

# SW-Eng. SW-inten. Systeme im Fzg

## Herausforderungen der Zukunft



Günter Reichart, Alexandre Saad

**BMW Group**



# Herausforderungen der Zukunft

## Content

- Visionen und Herausforderungen
- Beherrschung von Produktlinien
- Beherrschung von Kompatibilität
- Beherrschung von Zuverlässigkeit
- Beherrschung von Autonomie
- Zusammenfassung



# Vision und Herausforderungen

## Rahmenbedingung

### Produktoffensive

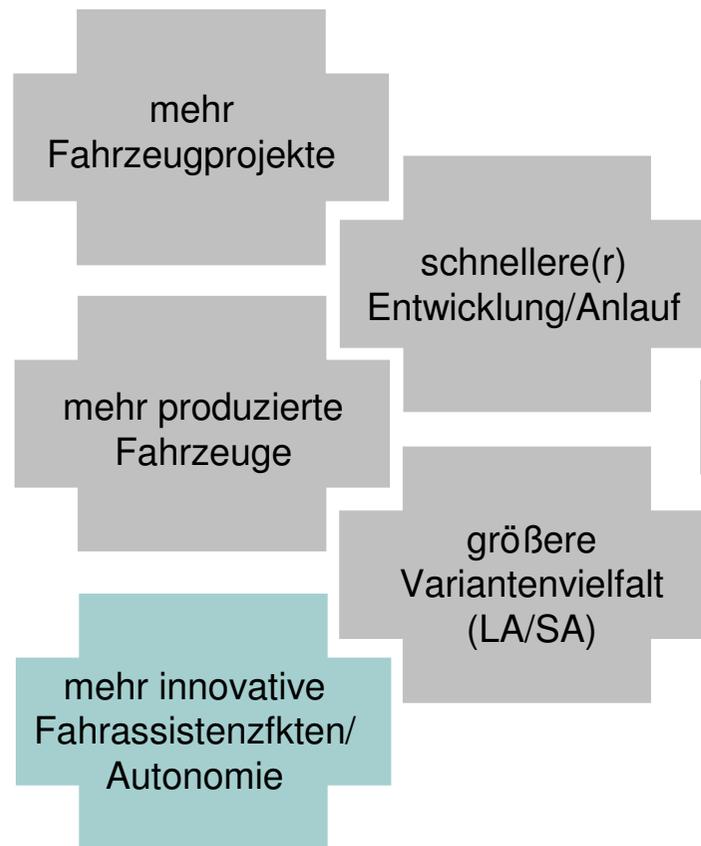
Rendite-orientiertes Wachstum der BMW Group bedeutet

- mehr Fahrzeugprojekte, mehr Produktionsanläufe
- mehr produzierte (verkaufte) Fahrzeuge
- größere Variantenvielfalt pro Fahrzeugprojekt
- innovative Fahrzeugfunktionen
- schnellerer Anlauf / steilere Kammlinien

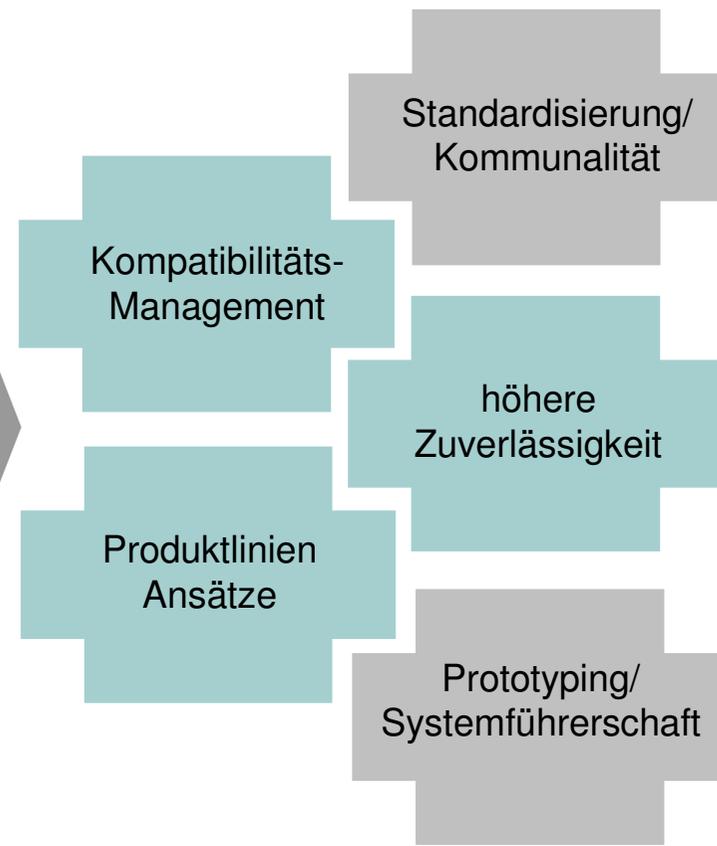
# Vision und Herausforderungen

## Beherrschung von Innovationen und Kosten

### Treiber des Umsatz-Wachstums



### Barrieren des Kosten-Wachstums



# Vision und Herausforderungen

## Software Vision

### **Automotive Software Vision**

Realisierung innovativer SW-basierter Funktionalität im Fzg

- zur Erhaltung und Erhöhung der Wettbewerbsfähigkeit
- mit definierter, messbarer (Software-) Qualität
- bei hoher Termintreue (und Produktivität)
- verbessertem Time to Market (Software-Zyklen!) und
- Beherrschung Deployment/Maintenance der Software

# Herausforderungen der Zukunft

## Content

- **Beherrschung von Produktlinien**

- **Problemstellung**
- **Definition und Abgrenzung**
- **Varianz von Software und Funktionalität**
- **Produktlinien Architekturen (PLA)**
- **Resumee und offene Fragen**



# Beherrschung von Produktlinien

## Produktlinien

### Produktlinienansätze

What is a software system family?

We consider a set of programs to constitute a family whenever it is worthwhile to study programs from the set by first studying the common properties of the set and then determining the special properties of the individual family members.

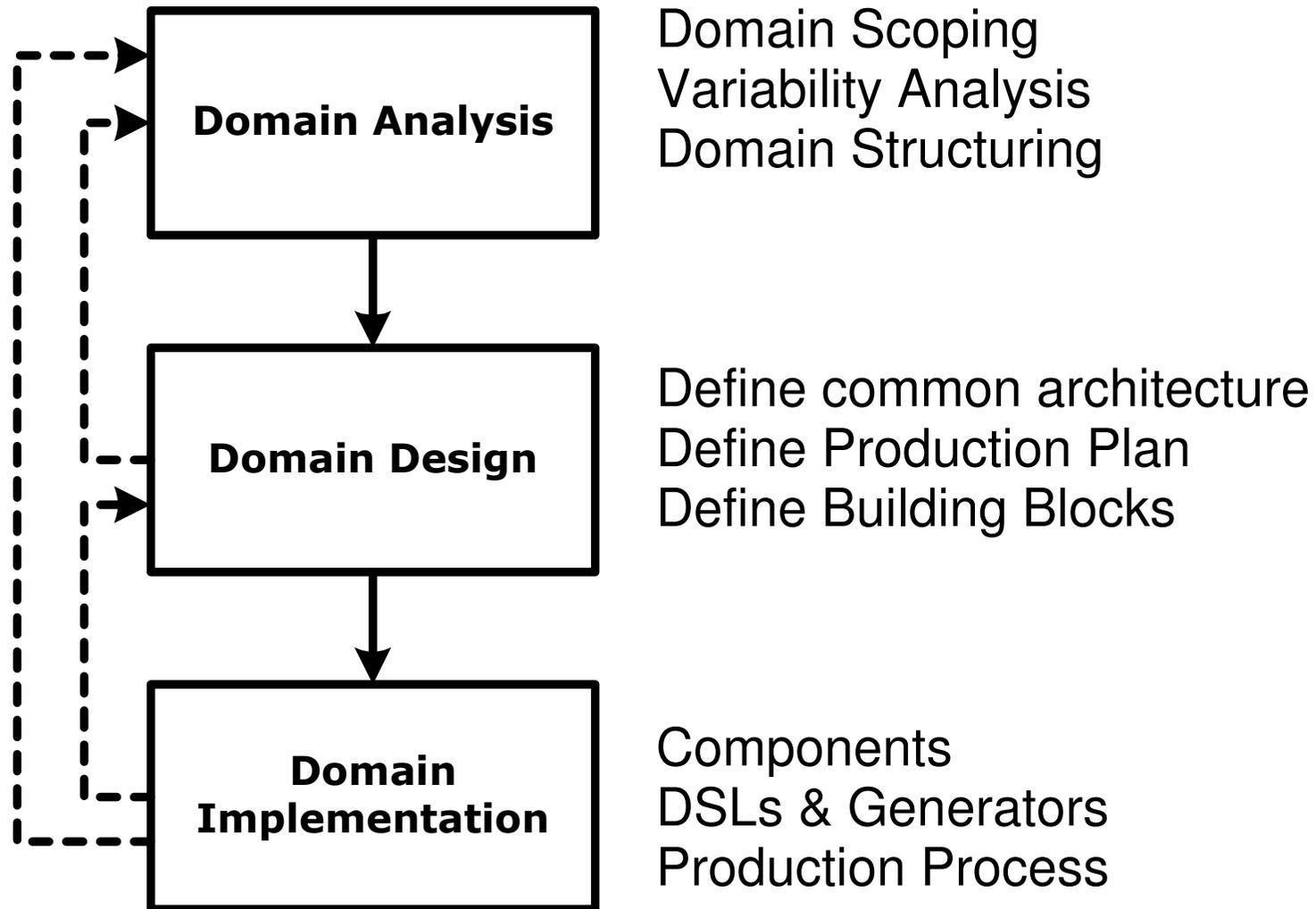
*Definition by Parnas*

### Domain-Engineering

- Identifikation **gemeinsamer** Merkmale
- Identifikation **spezifischer** Merkmale
- Bsp: Motoren bez. Zylinderanzahl, Einspritzsystem, Kühlungssystem, etc.

