

Fahrerassistenzsysteme im Kraftfahrzeug

Prof. Dr.-Ing. Markus Lienkamp



Vorlesungsübersicht

01 Einführung 28.04.2022 – Prof. Lienkamp	01 Einführung 28.04.2022 – Prof. Lienkamp	01 Übung Einführung 28.04.2022 – Hoffmann
02 Sensorik / Wahrnehmung I 05.05.2022 – Prof. Lienkamp	02 Sensorik / Wahrnehmung I 05.05.2022 – Prof. Lienkamp	02 Sensorik / Wahrnehmung I 05.05.2022 – Prof. Lienkamp
03 Sensorik / Wahrnehmung II 12.05.2022 – Dr.-Ing. Diermeyer	03 Sensorik / Wahrnehmung II 12.05.2022 – Dr.-Ing. Diermeyer	03 Übung Sensorik / Wahrnehmung II 12.05.2022 – Schimpe
04 Sensorik / Wahrnehmung III 19.05.2022 – Schimpe	04 Sensorik / Wahrnehmung III 19.05.2022 – Schimpe	04 Übung Sensorik / Wahrnehmung III 19.05.2022 – Schimpe
05 Funktionslogik / Regelung 02.06.2022 – Dr.-Ing. Winkler	05 Funktionslogik / Regelung 02.06.2022 – Dr.-Ing. Winkler	05 Funktionslogik / Regelung 02.06.2022 – Dr.-Ing. Winkler
06 Übung Funktionslogik / Regelung 09.06.2022 – Dr.-Ing. Winkler	06 Funktionale Systemarchitektur 09.06.2022 – Prof. Lienkamp	06 Aktorik 09.06.2022 – Prof. Lienkamp
07 Deep Learning 23.06.2022 – Majstorovic	07 Deep Learning 23.06.2022 – Majstorovic	07 Übung Deep Learning 23.06.2022 – Majstorovic
08 MMI 30.06.2022 – Prof. Bengler	08 MMI 30.06.2022 – Prof. Bengler	08 MMI Übung 30.06.2022 – Prof. Bengler
09 Controllability 07.07.2022 – Prof. Bengler	09 Controllability 07.07.2022 – Prof. Bengler	09 Übung Controllability 07.07.2022 – Winkle
10 Entwicklungsprozess 14.07.2022 – Dr.-Ing. Diermeyer	10 Entwicklungsprozess 14.07.2022 – Dr.-Ing. Diermeyer	10 Übung Entwicklungsprozess 14.07.2022 – Hoffmann
11 Analyse und Bewertung FAS 21.07.2022 – Dr.-Ing. Feig	11 Analyse und Bewertung FAS 21.07.2022 – Dr.-Ing. Feig	11 Übung Analyse und Bewertung FAS 21.07.2022 – Dr.-Ing. Feig
12 Aktuelle und künftige Systeme 28.07.2022 – Prof. Lienkamp	12 Aktuelle und künftige Systeme 28.07.2022 – Prof. Lienkamp	12 Aktuelle und künftige Systeme 28.07.2022 – Prof. Lienkamp

- 毛雷尔认为，开发过程是如何构建的？如何评估和开发通过的子步骤的概念原型？

- 什么是“安全”，它可以细分为哪些子领域？

- ISO 26262 标准涉及哪些内容，其核心要素是什么？

- 如何根据 ISO 26262 的 G&R 分析方法对系统进行分析和评估？

Leitfragen

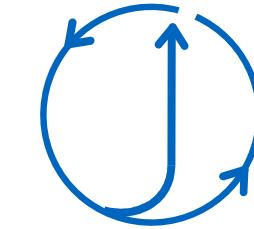
10 – Entwicklungsprozess und Funktionale Sicherheit

- Wie ist der Entwicklungsprozess nach Maurer aufgebaut?
Wie können prototypische Konzepte für die durchlaufenen Teilschritte bewertet und entwickelt werden?

- Was bedeutet „Sicherheit“ und in welche Teilbereiche kann sie untergliedert werden?

- Womit beschäftigt sich die ISO 26262 und was sind ihre Kernelemente?

- Wie kann ein System entsprechend der G&R-Analyse nach ISO 26262 analysiert und bewertet werden?



[1]



[2]



[3]

**Entwicklungsprozess und
Funktionale Sicherheit
Dr.-Ing Frank Diermeyer
(Simon Hoffmann, M.Sc.)**

Agenda

10 Entwicklungsprozess und funktionale Sicherheit

 10.1 Entwicklungsprozess

 10.2 Funktionale Sicherheit



**Entwicklungsprozess und
Funktionale Sicherheit
Dr.-Ing Frank Diermeyer
(Simon Hoffmann, M.Sc.)**

Agenda

10 Entwicklungsprozess und funktionale Sicherheit

 10.1 Entwicklungsprozess

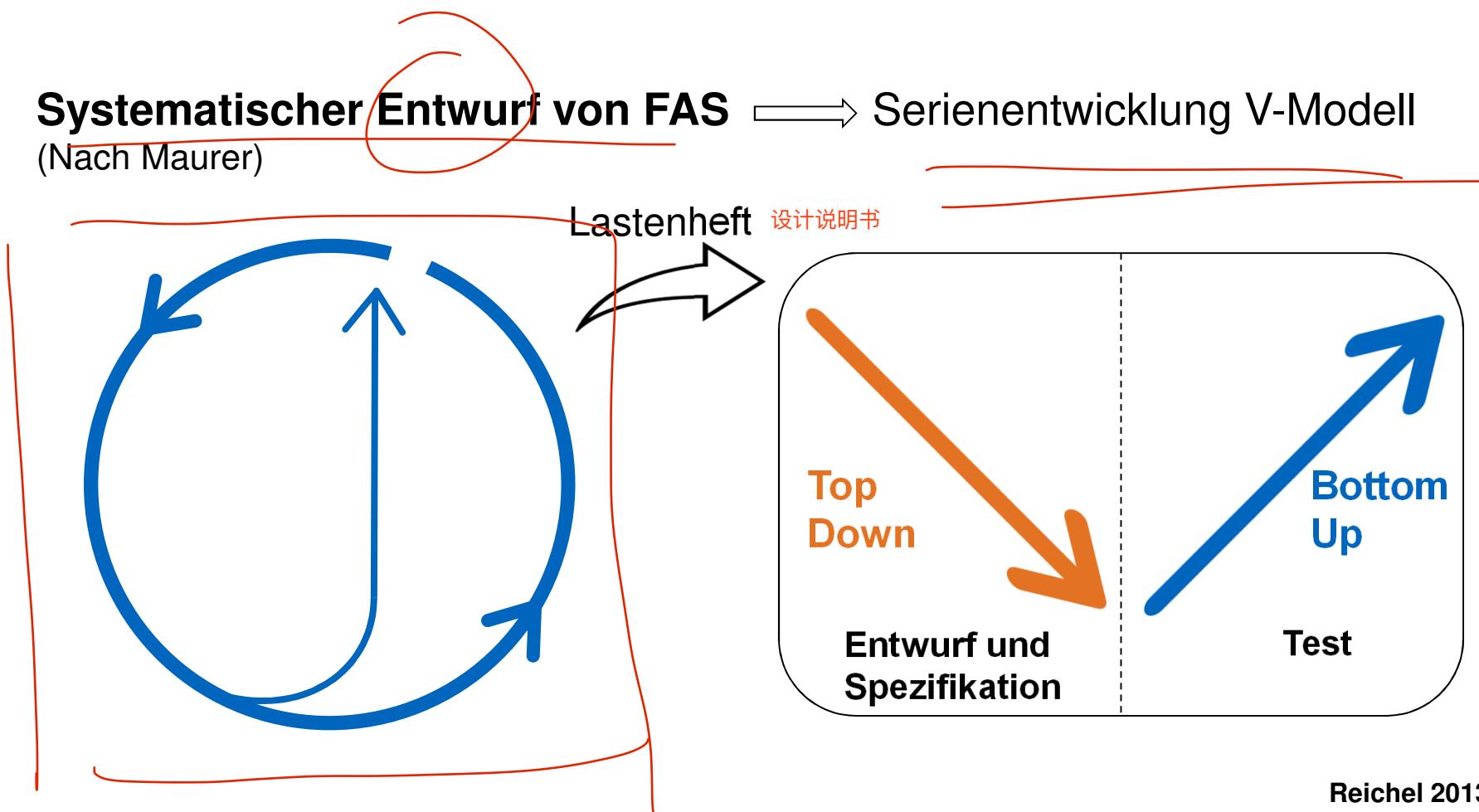
 10.1.1 Systematische Konzeptentwicklung

 10.1.2 Beispiel ANB

 10.2 Funktionale Sicherheit

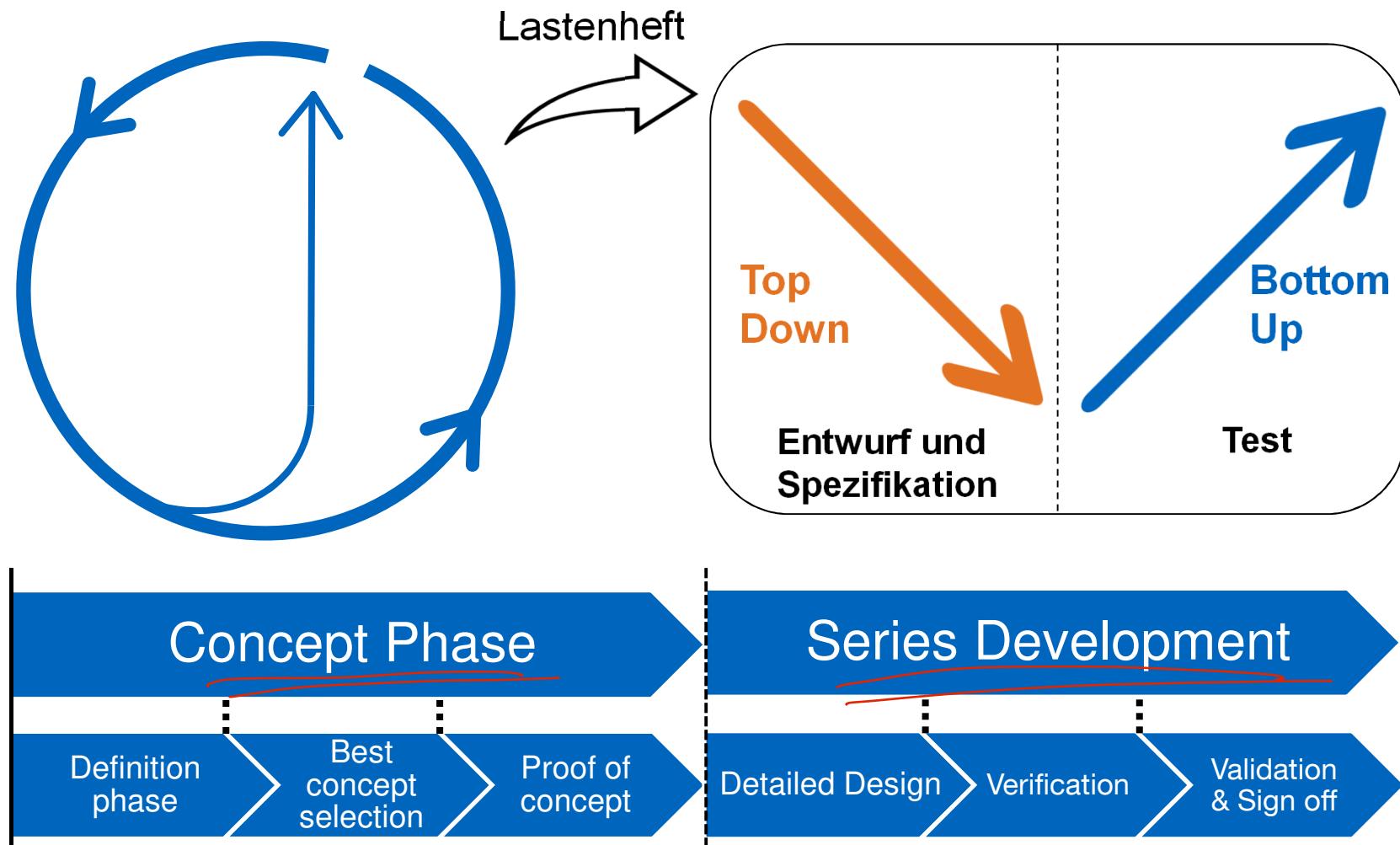


Entwicklungsprozesse für HAF

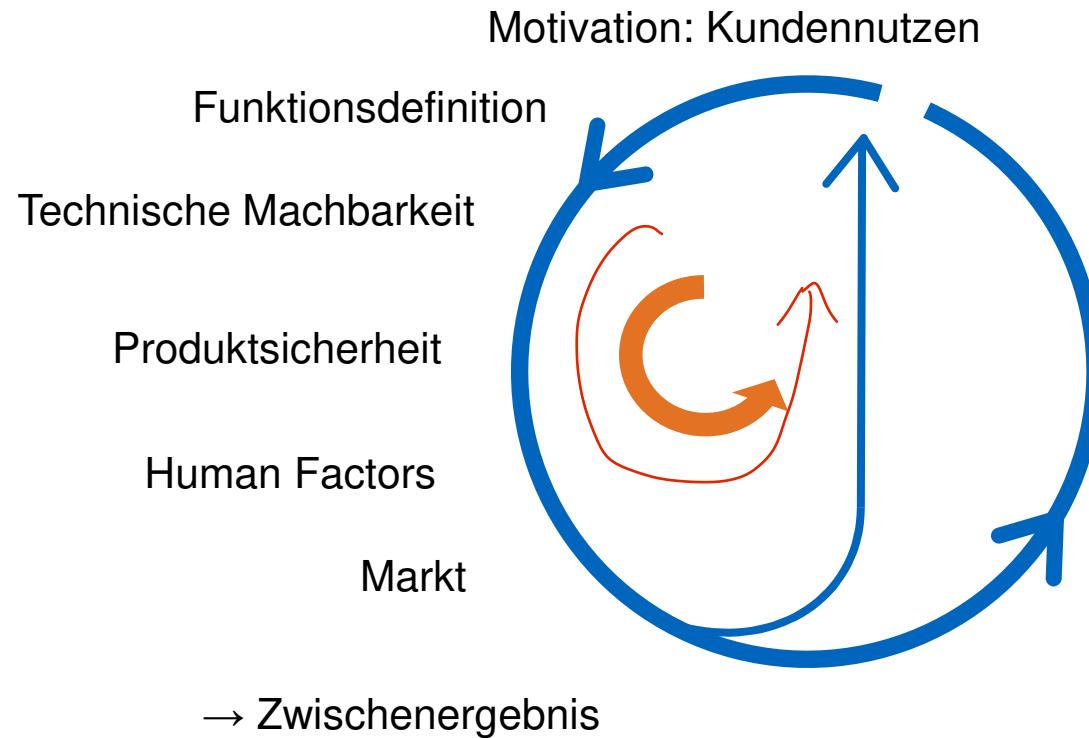


Reichel 2013

Einordnung des Code of Practice



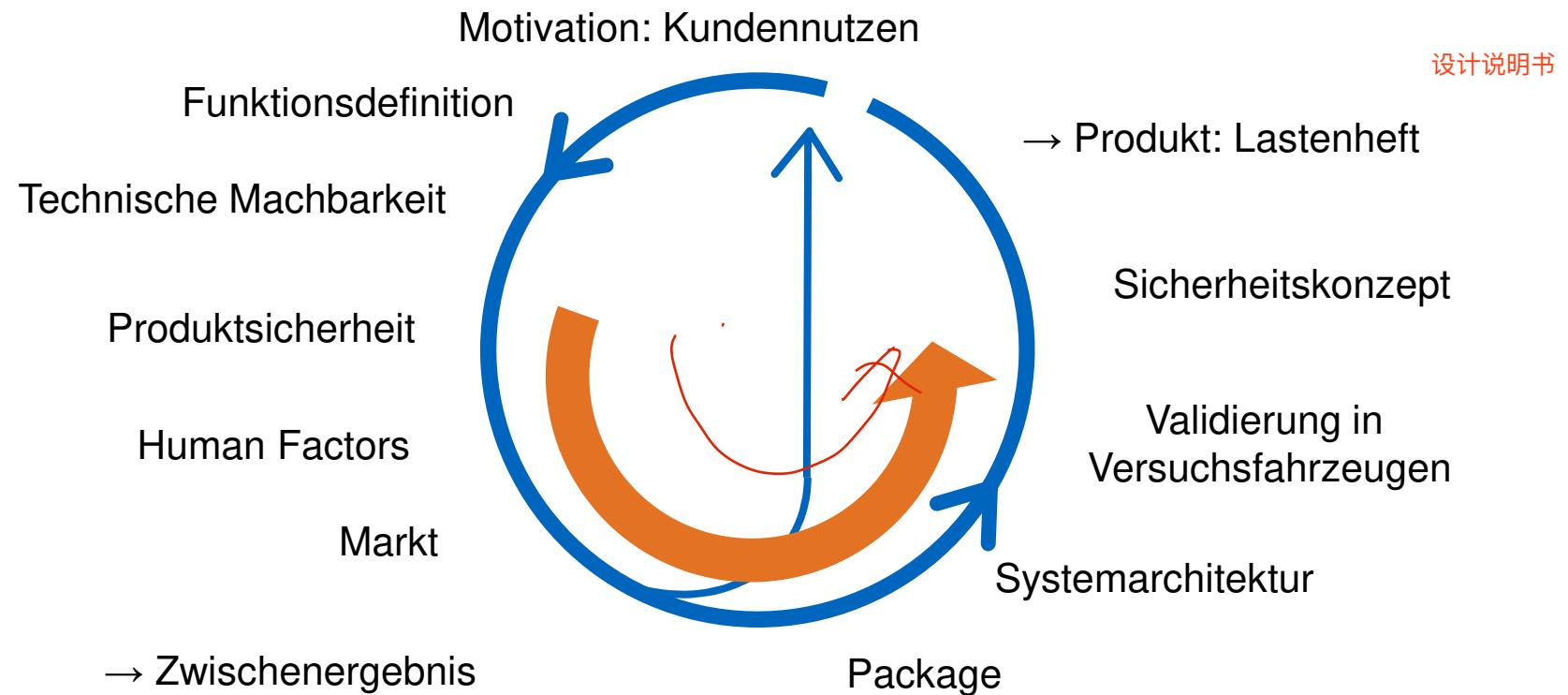
Systematischer Entwurf



Kommentarfolie

Die Abbildung zeigt einen Vollkreis, der eine komplette Iterationsschleife umfasst. Nach weniger als der Hälfte des Kreises ist ein „Abkürzungspfad“ definiert, der wieder zum Ausgangspunkt des Entwicklungsprozesses führt. Durch die beschriebene Struktur ergeben sich zwei Iterationsschleifen: Die erste, zeitlich kürzere und deutlich Ressourcen sparende Schleife erfordert Expertenwissen aus unterschiedlichen Bereichen. Die Arbeiten werden entweder theoretisch durchgeführt oder durch eine Reihe von aneinandergereihten X-in-the-Loop-Werkzeugen; während dieser Phase werden keinerlei Prototypen hergestellt. Der Ansatz ist dann besonders wirkungsvoll, wenn die im Unternehmen verfügbaren Experten, bei Bedarf verstärkt durch externe Wissensträger, in dieser Iterationsschleife möglichst die zentralen Auslegungskonflikte identifizieren und eine fundierte Auswahl treffen zwischen den realisierbaren und den wünschenswerten, aber noch nicht realisierbaren Assistenzfunktionen. [Winner S. 926f]

