Sicherheit und Zuverlässigkeit in der Software-Entwicklung

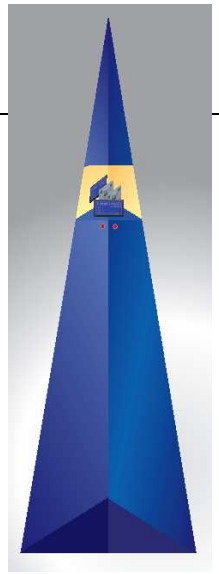
Sergio Montenegro

sergio@first.fhg.de

Holger Schlingloff

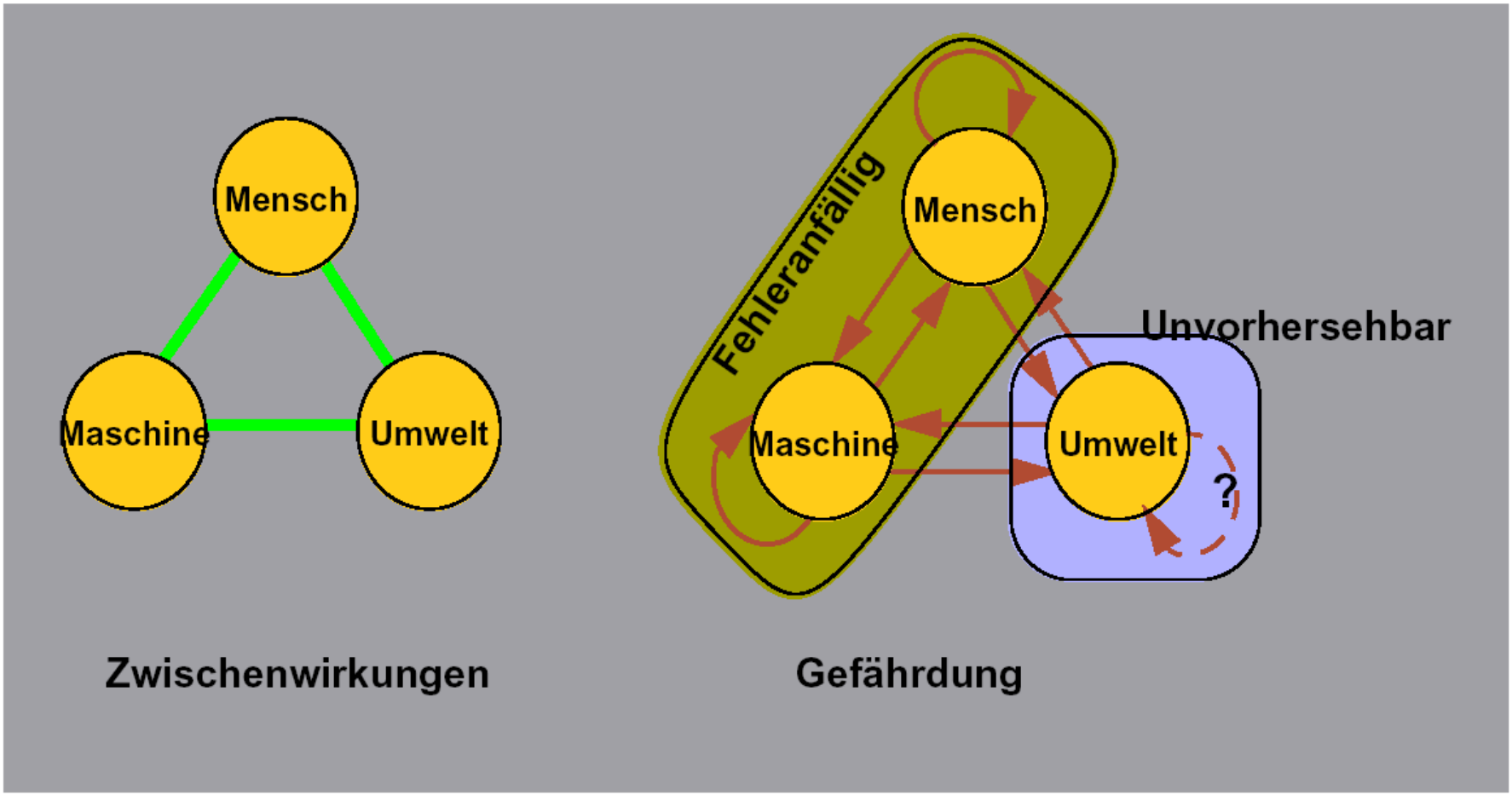
Holger.Schlingloff@first.fhg.de

Hazard & Risiko Analyse



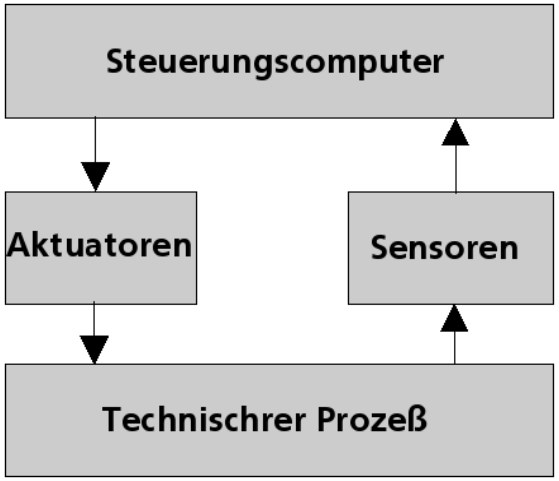
Fraunhofer Institut
Rechnerarchitektur
und Softwaretechnik