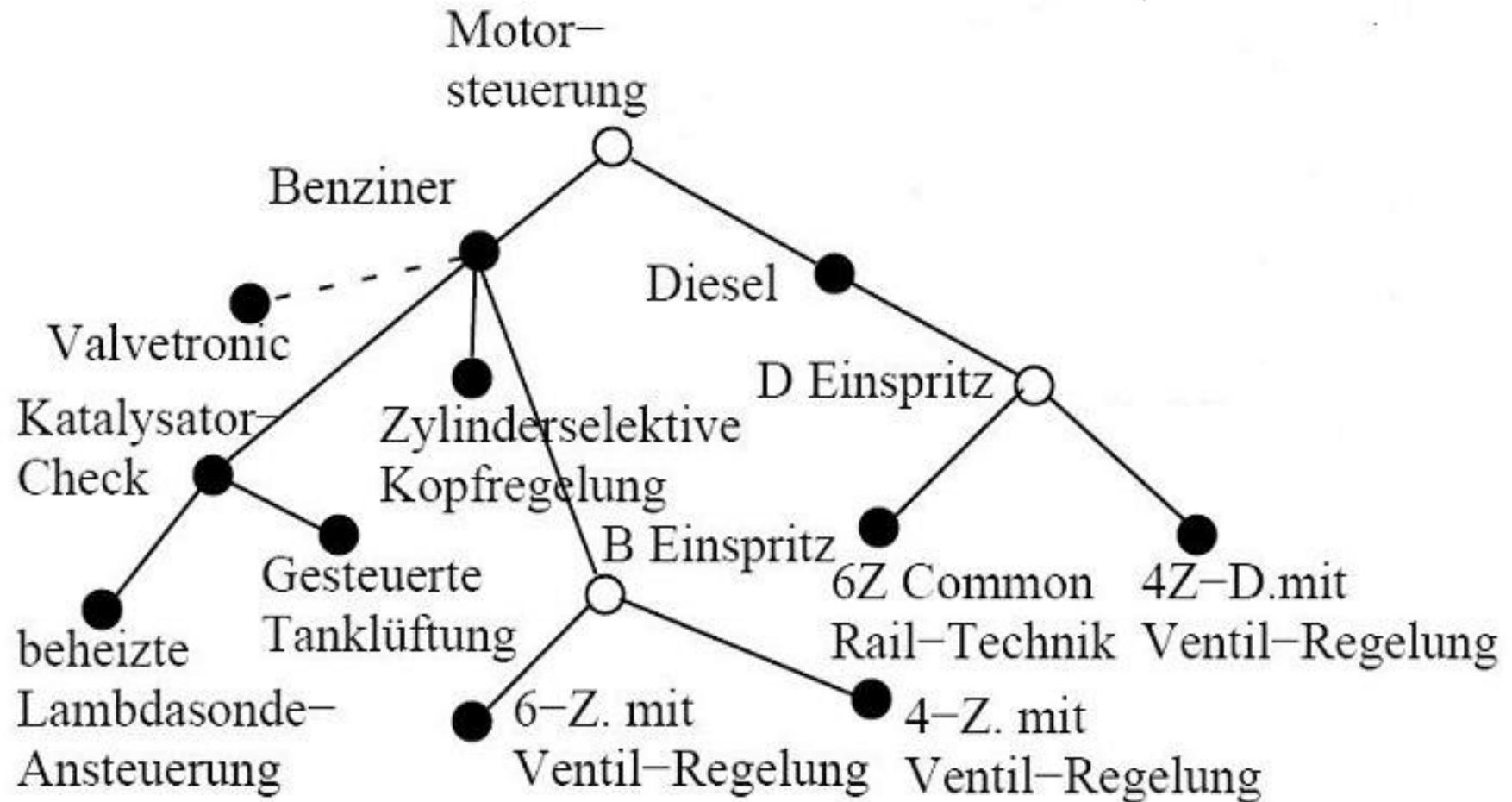
# Beherrschung von Produktlinien

## Produktlinien Engineering



# Beherrschung von Produktlinien

## Variabilität in der Motorsteuerung



# **Beherrschung von Produktlinien**

## **Resumee und offene Fragen**

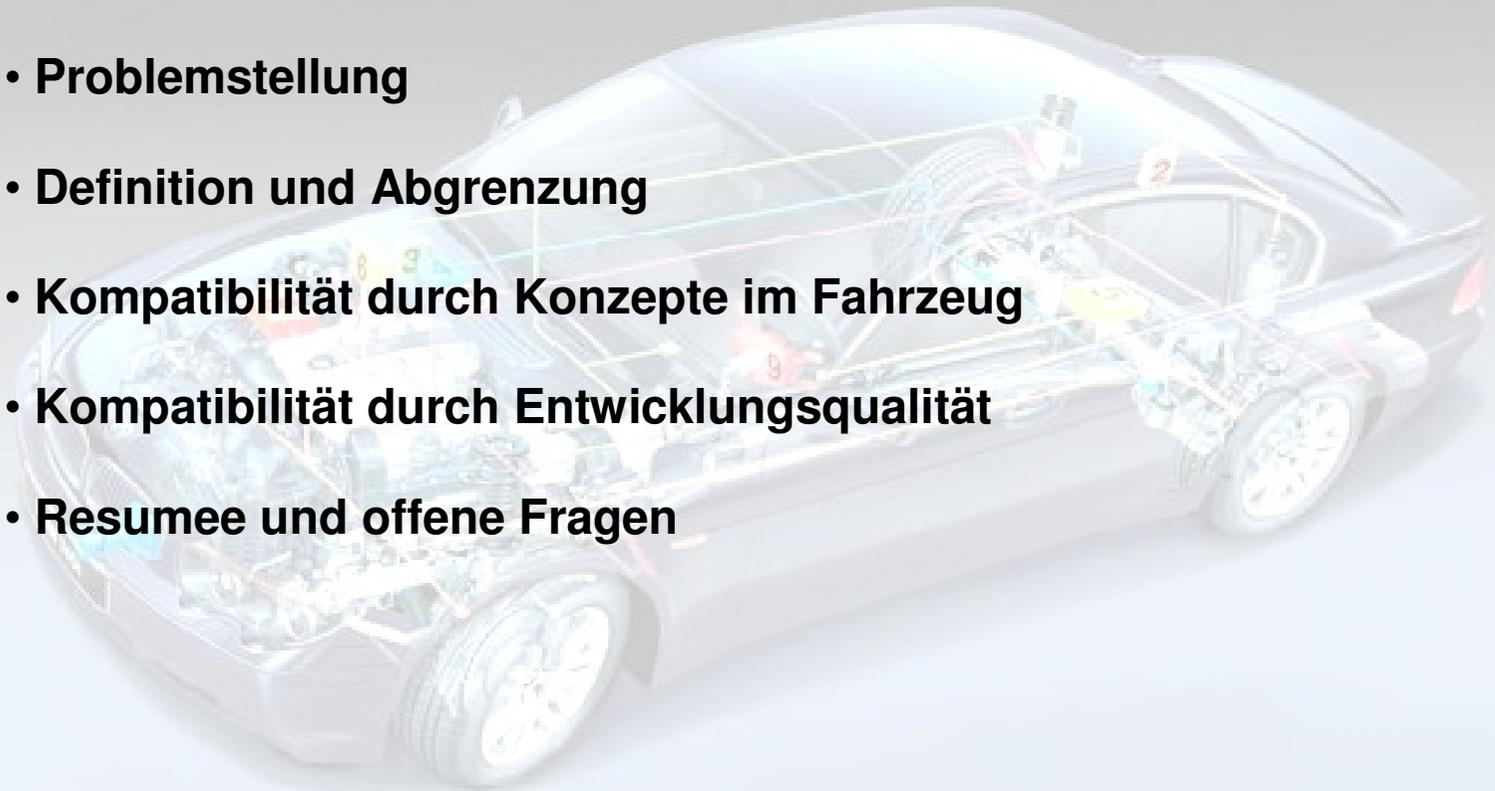
- **Resumee**
  - **Produktlinien stellen interessanten Ansatz zur Beherrschung von Variabilität dar.**
  - **Unterschiedlicher Anwendungsstand in einzelnen Fahrzeug-Domänen**
- **Offene Fragen**
  - **Durchgängige Methodiken und Werkzeuge für das Produktlinien Engineering**
  - **Geschäftsmodelle für die Zulieferindustrie ist ungeklärt. Einmalaufwände? Lizenzmodelle?**