Systematischer Entwurf



**Entwicklungsprozess und
Funktionale Sicherheit
Dr.-Ing Frank Diermeyer
(Simon Hoffmann, M.Sc.)**

Agenda

10 Entwicklungsprozess und funktionale Sicherheit

 10.1 Entwicklungsprozess

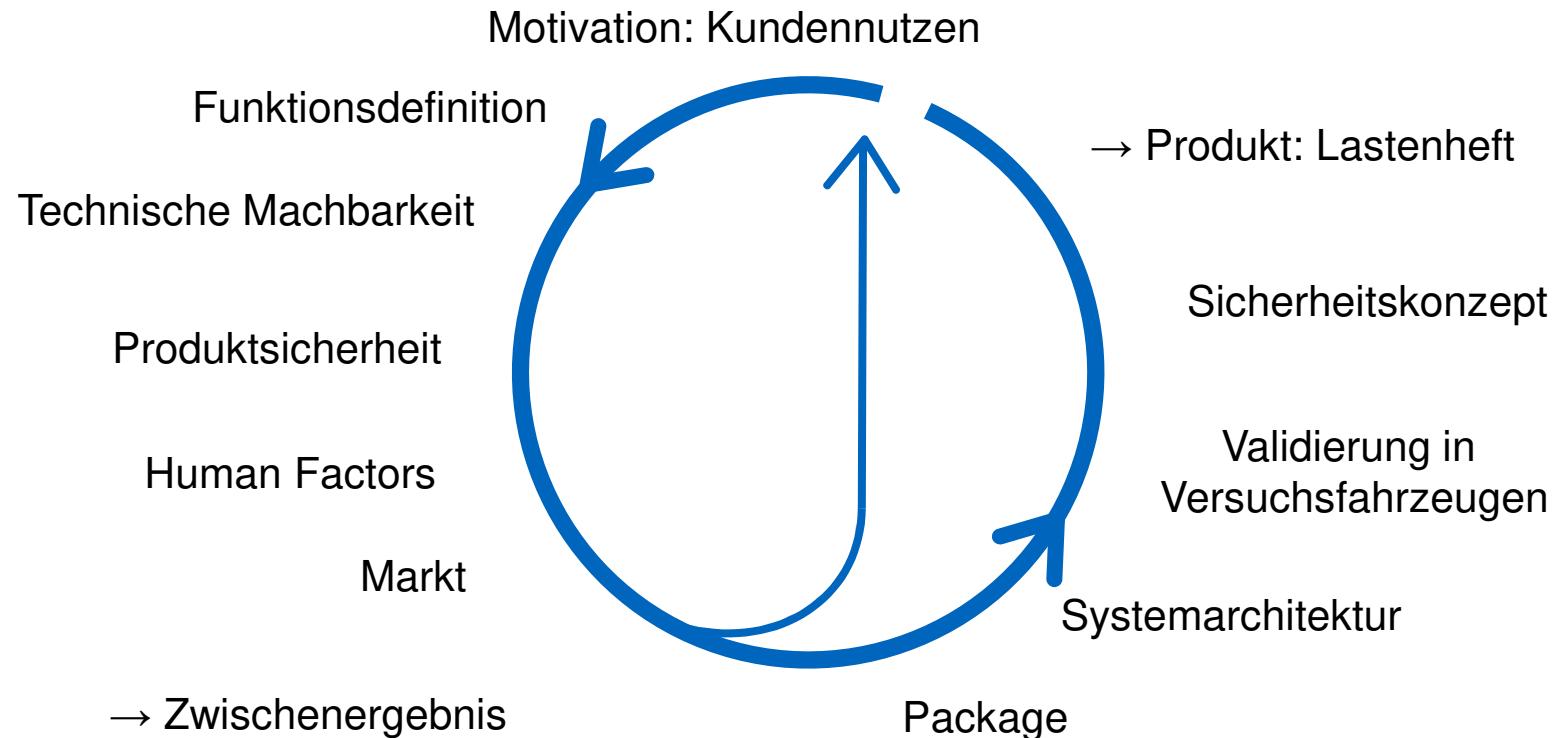
 10.1.1 Systematische Konzeptentwicklung

 10.1.2 Beispiel ANB

 10.2 Funktionale Sicherheit



Beispiel: Systematischer Entwurf einer Automatische Notbremsfunktion (ANB)



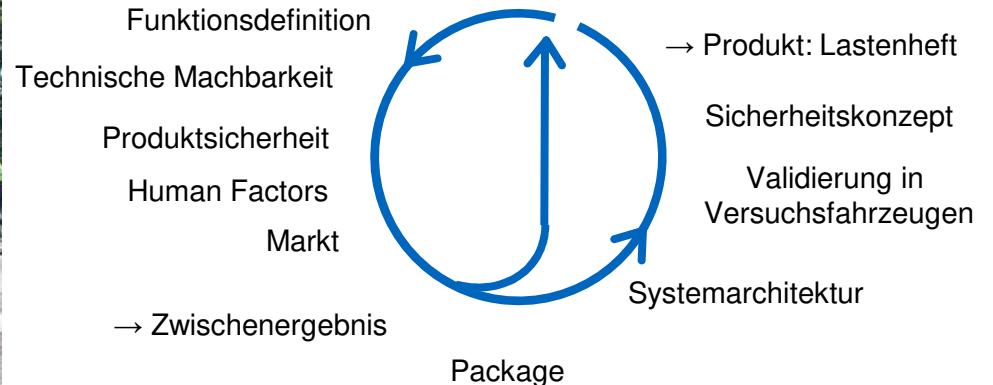
Motivation

检测可能造成严重破坏的事故类型

- Aufspüren von Unfalltypen mit großem Schadenpotential



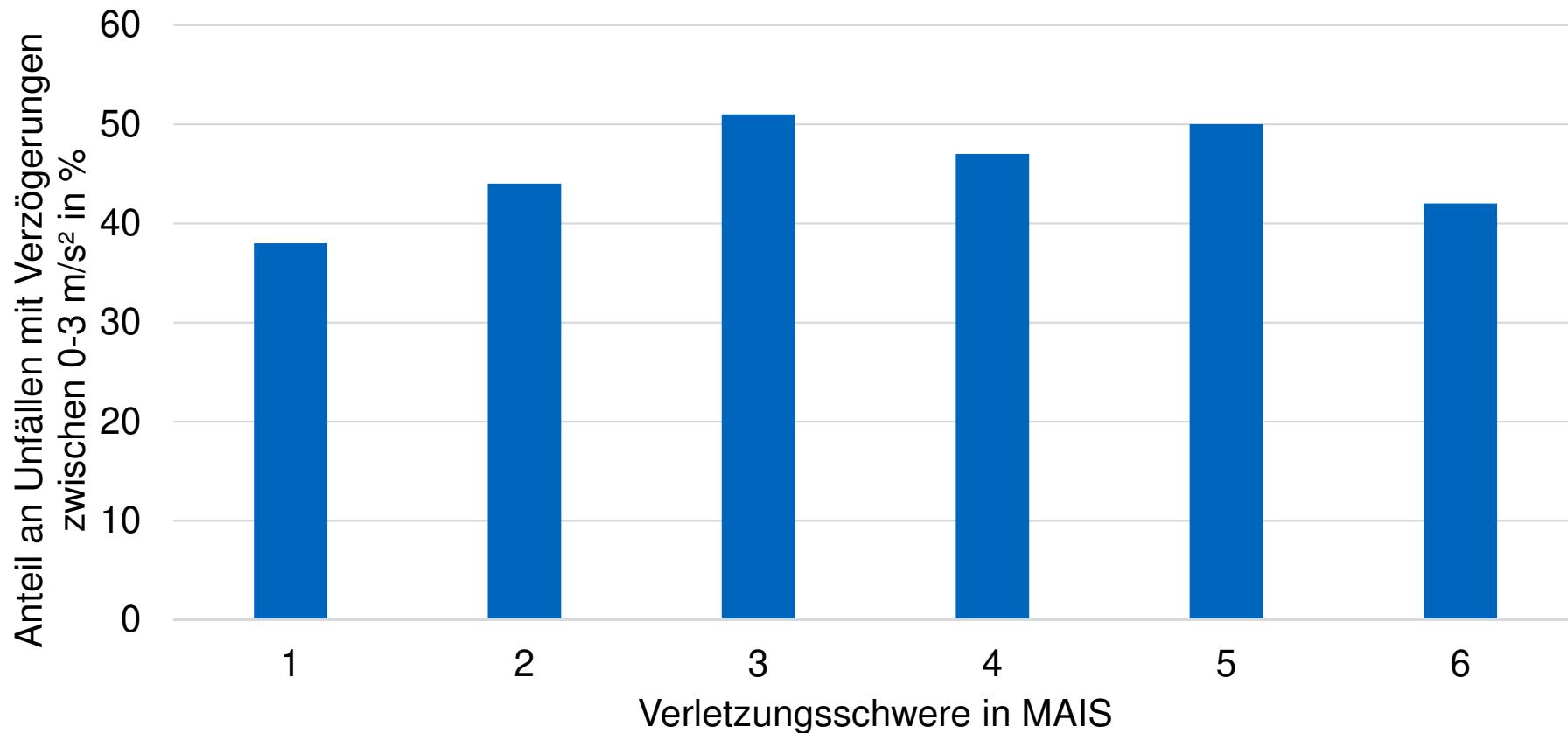
Motivation: Unfallschwereminderung



Maurer, TUBS

Theoretisches Potential von ANB

Bremsverzögerung bei Unfällen mit unterschiedlicher
Verletzungsschwere ohne ANB

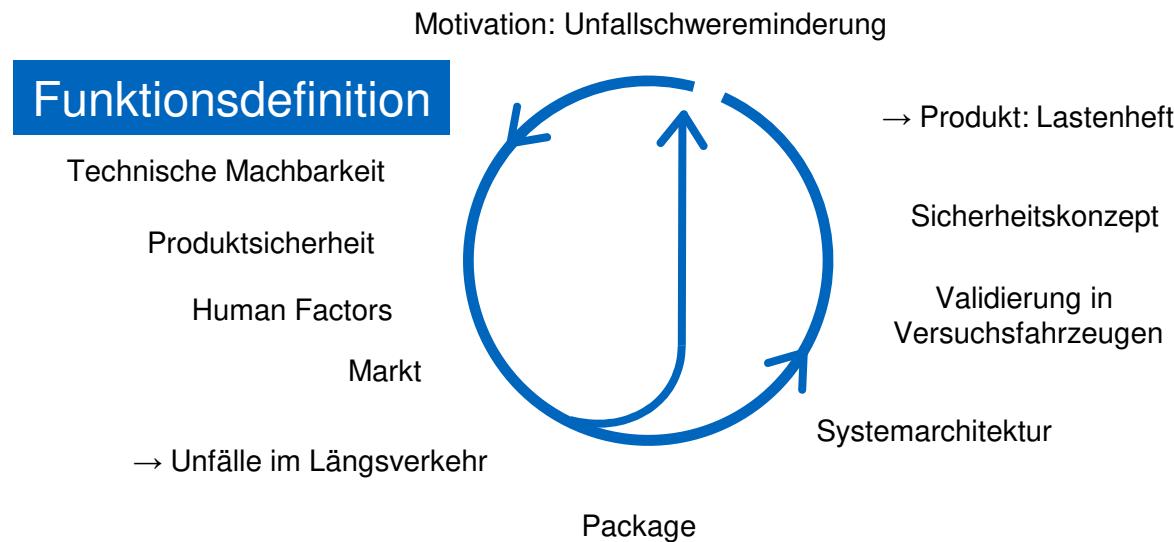


Kopischke 2000

Funktionsdefinition

- Entwurf von Funktionsdefinitionen nach der Response-Checklist (Kopf et al., 1999)
- Diskussion und Auflösung von Auslegungskonflikten

讨论和解决解释方面的冲突

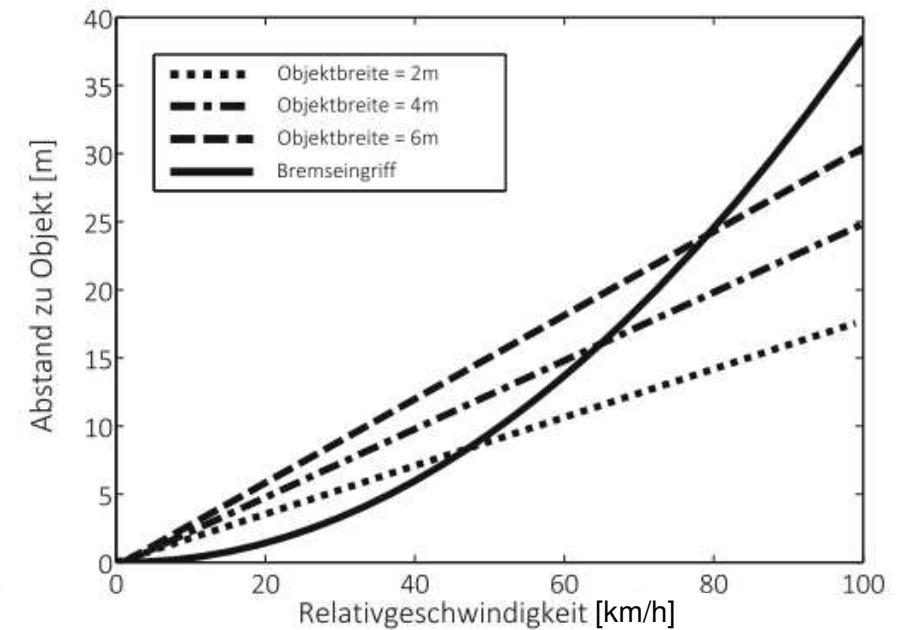
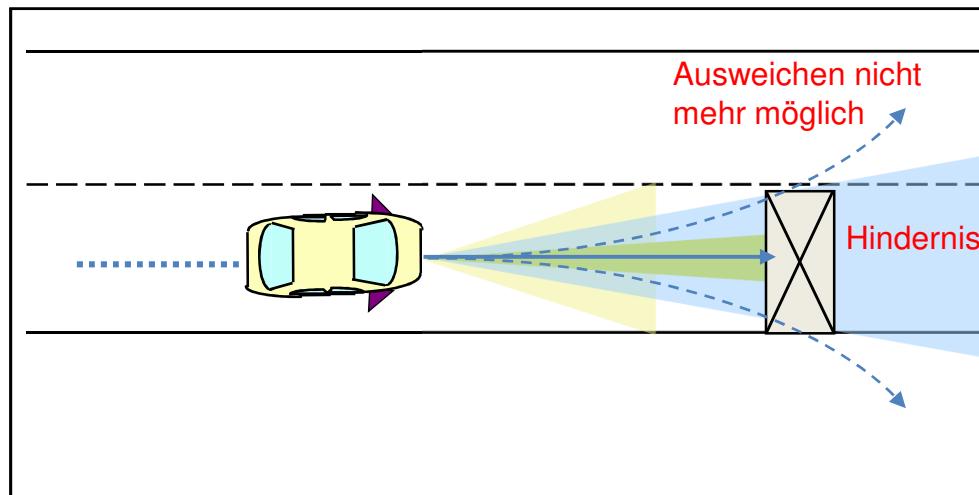


Maurer, TUBS

"紧急制动，即以最大减速度进行制动干预，在物理驾驶无法防止事故发生时启动。这给驾驶员留出了完全的自由空间，只有当他无法再防止碰撞时，才会触发制动器，无论他的驾驶技术有多高超....."。(科皮施克，2000 年)

