

Automotive – Safety & Security 2006

12. bis 13. Oktober 2006, Stuttgart

Zuverlässigkeitsmanagement

- Ein zentraler Prozess zur Umsetzung von Innovationen
in zuverlässige und sichere Fahrzeuge der Großserie -

Dr. P. Kafka, Dr. R. Spallek



philotech

Inhalt

- Einführung
- Zum Stand der Technik
 - Automotive
 - Andere
- Zur Weiterentwicklung des Prozesses
 - programmatisch
 - analytisch
 - methodisch
- Beispiele
- Schlussfolgerungen

Einführung

- Treiber
 - Wunsch nach individueller Mobilität (Kunde)
 - Unternehmerische Verwirklichung (Automotive)
- Herausforderung
 - Marktbehauptung
 - Großsegment und / oder Marktnische
 - Schnelle Modellwechsel → kurze Entwicklungszeit
 - Weiterentwicklung der Mechatronik
 - Vermeidung und Beherrschung von Fehlfunktionen
 - Minimierung Rückruf, Garantie, Schadensersatz
 - Umsetzung Zuverlässigkeitsmanagement (ZVM) in gelebte Prozesse

Zum Stand der Technik

ZVM - Automotive

- Bewährte Konstruktionsmerkmale
- Vielfältige Tests, Einzelversuche, Flottenversuche
- Aufgaben- und Verantwortlichkeitstrennung zwischen OEM und Tiers **verbesserungsbedürftig**
- Fahrzeugweites Denken und Analysieren begrenzt
- ZVM nur **bruchstückhaft** entwickelt und eingeführt
- ZV-Zielvorgaben für OEM und Tiers erst im Entstehen
- Viele Methoden „**nebeneinander**“ (z. B. Koppelmatrix, FMEA, Bus-Analyse, Kabelbaum-Simulation, FTA)
- ZV-Daten, z. B. Ausfallraten **kaum** verfügbar

Zum Stand der Technik

ZVM – Automotive

Heutige Fahrzeuge haben mehrere Bussysteme (CAN, MOST, Flexray) mit ca. 70 Steuergeräten

Daraus entsteht unweigerlich ein sehr komplexes Funktions- und Ausfallnetz

Die Konsequenz ist: Weiterentwicklung der Analysetechnik erforderlich

Anhang: Beispiel einer Flexray Analyse [Rabenberger2005]

Quelle: Promotion T. Kutritz, Uni Berlin, 2004

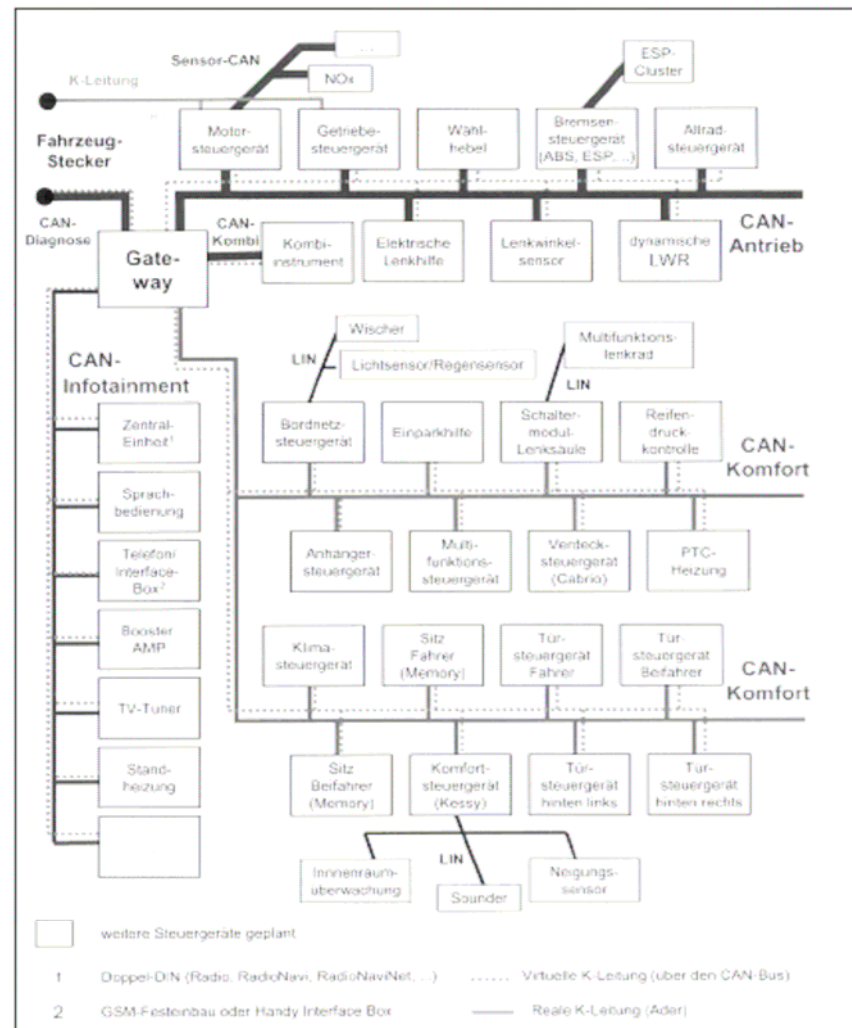
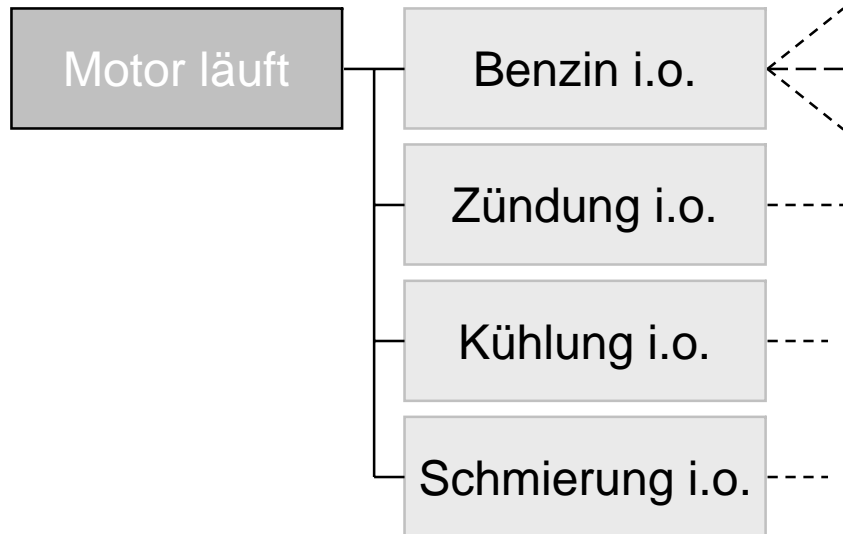


