UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft
Institut für Informatik
Arbeitsgruppe Softwaretechnik

Gefahrenanalyse mittels Fehlerbaumanalyse

von Eike Schwindt

Vortrag im Rahmen des Seminars

Analyse, Entwurf und Implementierung zuverlässiger Software

30. Januar 2004

Agenda

- Motivation
- Einordnung der Verfahren
- Vorstellung des Beispielsystems
- Grundlagen und Syntax der Fehlerbaumanalyse
- Fehlerbaumsemantik am Beispiel
- Anwendung auf Software
- Zusammenfassung

Motivation

- technische Systeme enthalten neben »klassischer« Hardware zunehmend Mikrocontroller und Software
- garantierte und nachprüfbare Aussagen über Sicherheit des Gesamtsystems erforderlich

⇨ Betrachtung dreier formaler Verfahren zur Gefahrenanalyse und Untersuchung ihrer Eignung für hybride Systeme und Software:

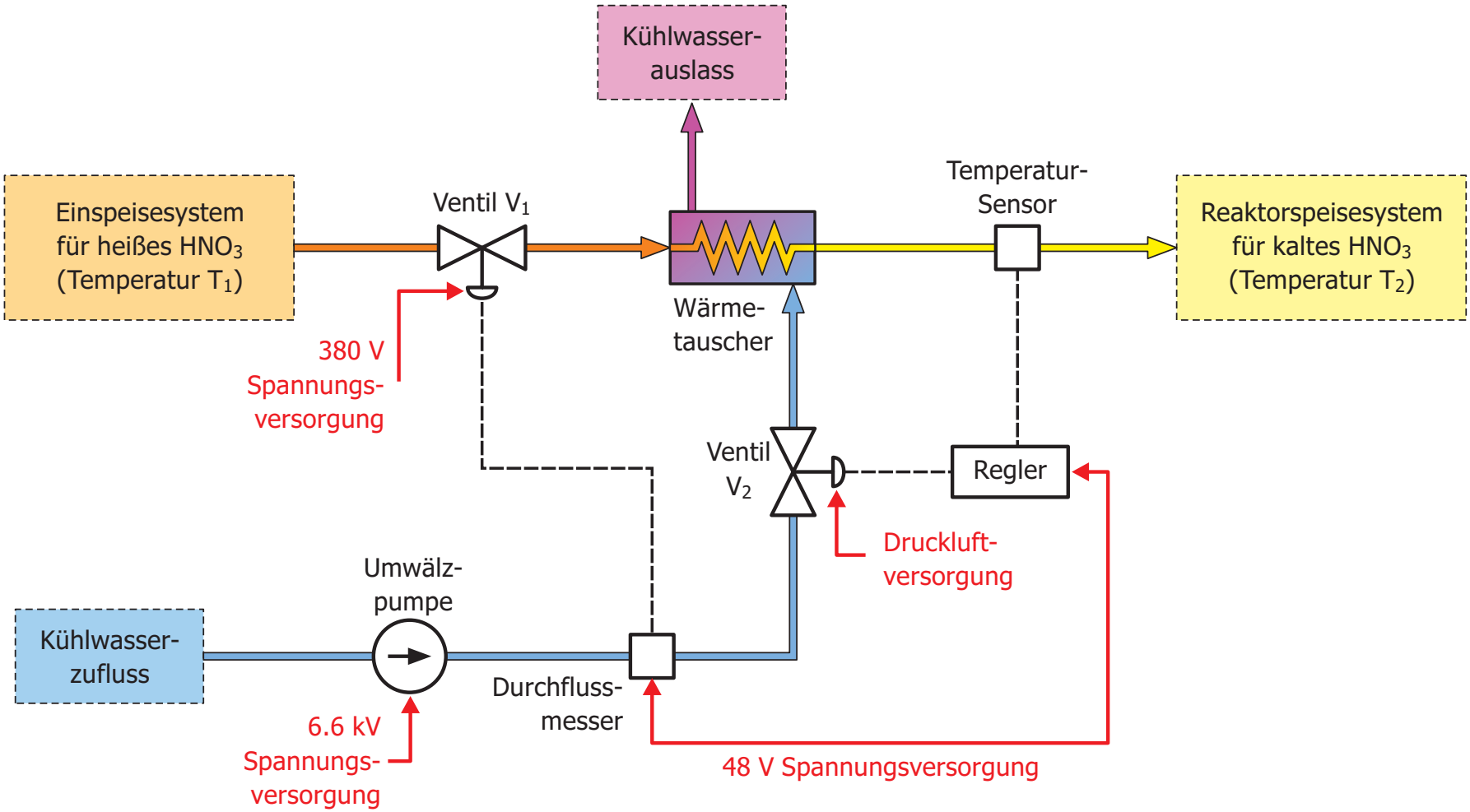
Fehlerbaumanalyse, FMEA, HAZOP

Einordnung der Verfahren [1]

	Gefahrenursache	
	bekannt	unbekannt