Funktionsdefinition Automatische Notbremse

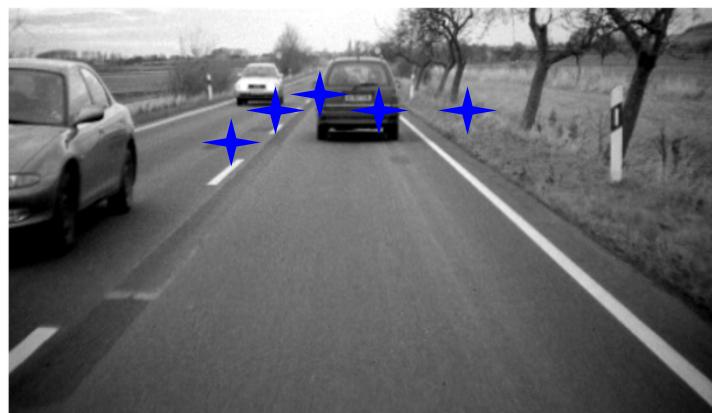
„Eine Notbremsung, d.h. Bremseingriff mit max. Verzögerung, wird dann veranlasst, wenn ein Unfall fahrphysikalisch nicht mehr zu verhindern ist. Damit wird dem Fahrer weiterhin jede Freiheit gelassen und nur dann ausgelöst, wenn er auch bei noch so guten Fahrfähigkeiten die Kollision nicht mehr verhindern könnte...“ (Kopischke, 2000)



Technische Machbarkeit

- Auswahl geeigneter Sensorik, Aktorik und Steuergeräte
- Grenzen der Komponenten

Motivation: Unfallschwereminderung



Radar-Objekte



Technische Machbarkeit

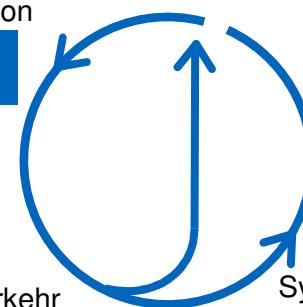
Funktionsdefinition

Produktsicherheit

Human Factors

Markt

→ Unfälle im Längsverkehr



→ Produkt: Lastenheft

Sicherheitskonzept

Validierung in
Versuchsfahrzeugen

Systemarchitektur

Package



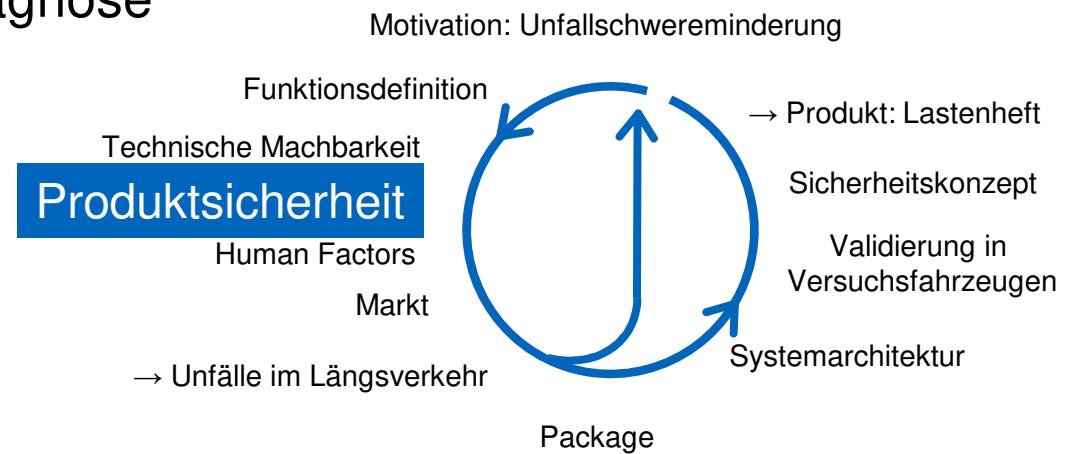
Maurer, TUBS

Produktsicherheit

- Entwicklung nach dem Stand der Technik
- Anforderungen in Funktionsdefinition berücksichtigen
- Redundante Sensorik auch für die Wahrnehmung (Gerichte suchen Analogien)?
- Kommunikation von Funktionslücken und Systemgrenzen
- Fähigkeit zur Selbstdiagnose
- Datenrekorder?

产品安全

- 根据最新技术进行开发
- 在功能定义中考虑需求
- 冗余传感器技术也用于感知（法院寻找类比）？
- 沟通功能差距和系统限制
- 自我诊断能力 动机：将事故的严重程度降至最低



Maurer, TUBS

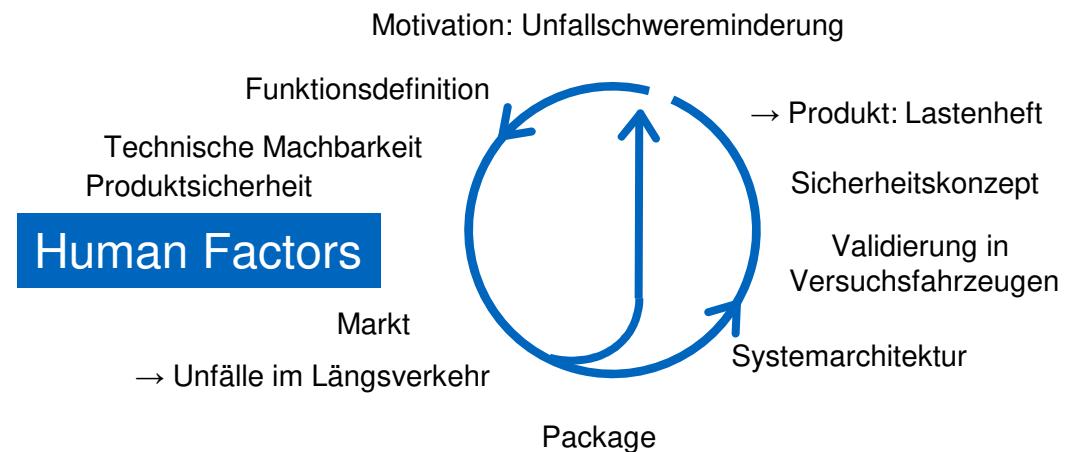
Human Factors

- Bedienbarkeit und Fehlgebrauch (Misuse)
- Verhalten an Systemgrenzen
→ Bereits in Kapiteln 6 und 7 ausführlich behandelt
- nutzertransparente Funktionsdefinition

可用性和滥用

- 系统边界行为 已在第 6 章和第 7 章中详细阐述

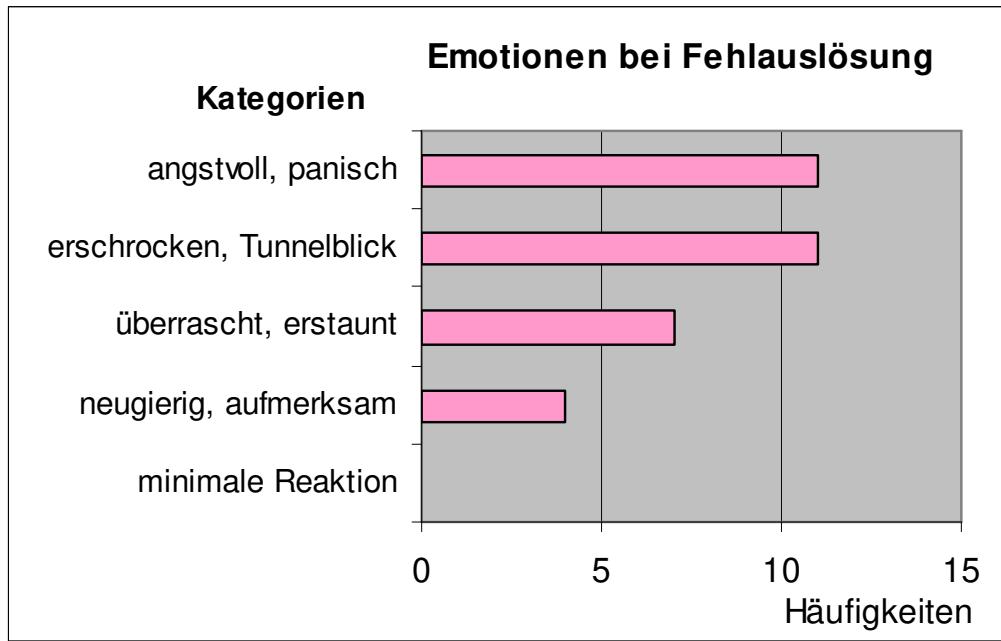
- 对用户透明的功能定义



Maurer, TUBS

Human Factors

Verhalten an Systemgrenzen



angstvoll, panisch

Färber 2003

Human Factors

Nutzertransparenz

- Welche Erwartungen hat der Kunde an das System?
 - Vermarktung/ Werbung vs. Systemauslegung
 - Häufig auch unpräzise Berichterstattung
- Was wird dem Nutzer über das HMI vermittelt?
 - Systemverständnis
 - Vermeidung von Missbrauch
- Bsp.: Tesla Autopilot



futurezone.at

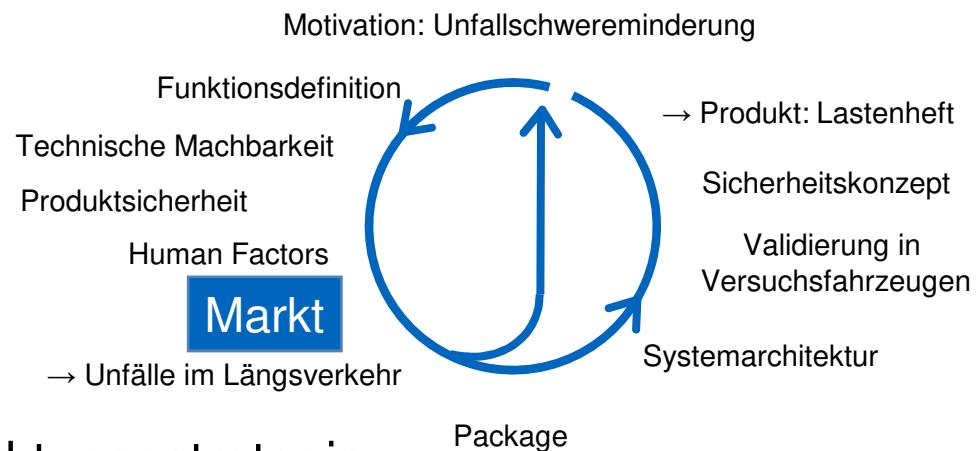
Markt

- 制定营销战略
- 评估市场机遇
- 品牌特定功能定义?
- 先于客户确定目标价格?

包装

- 用户透明功能 (适销性)
- 目标冲突: 功能与上市时间
- 目标冲突: 功能与价格

- Entwicklung einer Vermarktungsstrategie
 - Abschätzen der Marktchancen
 - markenspezifische Funktionsdefinition?
 - Zielpreis vor Kunde?
 - nutzertransparente Funktion (Vermarktbarkeit)
 - Zielkonflikt: Funktionalität versus Zeitpunkt der Markteinführung
 - Zielkonflikt: Funktionalität versus Preis

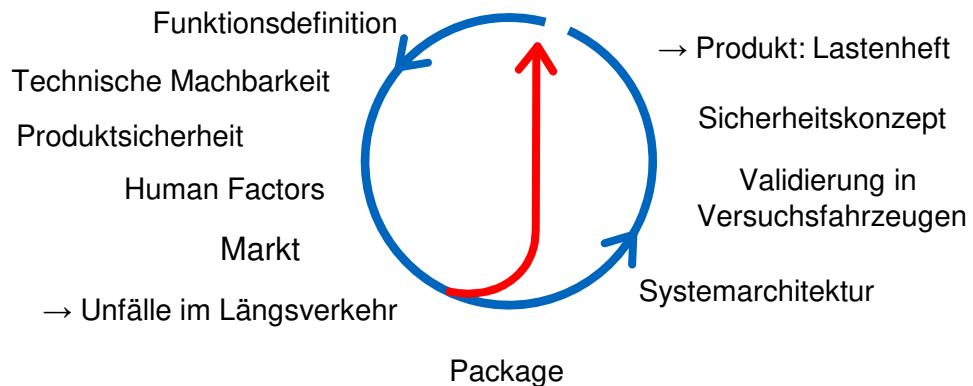


2. Iteration Nutzenanalyse

Motivation: Unfallschwereminderung

- 根据事故数据库对系统效益进行量化预测
- 评估不同的系统版本（可能的变体）：
- 有无视觉分类
- 不同的检测范围
- 不同的制动系统

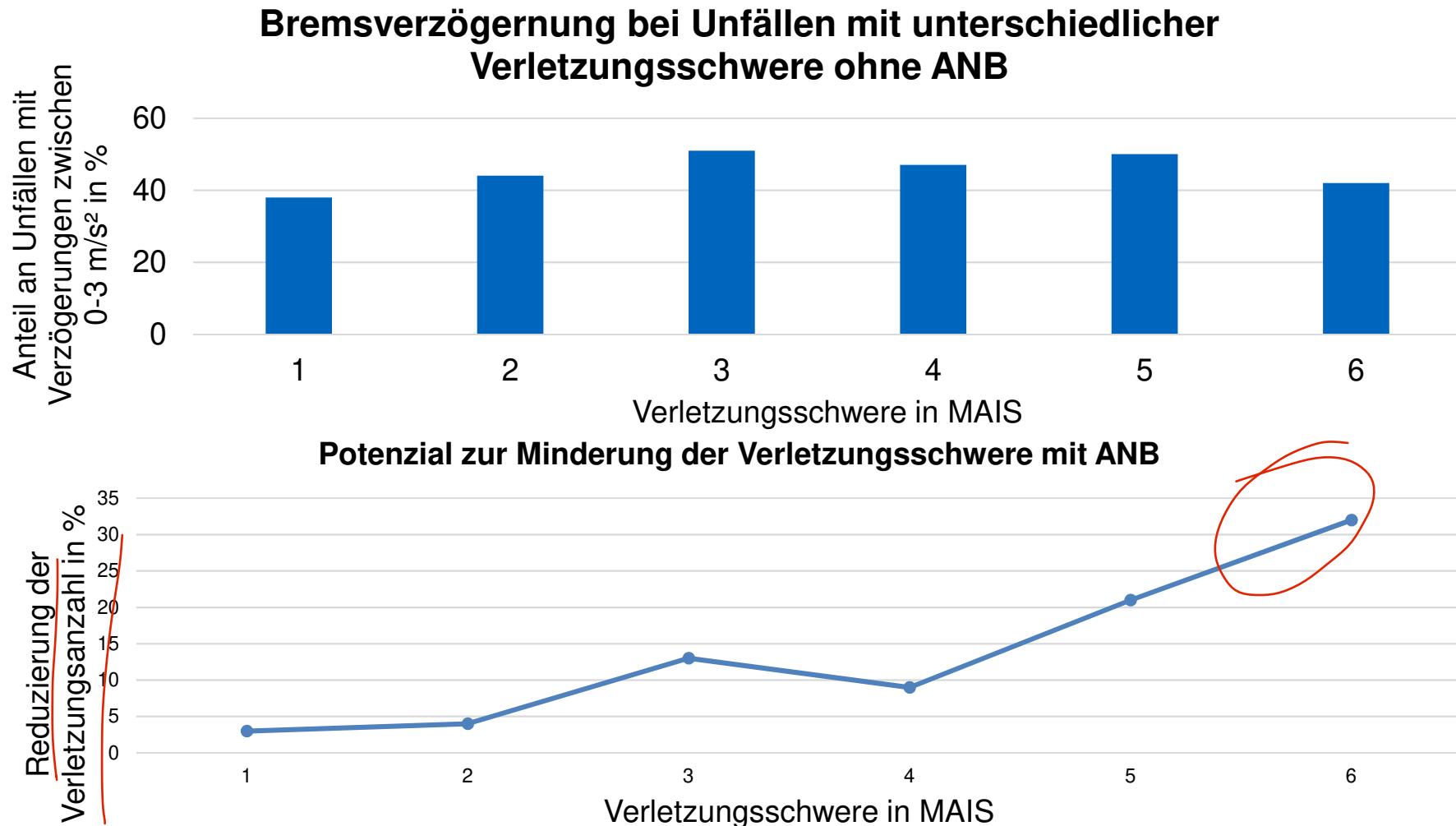
详见第 11 章



- quantitative Prognose über Nutzen des Systems aufgrund von Unfalldatenbanken
 - Bewertung unterschiedlicher Systemausprägungen (mögliche Varianten):
 - mit oder ohne visuelle Klassifikation
 - unterschiedliche Erfassungsbereich
 - unterschiedliche Bremssysteme
- Wird in Kapitel 11 ausführlich behandelt