Abbildung 3.5: Vernetzte Elektronik im Volkswagen Golf des Baujahres 2004 (Quelle Volkswagen)

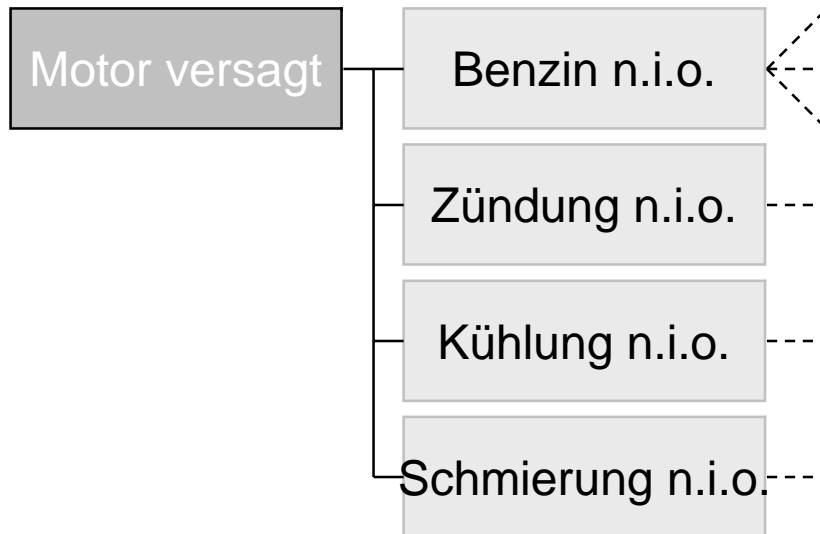
Zum Stand der Technik

ZVM – Automotive – FMEA Prinzip

Funktionsnetz



Fehlernetz

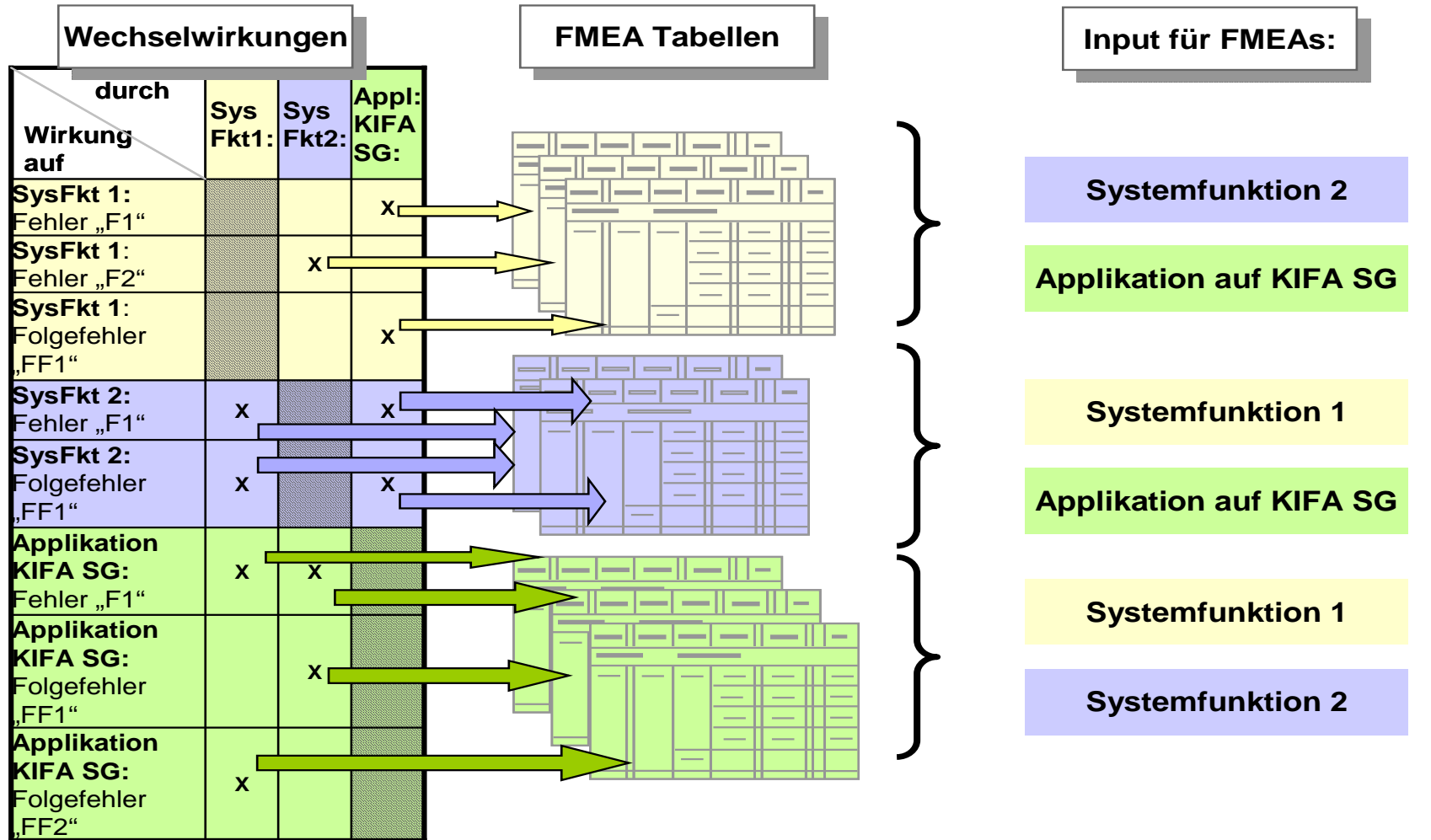


Typische FMEA Tabelle; Problem: Fehlerfolge wird Fehlerursache auf nächst höherer Ebene

Fehler i bis n	Fehler-Ursache	Fehler-Folge	Häufigkeit 1 bis 10	Schwere 1 bis 10	Entdeckbarkeit, 1 bis 10	Risiko Prioritätszahl	Abhilfe Maßnahme
Steck- verbindung defekt	Kontakte korrodiert	Steuergerät X ausgefallen	7	2	3	42	Reserve Anzeige

Zum Stand der Technik