# Herausforderungen der Zukunft

## Content

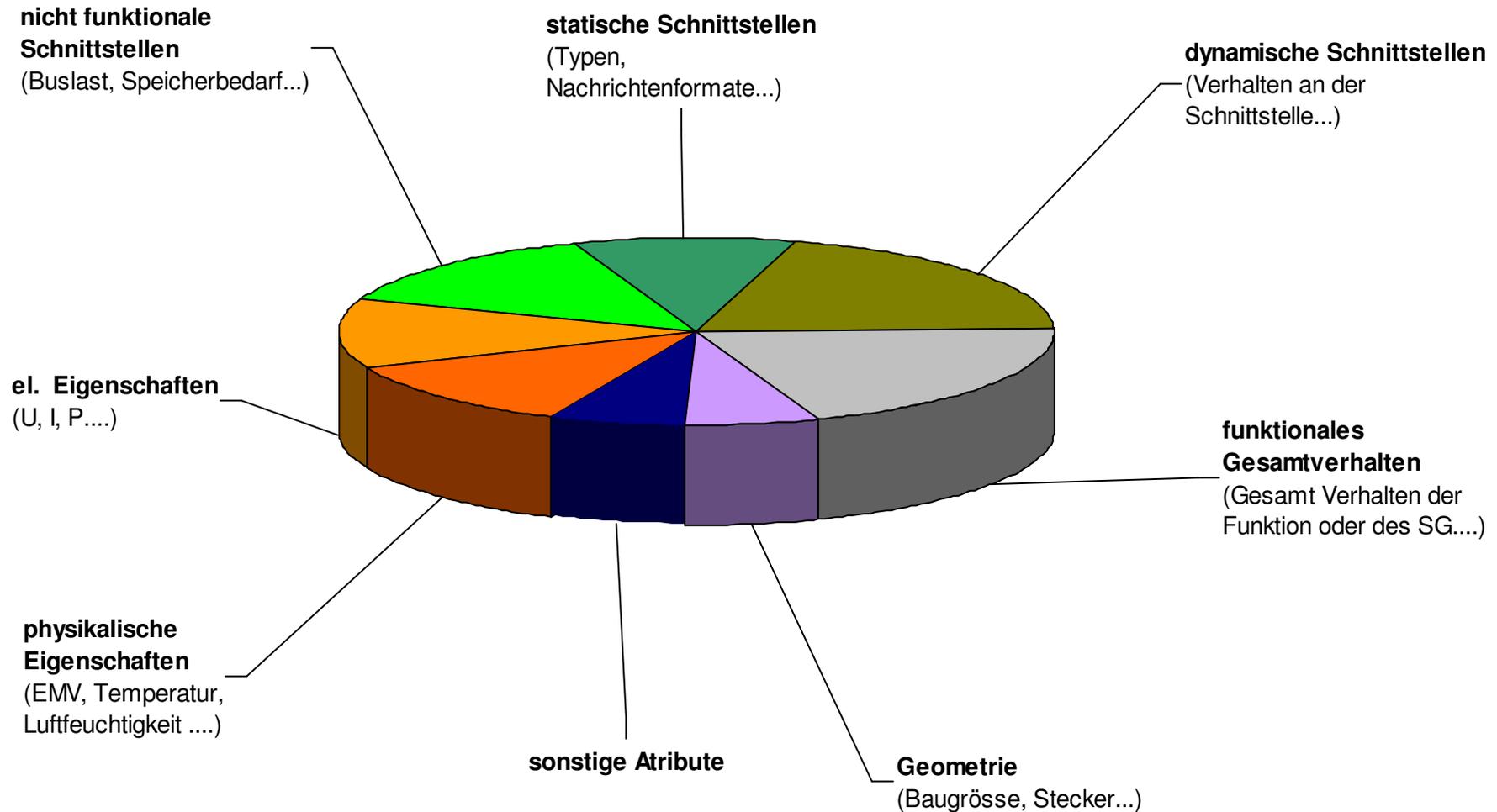
- **Beherrschung von Kompatibilität**

- **Problemstellung**
- **Definition und Abgrenzung**
- **Kompatibilität durch Konzepte im Fahrzeug**
- **Kompatibilität durch Entwicklungsqualität**
- **Resumee und offene Fragen**



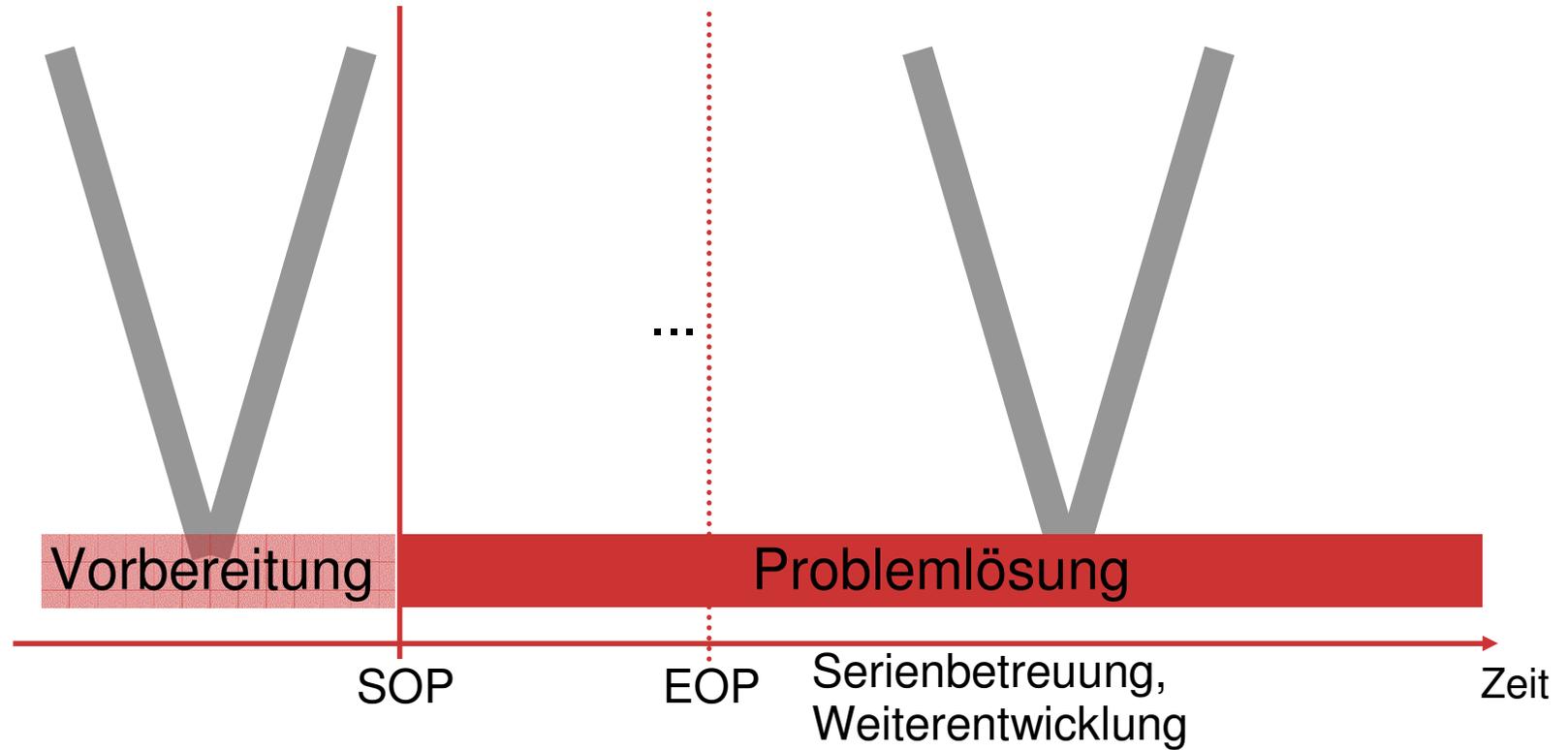
# Beherrschung von Kompatibilität

## Kompatibilitätseigenschaften



# Beherrschung von Kompatibilität

## Kompatibilität im Lebenszyklus

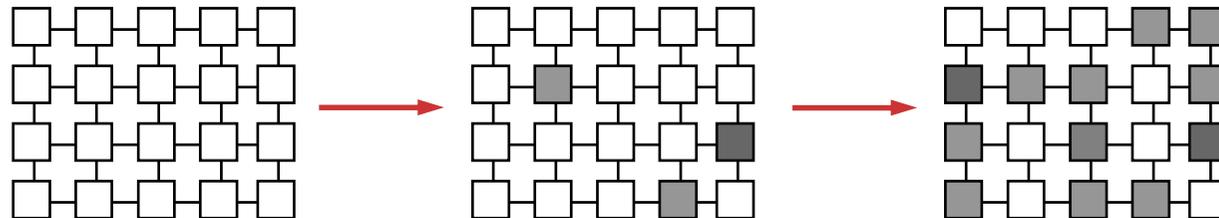


# Beherrschung von Kompatibilität

## Lebenszyklusproblematik

Beispiel: Nach 12 Jahren muss ein ausgefallenes Steuergerät in einem Altfahrzeug ersetzt werden. Die CPU wird seit 9 Jahren nicht mehr hergestellt.

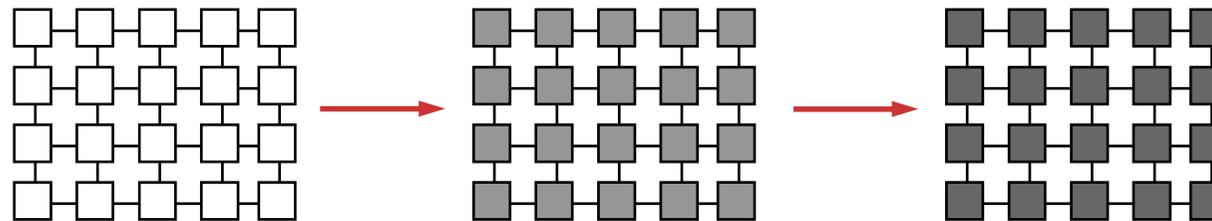
- Unterschiedliche Lebenszyklen von Fahrzeug, HW und SW machen Änderungen über den Lebenszyklus unvermeidbar.
  - Neue HW
  - Neue SW Versionen (Erweiterungen und Bug Fixes)
- (Pflege von HW und SW über den Fahrzeuglebenszyklus wirtschaftlich nicht wünschenswert)