Maurer, TUBS

Theoretisches Potenzial von ANB



nach Kopischke 2000

Einfluss der Totzeit



Automatische
Notbremse

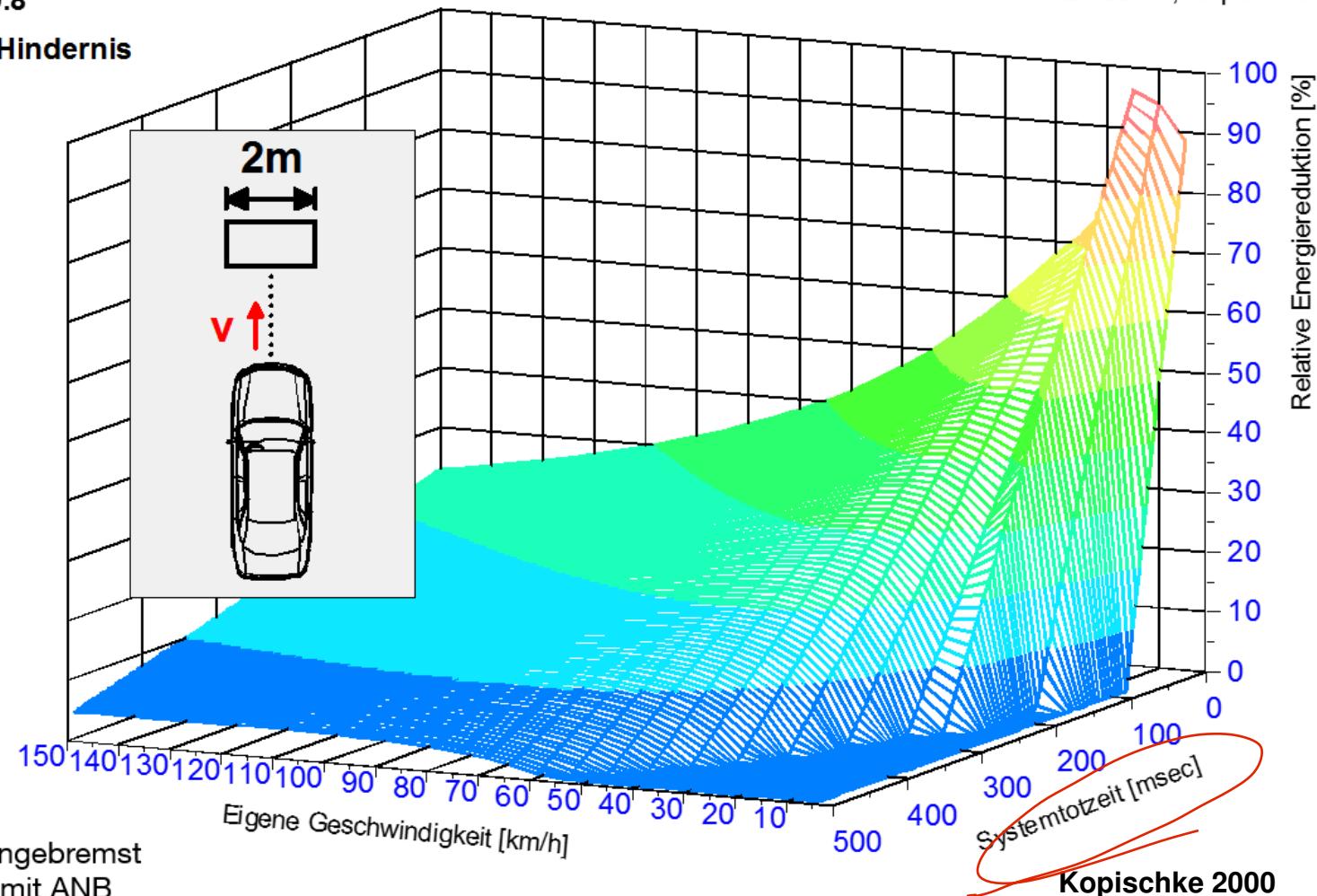
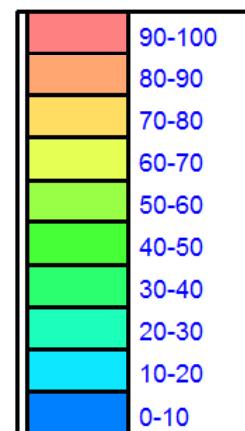
Statisches Modell

$$\mu = 0.8$$

2m Hindernis

Relative
Energiereduktion
durch ANB [%]

$$\frac{\Delta E}{E_0} = \frac{E_0 - E_{\text{koll}}}{E_0}$$



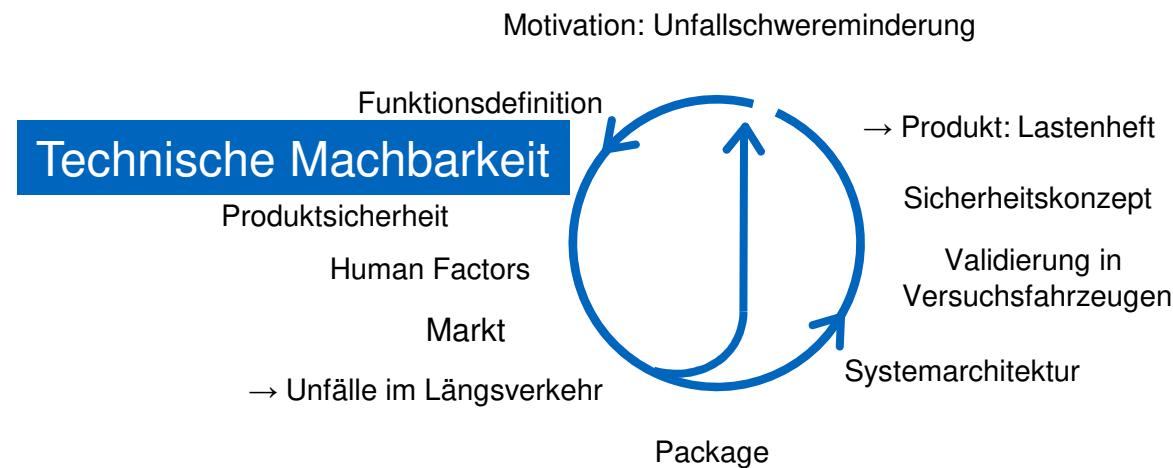
E_0 : Stoßenergie ungebremst

E_{koll} : Stoßenergie mit ANB

Datei: SkpSM14
27.08.99, Kopischke

Technische Machbarkeit

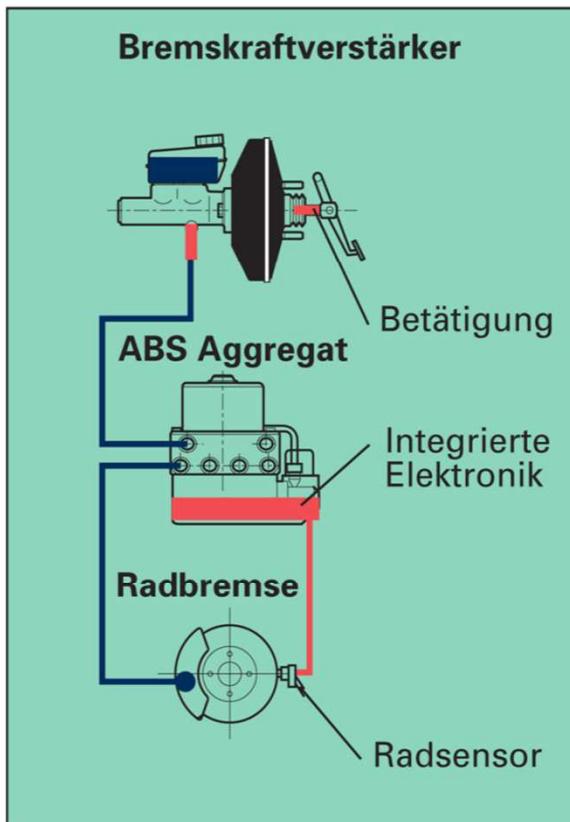
- Auswahl geeigneter Sensorik, Aktorik und Steuergeräte
- Auswahl geeigneter Wahrnehmungsalgorithmen



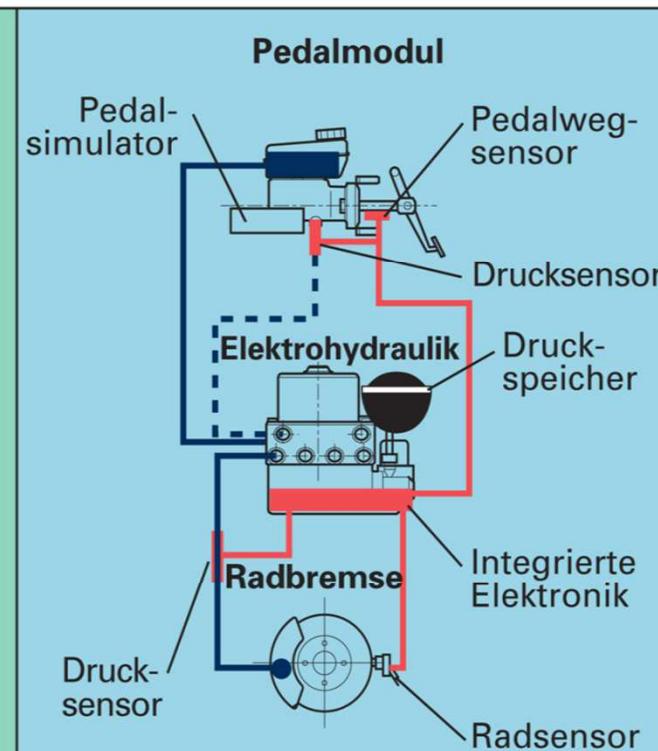
Maurer, TUBS

Technische Machbarkeit: Aktorik

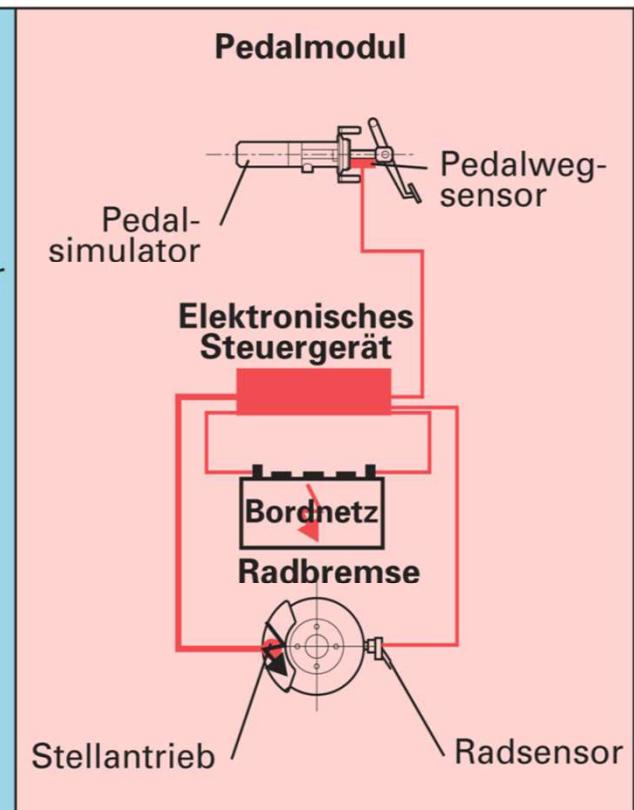
Hydraulische Bremsanlage



Elektro-Hydraulische
Bremsanlage (EHB)



Brake-by-Wire (EMB)

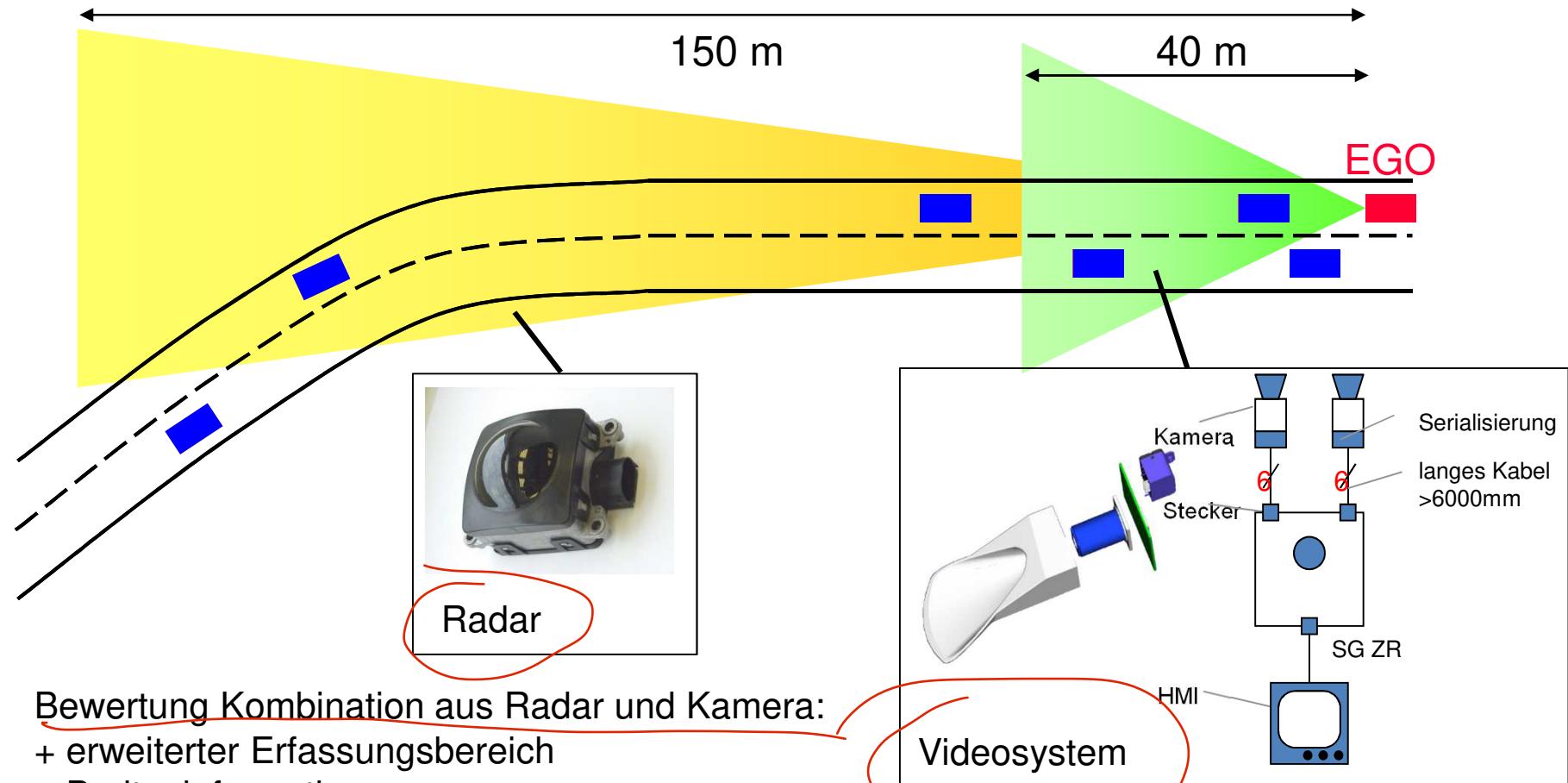


— Elektrik / Elektronik

— Hydraulik

Wörsdörfer 2000

Technische Machbarkeit: Sensorik

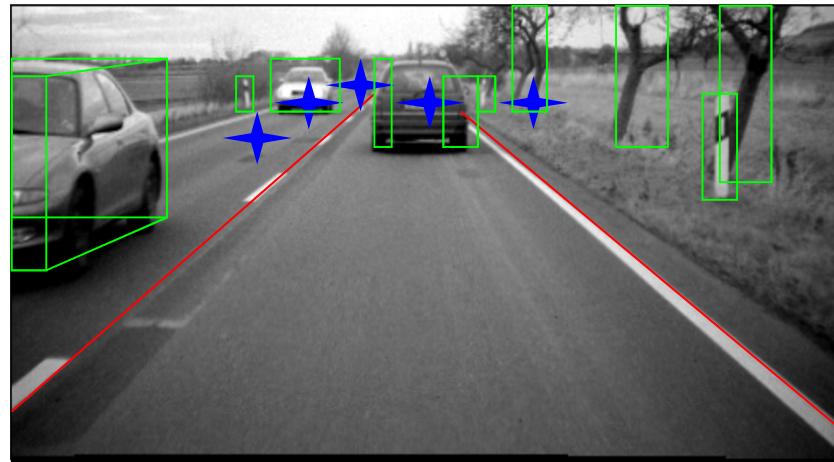


Bewertung Kombination aus Radar und Kamera:

- + erweiterter Erfassungsbereich
- + Breiteninformation
- + Fahrstreifeninformation
- + Redundanz
- höhere Kosten

Maurer, TUBS

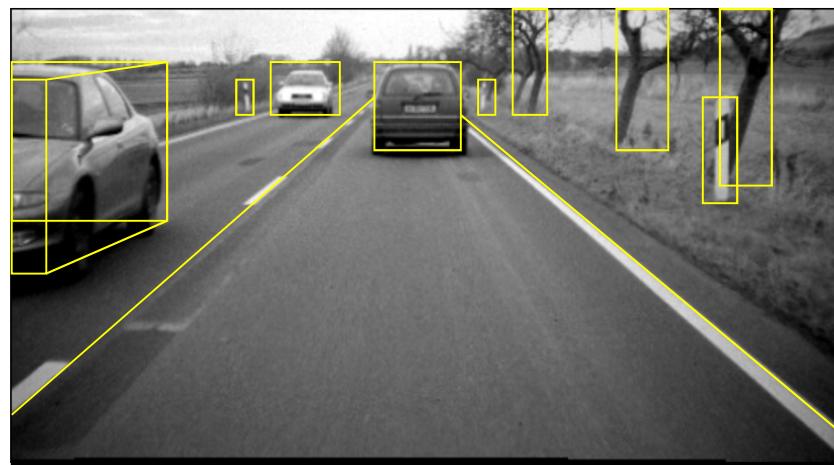
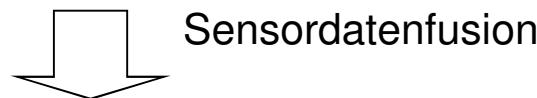
Technische Machbarkeit: Sensorik



