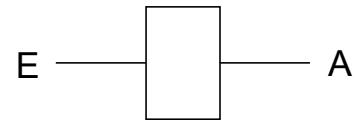
Oder-Verknüpfung



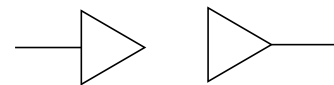
Und-Verknüpfung



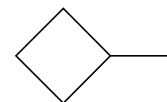
Kommentar



Übertragungsausgang, -eingang



Sekundäreingang

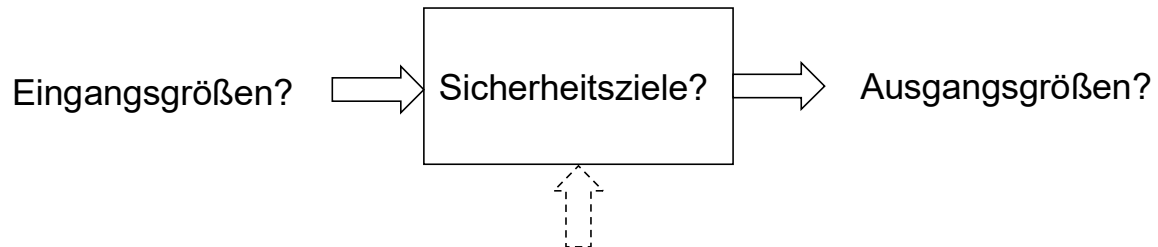


Vorgehen bei der Analyse

1. Systemanalyse
2. Unerwünschtes Ereignis und Ausfallkriterium
3. Relevante Zuverlässigkeitskenngröße und Zeitintervall
4. Ausfallraten der Komponenten
5. Aufstellung des Fehlerbaumes
6. Auswertung des Fehlerbaumes

Vorgehen bei der Analyse: 1. Systemanalyse



Systemfunktion: Abstraktion des Systems als Black Box



Weitere Analysen:

- Umgebungsbedingung (z.B. Temperaturschwankungen)
- Hilfsquellen (z.B. Spannungsversorgung)
- Organisation des Verhaltens
 - Wie wirken die Komponenten zusammen
 - Wie reagiert das System auf Umgebung
 - Wie reagiert das System auf Ausfall der Hilfsquellen

Vorgehen bei der Analyse: 2. Unerwünschtes Ereignis

- Klare Definition der unerwünschten Ereignisse oder des Ausfallkriteriums.
- Untersuchung von:
 - Sicherheit des Systems.
Unerwünschte Ereignis: Ausfall des Systems 
 - Sicherheit einer Funktion des Systems
Unerwünschte Ereignis: Ausfall einer Funktion des Systems 

Vorgehen bei der Analyse:

3. Rel. Zuverlässigkeitskenngrößen

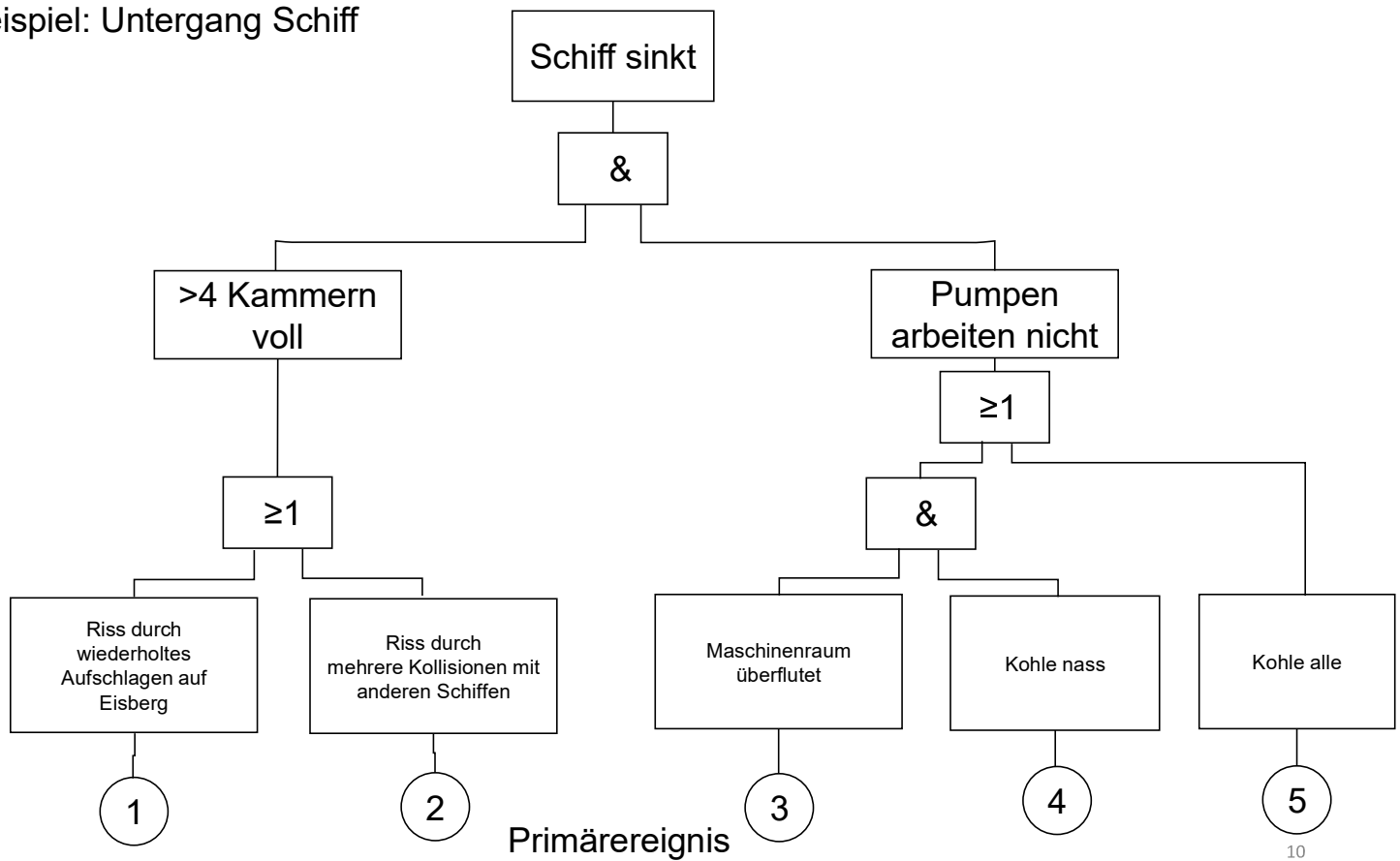
- Nichtverfügbarkeit zu einem Zeitpunkt (oder Mittelwert im Zeitintervall)
- Ausfallhäufigkeit (zwischen zwei Wartungsintervallen)

4. Ausfallart der Komponenten

Ist das unerwünschte Verhalten klar, dann folgt daraus die Ausfallarten der für den Fehlerbaum entscheidende Komponenten.

Vorgehen bei der Analyse: 5. Aufstellen des Fehlerbaumes

Beispiel: Untergang Schiff

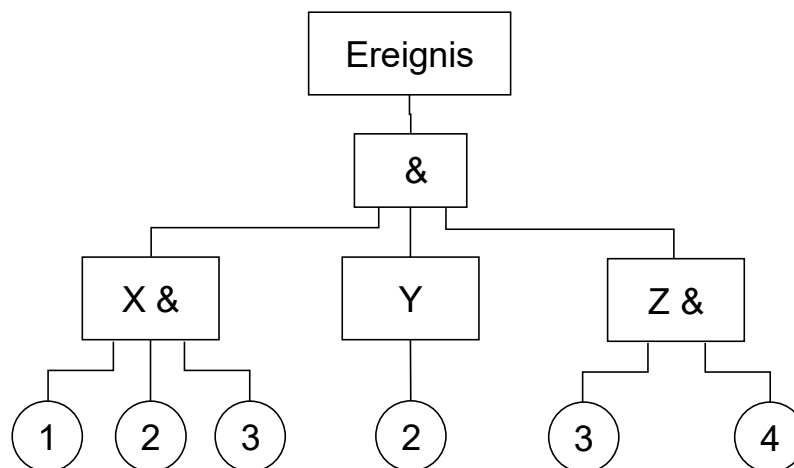


Vorgehen bei der Analyse: 6. Auswertung des Fehlerbaumes

Qualitative Auswertung

- Bestimmung des Ausfallkombinationen (Cut Sets)
- Von besonderem Interesse sind die Minimal Cut Sets: Ausfallkombination die keine weiteren Ausfallkombinationen enthalten