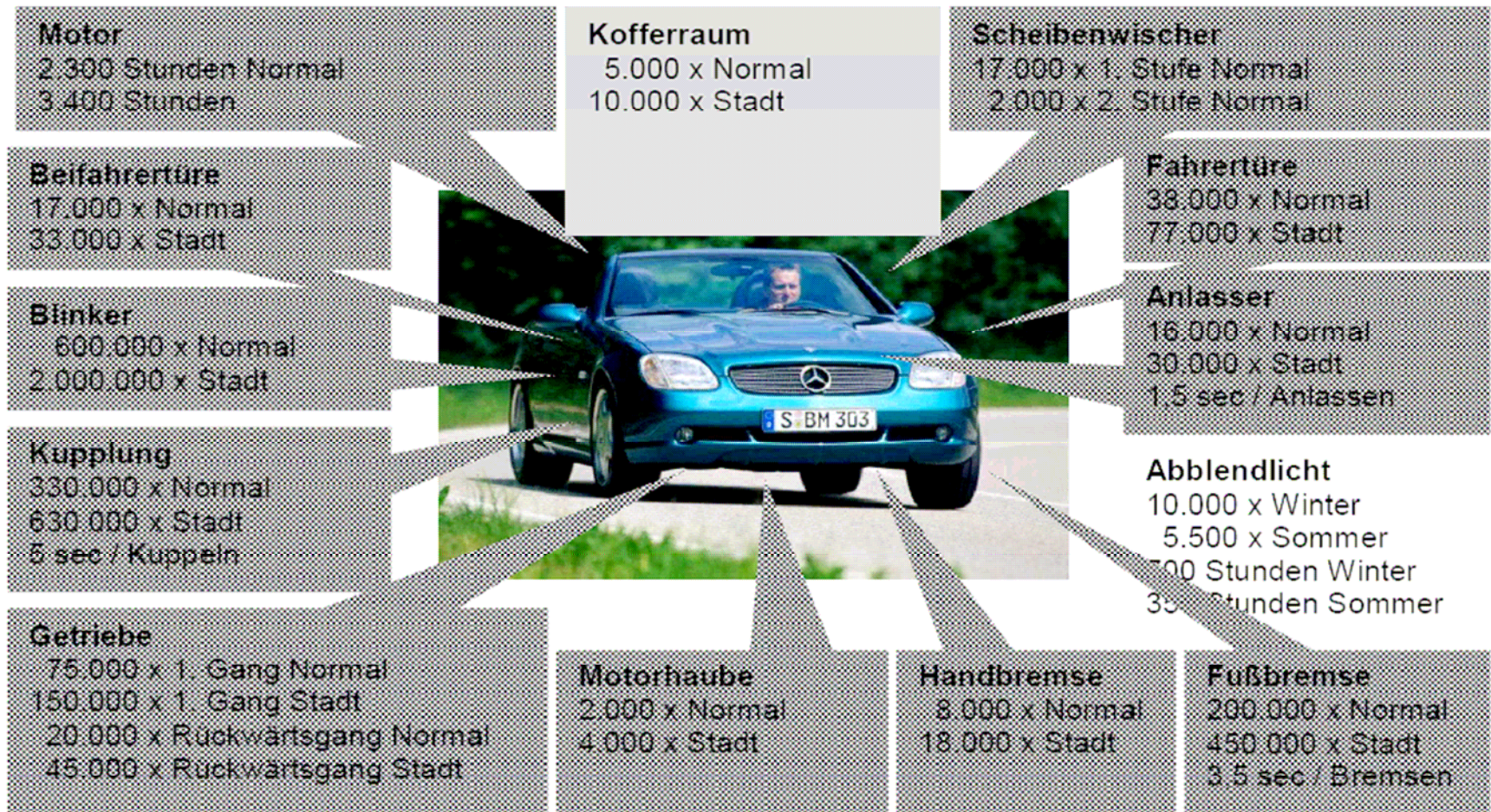
ZVM – Automotive – FMEA Koppelung



Zum Stand der Technik

ZVM - Automotive - Typische Lebensdauer-Vorgaben

(Quelle J. P. Bläsing, FH Ulm)



philotech

... ein Name ist
Programm

Zum Stand der Technik

ZVM - Andere

- Luftfahrt, Kerntechnik und Raumfahrt zeigen ein **breites und tiefes ZVM**.
- Sehrwohl ist der **ideale** Prozess:
 - Ziel
 - Umsetzung
 - Nachweis
 - Monitoringauch dort noch nicht voll erreicht
(siehe auch neue VDI Richtlinie 4003)
- Treiber dort war der **hohe** Anspruch an „Sicherheit“
- Die „neue“ Technik (Kerntechnik) profitierte vom **Fehlen** „gewachsener Systeme“