Gefärdung

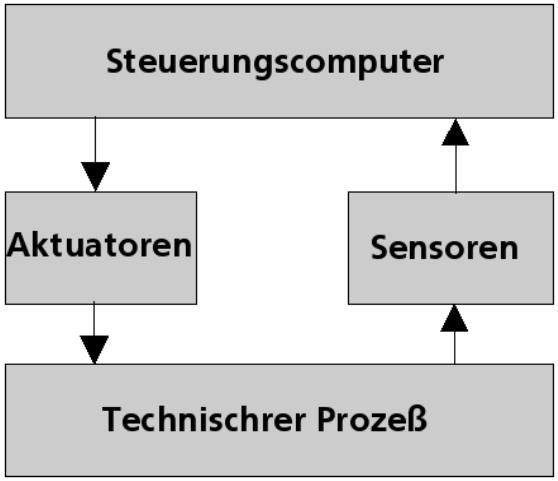


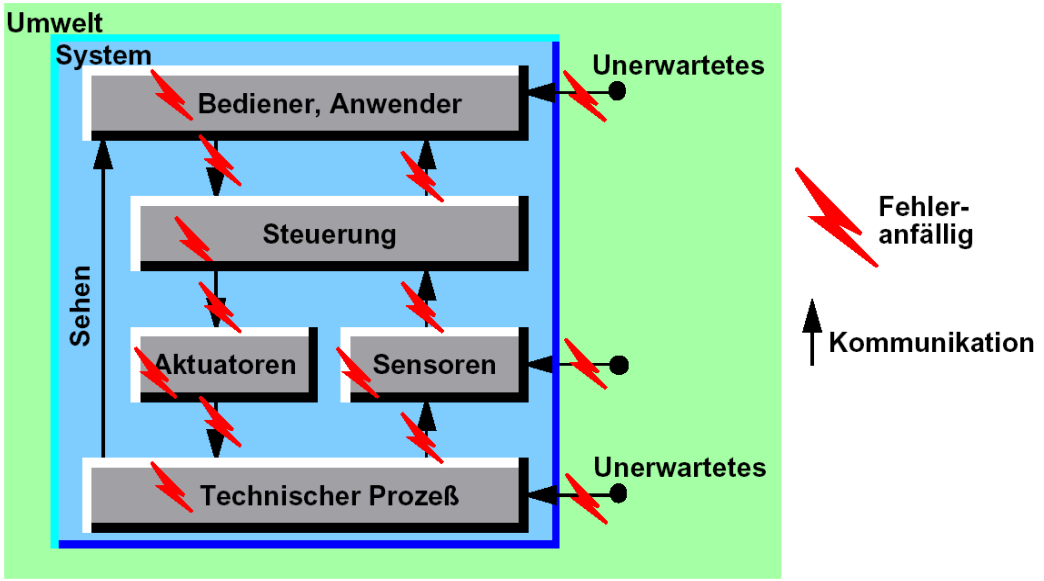
Das Systemdreieck

Die Steuerung... Die Maschine

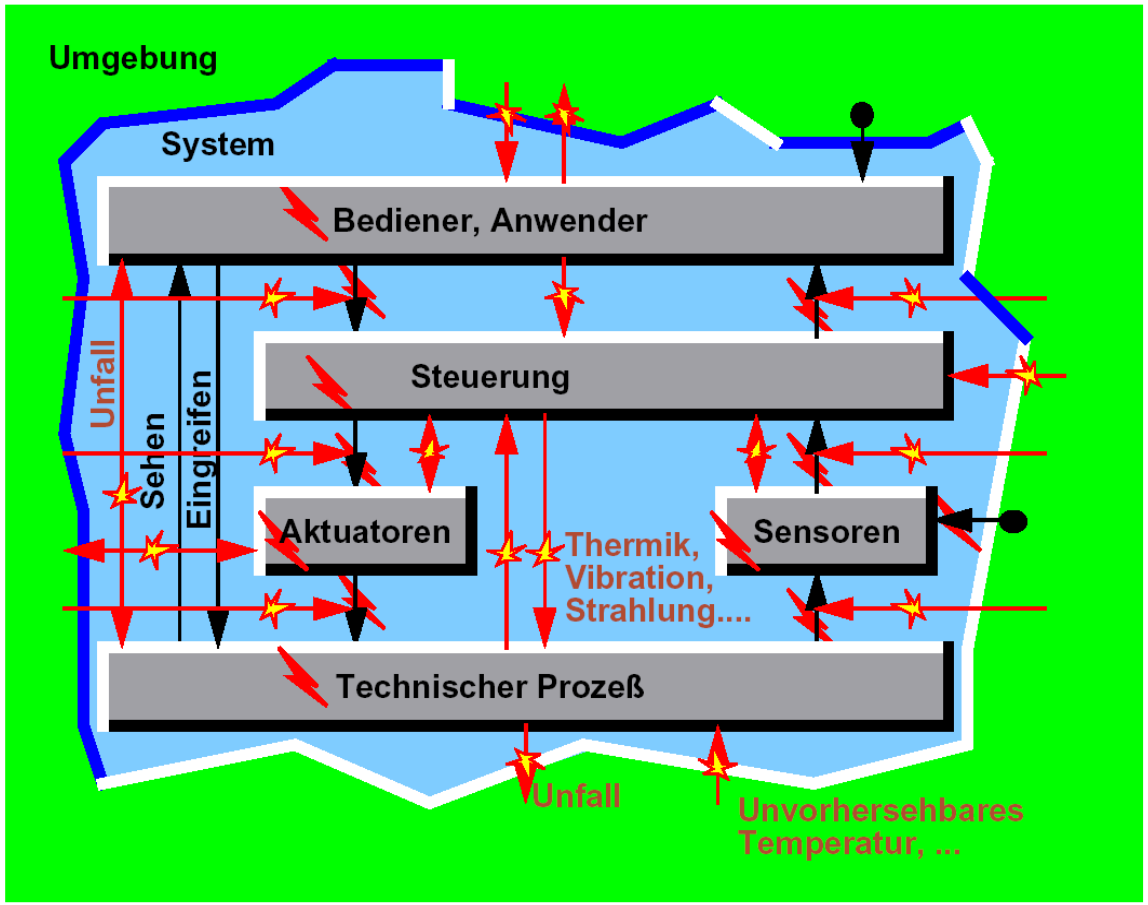


Die Steuerung





Die Steuerung



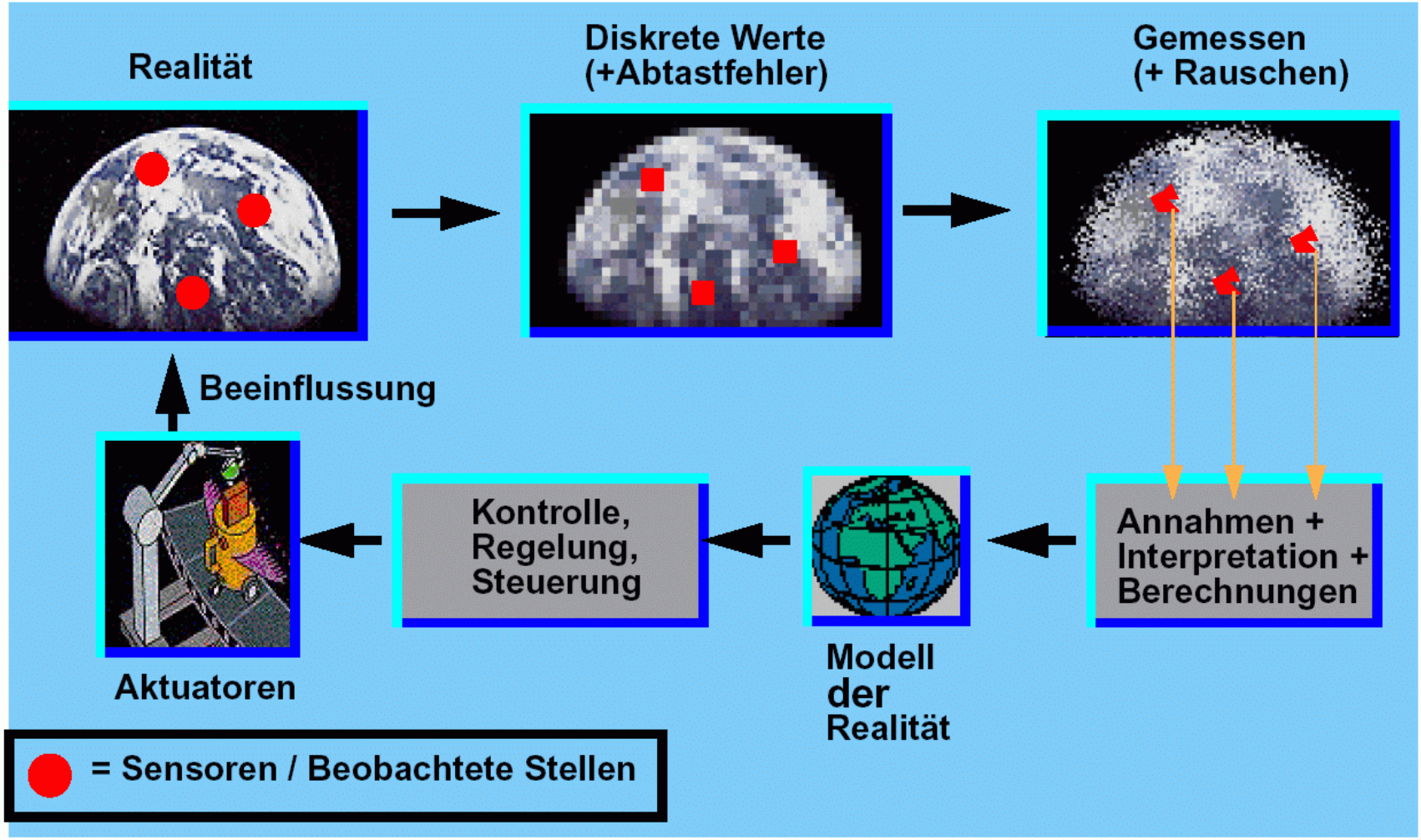
Kontrollierte Beeinflussung
Kommunikation,
Befehle, Zustandsinformationen