Auswirkungen von Komponentenversagen bekannt	Beschreibung des Systemverhaltens	Deduktive Analyse (Fehlerbaumanalyse)
Auswirkungen von Komponentenversagen unbekannt	Induktive Analyse (FMEA)	Explorative Analyse (HAZOP)

[1] nach Fenelon, McDermid, Nicholson und Pumfrey: *Towards Integrated Safety Analysis and Design*

Vorstellung des Beispielsystems



Fehlerbaumanalyse

engl.: Fault Tree Analysis (FTA)

- entwickelt 1961 zur Untersuchung eines Raketenabschuss-Systems
- seit längerem standardisiert (DIN und IEC)
- dient der Ursachenermittlung von Systemversagen
- ermöglicht qualitative und quantitative Analysen
- deduktive Top-Down-Methode
- graphische Repräsentation kausaler Abläufe

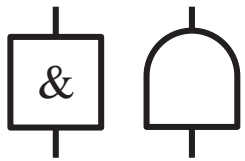
Vorgehensweise

FTA besteht aus:

1. Systemdefinition
   (TOP Ereignis, Systemgrenzen, »Auflösung«, …)
2. Fehlerbaum-Konstruktion
   Zurückführen der Ursache des TOP Ereignis auf Kombinationen von Komponentenversagen mittels logischer Verknüpfungen
3. qualitativer und quantitativer Analyse
4. Dokumentation der Ergebnisse