Zum Stand der Technik

ZVM - Andere

- Methodisch ist dort die **ganzheitliche** (Mensch, Maschine, Umwelt) und **produktweite** (über Systemgrenzen hinweg) Analysetechnik relativ weit entwickelt (wobei auch dort oftmals gewachsene Firmenstrukturen dem im Wege stehen)
- Daten-Probleme haben dem Grundsatz nach **alle**; doch es gibt **erfreuliche** Beispiele, wo über Firmen- bzw. Betreiber-grenzen hinweg z. B. Ausfallraten von im Einsatz befindlichen Komponenten **veröffentlicht** werden (z. B. T-Book, Schweden; ZEDB, VGB PowerTech e.V., D; OREDA, Norwegen)

Zum Stand der Technik

ZVM – Andere - Resümee

Eine „große Weiche“ in der Vorgehensweise zum ZVM in den verschiedenen Industrien ist:

- verfahren wir **weiterhin** „qualitativ“ (erfahrungsorientiert)
- oder
- verfahren wir **auch** „quantitativ“ (wahrscheinlichkeitsorientiert)

Häufigste Argumente **gegen** die quantitative Erweiterung:

- Ergebnisse sind nicht **beweisbar** (kann man „gesund rechnen“)
- **keine** Daten

was genaueren Betrachtungen **nicht** standhält

Zur Weiterentwicklung des Prozesses

Programmatisch:

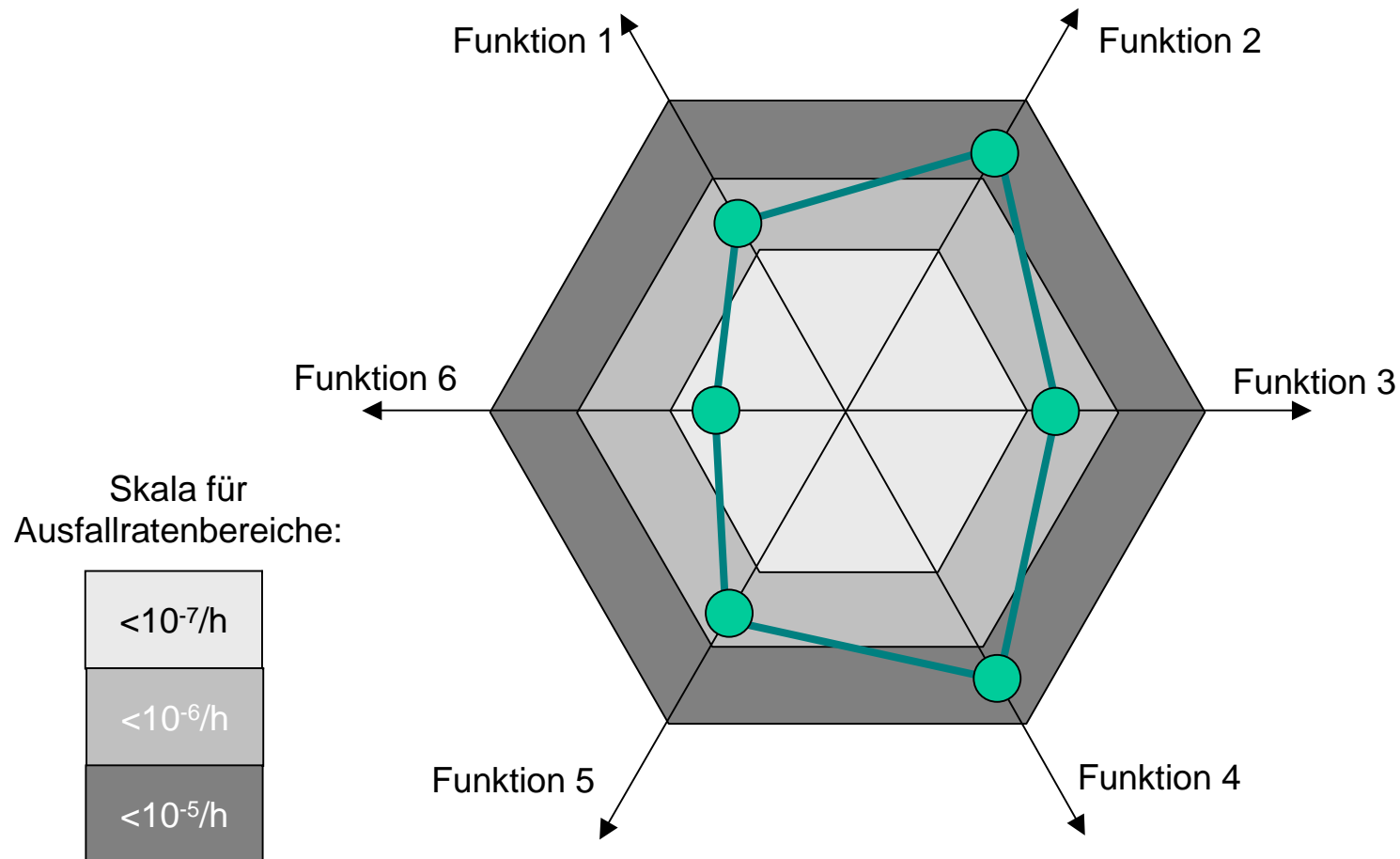
Umsetzung eines klassischen Managementprozess
mit den drei Elementen:

- Festlegung und Einsetzen der **ZV-Strategie**
Aufgabe der Firmenleitung
- Ausarbeitung und Durchführung des **ZV-Programms**
Aufgabe der Fachgremien (generisch ausgerichtet)
- Ausarbeitung und Durchführung des **ZV-Plans**
Aufgabe der Projektleitung (projektspezifisch ausgerichtet)

Charakteristikum der Inhalte: „vom Groben ins Feine“
und über den Lebenszyklus

Beispiel: Automotive

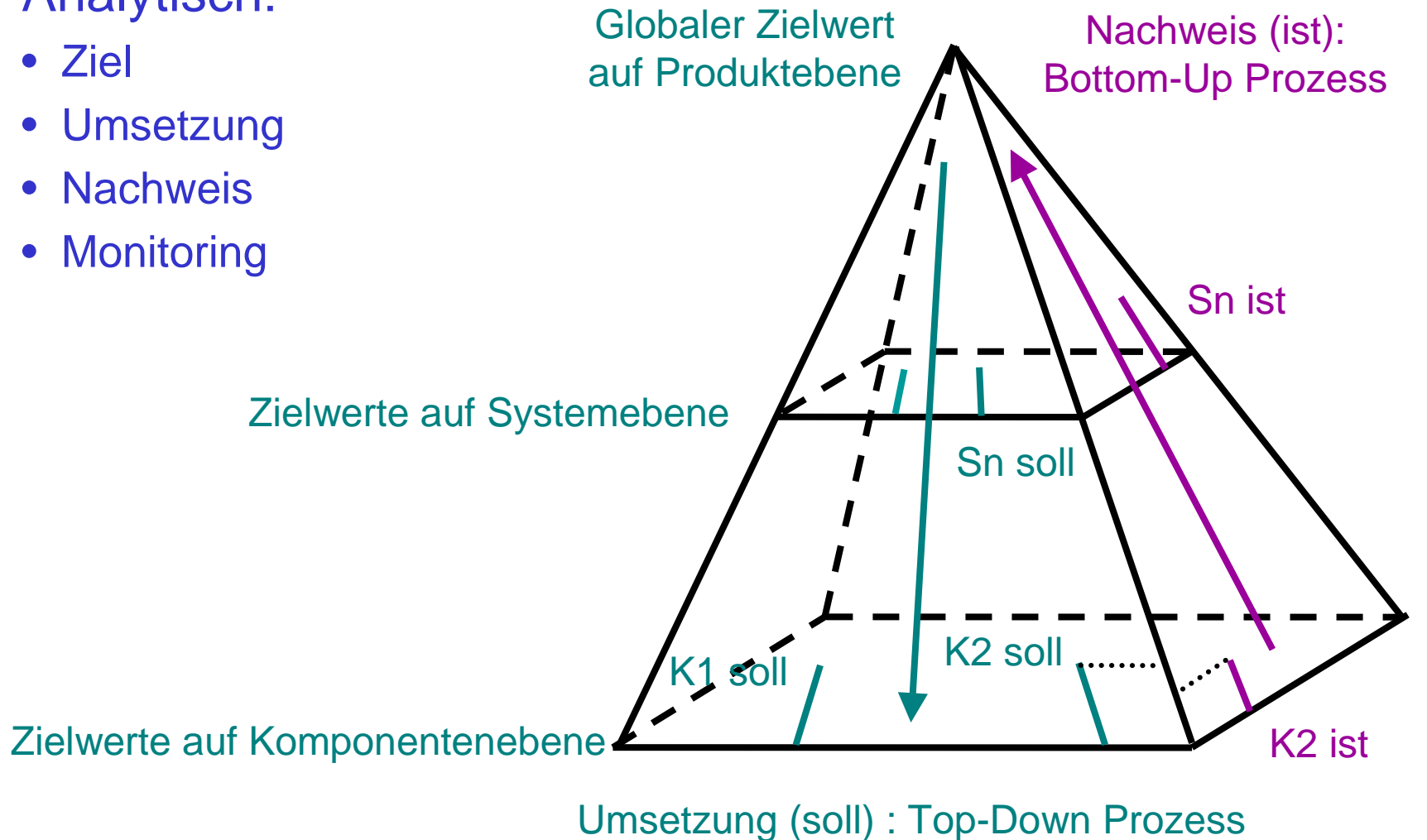
Programmatisch: Zielwerte für Ausfallraten
verschieden bedeutsamer Fahrzeugfunktionen (schematisch)