Ungeplante und
unerwünschte
Beeinflussung

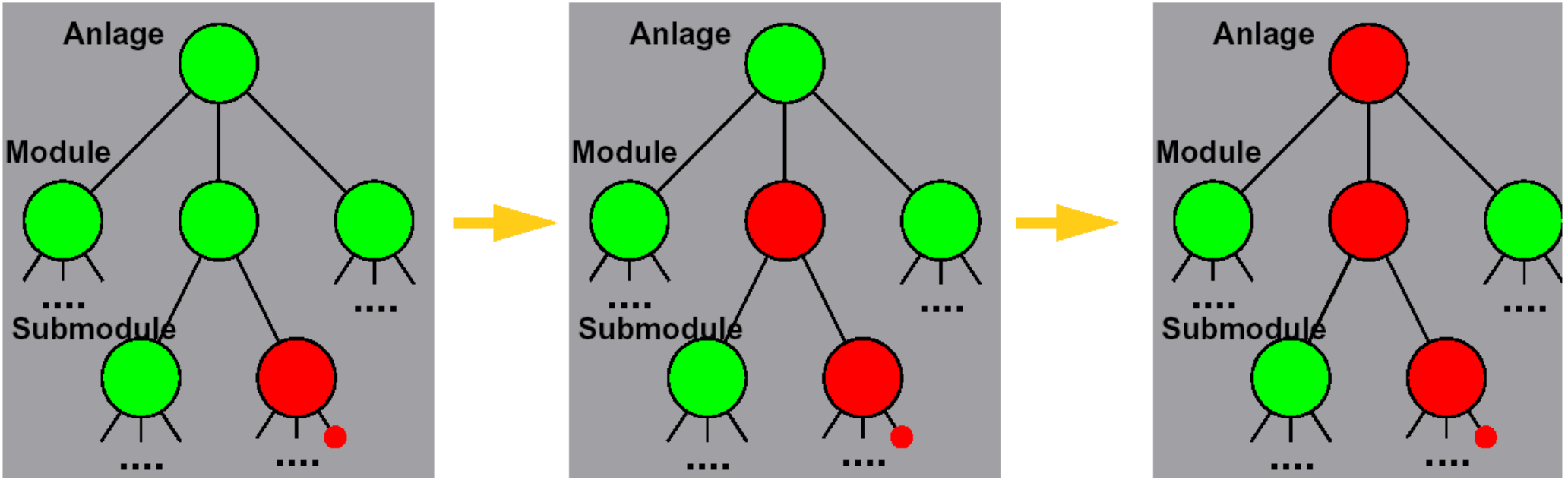
Fehler-
anfällig

FIRST
Fraunhofer Institut
Rechnerarchitektur
und Softwaretechnik

Die Steuerung sieht nicht die Realität



Fehlerfortpflanzung



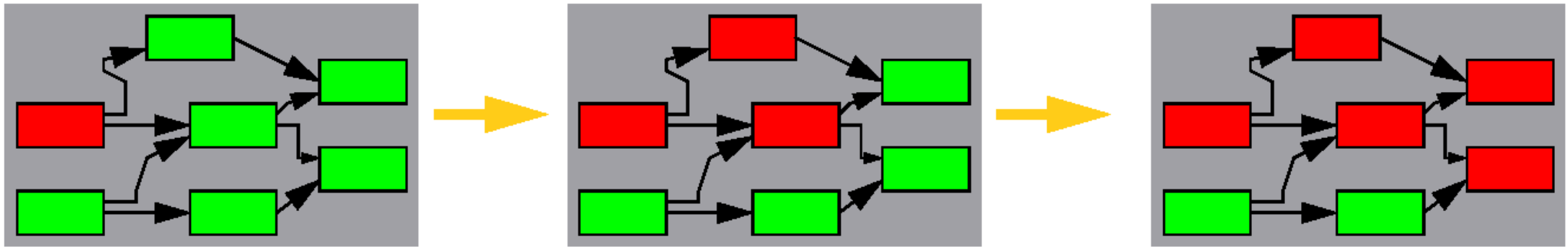
Funktionierendes Modul

Ausgefallenes Modul

Fehlerfortpflanzung in der Modulhierarchie

FIRST
Fraunhofer Institut
Rechnerarchitektur
und Softwaretechnik

Fehlrfortpflanzung in Software



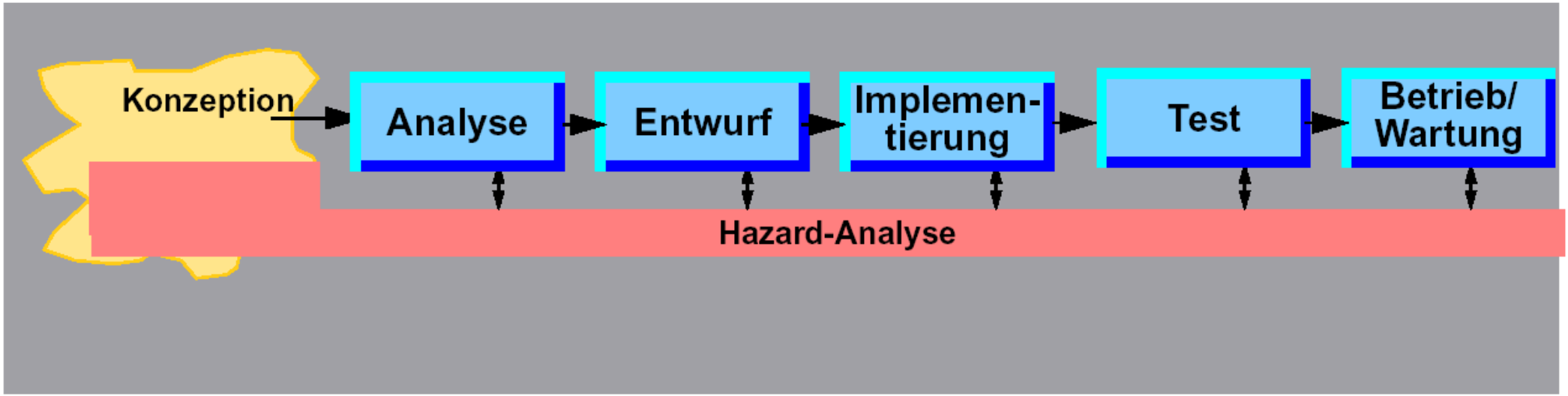
System-Daten-Fluß.

Funktionierendes Modul

Ausgefallenes Modul

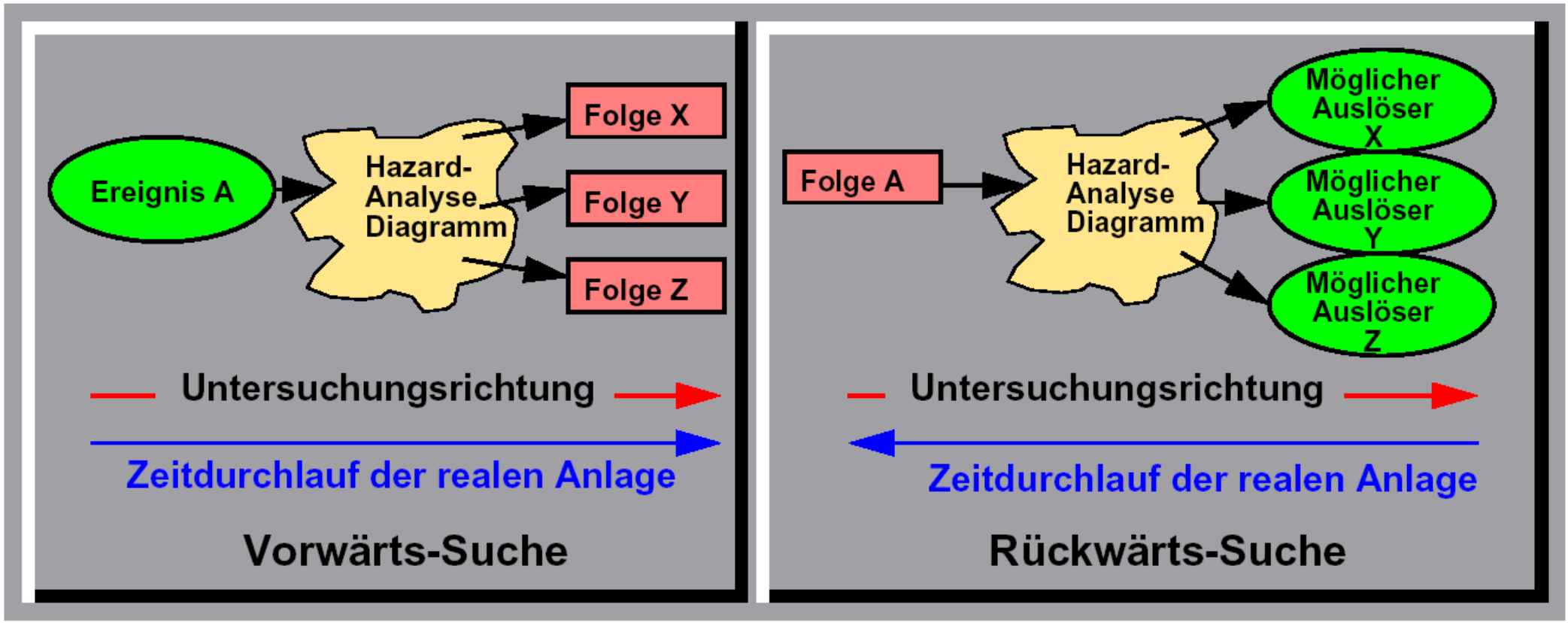
Fehlerfortpflanzung im Moduldatenfluß

Hazard- und Risiko-Analyse



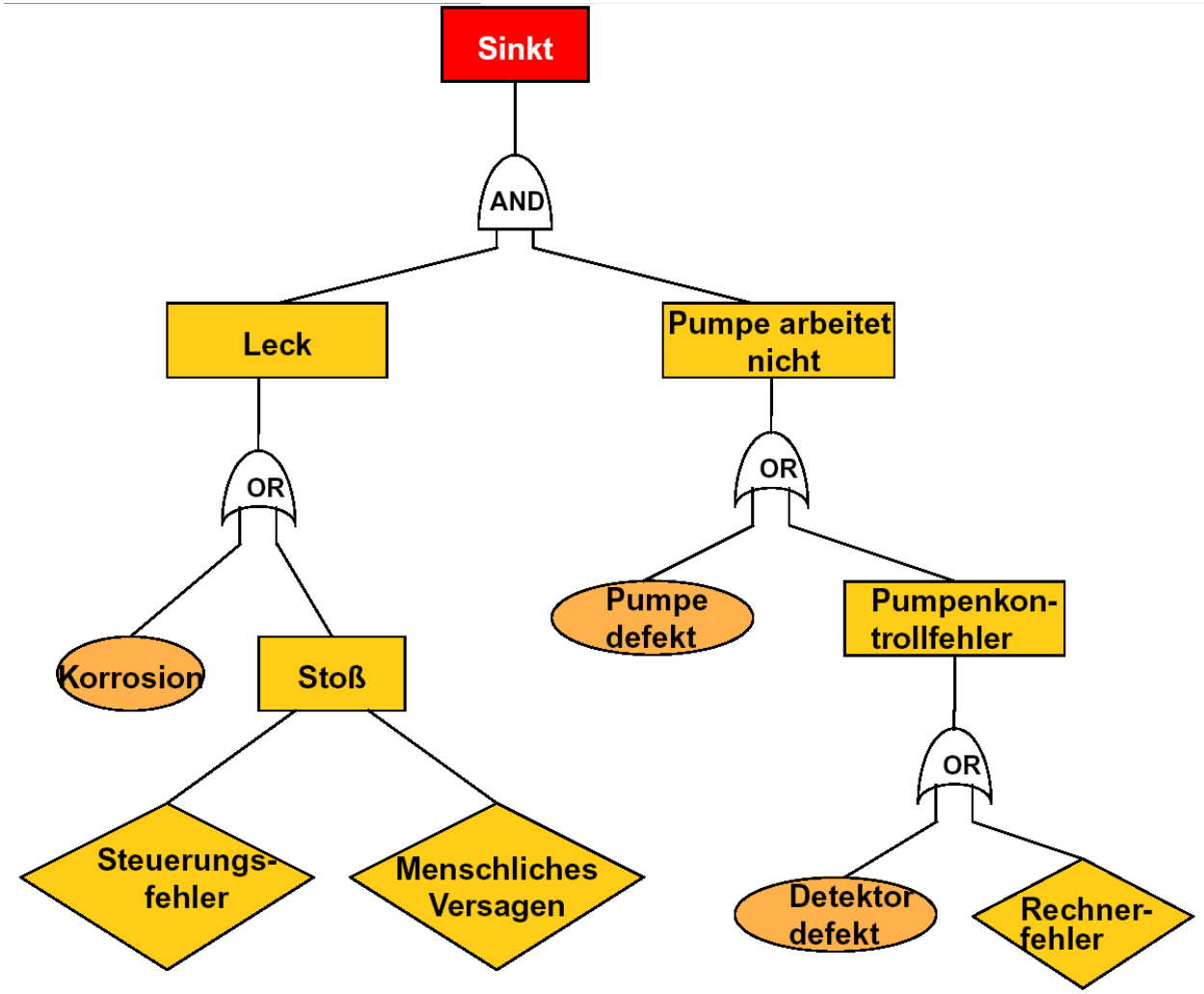
Wann wird die Hazard-Analyse durchgeführt?