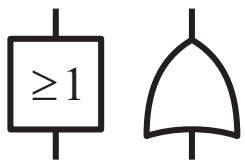
Fehlerbaum-Syntax

TOP Ereignis / Zwischenereignis

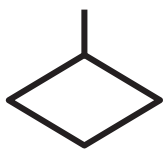


UND-Verknüpfung

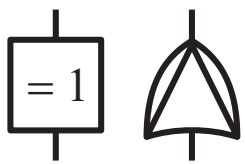
Primäres Ereignis



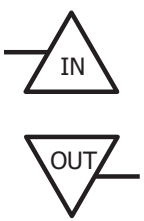
ODER-Verknüpfung



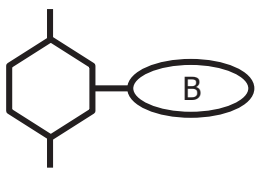
unentwickeltes Ereignis



X-ODER-Verknüpfung

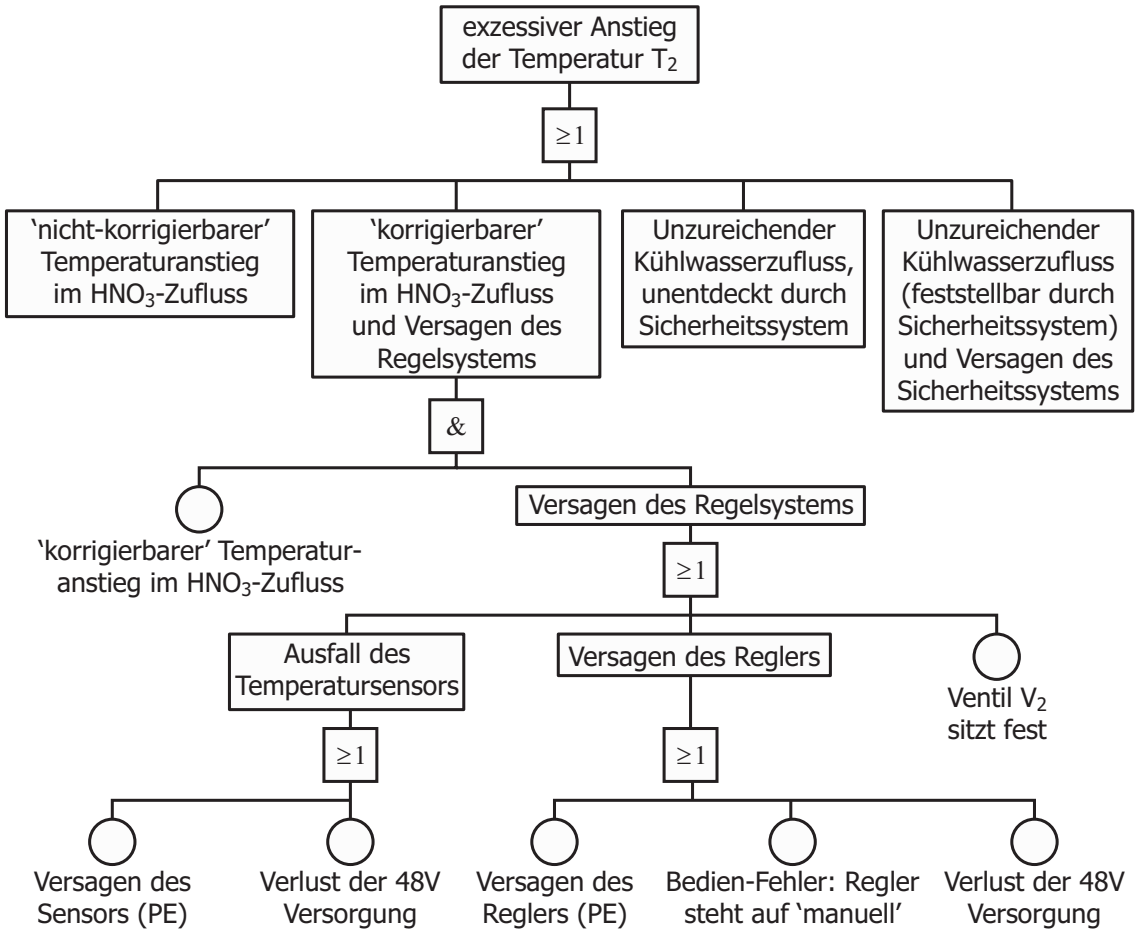


Transfer Symbole



Bedingte Verknüpfung

Fehlerbaumkonstruktion (1)