Radar-Objekte

Video-Fahrstreifen

Video-Objekte

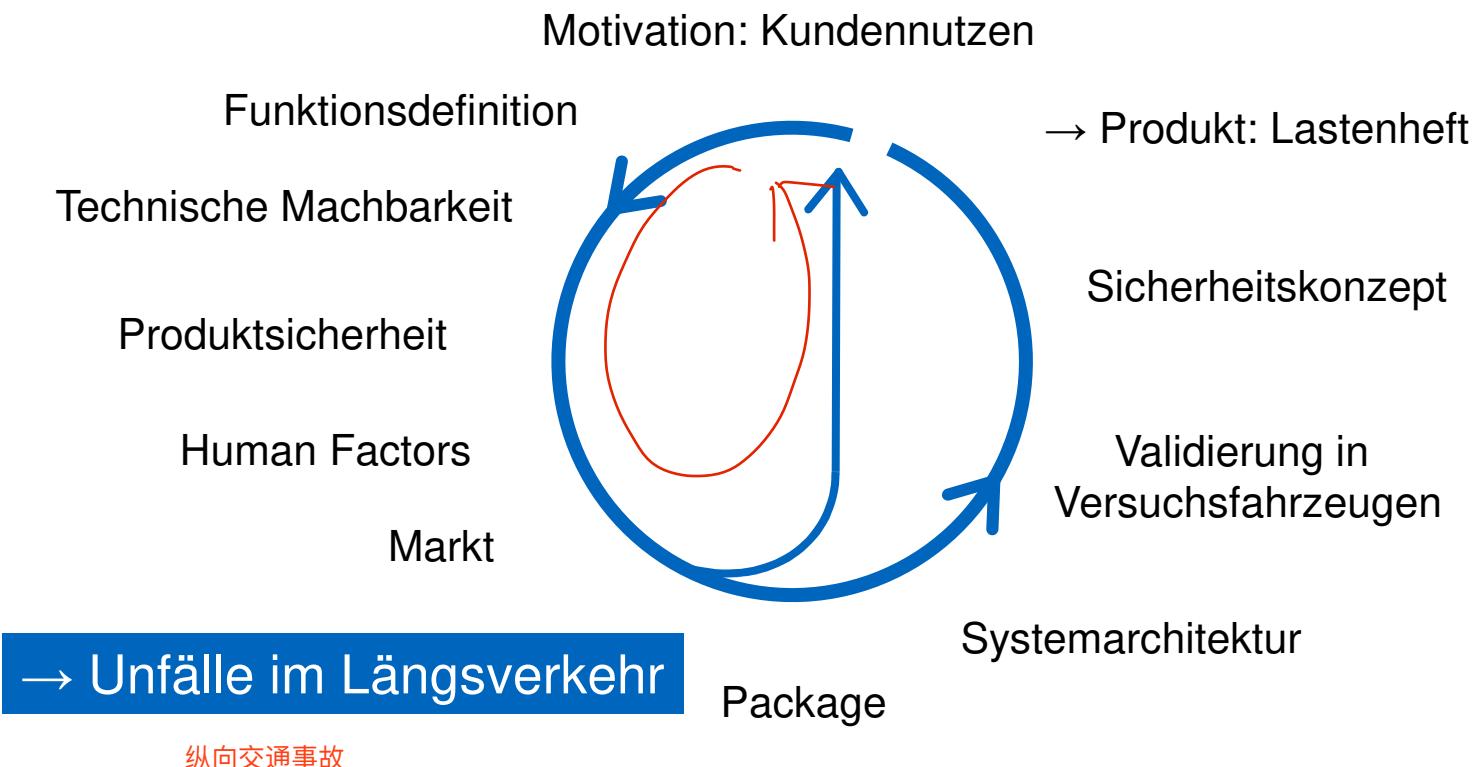


Fusions-Objekte

Maurer, TUBS

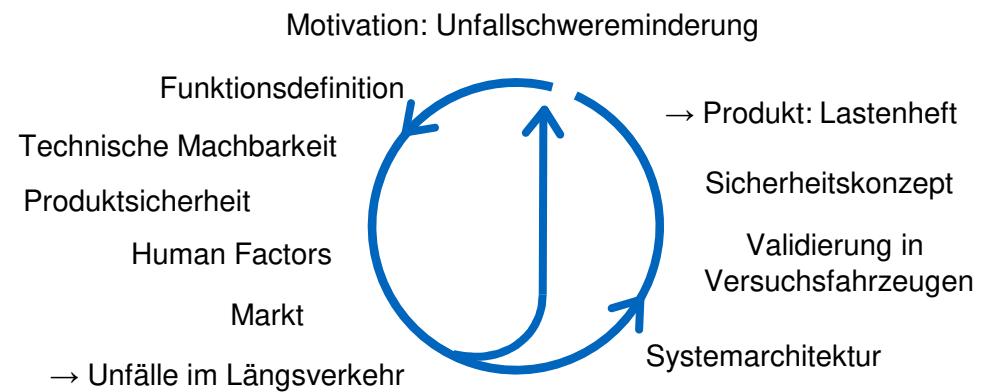
Zwischenergebnis

- optimierte Funktionsdefinition nach 2. Iteration



Package

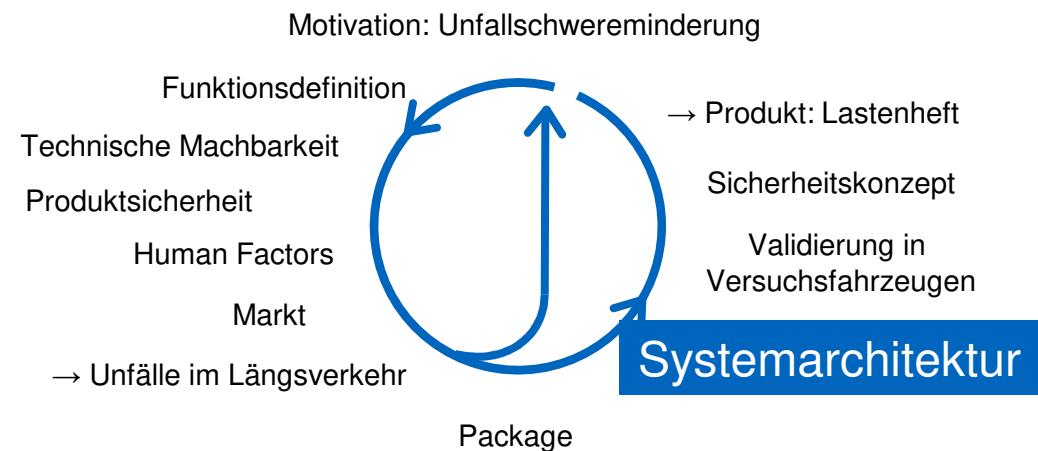
- 如果需要额外的传感器：包装
在早期阶段保持车内无安装位置
- 融入设计理念



- wenn zusätzliche Sensorik erforderlich:
Einbauorte frühzeitig im Fahrzeug freihalten
- Einbinden in das Designkonzept



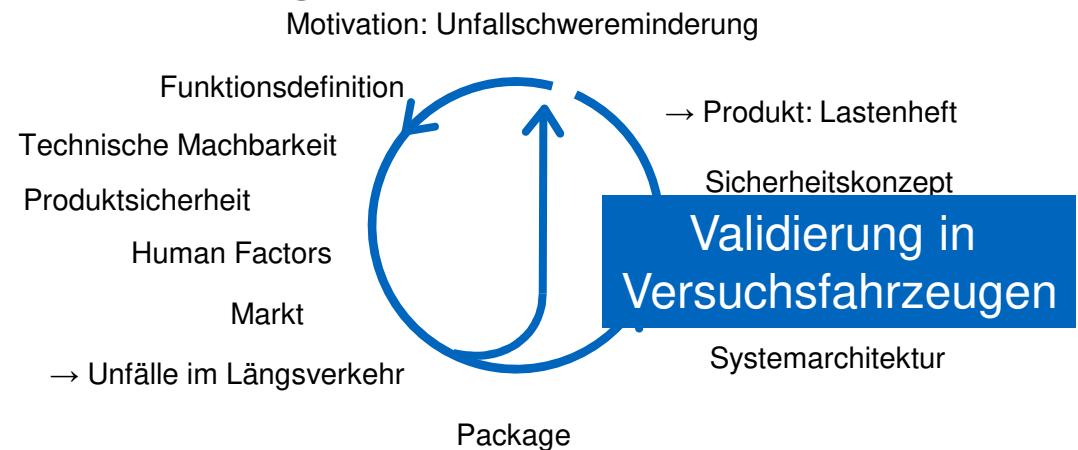
Systemarchitektur



- funktionale Systemarchitektur definieren
- Hardware und Prozessarchitektur entwickeln
- Software: Klassen, Objekte festlegen; Hierarchie und Verhalten definieren

- 定义功能系统架构
- 开发硬件和流程架构
- 软件: 定义类、对象; 定义层次结构和行为

Validierung in Versuchsfahrzeugen



- Validieren der Funktionsdefinitionen in Versuchsfahrzeugen
- Testkonzepte für Absicherung entwickeln (Wahrscheinlichkeit für Fehlauslösungen)

- 验证测试车辆的功能定义
- 开发验证测试概念 (误触发概率)

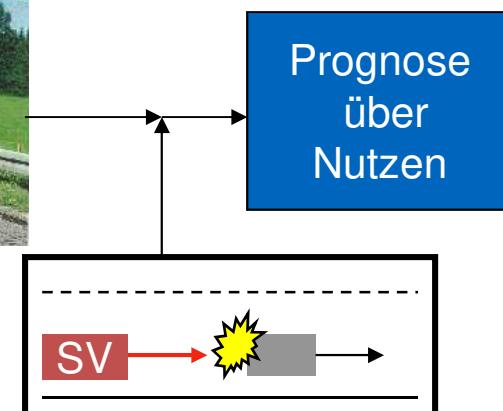
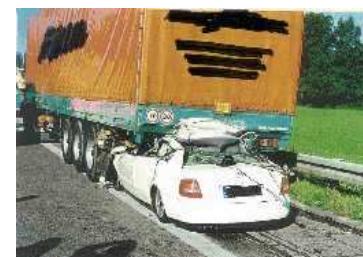
Testverfahren für Validierung ANB

Validierung in der Entwicklungsphase

Auslösetests mit Versuchsfahrzeugen...



... und in der Simulation

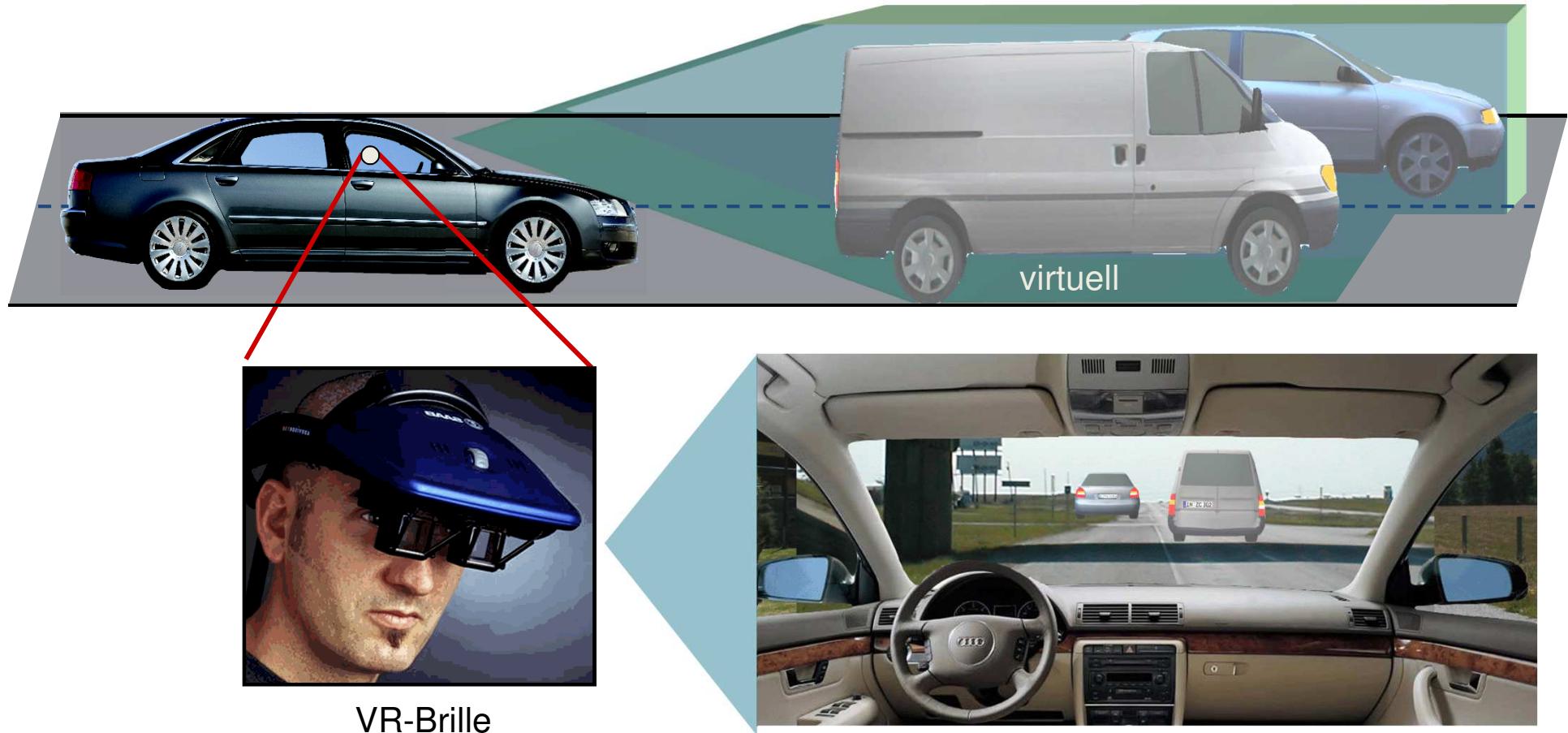


ANB: Fire-Tests



Testumgebung für Collision-Mitigation-Systeme

Vehicle-in-the-Loop-Prüfaufbau



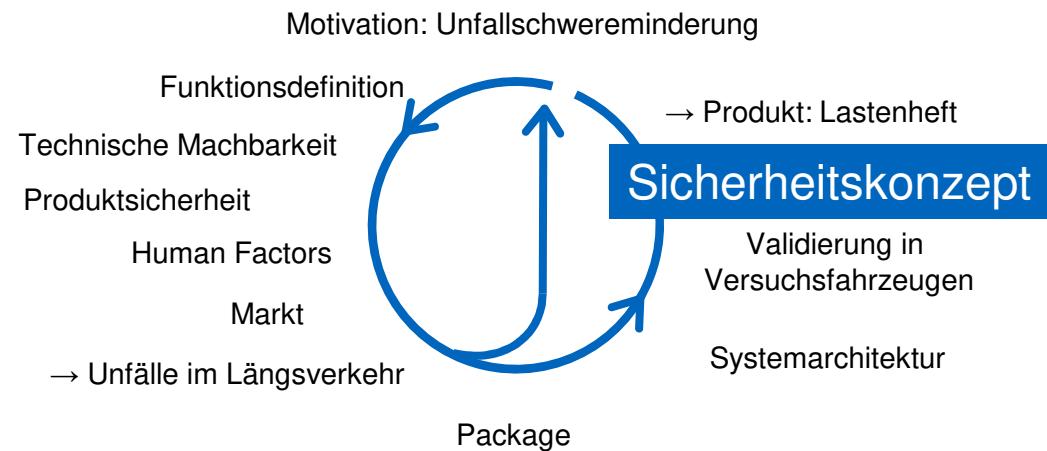
Erprobung und Abstimmung von FAS

NoFire-Test im öffentlichen Straßenverkehr



Sicherheitskonzept

- 安全包括使用安全和功能安全
 - 危害和风险分析:
 - 识别危险, 执行 FTA、FMEA、STPA
 - 确定安全目标
 - 创建安全概念
- 将在本章第二部分详细介绍



- Sicherheit umfasst Gebrauchssicherheit und Funktionale Sicherheit
 - Gefahren- und Risikoanalyse:
 - Hazards (Gefahren) identifizieren, FTA, FMEA, STPA durchführen
 - Sicherheitsziele definieren
 - Sicherheitskonzepte erstellen
- Wird im zweiten Teil dieses Kapitels ausführlich behandelt

Gefahren (Hazards) der ANB

例如

- 未经授权的触发:

在人类观察员认为不适当的情况下发生

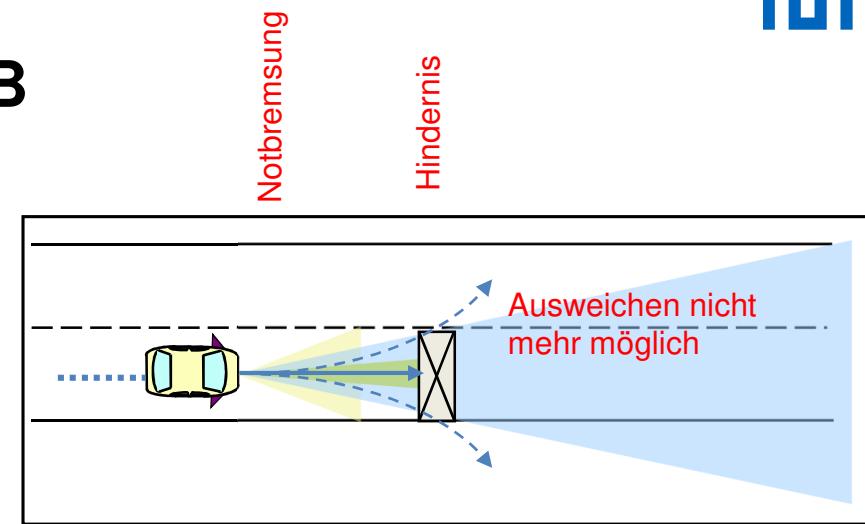
- 缺乏触发:

虽然人类观察者认为有必要，但不触发

Beispielsweise:

- unberechtigte Auslösung:
erfolgt, ohne dass ein menschlicher Beobachter sie für angemessen hält