Hazard- und Risiko-Analyse



Vorwärts- und Rückwärts-Suche

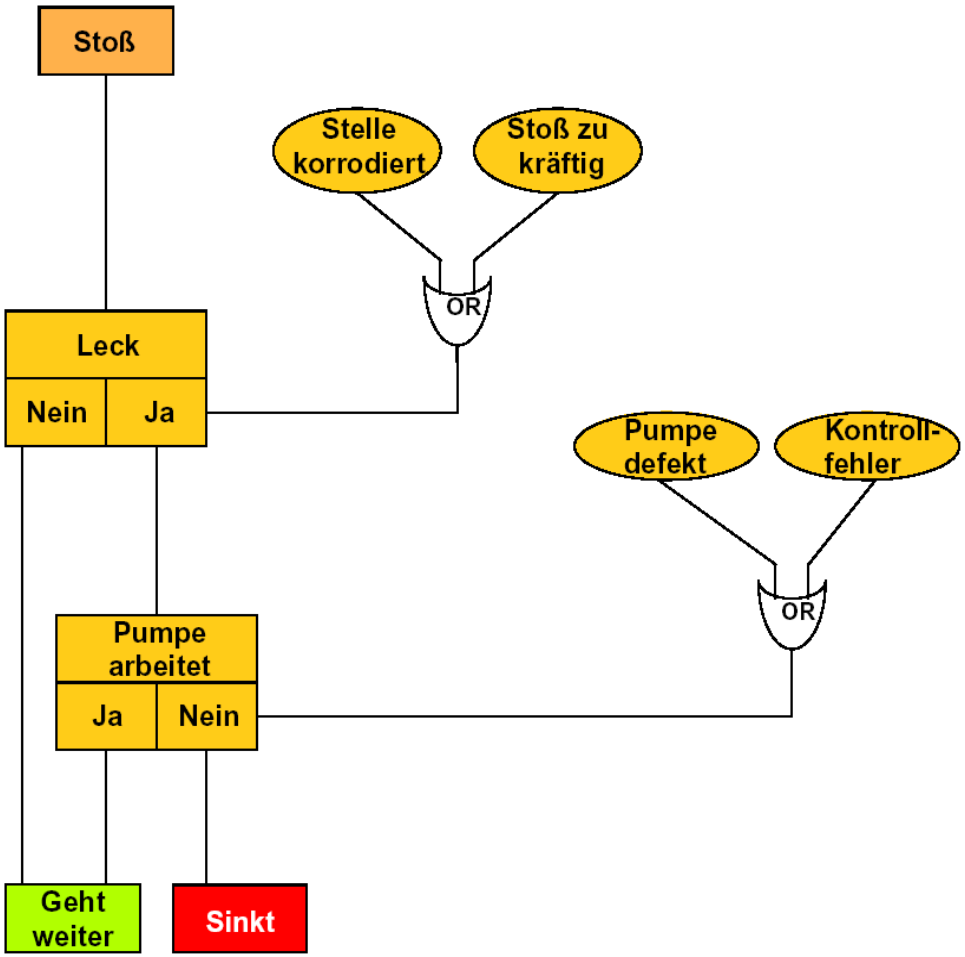
Hazard- und Risiko-Analyse .. Fault Tree Analysis



Beispiel eines FTA-Diagramms

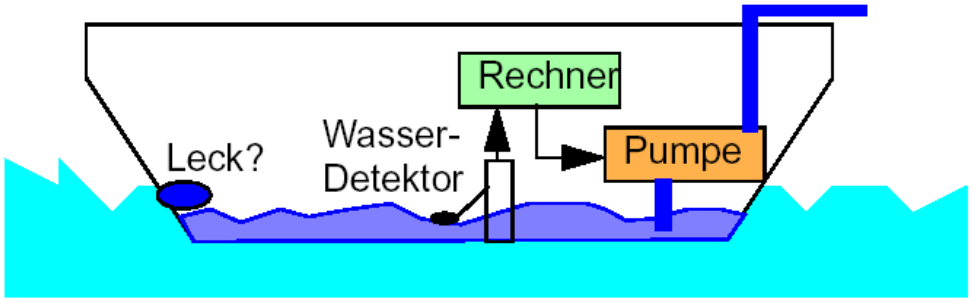
FIRST
Fraunhofer Institut Rechnerarchitektur und Softwaretechnik

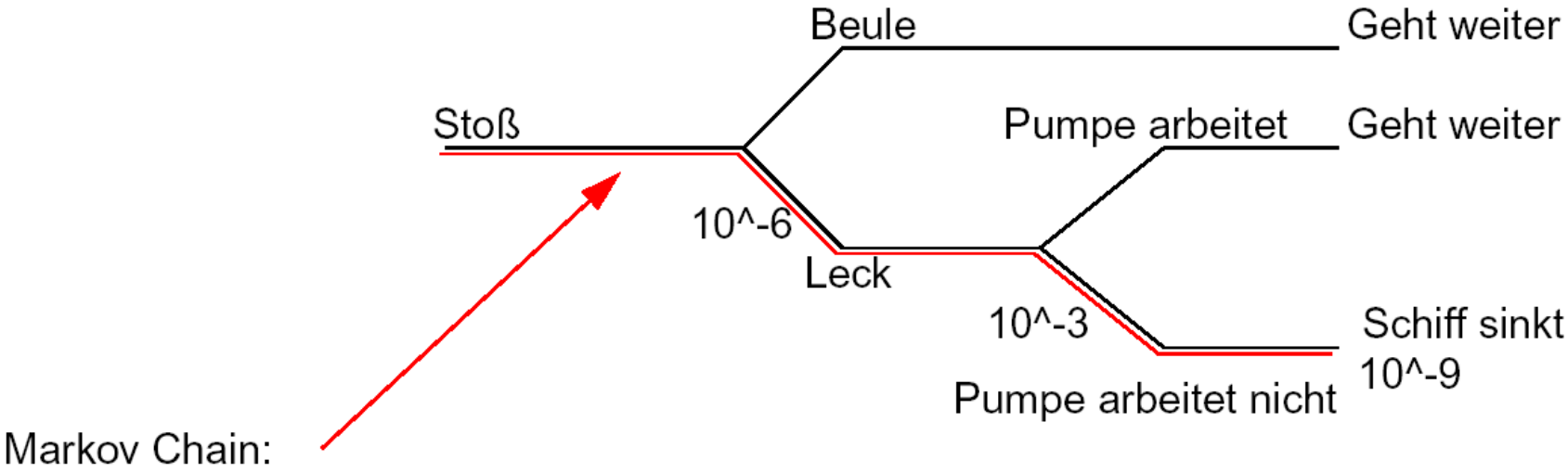
Hazard- und Risiko-Analyse... Cause Effekt Analysis