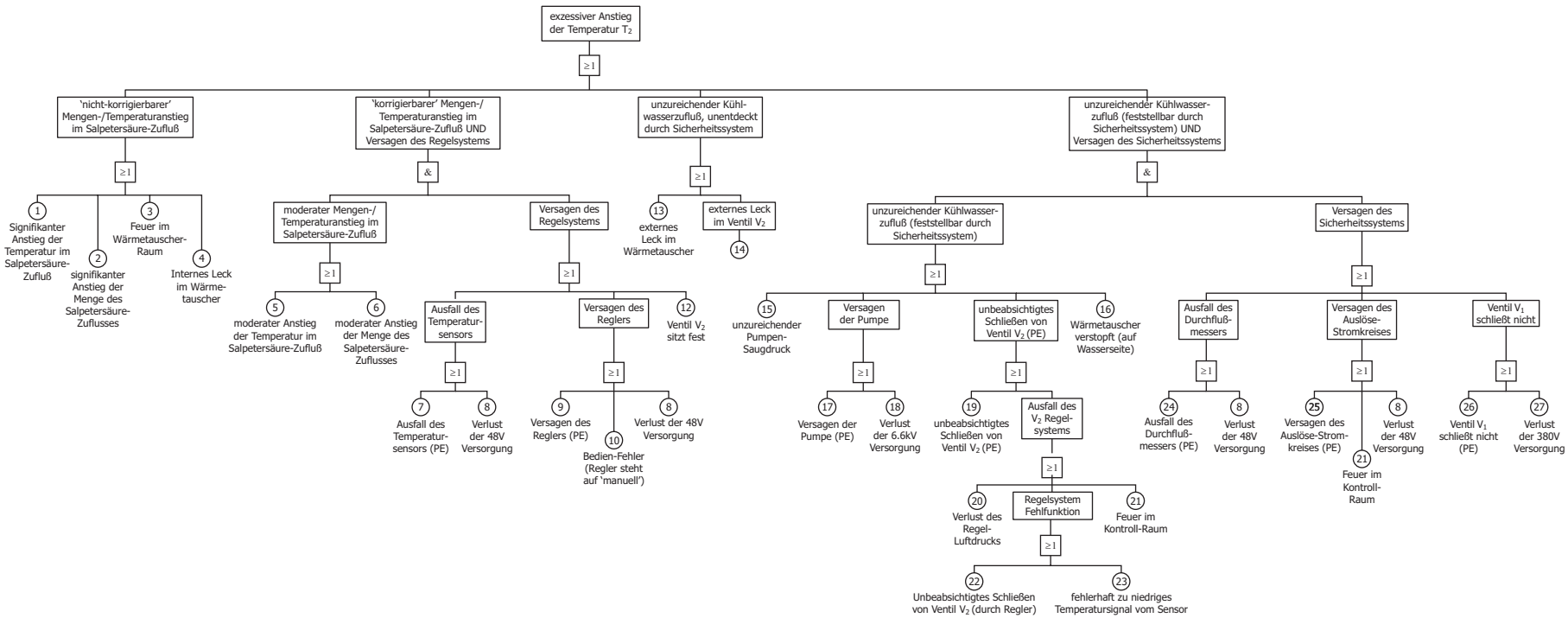
- Identifizieren des TOP Ereignis
- Identifizieren der Verursacher der ersten Ebene
- Verbinden durch log. Verknüpfungen
- Wiederholen/Fortsetzen für die nächsten Ebenen

  ...

- bis Primäre Ereignisse erreicht sind

Fehlerbaumkonstruktion (2)

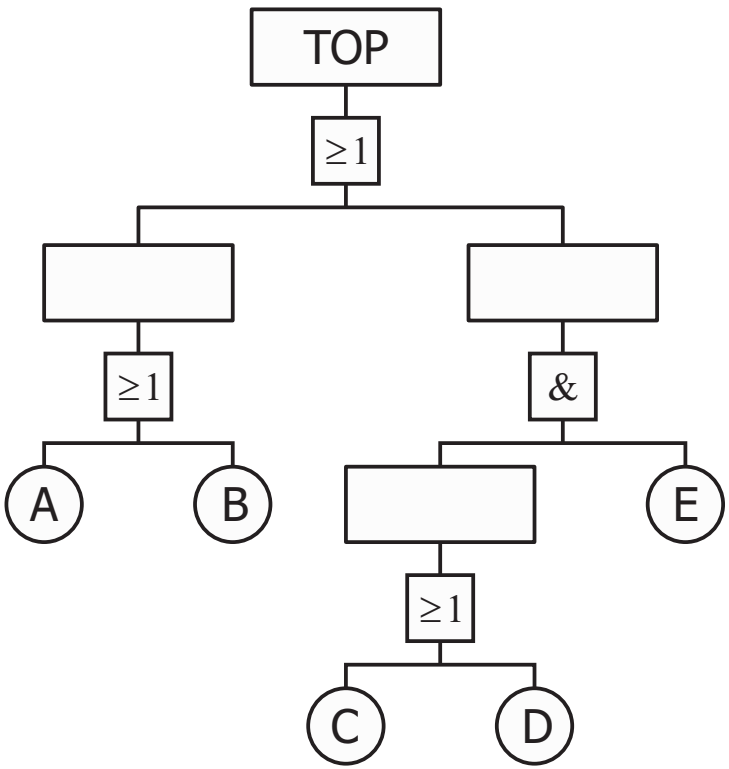
Gesamtansicht des kompletten Fehlerbaumes:



Qualitative Analyse

Fehlerbaum entspricht einer logischen Gleichung

⇨ ermöglicht Bestimmung von:

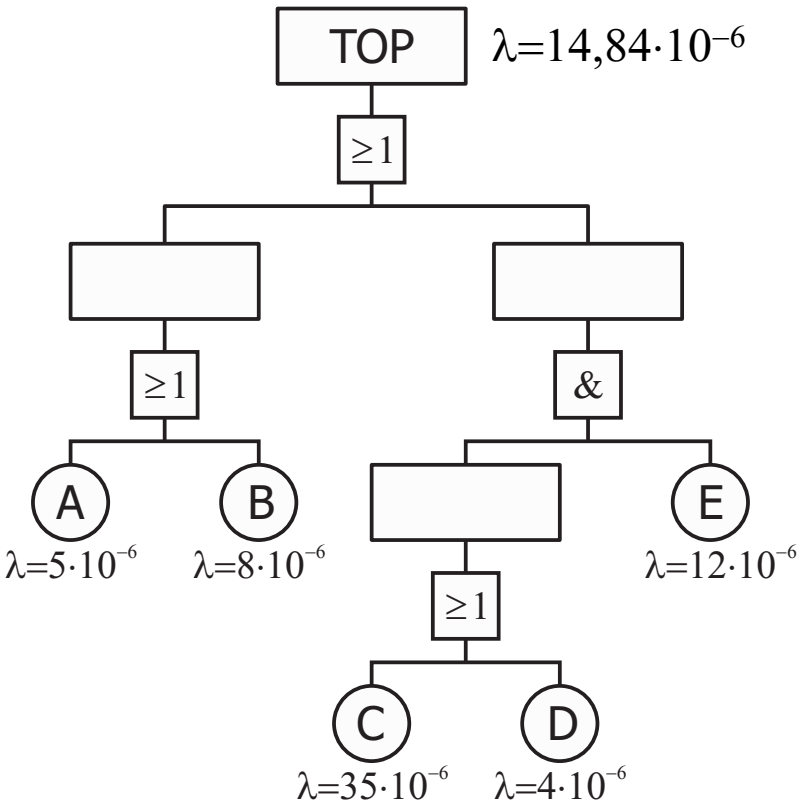


- *Minimal Cut Sets* (MCS)
  {A} , {B} , {C,E} , {D,E}
- *Single Point Failures*
  {A} , {B}
- Anfälligkeiten für *Common Mode* Fehler

Quantitative Analyse

Ausfallw'keiten oder –raten aller Komponenten bekannt

⇨ weitere Berechnungen möglich:



- Ausfallw'keit oder -rate des Gesamtsystems
- quantitativer Beitrag einzelner Komponenten liefert Rangliste ihrer Wichtigkeit

⇨ Ansätze zur gezielten Verbesserung des Systems

FTA für Software/hybride Systeme

Einsatz in der Designphase:

- identifiziert potentiell gefährliche Module/Schnittstellen bzw. risikobehafteten Programm-Output
- liefert Anforderungsdefinitionen für SW
- bietet Ansätze für präventive oder protektive Maßnahmen
- Schwierigkeiten:
  - Fehlerbäume allein unzureichend zur Modellierung komplexer Systeme
  - FTA erfordert genaue Kenntnisse des Systems ⇨ in der Designphase nicht vorhanden

Software Fault Tree Analysis (SFTA) [2]

Einsatz direkt auf Quellcode-Ebene:

- unerwünschter Programm-Output wird als TOP Ereignis definiert
- Umwandlung von Statements in Fehlerbaumausdrücke mittels Templates
- Ergebnis ist graphische Repräsentation einer »umgekehrten« Verifikation

⇨ ebenso wie Verifikation nur für kurze Programme praktikabel

[2] nach Leveson: *Safeware – System Safety and Computers*

Bewertung des Verfahrens

Nachteile

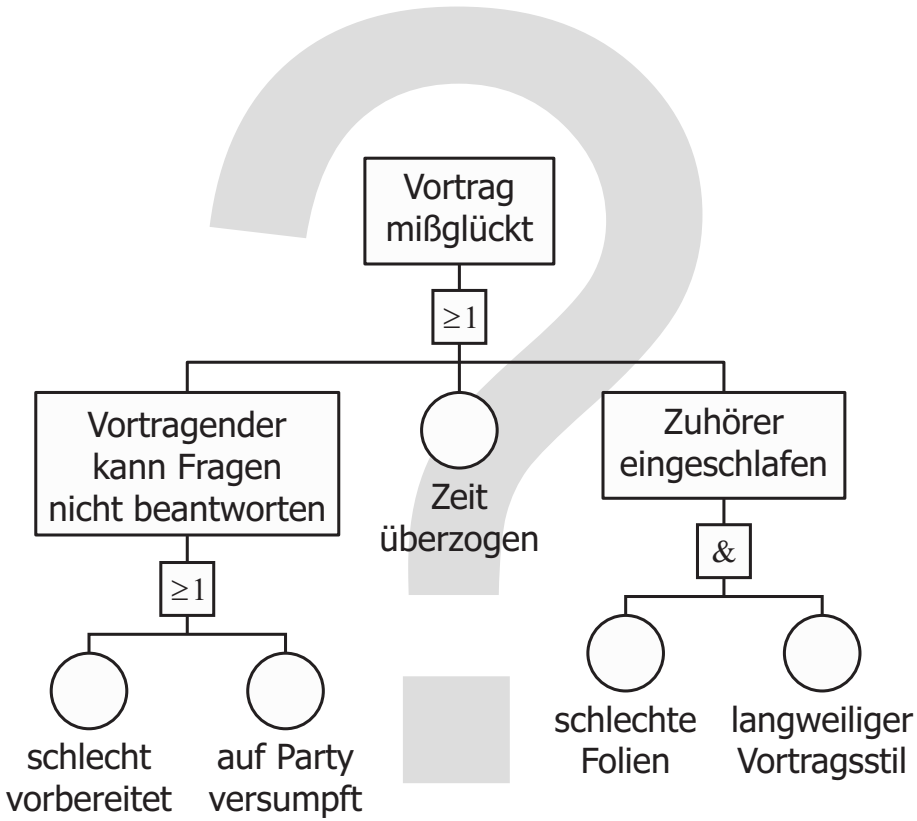
- TOP Ereignis muss *vorher* bekannt sein, neue Gefahren werden nicht entdeckt
- je TOP Ereignis ein Baum
- umfangreiche Fehlerbäume schon aus kleinen Systemen
- genaue Kenntnis des Systems erforderlich
- eingeschränkte Möglichkeiten zur Modellierung dynamischer Prozesse
- quantitativen Daten oft nicht für alle Komponenten vorhanden

?

Vorteile

- erfordert intensive Untersuchung des Systems und des Zusammenwirkens der Komponenten
- im Idealfall nachprüfbare qualitative und quantitative Aussagen über Zuverlässigkeit des Systems und Bedeutung von Komponenten
- Einschätzung der Anfälligkeit für Common Causes
- modularer Aufbau ermöglicht Bearbeitung im Team

Noch Fragen ?


Vortrag mißglückt
≥1
Vortragender kann Fragen nicht beantworten
Zeit überzogen
Zuhörer eingeschlafen
≥1
&
schlecht vorbereitet
auf Party versumpft
schlechte Folien
langweiliger Vortragsstil