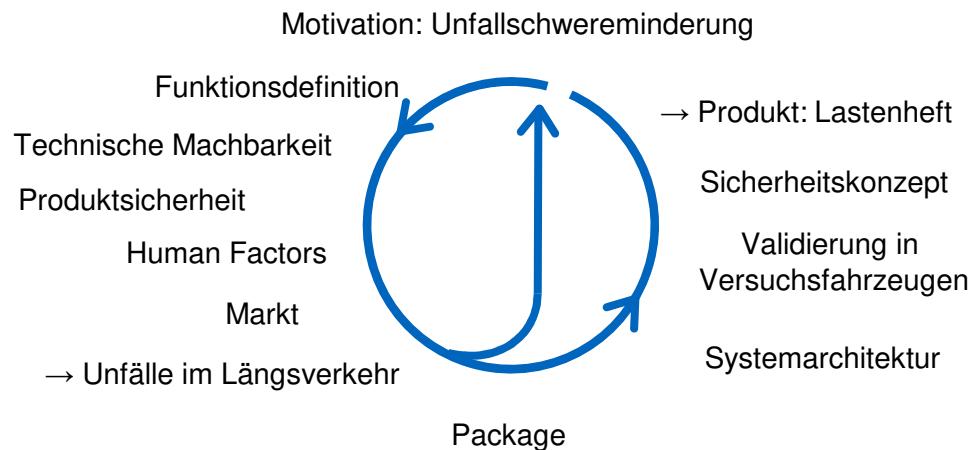
- fehlende Auslösung:
erfolgt nicht, obwohl ein menschlicher Beobachter sie für erforderlich hält



Kopischke 2000

Fazit

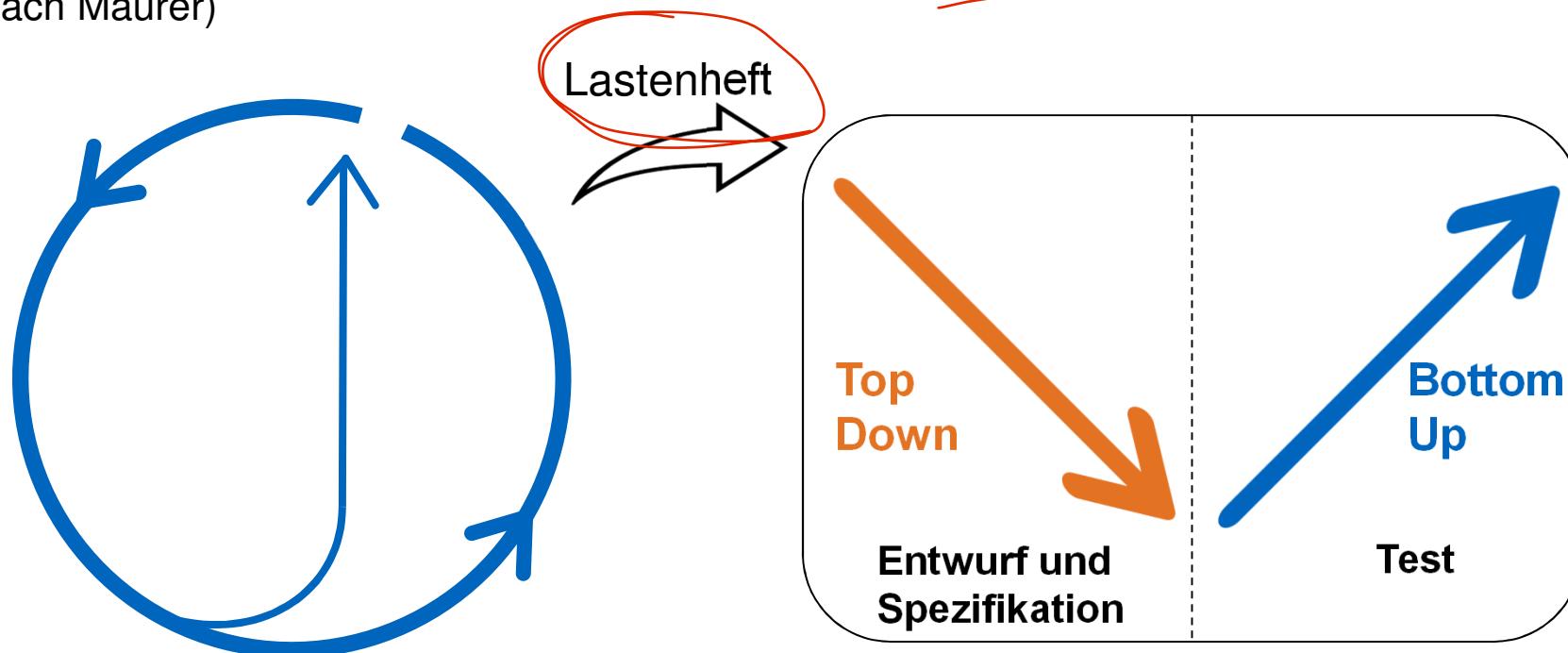
- 在概念阶段支持采用系统方法:
 - 以客户为导向的系统设计
 - 市场化系统的系统设计
 - 识别设计冲突
 - 客观讨论设计冲突 风险效益评估
- 安全系统的开发过程



- Systematische Vorgehensweise in der Konzeptphase unterstützt:
 - kundenorientierten Systementwurf
 - Systementwurf marktfähiger Systeme
 - Identifikation von Auslegungskonflikten
 - sachliche Diskussion der Auslegungskonflikte
 - Risiko-Nutzen-Abschätzung
- Entstehungsprozess von Sicherheitssystemen

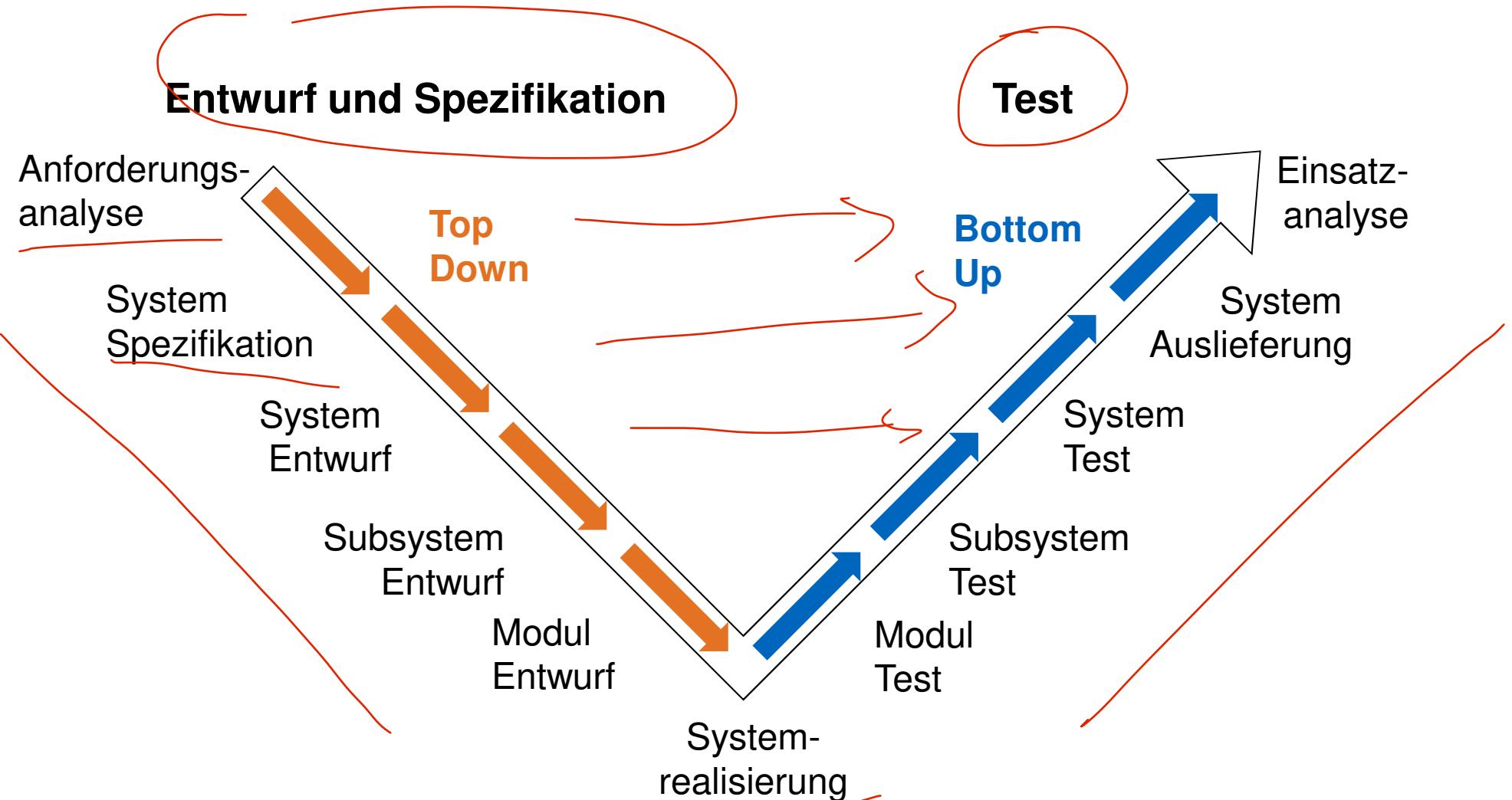
Übernahme der Erkenntnisse in Serienentwicklungsprozess

Systematischer Entwurf von FAS
(Nach Maurer)



Reichel 2013

Entwicklungsmodell: V-Modell



**Entwicklungsprozess und
Funktionale Sicherheit
Dr.-Ing Frank Diermeyer
(Simon Hoffmann, M.Sc.)**

Agenda

10 Entwicklungsprozess und funktionale Sicherheit

 10.1 Entwicklungsprozess

 10.2 Funktionale Sicherheit

 10.2.1 Sicherheit und Risiko

 10.2.2 ISO 26262



Sicherheit von technischen Systemen

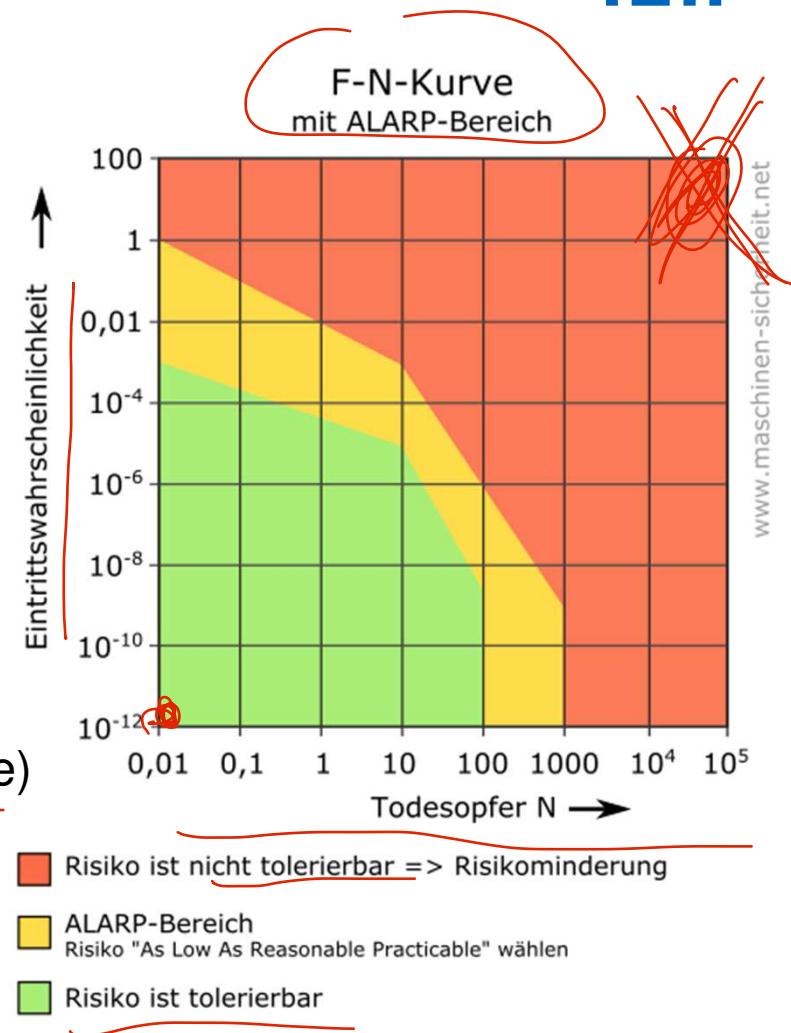
- Was bedeutet Sicherheit?
 - „Safety: absence of unreasonable risk“ [ISO 26262]
- Risiko muss unter einem Grenzwert bleiben
 - „Risk: combination of the probability of occurrence of harm and the severity of that harm“ [ISO 26262]
- Verschiedene Teilespekte müssen betrachtet werden
 - Funktionale Sicherheit [ISO 26262]
 - Gebrauchssicherheit (SOTIF: Safety of the intended functionality) [ISO/PAS 21448]
 - Angriffssicherheit (Cyber Security) [ISO/SAE 21434]

Normen im Automotive Bereich

Functional Safety ISO 26262	SOTIF ISO/PAS 21448	Cyber Security ISO/SAE 21434 oder SAE J3061
<p>Ziel: Vermeiden von Gefahren welche durch das <u>Versagen</u> von E/E Systemen entstehen.</p> <p>避免 E/E 系统故障造成的危害。</p> <p>Beispiel:</p> <ul style="list-style-type: none">• Ausfall Radar Sensor• Fehler im Hydraulikaggregat (ESP)	<p>Ziel: Vermeiden von Gefahren welche durch bei bestimmungsgemäßen Gebrauch oder zu erwartendem Fehlgebrauch auftreten.</p> <p>Beispiel:</p> <ul style="list-style-type: none">• LiDAR Auflösung nicht ausreichend für Fußgänger• Fahrer verletzt Überwachungspflicht	<p>Ziel: Vermeiden von Gefahren welche durch <u>Cyber Angriffe</u> entstehen.</p> <p>Beispiel:</p> <ul style="list-style-type: none">• Zugriff auf Aktorik über Fahrzeug WLAN <p>ISO/SAE 21424 aktuell nur als Draft verfügbar. Finale voraussichtlich ab Mitte 2021.</p>

Risikoreferenz und -akzeptanz

- As low as Reasonably Practicable (ALARP)
 - Vertretbare Risikoreduktionsmaßnahmen müssen ergriffen werden
- Globalement Au Moins Aussi Bon (GAMAB)
 - Mindestens gleiche Sicherheit (wie vergleichbare bestehende Systeme)
- Minimum Endogenous Mortality (MEM)
 - Sterberate durch technische Systeme darf nicht über normaler Sterblichkeitsrate liegen
- Sicherheitsnormen mit Empfehlungen für Fehlerraten



Alternativer Lösungsansatz für neue Systeme

Lösungsansatz für Systeme mit erhöhter Fehlerwahrscheinlichkeit aus der Wirtschaftsethik

- Kernaussage: Ein System mit erhöhter Fehlerwahrscheinlichkeit ist dann konsensfähig, wenn die Individuen „größere Vorteile erwarten können als vom alten System“.→ Sinkt der Erwartungswert eines Schadensfalles durch das Sicherheitssystem und entsteht gleichzeitig ein weit geringeres Risiko für einen anderen Schadensfall gleicher Schwere, so kann der Einzelne der neuen Regelung zustimmen.
- Risikominderung der Hersteller durch Fonds (Versicherungen, Hersteller)

新系统的替代解决方案

针对因商业道德而增加出错概率的系统的解决方法

- 核心提示：如果个人能够期望 "从旧系统中获得更大的好处"，那么出错概率增加的系统就能够达成共识。

如果安全系统降低了损失事件的预期值，同时发生同样严重程度的另一损失事件的风险大大降低，那么个人就会同意新系统。

- 通过基金（保险公司、制造商）使制造商的风险最小化

Homann 2005

Alternativer Lösungsansatz

Beispiel Sicherheitssystem

假设

- 安全系统每年可避免 10^*x 人死亡
- 然而，该安全系统每年会造成额外 x 人死亡
- 在所有车辆都配备该安全系统的情况下，个人受到伤害的预期值会降低，社会中的所有个人都会同意
- 与 "保险业（作为社会的代理人）、汽车协会、政府、TÜV、消费者保护组织" 进行公开交流与合作

- Annahmen:
 - Ein Sicherheitssystem verhindert 10^*x Todesfälle im Jahr
 - Dieses Sicherheitssystem verursacht aber zusätzlich x Todesfälle im Jahr
- der Erwartungswert sinkt, dass der Einzelne in einem Szenario, in dem alle Fahrzeuge mit diesem Sicherheitssystem ausgerüstet sind, geschädigt wird
→ zustimmungsfähig für alle Einzelnen in der Gesellschaft
- offene Kommunikation und Zusammenarbeit mit „Versicherungswirtschaft (als Agent der Gesellschaft), Automobilverbänden, Staat, TÜVs, Verbraucherschutzorganisationen“

**Entwicklungsprozess und
Funktionale Sicherheit
Dr.-Ing Frank Diermeyer
(Simon Hoffmann, M.Sc.)**

Agenda

10 Entwicklungsprozess und funktionale Sicherheit

 10.1 Entwicklungsprozess

 10.2 Funktionale Sicherheit

 10.2.1 Sicherheit und Risiko

 10.2.2 ISO 26262



Funktionale Sicherheit: ISO 26262

Betrachtet Gefahren aufgrund von Systemfehlern

- “functional safety: absence of unreasonable risk due to hazards caused by malfunctioning behaviour of E/E systems” [ISO26262]
- ISO 26262: Road vehicles – Functional safety
 - INTERNATIONAL STANDARD
 - Scope: Funktionale Sicherheit von E/E-Komponenten in Serienfahrzeugen
 - Spezialisierung der IEC 61508 für den Automobilbereich: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems

→ Damit für alle Serienfahrerassistenzsysteme relevant

Systementwicklung nach ISO 26262

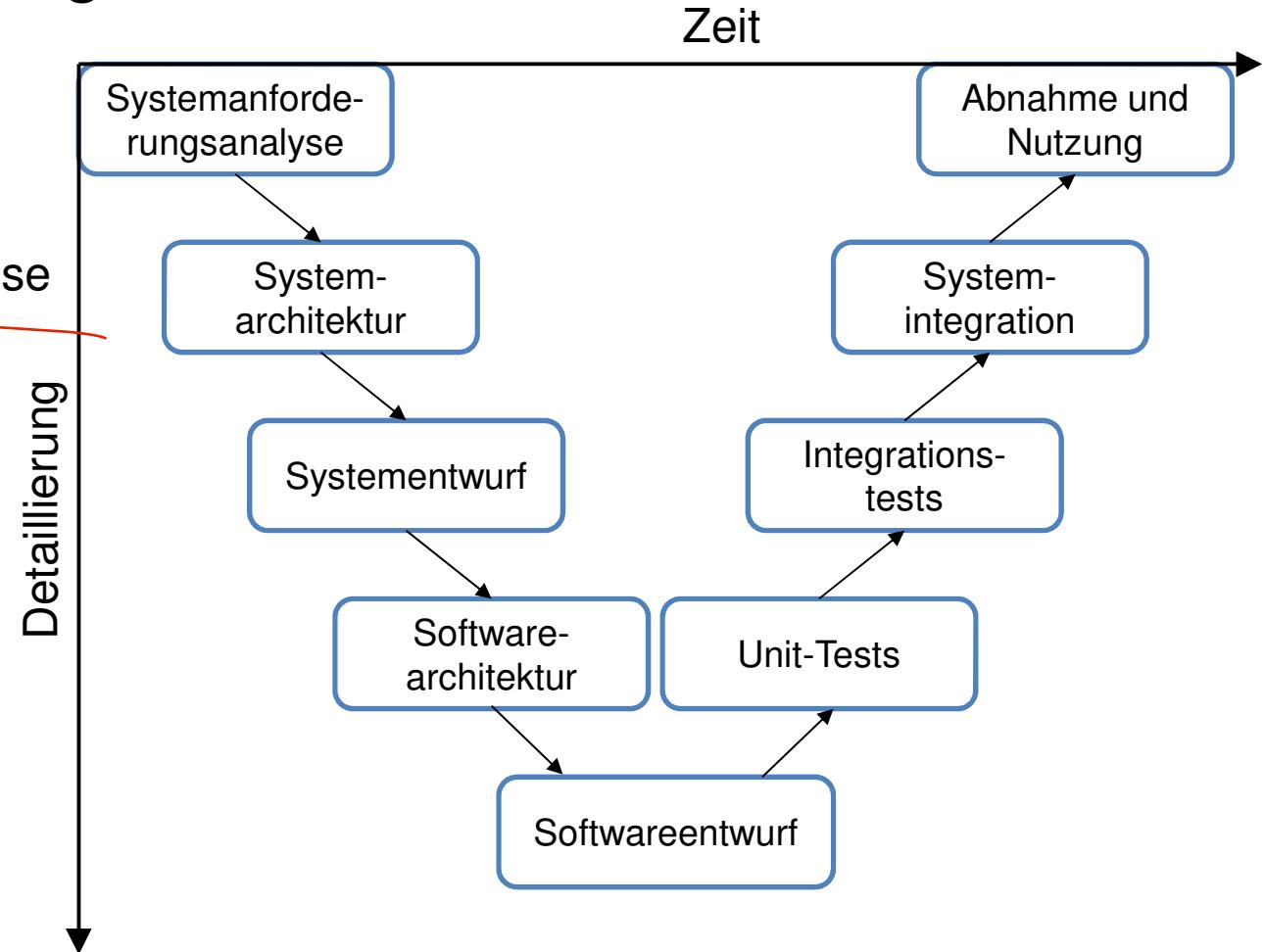
ISO 26262 spezifiziert

- Entwicklungsprozesse
- Anforderungen

Jeweils für

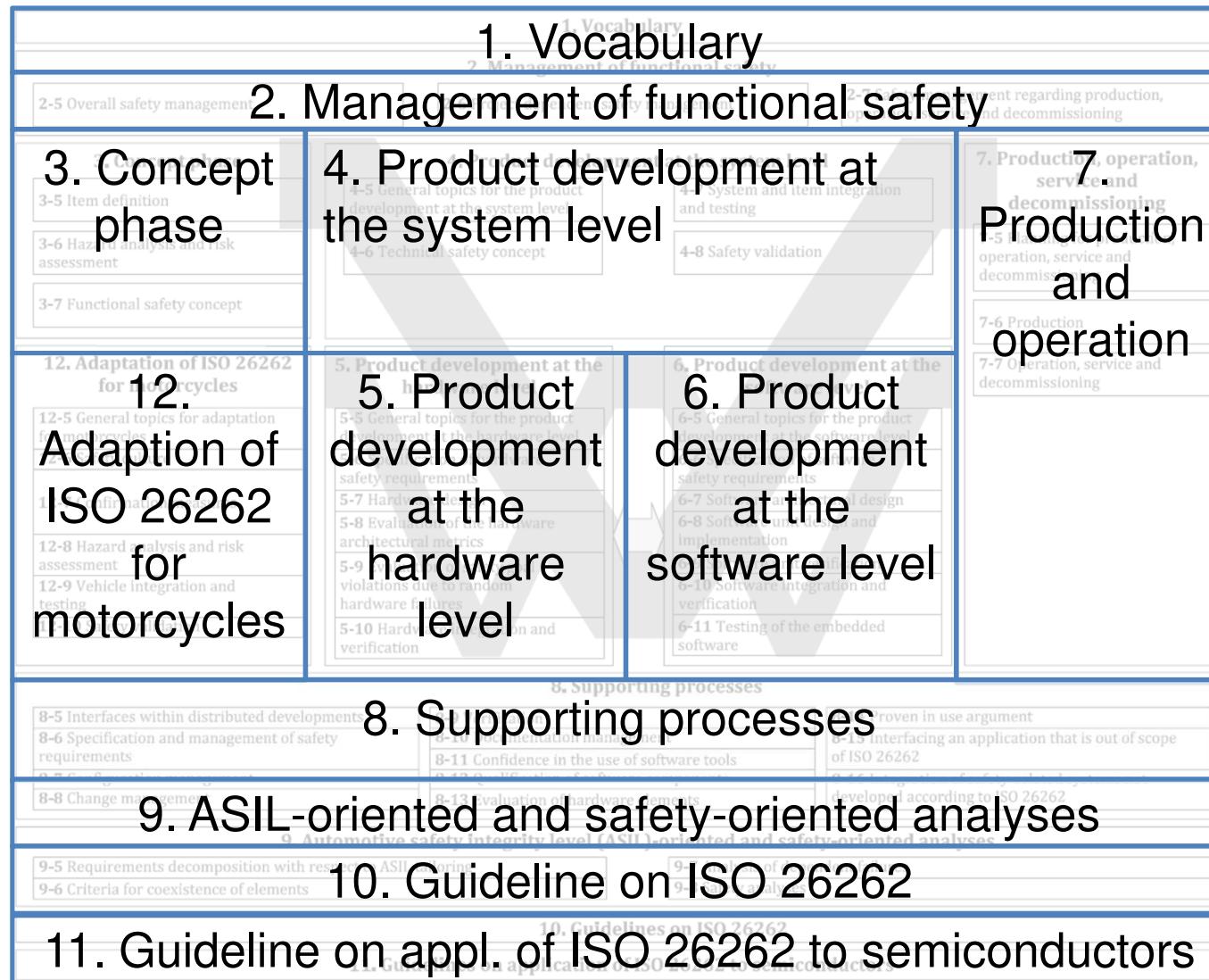
- Systemebene
- Hardwareebene
- Softwareebene

in Anlehnung an
geschachtelte
V-Modelle



Giesler, Audi

ISO 26262 – Übersicht



Management of functional safety

- Allgemeine Managementstrukturen
 - Safety culture
 - Competence management
 - Quality Management
- Safety management in der Konzeptphase
 - Benennung safety manager: plant und überwacht safety activities
 - Confirmation measures: reviews, functional safety audits and assessments, je nach ASIL Unabhängigkeit der Bewerter
- Safety management nach SOP
 - 一般管理结构
 - 安全文化
 - 能力管理
 - 质量管理
 - 概念阶段的安全管理
 - 任命安全经理：计划和监督安全活动
 - 确认措施：审查、功能安全审计和评估，取决于 ASIL 评估人员的独立性
 - 根据 SOP 进行安全管理

Konzeptphase

- Item Definition (Item: System um eine Funktion auf Fahrzeugebene umzusetzen)
- Initiation of the safety life cycle
- Hazard analysis and risk assessment (Gefährdungs- und Risikoanalyse (G&R))
- Safety concept (Sicherheitskonzept)

概念阶段

- 项目定义 (项目: 在车辆层面实现功能的系统)
- 启动安全生命周期
- 危害分析和风险评估 (G&R)
- 安全概念

- 项目：在车辆层面实现某项功能的系统或系统阵列，适用 ISO 26262 标准
- 项目的定义和描述
- 功能和非功能要求（系统状态、限制、法律要求、已知故障模式）
- 系统边界和接口（系统要素、依赖关系以及与环境和其他项目的交互关系）
- 项目定义必须为 ISO26262 的以下阶段提供足够的项目信息

Item Definition

- **Item:** system or array of systems to implement a function at the vehicle level, to which ISO 26262 is applied
- Definition und Beschreibung des Items
 - Funktionale und nichtfunktionale Anforderungen (Systemzustände, Einschränkungen, rechtliche Anforderungen, bekannte Ausfallarten)
 - Systemgrenzen und Schnittstellen (Elemente des Systems, Abhängigkeiten und Interaktionen mit der Umwelt und anderen Items)
- Item Definition muss ausreichend Informationen über das Item für die folgenden Phasen der ISO26262 bereitstellen

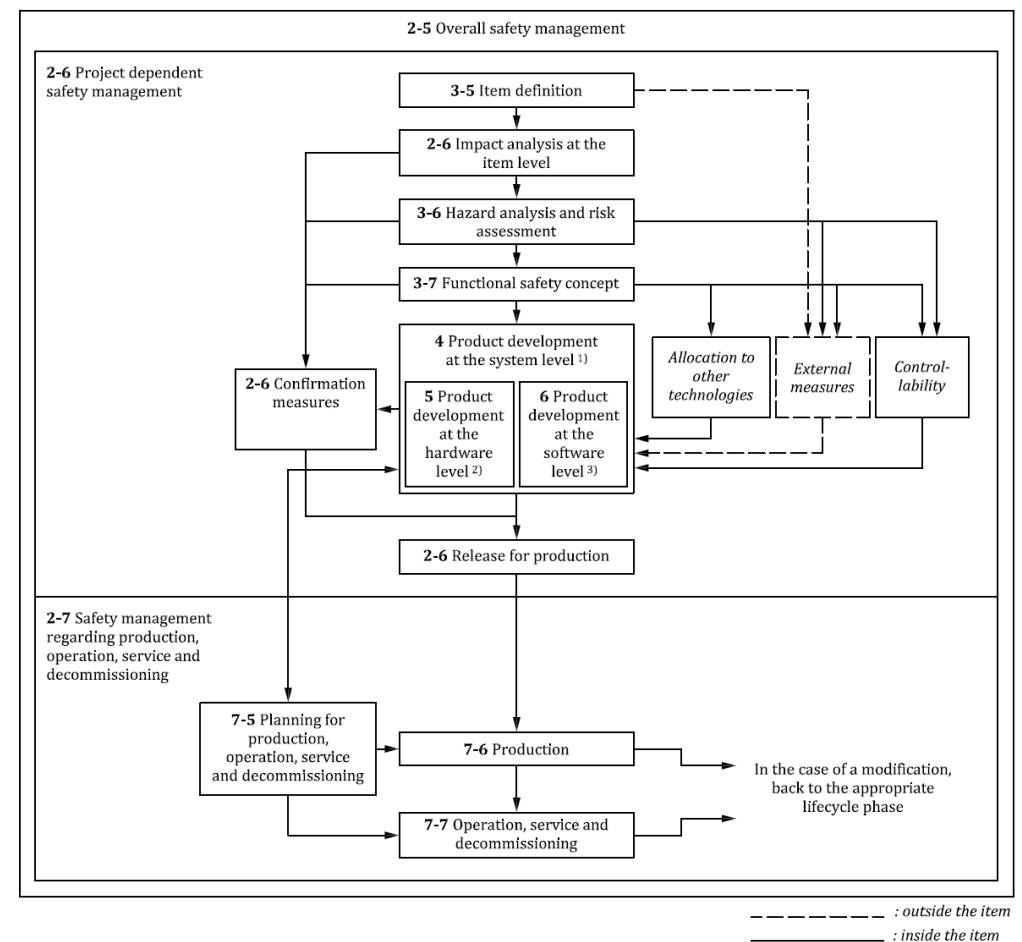
Bsp: Fahrerairbag im Lenkrad mit Auslöseeinheit (inkl. Sensoren)

- Elemente: Sensoren, Übertragung, Auslöseeinheit, Airbag
- Anforderung: Auslösung nur bei Crash (Auslösung zu definieren)
- ...

Initiation of the safety life cycle

- Unterscheidung: neues Item oder modifiziertes Item
- Bewertung ob safety life cycle bei Modifikation reduziert werden kann

- 区别: 新项目或修改后的项目
- 评估是否可以通过修改缩短安全寿命周期



Hazard analysis and risk assessment

目标

- 系统识别和评估系统的潜在危害和风险

方法

- 确定系统的主要功能并识别潜在故障
- 确定可能发生故障的相关情况
- 量化在相关情况下发生故障所产生的危害和风险

备注

- 情况选择不得导致 ASIL 降低（由于考虑过于详细）
- 独立于安全概念的考虑 G&R 是安全概念的基础

▪ Zielsetzung

- Systematische Ermittlung und Bewertung potenzieller Gefahren und Risiken eines Systems

▪ Methodik

- Definition der Hauptfunktionen des Systems und Ermittlung der potenziellen Fehlfunktionen
- Ermittlung der relevanten Szenarien, in denen die Fehlfunktionen auftreten können
- Quantifizierung der Gefahren und Risiken, die sich durch das Auftreten der Fehlfunktionen in den relevanten Szenarien ergeben

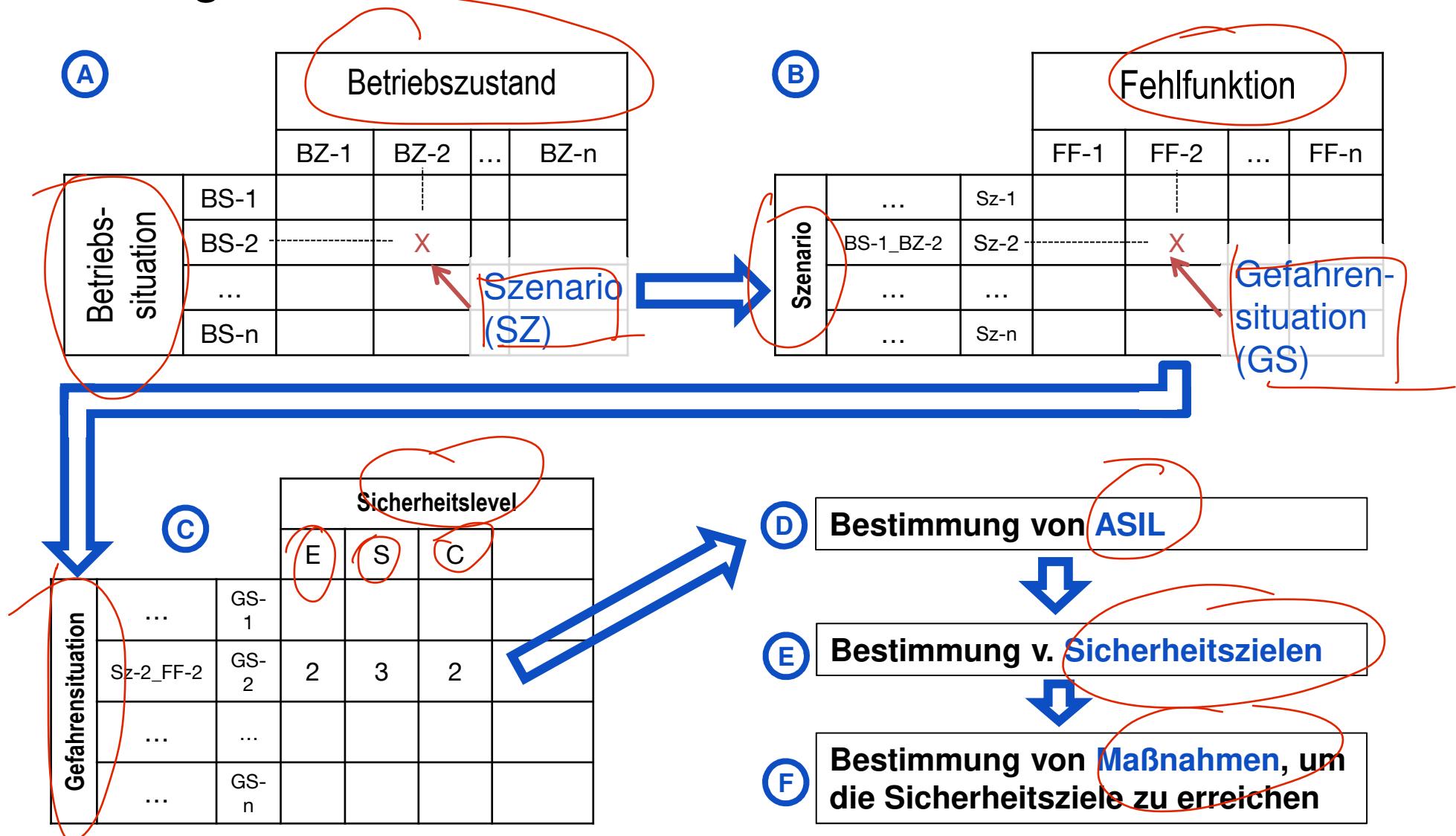
▪ Anmerkung

- Situationsauswahl darf nicht zu ASIL-Reduktion führen (durch zu detaillierte Betrachtung)
 - Betrachtung unabhängig vom Sicherheitskonzept
- G&R ist Grundlage für das Sicherheitskonzept