# Beherrschung von Kompatibilität

## Heute: Integrations-Stufen (I-Stufen)

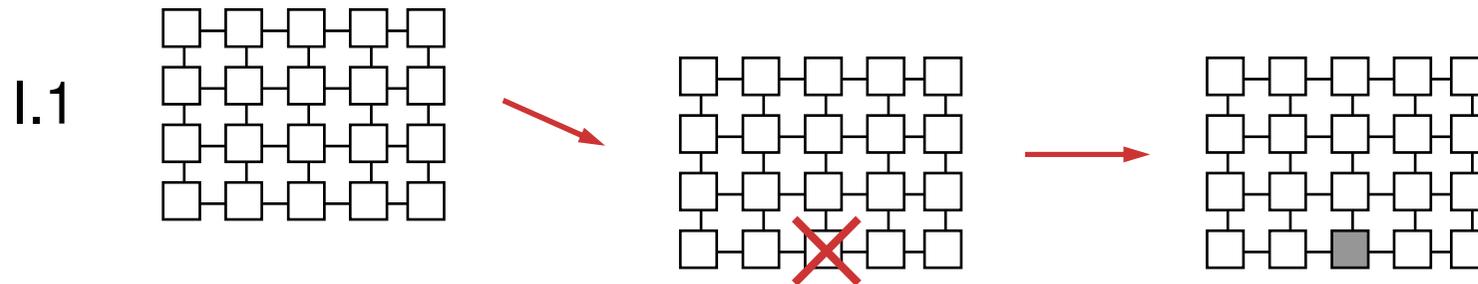
- Freigabe erfolgt basierend auf Einzelkonfigurationstest:  
I-Stufen (Vernetzungskompatibilität)
- I-Stufen sind vergleichbar mit Baselineing im SW-Konfigurationsmanagement



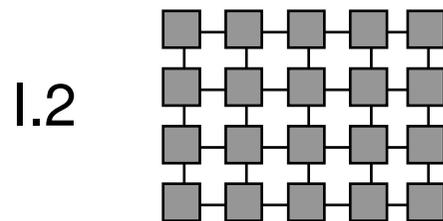
- Problem: Update eines Elements im **Service** erzwingt Update aller Elemente
  1. Kosten durch erzwungenen HW Austausch
  2. Kosten durch Fahrzeugprogrammierung
  3. (Testaufwand wenn viele Konfigurationen freigegeben werden sollen)
  4. „SW als Produkt“ nicht tiefgreifend möglich
- Praxis: Aufweichen der I-Stufen, parallele I-Stufen (-> Kosten für parallele Pflege alter SW-Stände)

# Beherrschung von Kompatibilität

## Idealvorstellung



Ersatzteileinbau allein basierend auf  
Test von I.1 und I.2, keine weitere  
Absicherung



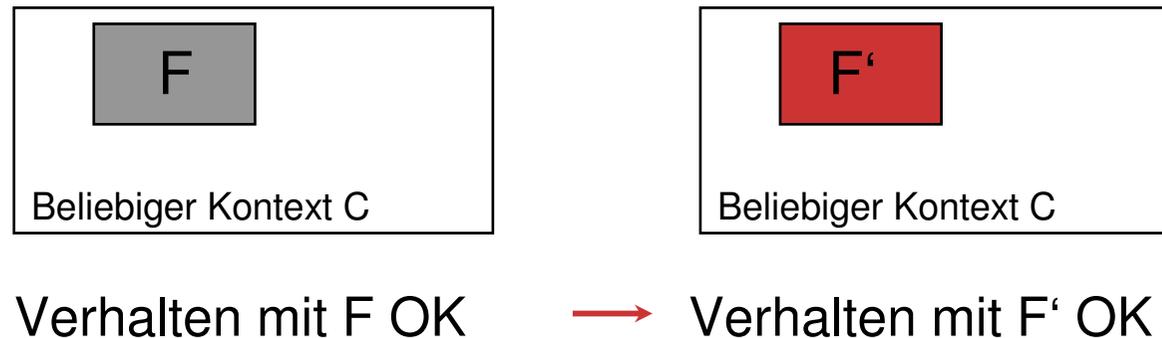
Freigabe nicht basierend auf Einzelkonfigurationstest, sondern  
Freigabe im **Service** für viele Konfigurationen

- entsprechende Absicherung nötig
- Idee der Rückwärtskompatibilität

# Beherrschung von Kompatibilität

## Rückwärtskompatibilität

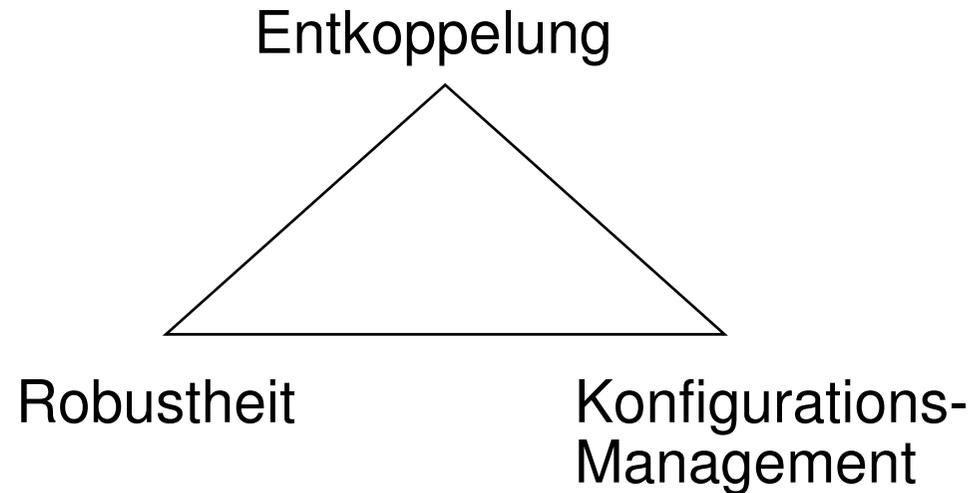
- **Rückwärtskompatibilität:** fehlerfreie Ersetzbarkeit der alten Version, in beliebigem Kontext (inkl. HW).
- Einschränkungen der Kontexte durch **Sollkontexte**, d.h. alle FZG-Varianten in denen Ersetzbarkeit gegeben sein soll.



- Rückwärtskompatibilität impliziert Vernetzungskompatibilität
- RK korrespondiert zum Schnittstellenbegriff: Interna einer Funktion sind irrelevant, allein das Wissen um die Schnittstelle reicht, um die Funktion nutzen zu können

# Beherrschung von Kompatibilität

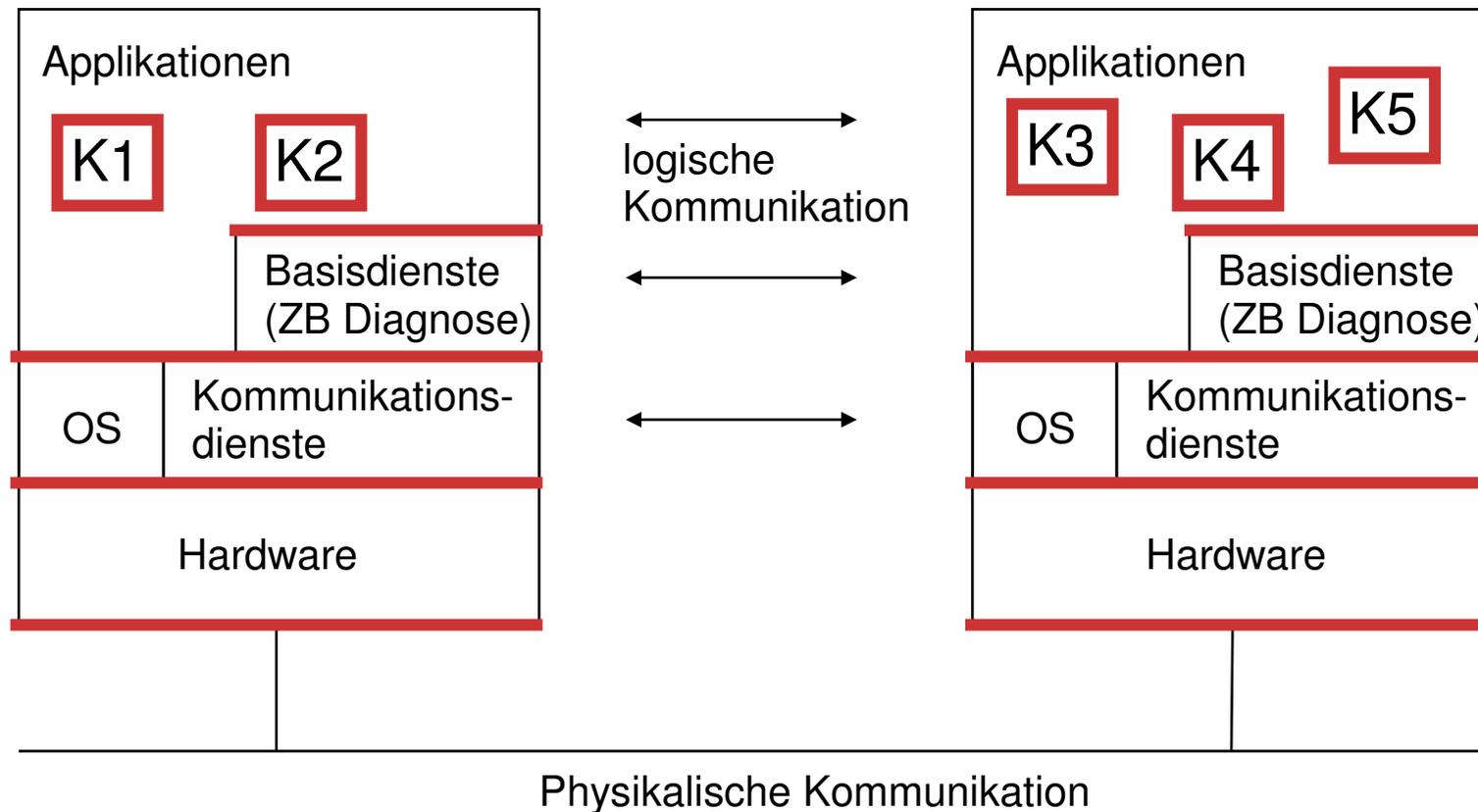
## Umgang mit Abhängigkeiten



- **Entkoppelung** eliminiert Abhängigkeiten von Komponenten  
=> Kompatibilität immer gewährleistet (Stand Alone Ansatz)
- **Robustheit** erhält Funktionsfähigkeit dort wo Entkoppelung nicht vollständig gegeben ist  
=> Negative Auswirkungen von Inkompatibilität begrenzt
- **Konfigurationsmanagement** identifiziert zulässige Konfigurationen von Komponenten, wo Entkoppelung und Robustheit nicht gegeben sind  
=> Explizite Festlegung von Kompatibilität