Beispiel eines CEA-Diagramms

Hazard- und Risiko-Analyse... Event Tree Analysis

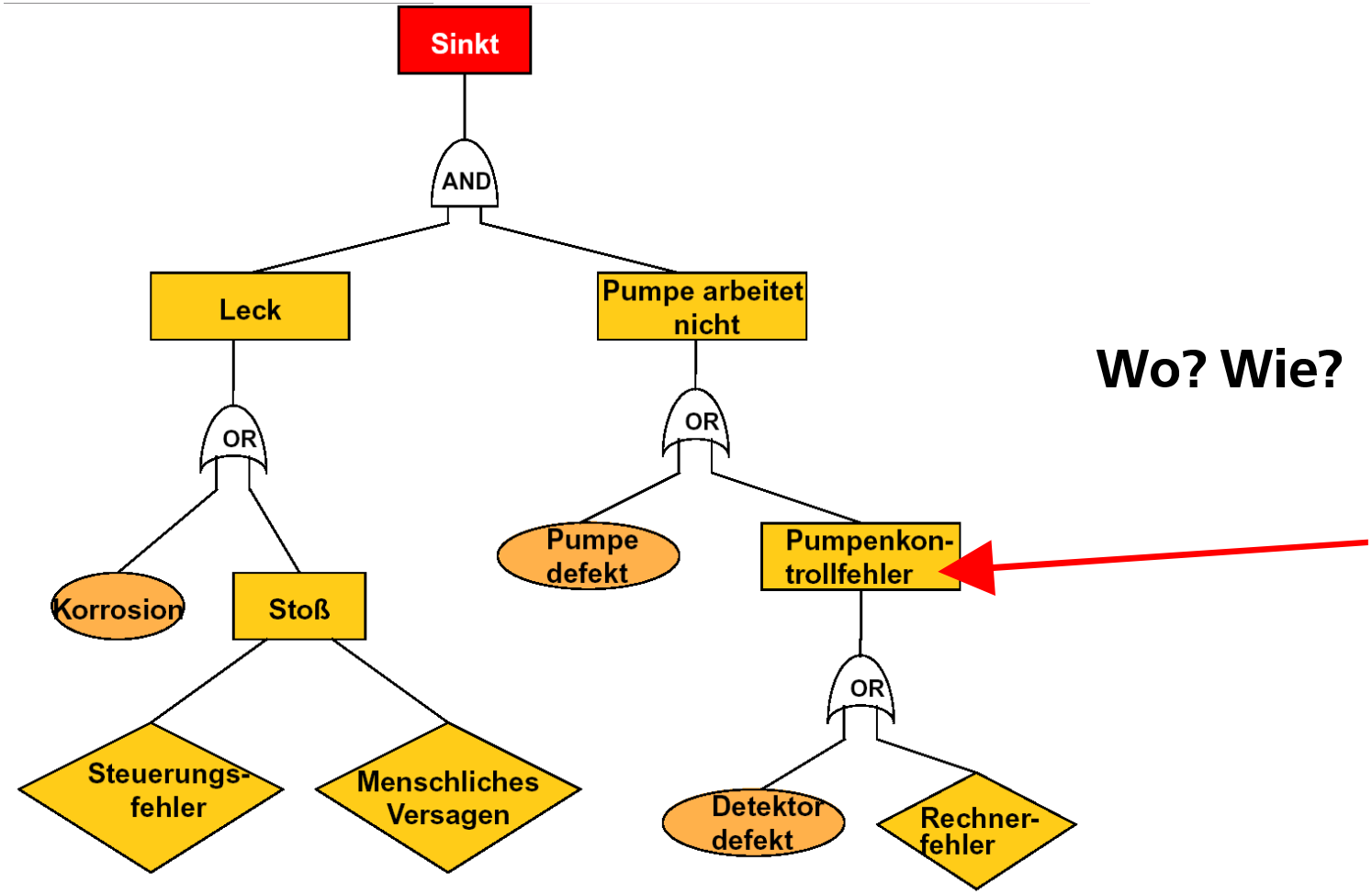




Markov Chain:
10^-6 * 10^-3 = 10^-9 = Wahrscheinlichkeit für das Sinken

Beispiel eines ETA-Diagramms

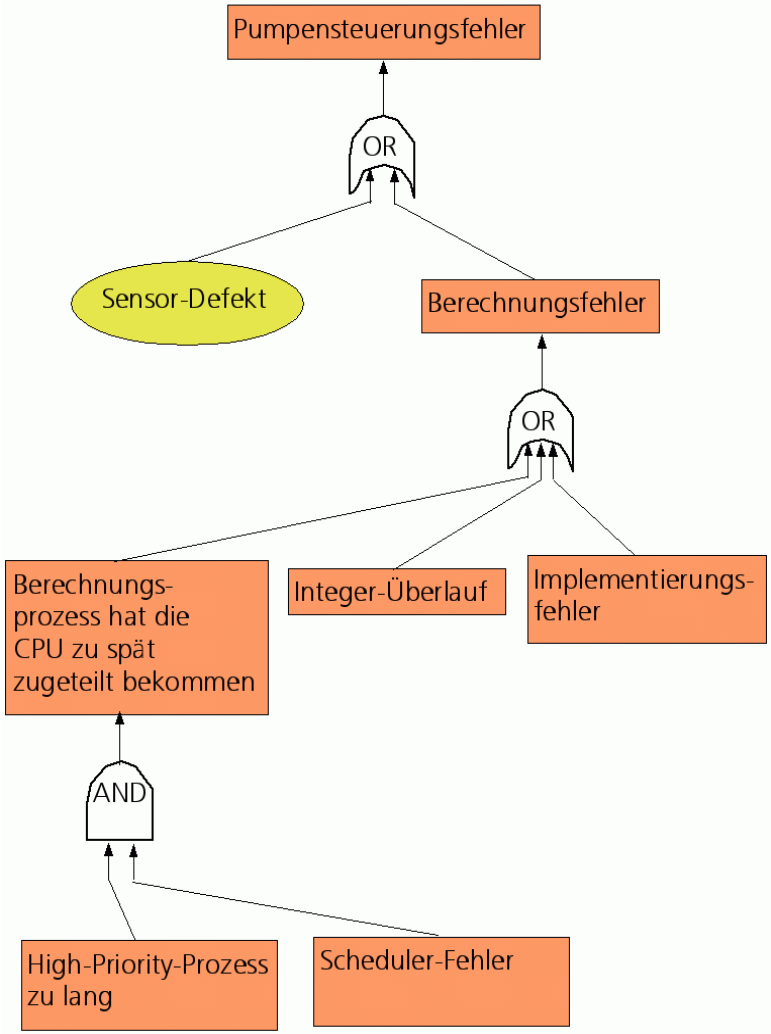
Software Hazard Analyse

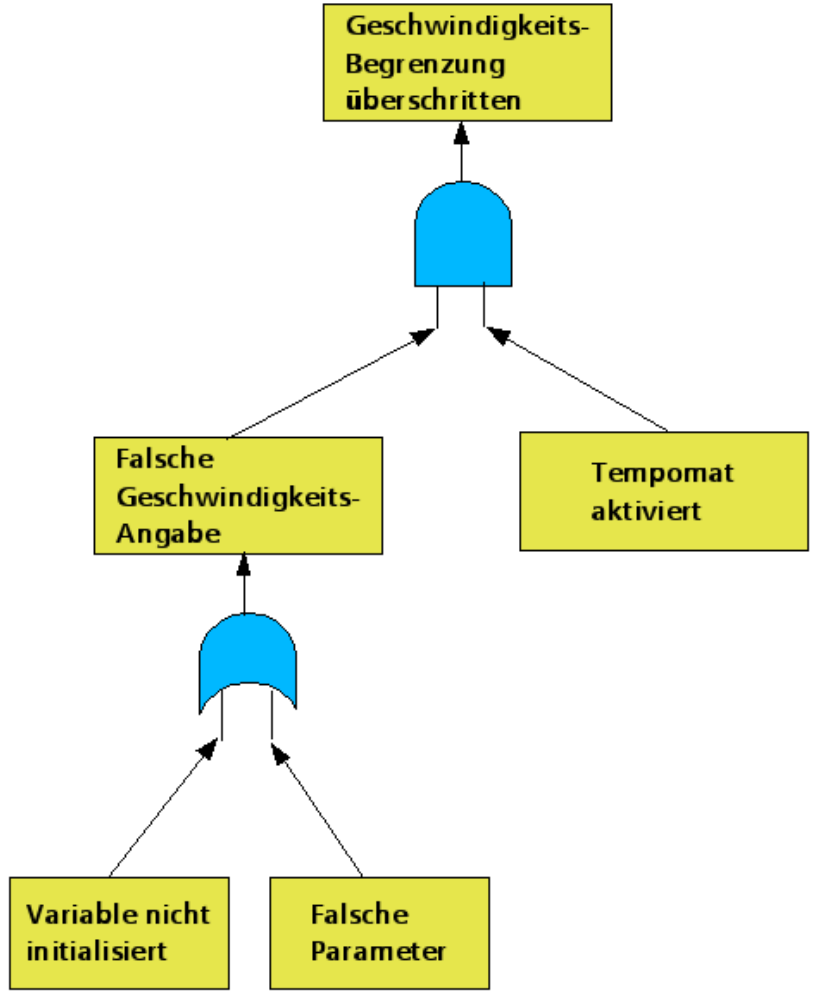


Wo? Wie?