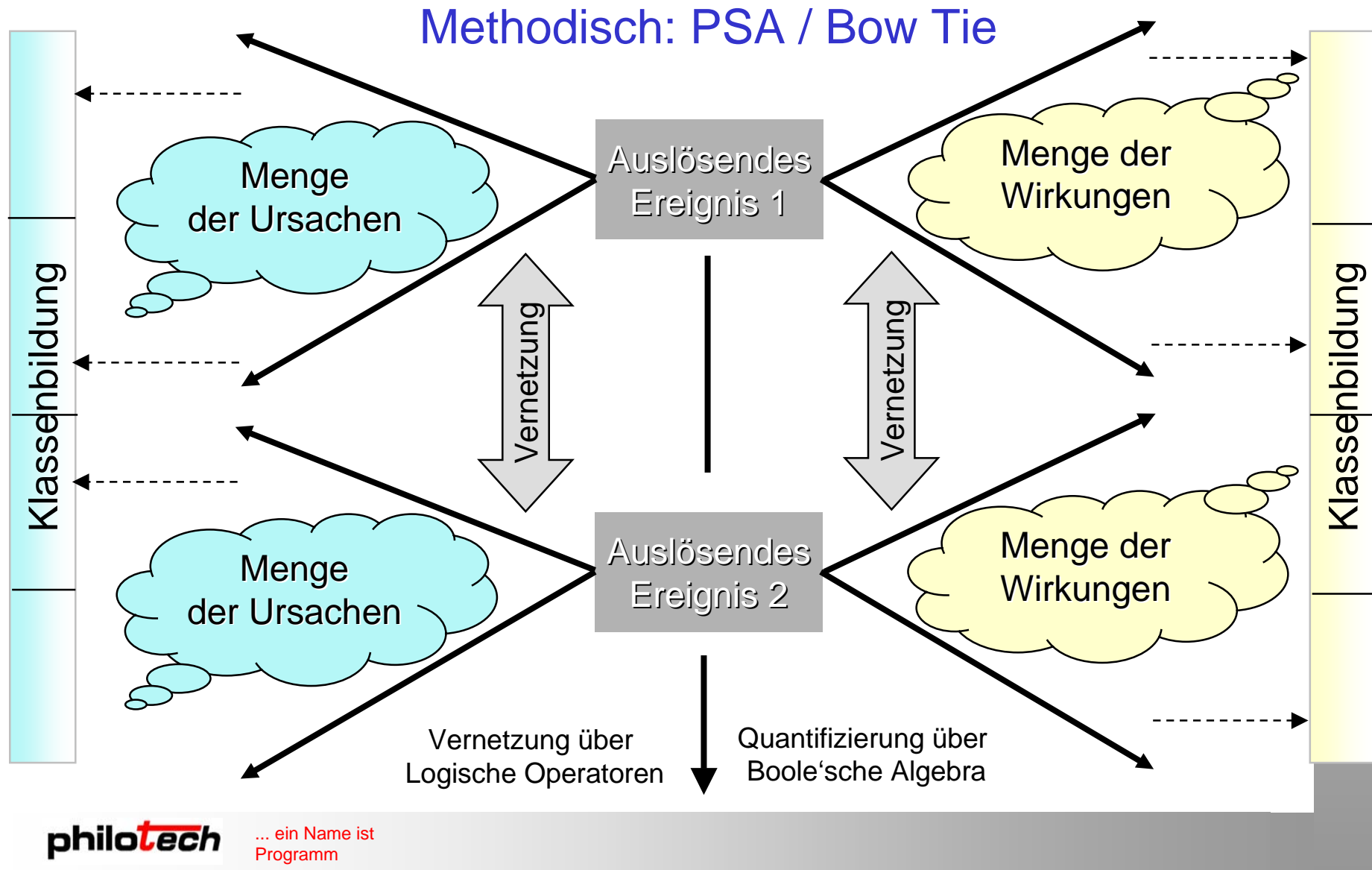
Zur Weiterentwicklung des Prozesses

Analytisch:

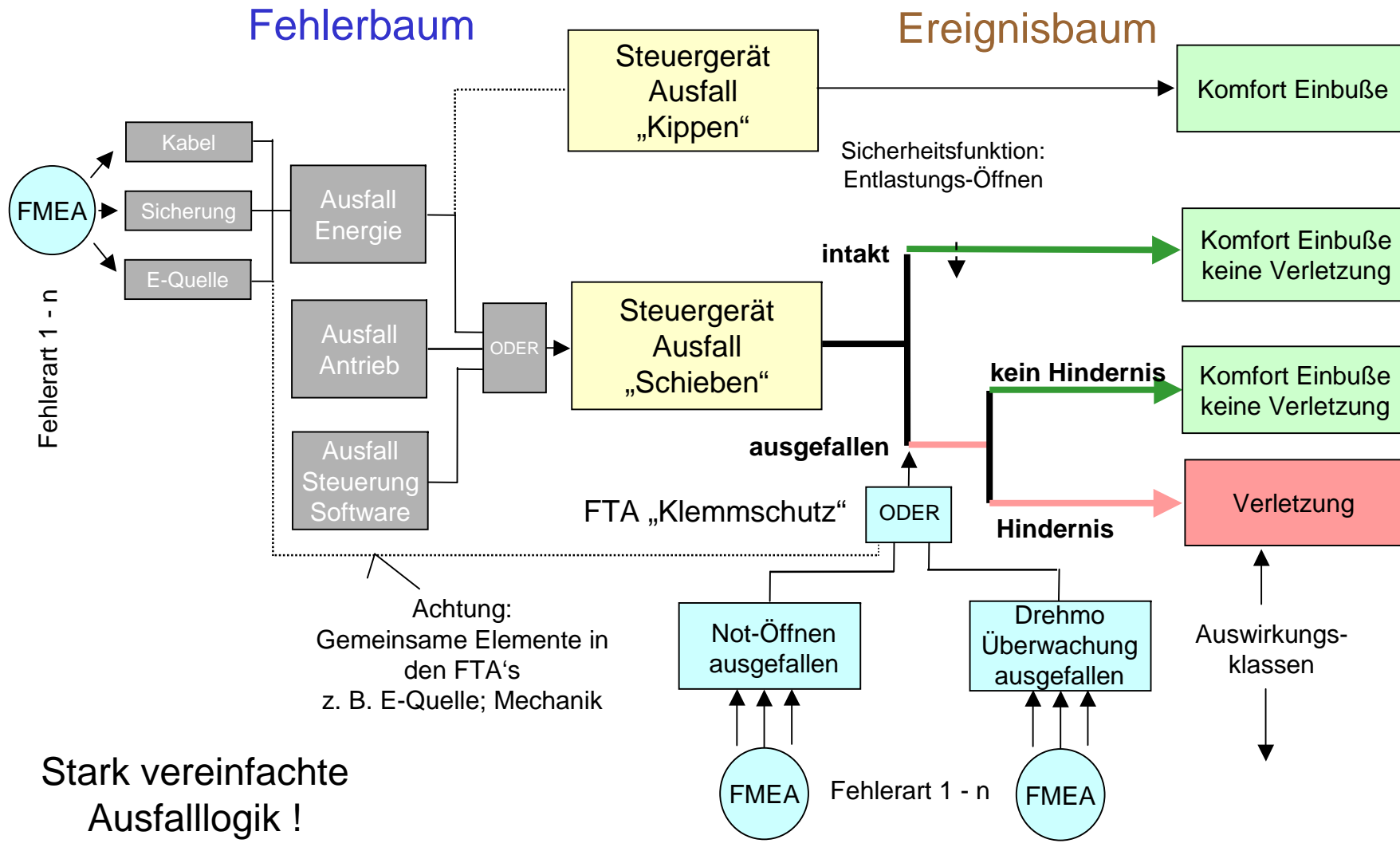
- Ziel
- Umsetzung
- Nachweis
- Monitoring