# Beherrschung von Kompatibilität

## Entkoppelung



- Schichtenbildung (vertikal)
- Komponentenbildung (horizontal)

# Beherrschung von Kompatibilität

## Robustheit

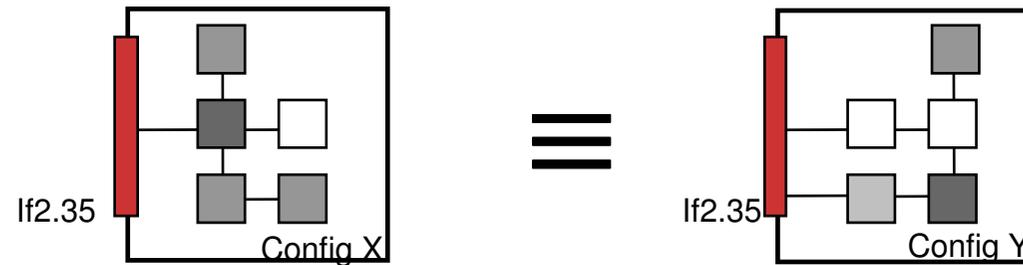
- Robustes Energie-Bordnetz
- Robustheit bzgl. Umweltbedingungen (EMV, ...)
- Robuste Kommunikation
  - **CAN** hinreichend robust: genug (Rest-)Bandbreite, sinnvolles Verhalten der SW Komponenten bei Kommunikationsfehlern  
(wie kann das getestet werden?)

⇒ Limitierung nicht funktionaler Wechselwirkung

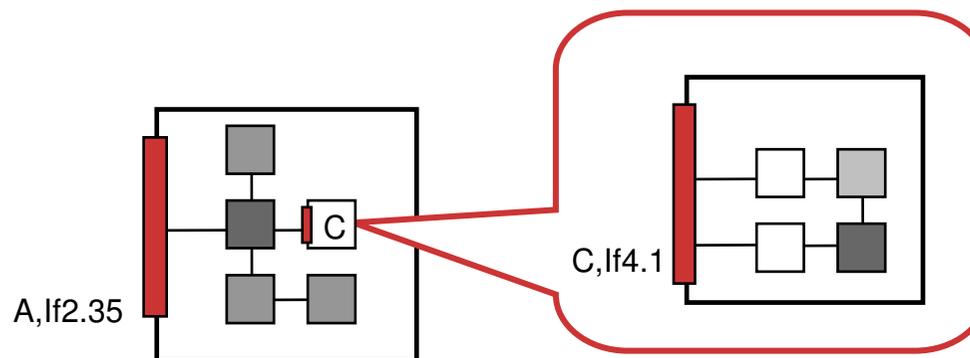
# Beherrschung von Kompatibilität

## Robustes Konfigurationsmanagement

- Schnittstellenversionen, die durch verschiedene Kombinationen von Komponentenversion realisiert werden können

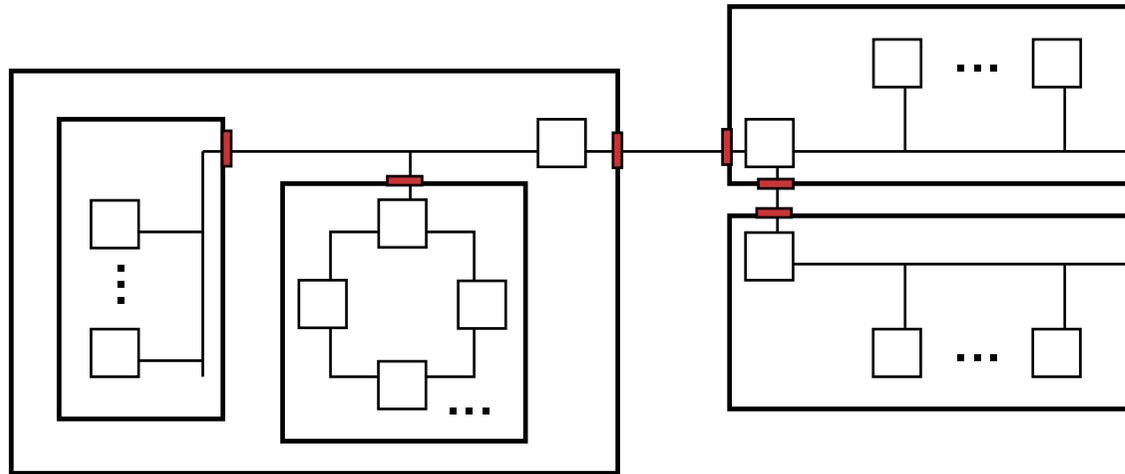


- Hierarchische Schachtelung von Schnittstellen möglich



# Beherrschung von Kompatibilität

## Robustes KonfigMgmt Anwendung



- Bordnetz-Ebene: legt Schnittstellenversion der Subsysteme fest
- Strategie für jedes Subnetz SIL abhängig

# **Beherrschung von Kompatibilität**

## **Resumee und offene Fragen**

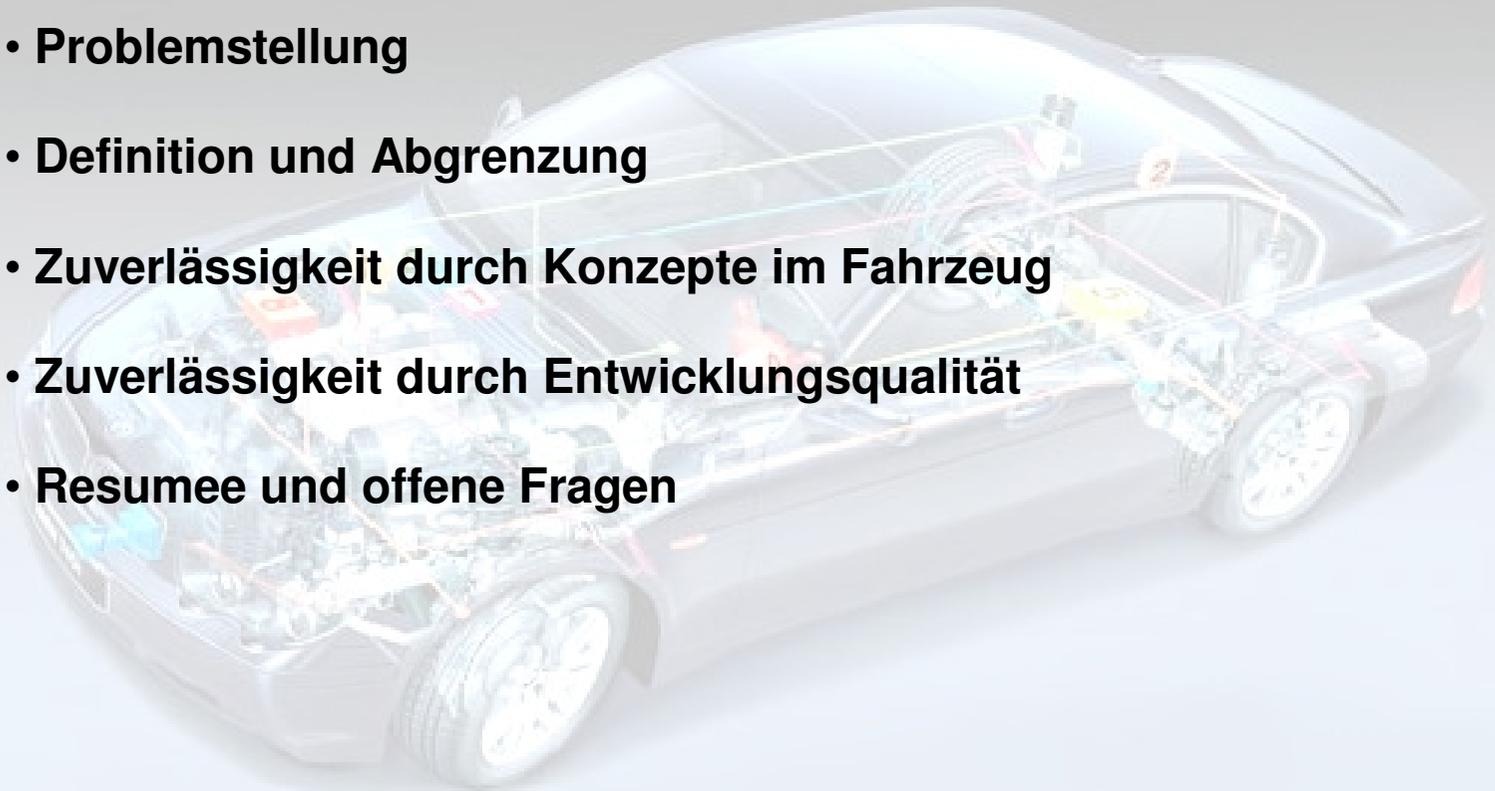
- **Resumee**
  - **Sicherung der Kompatibilität erfordert heute enorme Kosten bei mäßiger Beherrschung**
  - **Kompatibilität muss stärker im Design (linker Ast V-Modell) und nicht nur in der Integration (rechter Ast V-Modell) adressiert werden**
  - **Problem der Kompatibilität verschärft sich weiter: künftig mehr Varianten und kürzere Lebenszyklen der Komponenten**
- **Offene Fragen**
  - **Schärfe des Kompatibilitätsbegriffs: Inkompatibilität falls Schnittstellen Mismatch oder “negatives” Kundenerlebnis**
  - **Praktische Erreichbarkeit 100%er Kompatibilität: Reduktion von Inkompatibilitätsursachen, d.h. “nur” Verringerung der Inkompatibilität**
  - **Metriken für Kompatibilität**