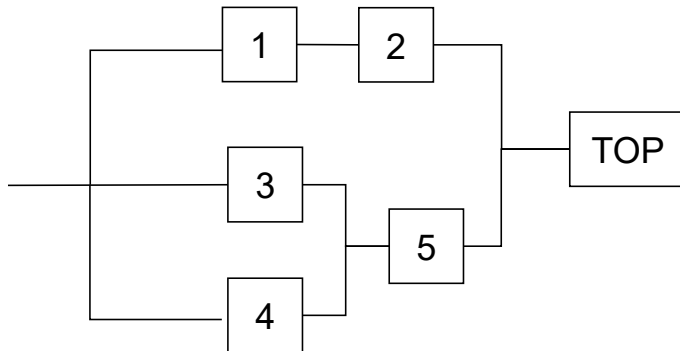
Cut Sets ist:
X, Y und Z



Minimal Cut Sets ist:
X und Z

Vorgehen bei der Analyse: 6. Auswertung des Fehlerbaumes

Pfade im Zuverlässigkeitsblockdiagramm mit Beispiel Untergang Schiff:



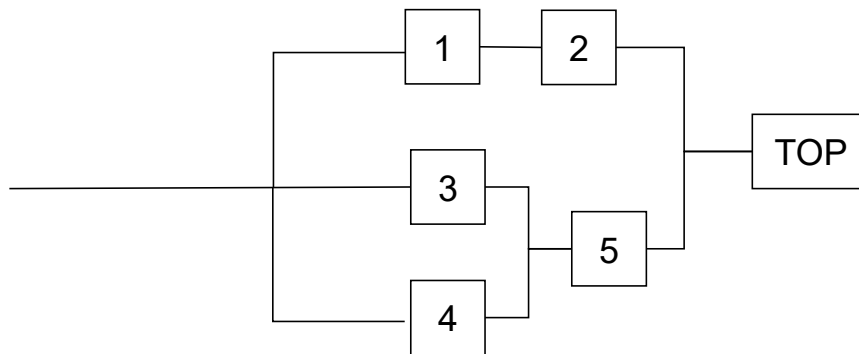
Primärereignisse:

- 1: Riss durch wiederholtes Aufschlagen
- 2: Riss durch mehrere Kollisionen
- 3: Maschinenraum überflutet
- 4: Kohle nass
- 5: Kohle alle

Minimalpfade sind die Mengen der funktionierenden Einheiten, die den Weg vom Eingang zum Ausgang verbinden: $P1=\{1,2\}$ $P2=\{3,5\}$ $P3=\{4,5\}$

Vorgehen bei der Analyse: 6. Auswertung des Fehlerbaumes

Minimal Cut Sets im Zuverlässigkeitsblockdiagramm mit Beispiel Untergang Schiff:



Minimal Cut Sets sind die kleinste Menge ausgefallener Einheiten, die beim Zuverlässigkeitsblockdiagramm den Weg vom Eingang zum Ausgang komplett versperren:

$$S1=\{1,5\}$$

$$S2=\{2,5\}$$

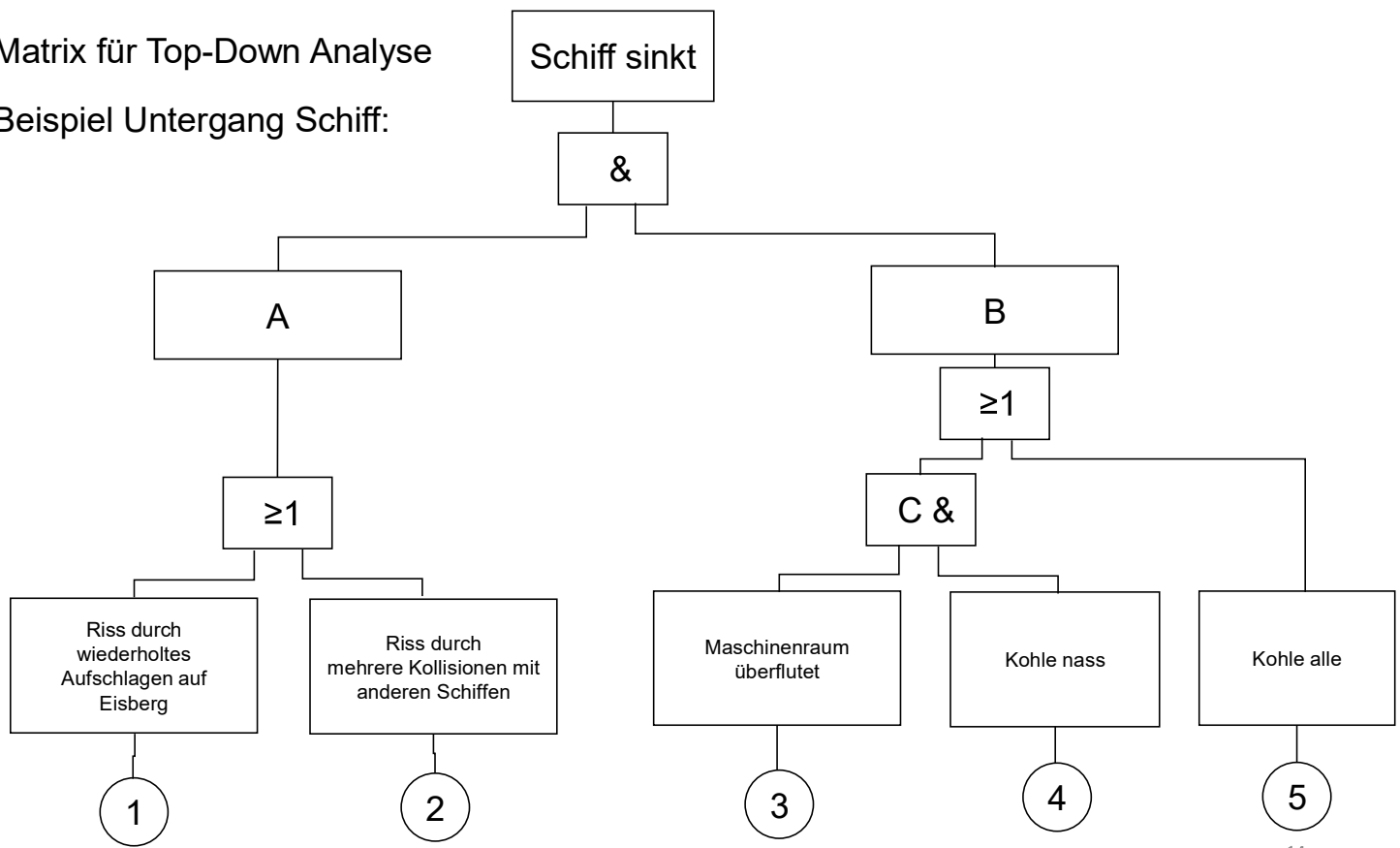
$$S3=\{1,3,4\}$$

$$S4=\{2,3,4\}$$

Vorgehen bei der Analyse: 6. Auswertung des Fehlerbaumes

Matrix für Top-Down Analyse

Beispiel Untergang Schiff:



Vorgehen bei der Analyse: 6. Auswertung des Fehlerbaumes

Algorithmus für Top-Down Analyse

- Beginnend mit dem obersten Ereignis (TOP) werden alle Ereignisse durch die darunterliegenden Ereignisse ersetzt
- Und-Gatter mit m Eingängen werden durch m Spalten mit den entsprechenden Eingangseignissen ersetzt
- Oder-Gatter mit n Eingängen werden durch n Zeilen mit den entsprechenden Eingangseignissen ersetzt
- Dies wird solange wiederholt bis nur noch Primäreignisse vorliegen (also keine Zwischenereignisse)

Vorgehen bei der Analyse: 6. Auswertung des Fehlerbaumes

Berechnung der Nichtverfügbarkeit

Die Nichtverfügbarkeit U eines Systems berechnet sich aus den Nichtverfügbarkeiten U_i der Komponenten.

Die Nichtverfügbarkeit einer Komponente berechnet sich aus ihrer Ausfallrate λ_i und ihrer Reparaturrate μ_i .

Die Verfügbarkeit ist

Vorgehen bei der Analyse: 6. Auswertung des Fehlerbaumes

Berechnungsvorschriften

Gatter	Nichtverfügbarkeit
Oder Gatter	
Und Gatter	
Negation	

Verfahren liefert nur ein exaktes Ergebnis, wenn jedes Primärereignis nur einmal auftritt. Falls ein Primärereignis mehrfach im Fehlerbaum austritt, dann gilt der Baum als vermascht. In diesem Fall liefert das Ergebnis nur eine Abschätzung.

Bewertung der Fehlerbaumanalyse

- Es können komplexere Strukturen analysiert werden, als bei der Ereignisbaumanalyse oder bei dem Zuverlässigkeitsdiagramm.
- Ziel: Ermittlung der Wahrscheinlichkeit eines allgemeinen Systemausfalls.

Beschränkungen

- Ausfallraten der Ereignisse müssen berechenbar sein.
- Kann nicht angewendet werden für zeitliche Analysen.