Zur Weiterentwicklung des Prozesses



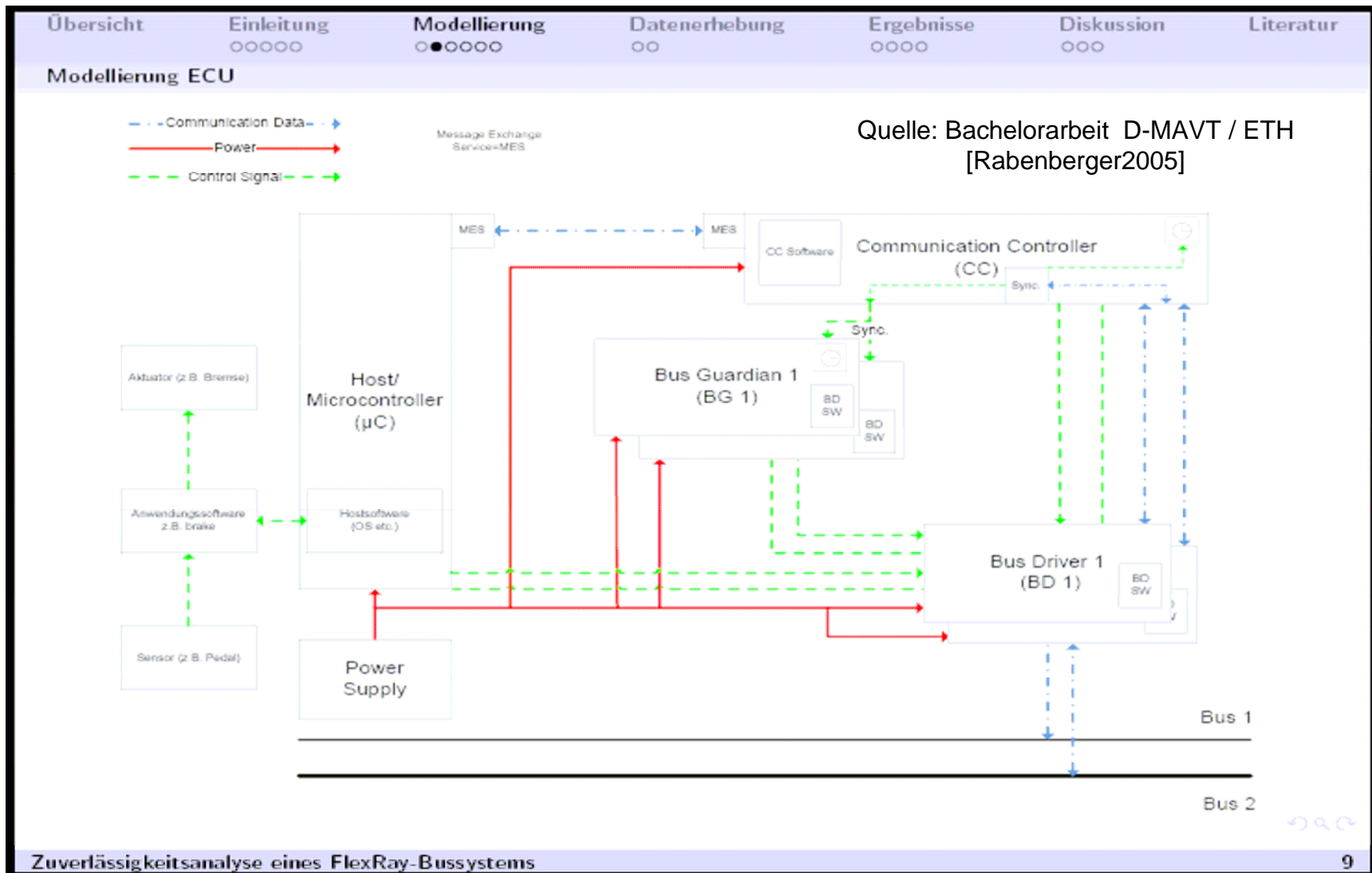
Zur Weiterentwicklung ein Beispiel



Schlussfolgerungen

- Seit jeher besteht das **Bestreben** der Automobilindustrie die Zuverlässigkeit von Nachfolgemodellen zu verbessern
- Diesbezügliche **Erfolge** gibt es
- Trotzdem **schlechte** Nachrichten:
 - Rückruf, Regress, Kosten- und Zeitdruck
- Durchgängiges Zuverlässigkeitsmanagement erst **bruchstückartig** zu erkennen
- **Unkorrelierte** Einzelanalysen und Informationsinseln
- **Fahrzeugweites** Denken und Handeln unterentwickelt
- **Elektronik und Software** die große Herausforderung
- Oftmals **eingengter** Branchenblick

Anhang



Anhang

Übersicht Einleitung ○○○○○ Modellierung ○○○●○○ Datenerhebung ○○ Ergebnisse ○○○○ Diskussion ○○○ Literatur

Modellierung ECU

System M2: Hardware & Software

Quelle: Bachelorarbeit D-MAVT / ETH [Rabenberger2005]

The diagram illustrates the architecture of System M2. It starts with a Power Supply (A, Hardware) connected to a Host (B, SW/HW). The Host connects to a MES (C, Software). The MES connects to a C. Controller (D, SW/HW). The C. Controller connects to a Synchronisation (E, Software) block. From the Synchronisation block, the signal splits into two parallel paths. Each path consists of a Bus Guardian (F and H, SW/HW) connected to a Bus Driver (G and I, SW/HW). Both paths then converge into a final Application Software (J, Software) block. A legend indicates that red boxes represent Software and white boxes represent Hardware.