# Herausforderungen der Zukunft

## Content

- **Beherrschung von Zuverlässigkeit**

- **Problemstellung**
- **Definition und Abgrenzung**
- **Zuverlässigkeit durch Konzepte im Fahrzeug**
- **Zuverlässigkeit durch Entwicklungsqualität**
- **Resumee und offene Fragen**



# Beherrschung von Zuverlässigkeit

## Problemstellung

**Fzg ist ein komplexes technisches System, dass aus vielen Funktionen (Subsystemen) besteht**

**Unterschiedliche Anforderungen bez. Zuverlässigkeit von Fkt  
vgl. SIL (Safety Integrity Level)**

### **Fahrsicherheitsrelevante Funktionen**

- Führungsrelevante Funktionen (Lenkung, Bremse, Stabilisierung)
- Sicherheitsrelevante Funktionen (Airbag, ABS, Crash-Erken., etc.)

### **Fahrrelevante Funktionen**

- Fkt. mit Auswirkung auf Fahrerlaubnis (Anzeigen, Außenlicht, ..)
- Fkt. mit Auswirkung auf Fahrfähigkeit (Liegenbleiber, Fzg-Zgng)

### **Convenience Funktionen**

- Funktionen ohne unmittelbare Fahrrelevanz (z.B. Entertainment, Klima, Karosserie, etc.)

# Beherrschung von Zuverlässigkeit

## Definition und Abgrenzung

### **Zuverlässigkeit (Reliability)**

- Fähigkeit eines Systems, für eine gegebene Zeit korrekt zu arbeiten. Dabei wird vorausgesetzt, dass das System zu Anwendungsbeginn korrekt ist und nur Ausfälle zur Unkorrektheit führen können.

### **Verfügbarkeit (Availability)**

- Betriebsfähigkeit zu einem Zeitpunkt; Wahrscheinlichkeit, dass ein System die tatsächlich angegebene Leistung erbringt (Regelbetrieb, Administration, Ausfall)

### **Robustheit (Robustness)**

- Fähigkeit eines Systems, auch bei Verletzung der spezifizierten Randbedingungen vereinbarte Funktionen zu erfüllen bzw. seine Funktionsfähigkeit zu erhalten (Begriff ist unscharf. Woran ist Robustheit zu messen? Spezifizierte Robustheit ist ein Widerspruch)

### **Sicherheit (Safety)**

- Freiheit von inakzeptablen Risiken (Risiko ist potenzielles Problem, das noch nicht eingetreten ist und proaktiv behandelt werden muss).

# **Beherrschung von Zuverlässigkeit**

## **Konzepte im Fahrzeug**

**Zahlreiche Konzepte fördern die Zuverlässigkeit eines Fzg-IT-Systems. Prinzipiell: was nicht vorhanden ist kann nicht ausfallen oder stören.**

### **Determinismus**

– Zeitbasierte Architekturen, Globale Systemzeit, Synchronisation

### **Zustandskonstistenz**

– Globaler Fahrzeugzustand, definierte Zustandsübergänge

### **Laufzeitüberwachung und Robustheit**

– Schnittstellen, Zustände, Energieverbrauch

### **Redundanz und Fehlertoleranz**

– Redundante Funktionen/Architekturen, Redundanzaktivierung

# **Beherrschung von Zuverlässigkeit**

## **Konzepte in der Entwicklung**

**Ähnlich wie Kompatibilität ist auch die Zuverlässigkeit eine Funktion der Entwicklungsqualität**

### **Entwicklungsqualität**

- Software-Reuse (vgl. Standards)
- Software-Generierung (aus “einfachen” Modelle)
- Nutzung von Middleware
- Testing

# **Beherrschung von Zuverlässigkeit**

## **Resumee und offene Fragen**

- **Resumee**
  - **Zuverlässigkeit komplexer, verteilter IT-Systeme im Fzg stellt heute eine der wesentlichen Herausforderungen dar.**
  - **Anwendung formaler Methoden des Reliability Engineerings für quantitative Aussagen für das Gesamt-Fzg-IT-System noch nicht flächendeckend im Einsatz**
- **Offene Fragen**
  - **Methoden und Metriken zur Bewertung von Bordnetz-Architekturen unzureichend**
  - **Partitionierung nach Zuverlässigkeitsgesichtspunkten**

# Herausforderungen der Zukunft

## Content

- **Beherrschung von Autonomie**

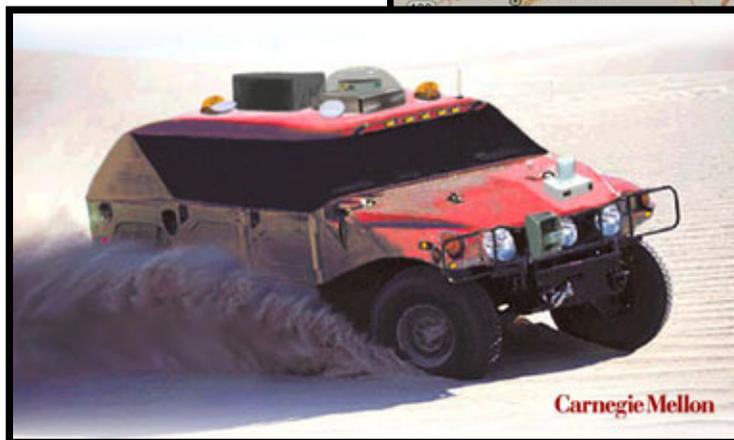
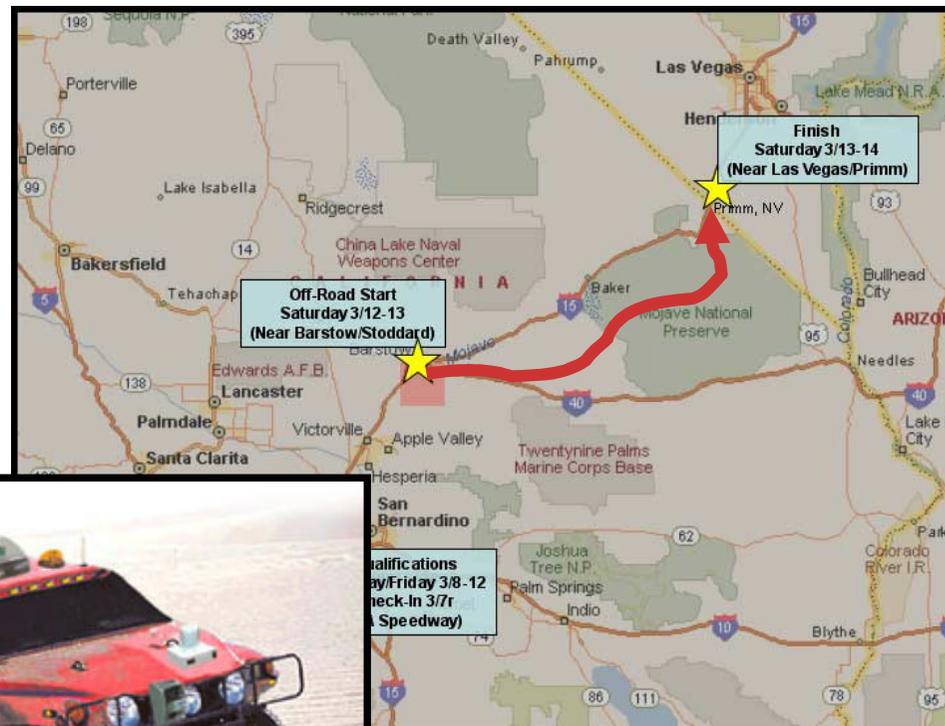
- **Problemstellung**
- **Definition und Abgrenzung**
- **Autonomie durch Assistenzfunktionen**
- **Autonomie und Systemgrenzen**
- **Resumee und offene Fragen**



# Beherrschung von Autonomie

## Rennen autonomer Fahrzeuge nach Las Vegas

**230 km autonom durch die Mojave Wüste (USA)**  
**Das beste der 23 Fahrzeuge schied bereits nach 11.8 km (5.1%) aus.**



# Beherrschung von Autonomie

## Problemstellung

Wie kann das Fahren noch sicherer, effizienter, ökonomischer und unterhaltsamer gemacht werden?

- Assistenzfunktionen, die selbständig aktiv sind (autonom)
- Unterscheidung (vgl. SIL) zwischen
  - primären Assistenzfunktionen
  - sekundären Assistenzfunktionen
  - tertiären Assistenzfunktionen
- Vollständige Autonomie des Gesamtfahrzeugs ist
  - weder rechtlich zulässig
  - noch konform zu BMW-Werten

# Beherrschung von Autonomie

## Fahrerassistenzsysteme

- **Fahrerassistenz Systeme** umfassen alle Funktionen, die **auf Basis erhöhter sensorischer Kompetenz** zu einer **Verbesserung des Fahrens beitragen**.
- Hierbei werden die beiden Ausprägungen „**Kompetenzsteigernd**“ und „**Entlastend**“ unterschieden.
- Fahrerassistenz Systeme leisten durch **Entlastung** und **Kompetenzsteigerung** des Fahrers einen wichtigen **Beitrag** in den Bereichen **Dynamik, Souveränität und Sicherheit**.