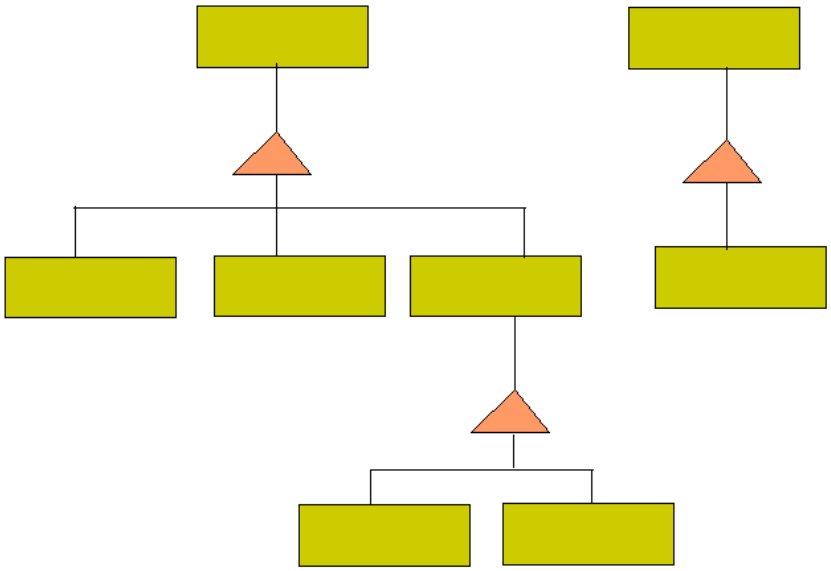
Beispiel eines FTA-Diagramms

Software Hazard Analyse



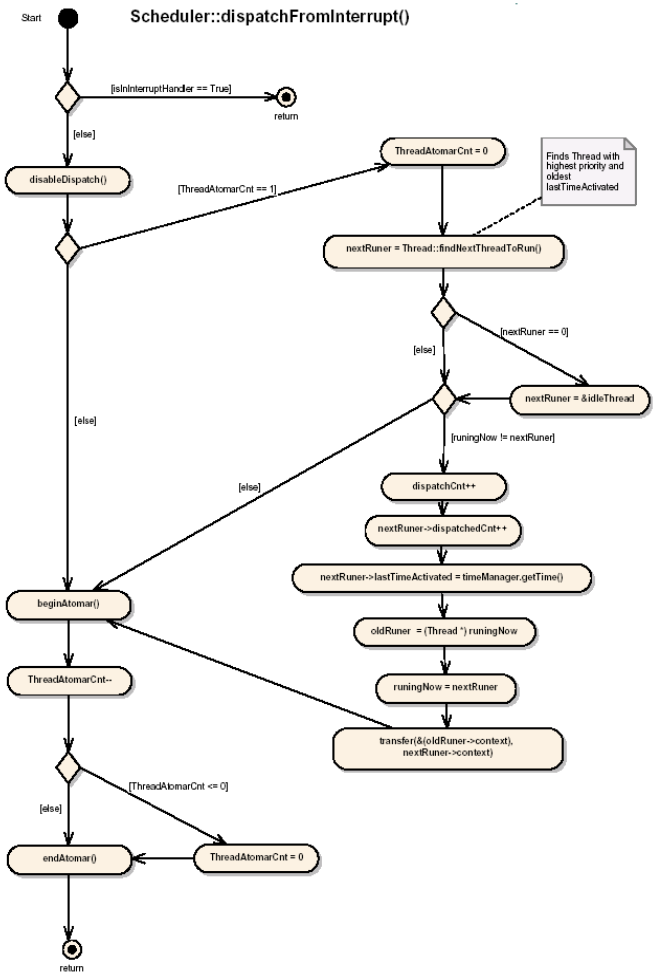


Software Hazard Analyse (so nicht)



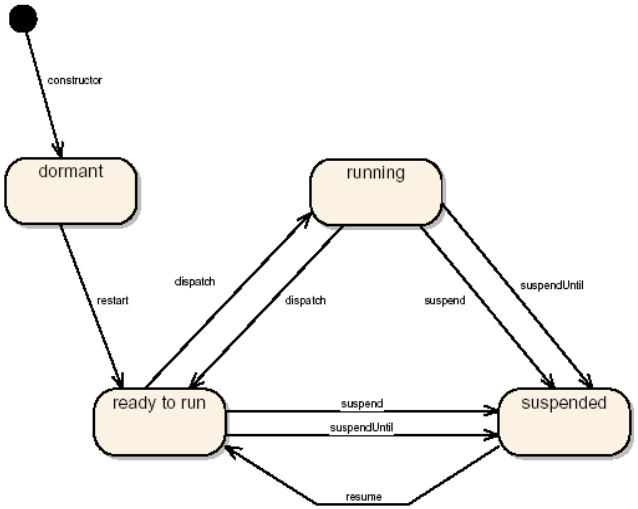
Classen diagram?
Kein Verhalten

Software Hazard Analyse (so nicht)



Flow diagram?
Zu Detaliert

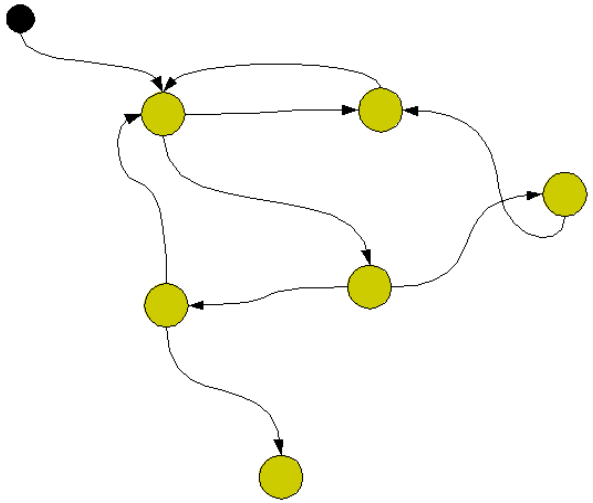
Software Hazard Analyse (so nicht)



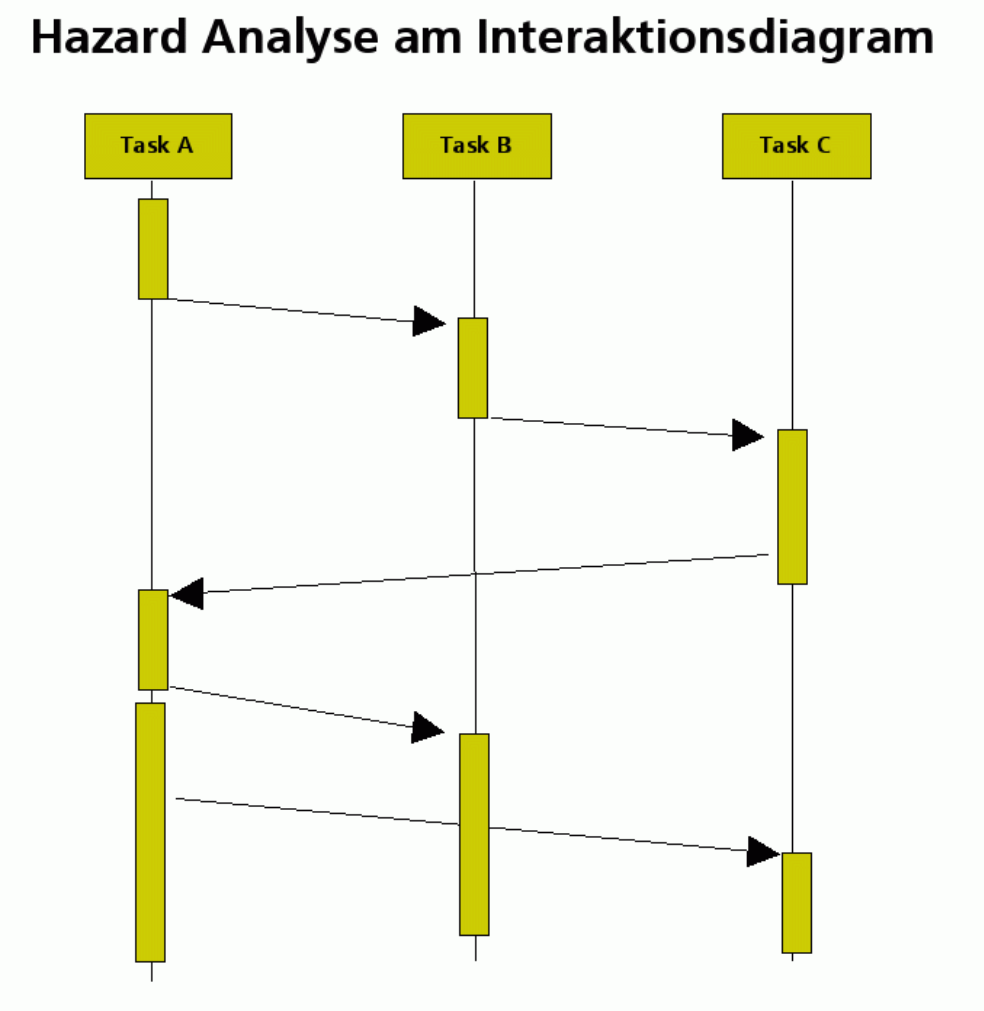
State diagram?

Wo kann etwas falsch laufen?

überall!