Annahmen

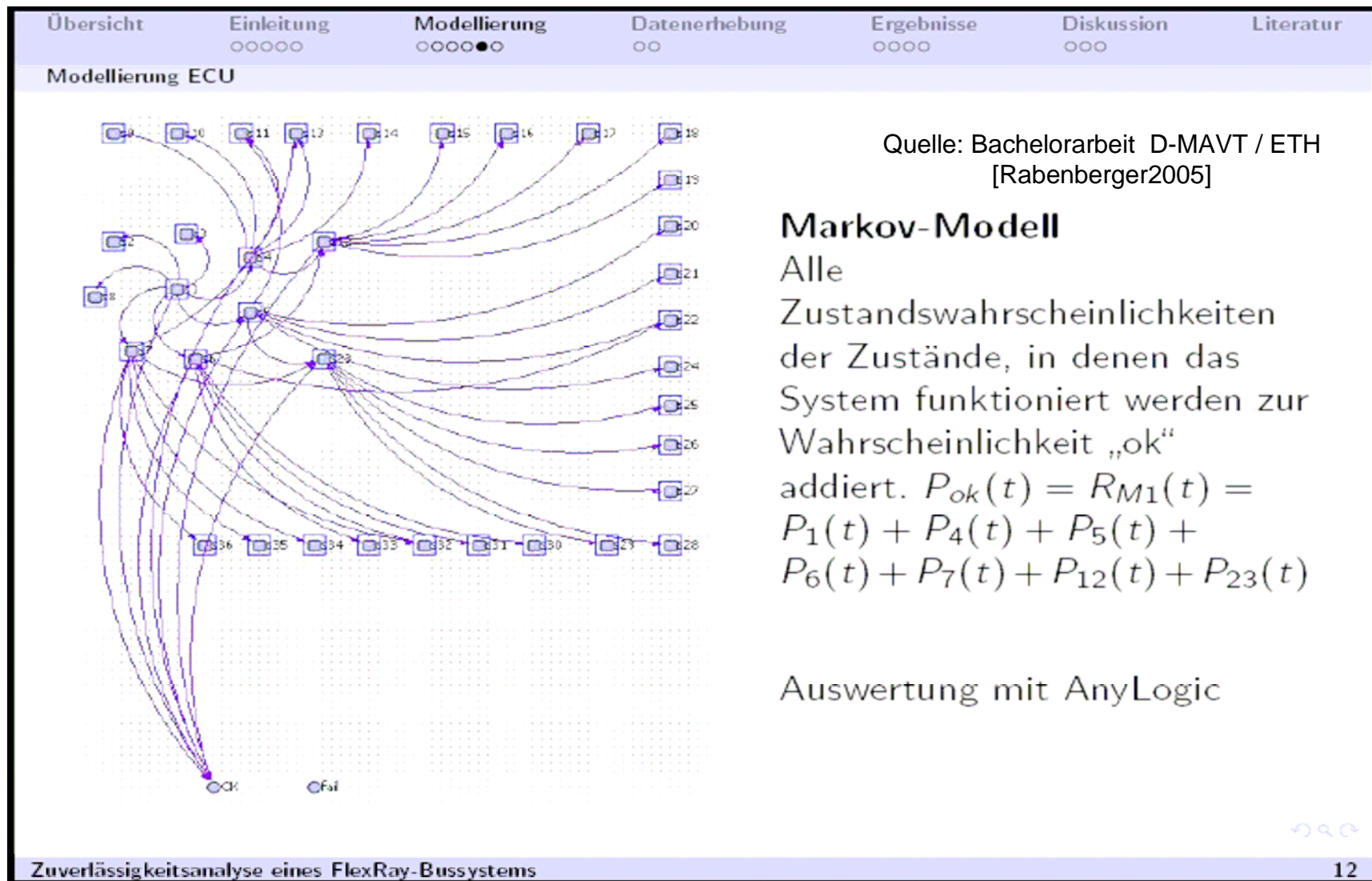
- Dauerbetrieb (kein Startup, Shutdown, keine Reparatur)
- Für die Komponenten gibt es nur die Zustände Fail (=0) / OK(=1)
- BG1/BD1 - BG2/BD2 werden zu 100% redundant genutzt.

Software (red box)
Hardware (white box)

Software auch probabilistisch behandelbar [Lit00]

Zuverlässigkeitsanalyse eines FlexRay-Bussystems 11

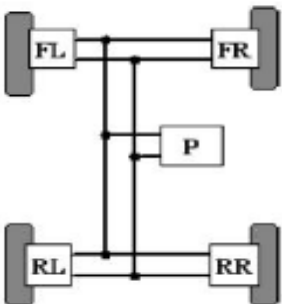
Anhang



Anhang

Übersicht Einleitung ○○○○○ Modellierung ○○○○○○ Datenerhebung ○○ Ergebnisse ○●○○ Diskussion ○○○ Literatur

Ergebnisse Gesamtsystem brake-by-wire



Quelle: Bachelorarbeit D-MAVT / ETH [Rabenberger2005]

Überlebenswahrscheinlichkeiten $t = 8000h$	
$R_{Sys,M1}$	0,9968
$R_{Sys,M2}$	0,9928
$R_{Sys,gefordert}$	$>0,9920$

Tabelle: Ergebnisse der Zuverlässigkeitsanalyse

Zuverlässigkeitsanalyse eines FlexRay-Bussystems 17

Danke für die Aufmerksamkeit



philotech

... ein Name ist
Programm