# Beherrschung von Autonomie

## Hierarchie für Autonomie im Fahrzeug

- Fahrer steuert Fahrzeug völlig selbstständig
- Fahrzeug mit teilweise autonomen Funktionen im Rahmen von Fahrerassistenzsystemen
  - beratende Subsysteme (Entscheidungen dieser Systeme können vom Benutzer jederzeit überschrieben werden)
    - automatische Aktivierung/Deaktivierung von Licht/Scheibenwischer
    - ACC (active cruise control)
    - AFS (active front steering)
    - ALC (active light control)
    - TLC (time to line crossing) in Kombination mit HC (heading control)
  - eingreifende Subsysteme
    - ABS (anti-lock braking system)
    - DSC (dynamic stability control)
    - Vollbremsung bzw. automatischer Notruf bei Unfall
- vollständig autonomes Fahrzeug

# Beherrschung von Autonomie

## Stärken und Schwächen

### **Schwächen (Leistungsabfall) des Fahrers bei**

- Stress
- Zeitdruck
- Ermüdung
- mehrere Aufgaben gleichzeitig (Multitasking)

### **Stärken autonomer Systeme bei**

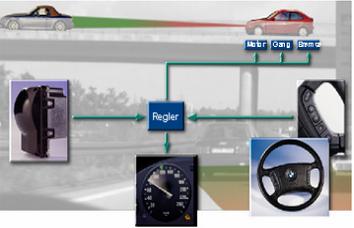
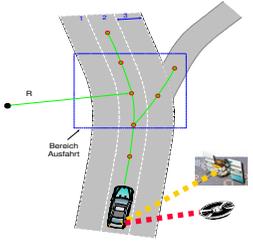
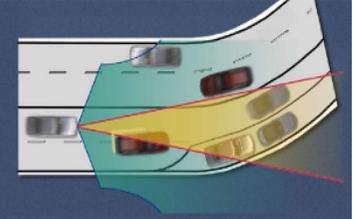
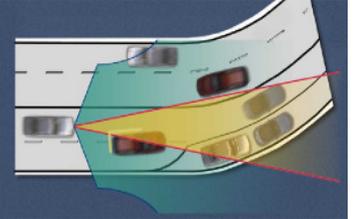
- Daueraufmerksamkeit
- Reaktionsgeschwindigkeit
- Erweiterte Sensorik
- Umsetzung komplexer Regelsysteme
- einfachen Entscheidungssituationen

### **Schwächen autonomer Systeme bei**

- komplexen Entscheidungssituationen (z.B. Beobachtung mehrerer Fahrzeuge bei Kolonnenfahrt)

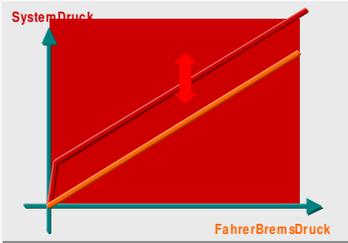
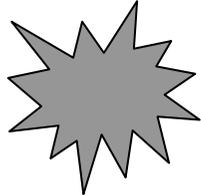
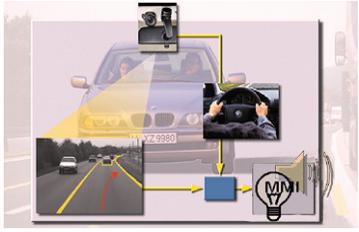
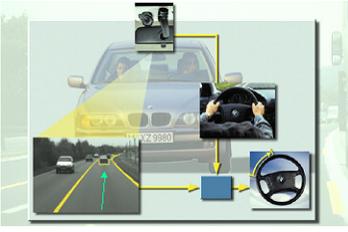
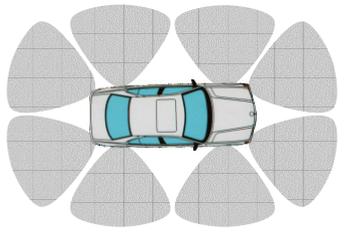
# Beherrschung von Autonomie

## Fahrerassistenzsysteme bei BMW (I)

<p><b>Dynamic Cruise Control</b></p> 	<p><b>Cruise Assist (FFP)</b></p> 	<p><b>ACC</b></p> 	<p><b>ACC + Navi</b></p> 
<p><b>ACC Stop&amp;Go 1</b></p> 	<p><b>ACC Stop&amp;Go 1+</b></p> 	<p><b>ACC Stop&amp;Go 2</b></p> 	<p>...</p>
<p><b>Navspeed 1</b></p> 	<p><b>Navspeed + VZE</b></p> 	<p><b>Curve Speed Assist</b></p> 	<p>...</p>

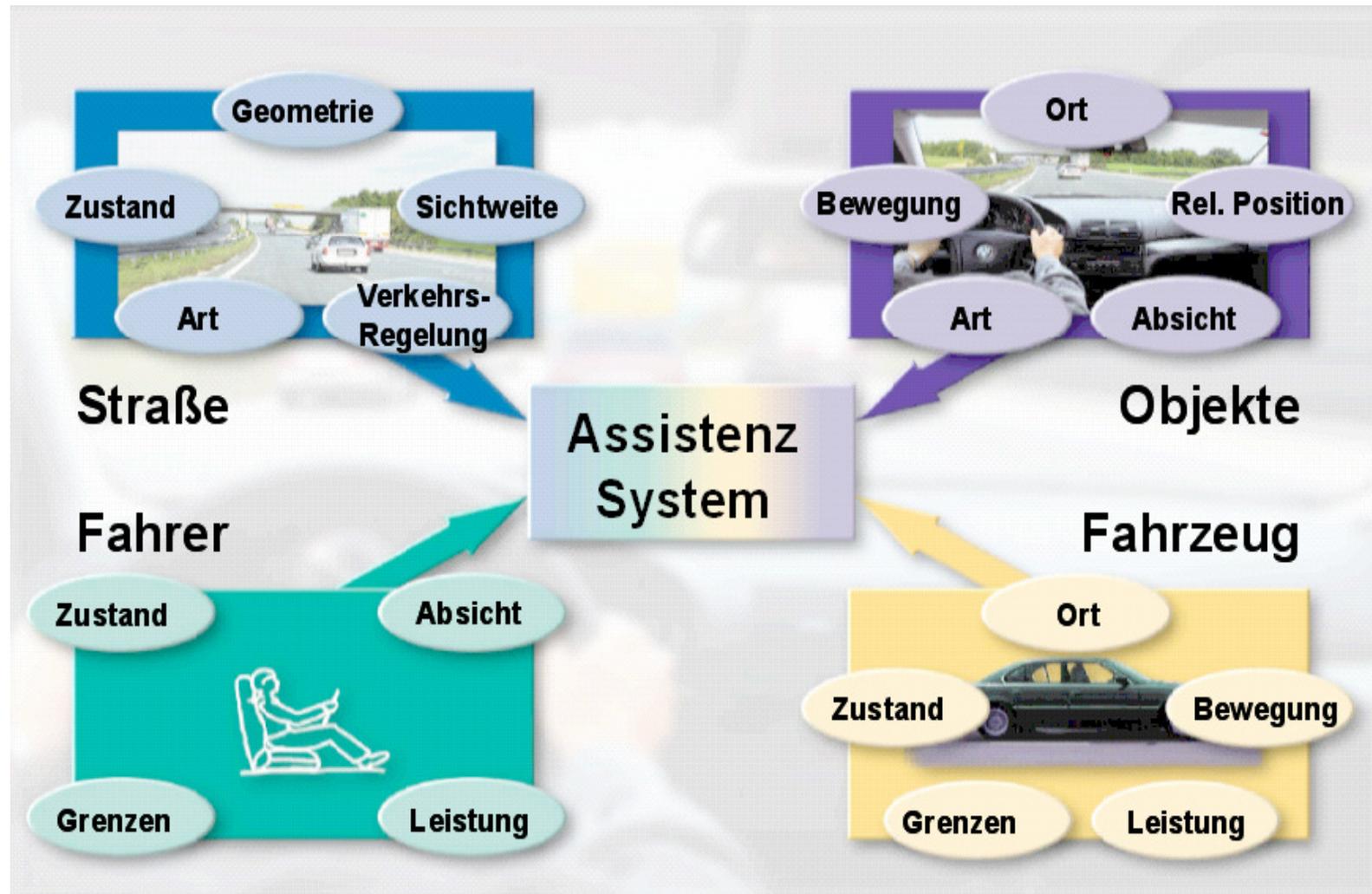
# Beherrschung von Autonomie

## Fahrerassistenzsysteme bei BMW (II)

<p><b>iBrake Aufahrwarnung</b></p> 	<p><b>iBrake Bremsassistent</b></p> 	<p><b>iBrake Aut. Notbremse</b></p> 	<p>...</p> 
<p><b>Time To Line Crossing</b></p> 	<p><b>Heading Control</b></p> 	<p><b>Spurwechsel-Warn.</b></p> 	<p><b>Spurwechsel-Ass.</b></p> 
<p><b>Parkpilot</b></p> 	<p><b>Einparkassistent</b></p> 	<p><b>(... Manuevrierassistent)</b></p> 	<p>...</p>