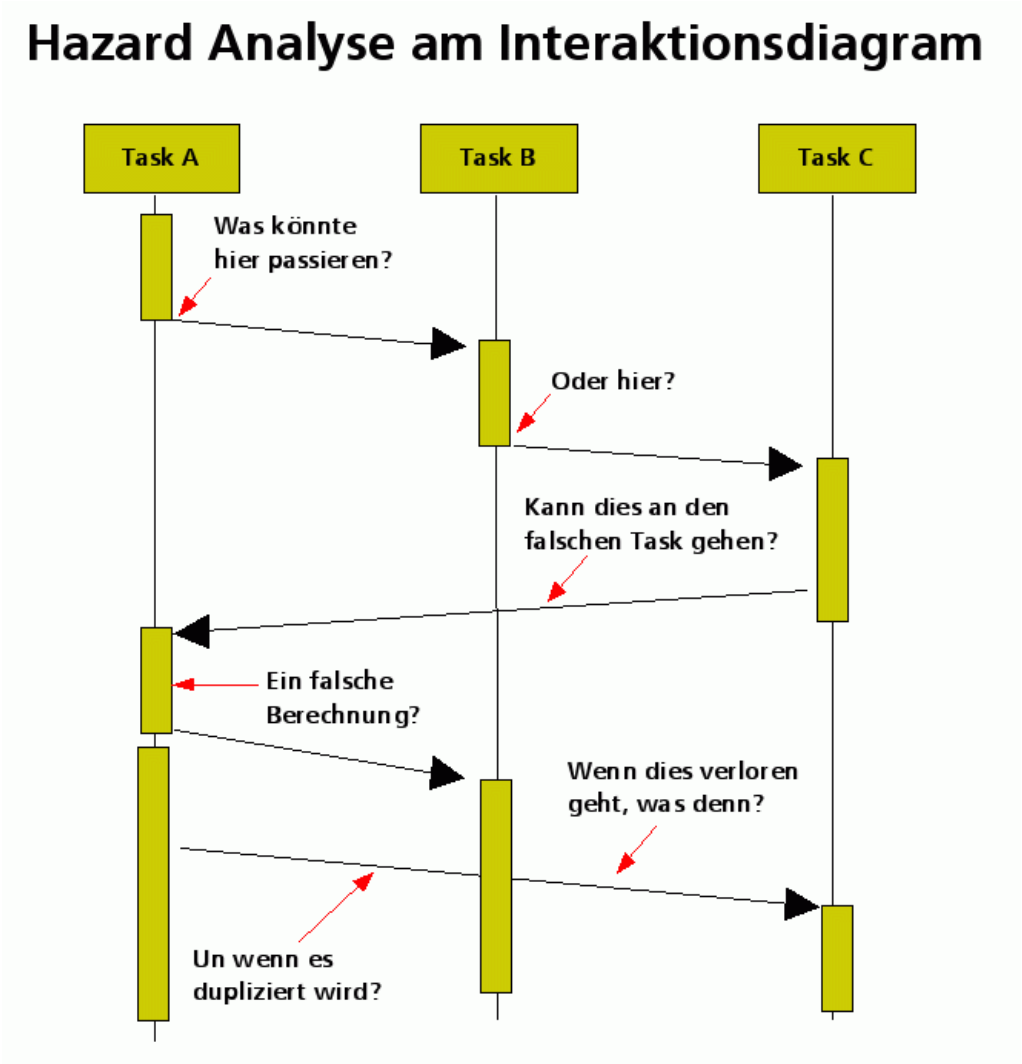
Software Hazard Analyse



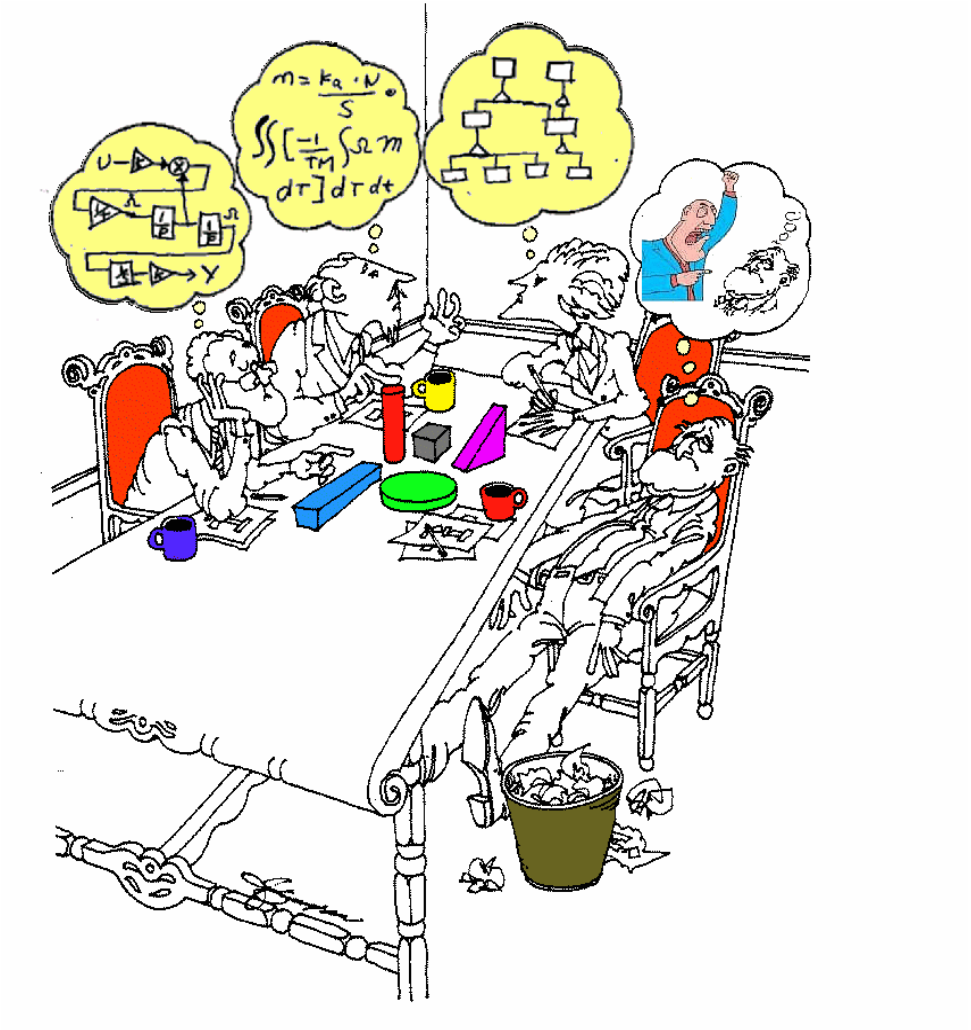
Interaktionsdiagram
Meine Empfehlung

Software Hazard Analyse

Hazard Analyse am Interaktionsdiagram

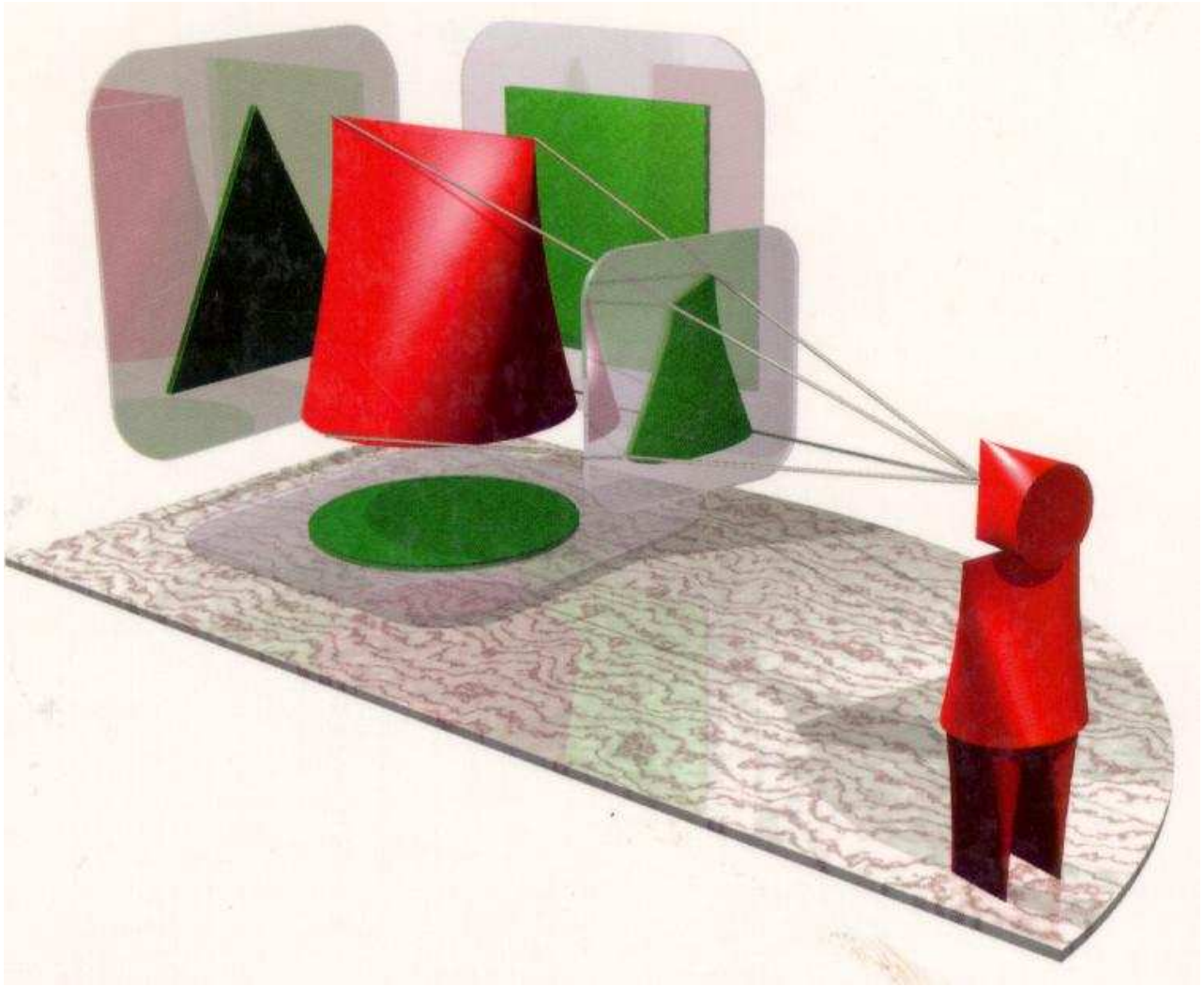


Hazard- und Risiko-Analyse... Nur mit interdisziplinären Teams



Fraunhofer FIRST Institut
Rechnerarchitektur
und Softwaretechnik

Hazard- und Risiko-Analyse... Nur mit interdisziplinären Teams

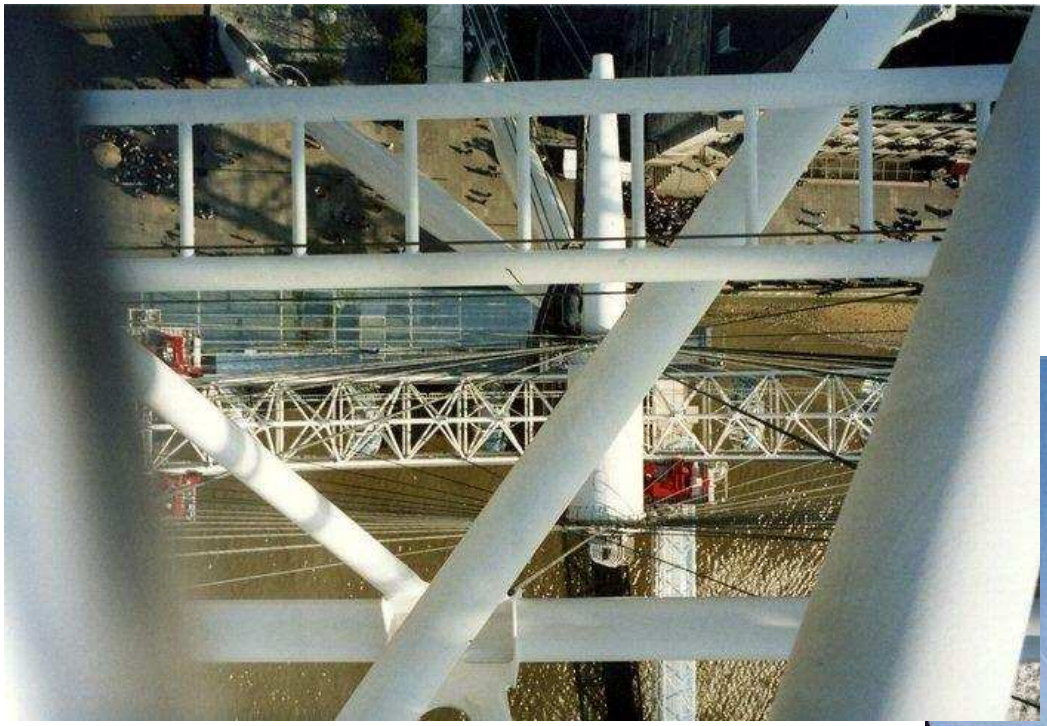


Fraunhofer FIRST Institut
Rechnerarchitektur
und Softwaretechnik

Hazard- und Risiko-Analyse... Nur mit interdisziplinären Teams

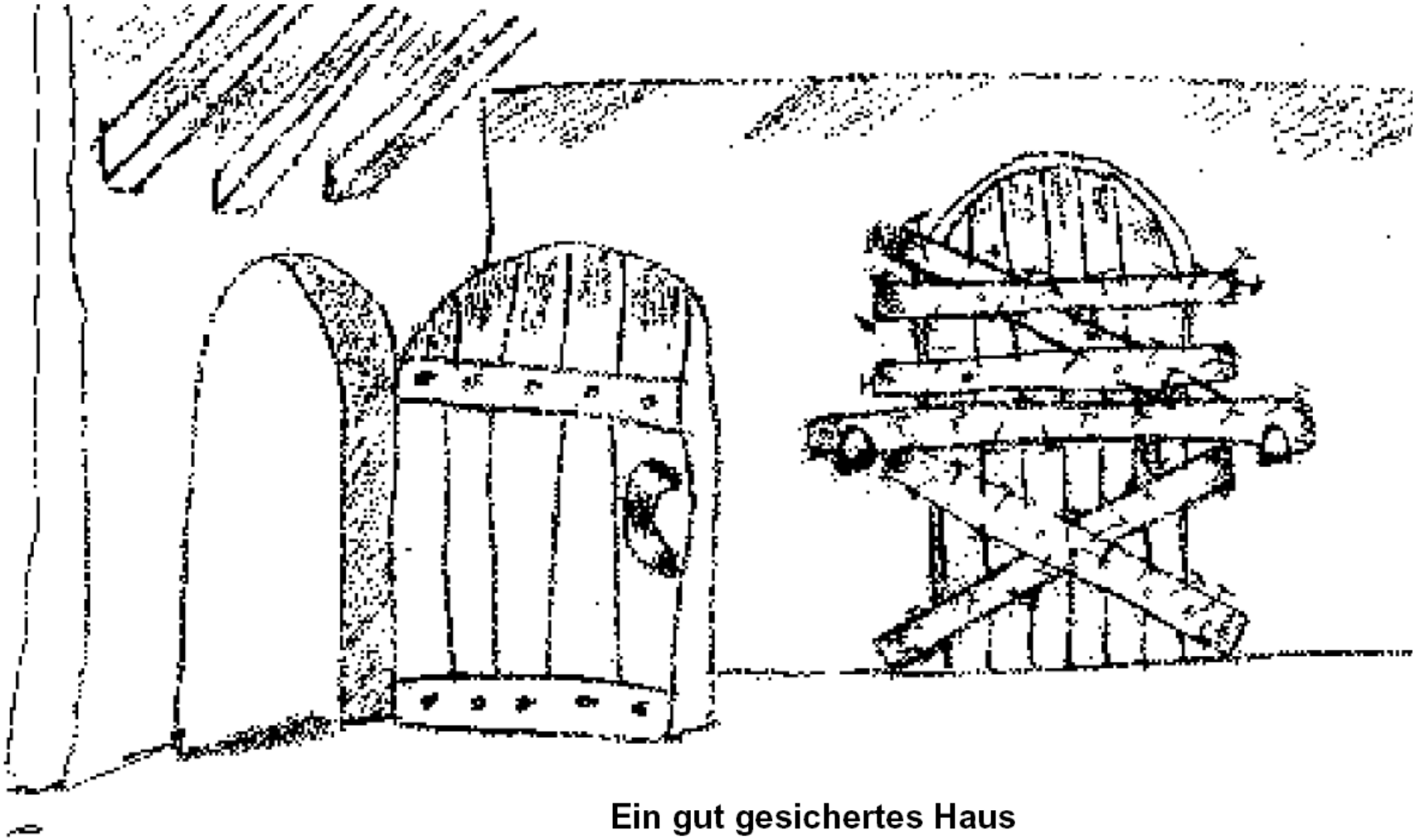
Fraunhofer FIRST Institut
Rechnerarchitektur
und Softwaretechnik

Hazard- und Risiko-Analyse... Nur mit interdisziplinären Teams



FIRST
Fraunhofer Institut
Rechnerarchitektur
und Softwaretechnik

Hazard- und Risiko-Analyse.. An alles denken!



Ein gut gesichertes Haus

FIRST
Fraunhofer Institut