# Beherrschung von Autonomie

## Informationsbedarf bei Fahrzeugführung



# Beherrschung von Autonomie

## Informationsquellen

**Kamera mit Bildverarbeitung**

**Abstands-Sensorik (Laser, Radar)**

**Positionierung via GPS**

**Datenbanken, Digitale Karten**

**Datenaustausch mit Infrastruktur**

**Sensoren für Straßenzustand und Sichtbedingungen**

**Fahrdynamik-Sensoren**

# **Beherrschung von Autonomie**

## **Fahrerassistenzsysteme und Systemgrenzen**

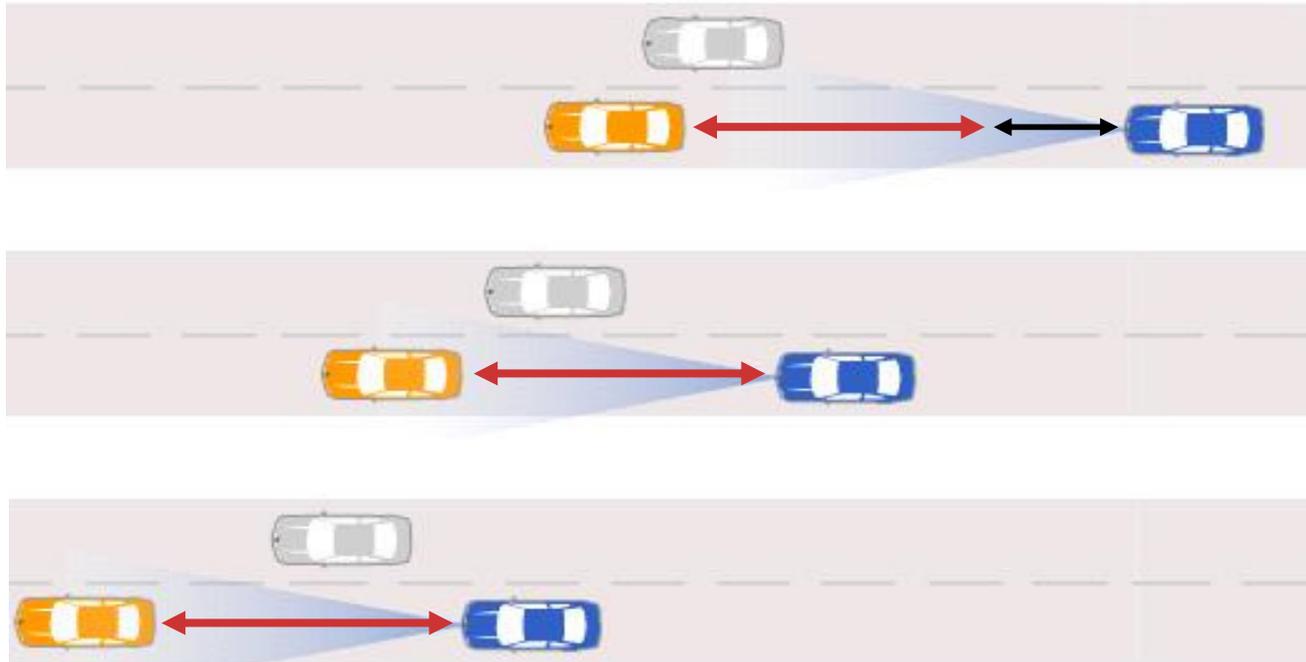
**Wann agiert eine Assistenzfkt autonom? Wann und wie erfolgt die (Rück-) Übergabe der Funktionalität an den Fahrer?**

### **Anforderungen an die Schnittstelle**

- Deterministisches Verhalten
- Einfach und intuitiv
- Jederzeit “überschreibbar” durch Fahrer
- Jederzeit deaktivierbar

# Beherrschung von Autonomie

## Systemgrenzen Adaptive Cruise Control (ACC)



# **Beherrschung von Autonomie**

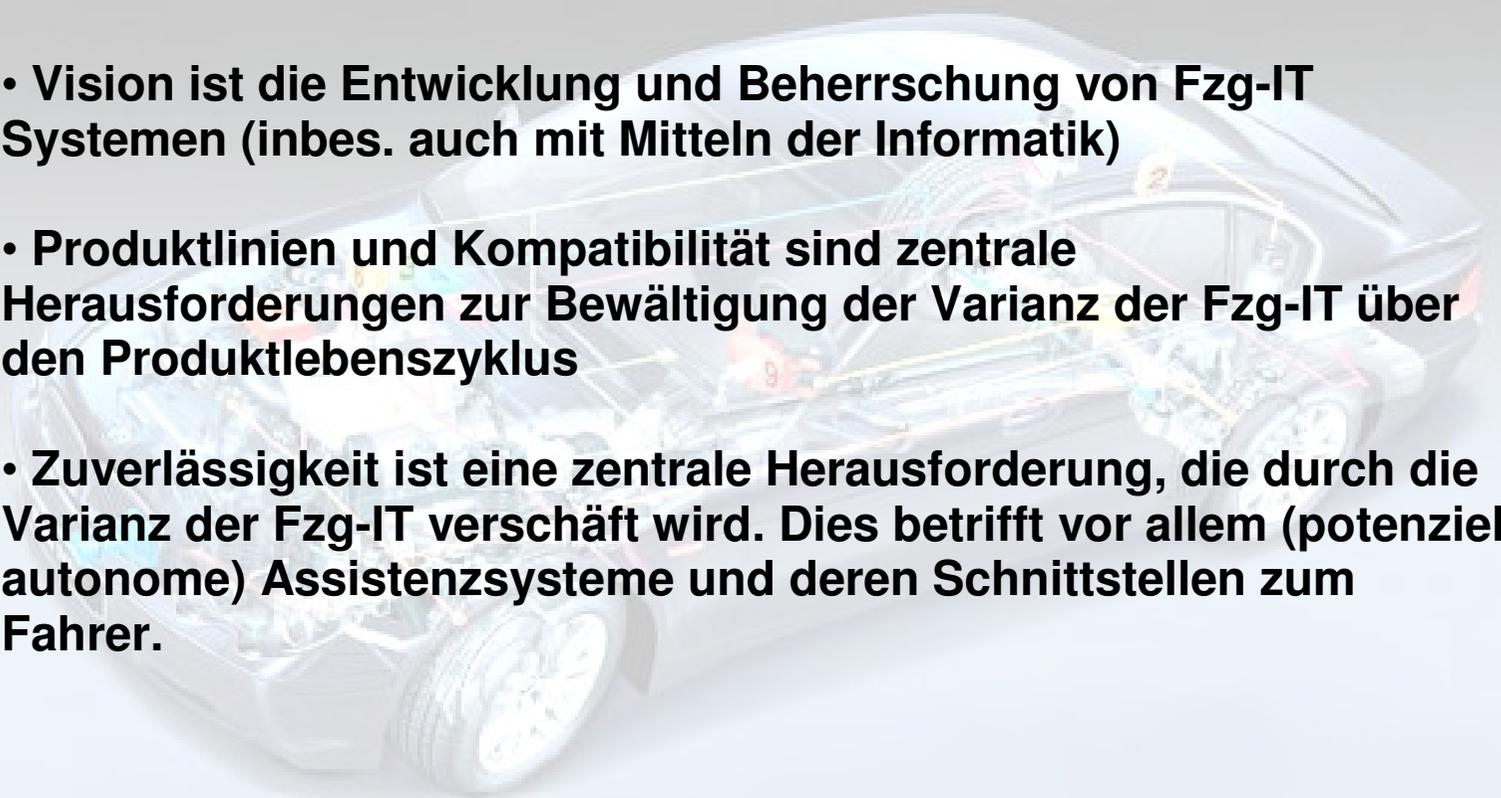
## **Resumee und offene Fragen**

- **Resumee**
  - **Heute existieren zahlreiche begrenzt autonom agierender Fahrassistenz-Funktionen**
  - **Entscheidend für den Nutzen (primärer) Assistenzsysteme ist der Umgang mit Systemgrenzen: Ab wann übernimmt der Fahrer die Fzg-Führung und wie erfolgt die Übergabe.**
  - **Die Nutzung autonomer Systeme wird neben der technischen Machbarkeit durch die Kundenakzeptanz und rechtliche Rahmenbedingungen geprägt. Der Fahrer bleibt weiterhin verantwortlich für die Fahrzeugführung.**
- **Offene Fragen**
  - **Integrierte Fahrer-, Fahrzeug- und Umweltmodelle zur Ableitung von Entscheidungen für Assistenzfunktionen**

# Herausforderungen der Zukunft

## Content

- **Zusammenfassung**

- **Vision ist die Entwicklung und Beherrschung von Fzg-IT Systemen (inbes. auch mit Mitteln der Informatik)**
  - **Produktlinien und Kompatibilität sind zentrale Herausforderungen zur Bewältigung der Varianz der Fzg-IT über den Produktlebenszyklus**
  - **Zuverlässigkeit ist eine zentrale Herausforderung, die durch die Varianz der Fzg-IT verschärfert wird. Dies betrifft vor allem (potenziell autonome) Assistenzsysteme und deren Schnittstellen zum Fahrer.**
- 

# Herausforderungen der Zukunft

## Resumee und Kernaussagen

**Ein Automobil ist ein komplexes, verteiltes IT-System. Die Informatik bietet Konzepte und Methoden (ggf. anzupassen) für die Entwicklung verteilter Funktionen.**

**Neben Innovationen bei Kundenfunktionen kommt der Infrastruktur im Fahrzeug als „Fundament“ eine zunehmend wichtige Bedeutung zu. Sie ermöglicht den robusten Betrieb und die kostengünstige Administration des IT-Systems.**

**Die Beherrschung von Produktlinien, Kompatibilität, Zuverlässigkeit und Autonomie sind ausgewählte Herausforderungen für die Zukunft von Fzg-IT-Systemen.**

**Die Informatik stellt bereits heute eine Schlüsseltechnologie in der Automobilentwicklung dar – und steht dennoch erst am Anfang ihrer enormen Möglichkeiten.**

# Herausforderungen der Zukunft

## Vielen Dank für Ihre Aufmerksamkeit