Rechnerarchitektur
und Softwaretechnik

Sicherheit ... Gefahr & Risiko

Risiko = f(Gefahr, Wahrscheinlichkeit)

Risiko = Folgen * Wahrscheinlichkeit

z.B.

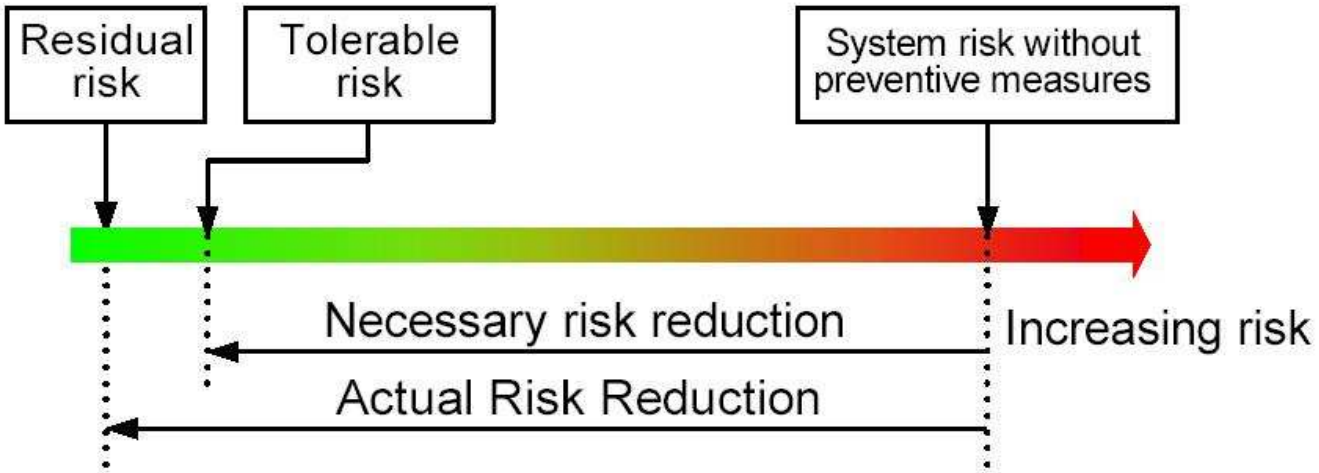
Folgen = 100 Tote,
Wahrscheinlichkeit = 10^{-9}/Stunde

Risiko = 100 Tote alle 10^{9} Stunden

Risiko Matrix

FOLGEN		Wahrscheinlichkeit (p in Lebenszeit)				
		E Unwahr-scheinlich < 10^-6	D Möglich 10^-6 .. 10^-3	C Gelegentlich 10^-3 .. 10^-2	B Wahr-scheinlich 10^-2 .. 10^-1	A Häufig > 10^-1
I	Katastrophal Todesfall	Sinken im offenen Meer	Feuer im Motorbereich	Schwimmer zu nah am Propeller		
II	Kritisch großer Schaden	*Sinken in Küsten-nähe*				
III	Marginal kleiner Schaden			Motor-schaden		
IV	Vernachlässigbar nicht der Rede Wert					Schlüssel Verlust Tank leer

Wie viel Risiko kann ich ertragen?



$$R = F \times C$$

R: Risk
F: Risk frequency
C: Consequence of the hazardous event

Was ist sicher? Zu Hause zu bleiben und nichts tun!
Aber: man muss etwas wagen um zu leben!