G & R nach ISO 26262

1. Basiert auf Item Definition
Interne Sicherheitsmechanismen werden nicht berücksichtigt
2. Identifizieren aller Betriebszustände und -modi des Gesamtsystems (=Kundenfunktionen)
3. Identifizieren aller Betriebssituationen, in denen sich das Item befinden kann
4. Systematische Identifikation aller Fehlfunktionen
 - auf Fahrzeugebene
 - Techniken: Brainstorming, Checklisten, FMEA, Feldstudien
5. Gefährliche Situationen als Kombination aus Fehlfunktion und Betriebssituation
6. Klassifizierung des gefährlichen Events: Bewertung der Schwere, Exposition und Kontrollierbarkeit
7. Bestimmung der ASIL für jedes gefährliche Ereignis
8. Festlegung von Sicherheitszielen

Vorgehensweise – Schema



Bewertungskriterien

Exposure (Häufigkeit der Situation)

Klasse	E0	E1	E2	E3	E4
Beschreibung	Unvorstellbar	Sehr niedrige Wahrscheinlichkeit	Niedrige Wahrscheinlichkeit	Mittlere Wahrscheinlichkeit	Hohe Wahrscheinlichkeit

Severity (Schwere eines möglichen Schadens)

Klasse	S0	S1	S2	S3
Beschreibung	Keine Verletzung	Leichte und mittlere Verletzung	Schwere Verletzung – Überleben wahrscheinlich	Lebensgefährliche Verletzung – Überleben unwahrscheinlich

Controllability (Beherrschbarkeit durch Benutzer/Person)

Klasse	C0	C1	C2	C3
Beschreibung	Im Allgemeinen beherrschbar	Einfach beherrschbar	Normalerweise beherrschbar	Schwierig oder nicht beherrschbar

ASIL Bestimmungstabelle

S	E	C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Sicherheitsziele

安全目标

- 为每个与 ASIL 相关的危险事件定义至少一个安全目标
- 安全目标的 ASIL = 指定危险事件的最大 ASIL

示例：安全气囊：

- 情景：在乡村道路上手动驾驶
- 故障：不合理展开，未发生碰撞
- 危险事件：驾驶员在手动驾驶过程中因启动而失控
- 暴露程度 E4（任何驾驶），严重程度 S3（与迎面而来的车辆、基础设施……相撞），可控性 C3（通常无法控制）
ASIL D
- 安全目标：必须防止安全气囊无故展开。

- Für jedes ASIL-behaftete gefährliche Ereignis mindestens ein Sicherheitsziel definieren
- ASIL des Sicherheitsziels = max. ASIL der zugeordneten gefährlichen Ereignisse

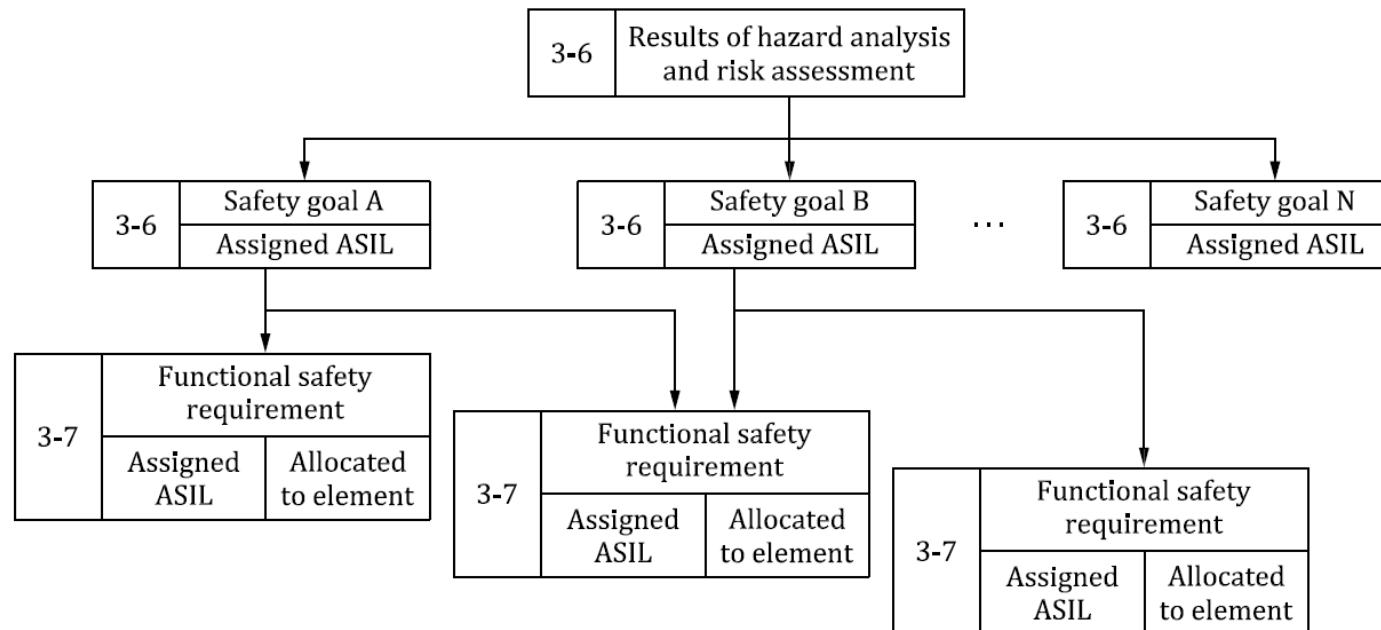
Beispiel Airbag:

- Szenario: manuelle Fahrt auf Landstraße
- Fehlfunktion: unbegründete Auslösung ohne Crash
- Gefährliches Ereignis: Fahrer verliert Kontrolle aufgrund Auslösung bei manueller Fahrt
- Exposure E4 (beliebige Fahrten), Severity S3 (Kollision mit Gegenverkehr, Infrastruktur ...), Controlability C3 (normal nicht beherrschbar) → ASIL D
- Sicherheitsziel: das unbegründete Auslösen des Airbags muss verhindert werden.

- 从安全目标推导出功能安全要求
- 为功能架构元素分配要求

Funktionales Sicherheitskonzept

- Funktionale Sicherheitsanforderungen aus Sicherheitszielen ableiten
- Anforderungen an funktionale Architekturelemente zuweisen



Beispiel Fahrerairbag

- Sicherheitsziel: Airbag darf nicht unbegründet auslösen (ASIL D)
- Sicherheitskonzept: redundanter Auslösemechanismus
- Sicherheitsanforderungen:
 - Auslösung nur, wenn beide Pfade schalten
 - Pfade unabhängig
 - ...

驾驶员安全气囊示例

- 安全目标：安全气囊不得无故展开（ASIL D）
- 安全概念：冗余展开机制 安全要求：
- 只有在两个路径都切换时才触发
- 路径独立 ...

Funktionales Sicherheitskonzept (2)

- Spezifikation der Sicherheitsanforderungen soll beinhalten:
 - operating modes
 - fault tolerant time interval
 - safe states
 - emergency operation interval
 - functional redundancies (e.g. fault tolerance)
- Verifikation des Sicherheitskonzepts:
 - Konsistenz zu den Sicherheitszielen
 - Fähigkeit, die gefährlichen Ereignisse zu vermeiden

功能安全概念 (2)

- 安全要求规范应包括

- 运行模式

- 容错时间间隔

- 安全状态

- 紧急运行时间间隔

- 功能冗余 (如容错)

验证安全概念:

10 Entwicklungsprozess und funktionale Sicherheit → 10.2 Funktionale Sicherheit → 10.2.2 ISO 26262

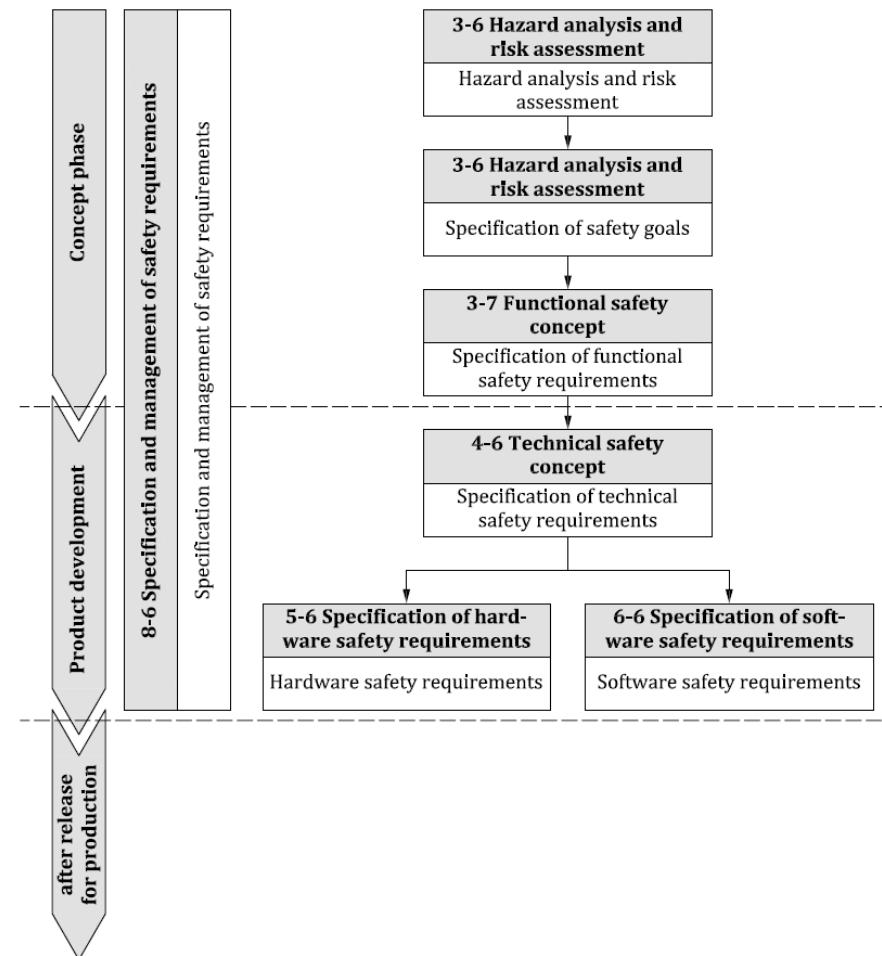
- 与安全目标的一致性

- 避免危险事件的能力

- 技术实施的安全要求
- 每种情况下对硬件和软件的具体要求
- 示例：技术安全概念（硬件）：
- 两个独立的加速度传感器
- 两个独立的点火电路

Technisches Sicherheitskonzept

- Sicherheitsanforderungen an die technische Umsetzung
- Jeweils spezielle Anforderungen für die Hardware und Software
- Bsp. Technisches Sicherheitskonzept (Hardware):
 - Zwei unabhängige Beschleunigungssensoren
 - Zwei unabhängige Zündungskreise

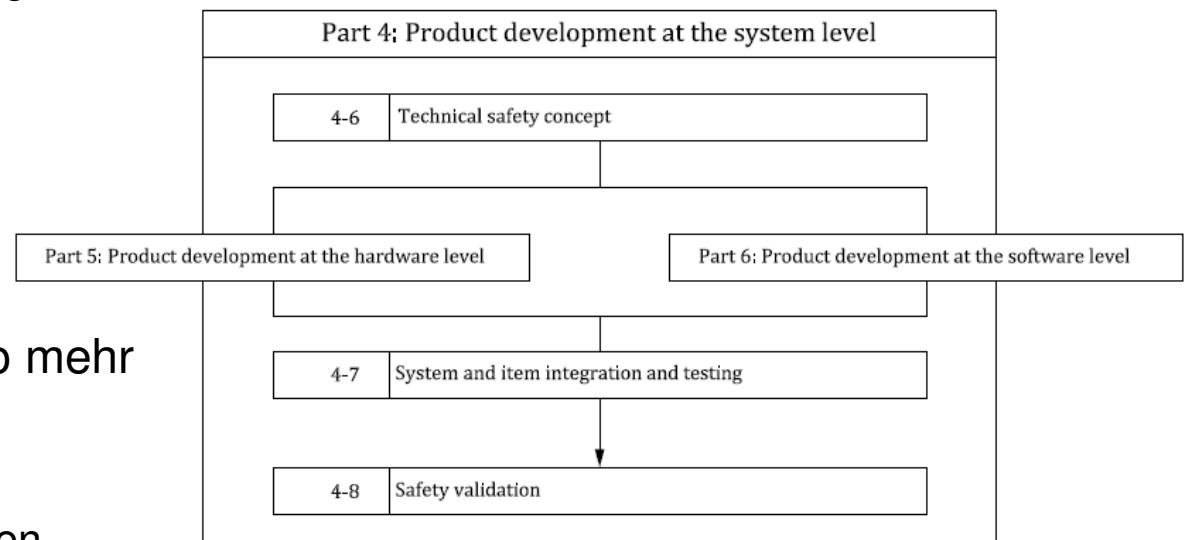


Anforderungen an die Produktentwicklung

- ASIL-abhängige Anforderungen an die Entwicklung auf den Ebenen

- System
- Hardware
- Software

- Je höher der ASIL, desto mehr bzw. aufwendigere
 - Methoden
 - Sicherheitsmechanismen
 - Nachweise



产品开发要求

- 在以下层面对开发提出与 ASIL 有关的要求

系统 硬件 软件

- ASIL 越高，系统就越复杂。

方法 安全机制 验证

- "如无特别说明, 应遵守 ASIL A、B、C 和 D 各分条的要求或建议"。

- 针对潜在故障的安全机制

- 来自 ASIL C: 潜在故障的检测

- 预防系统误差:

- 系统分析: 对所用方法的要求越来越高

Bedeutung der ASILs: Anforderungen an die Entwicklung

- “The requirements or recommendations of each subclause shall be complied with for ASIL A, B, C and D, if not stated otherwise.”
- Sicherheitsmechanismen gegen latente Fehler
 - ab ASIL C: Erkennung von latenten Fehlern
- Vermeidung von systematischen Fehlern:
 - Systemanalyse: steigende Anforderungen an die verwendeten Methoden

	Methods	ASIL			
		A	B	C	D
1	Deductive analysis	o	+	++	++
2	Inductive analysis	++	++	++	++

NOTE The level of detail of the analysis is commensurate with the level of detail of the design. Both methods can, in certain cases, be carried out at different levels of detail.

EXAMPLE An FMEA is done on hardware component level and provides the basic events of an FTA conducted at a higher abstraction level.

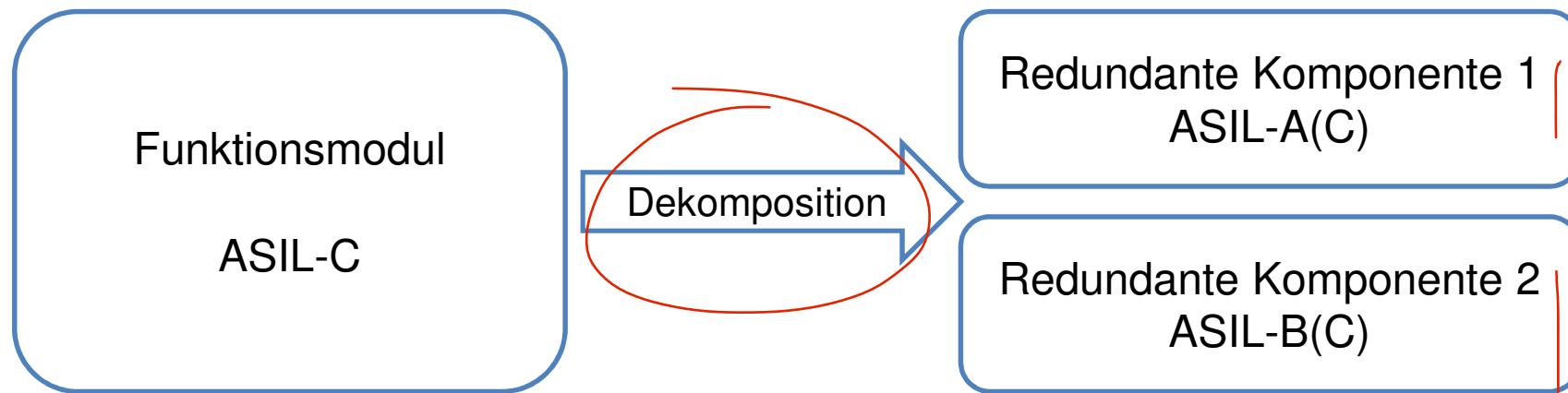
“++” highly recommended for the identified ASIL;

“+” recommended for the identified ASIL;

“o” no recommendation for or against its usage for the identified ASIL.

ASIL-Dekomposition durch Redundanz

Dekomposition hoher in niedrige Anforderungen



- Unter bestimmten Bedingungen ist die Dekomposition kritischer Komponenten in mehrere redundante Komponenten möglich
 - Unterschiedliche Hardware 在某些条件下，可以将关键部件分解为多个冗余部件
- 不同的硬件
 - Unterschiedliche Algorithmitk - 不同的算法
 - Unterschiedliche Software - 不同的软件
- Dabei gilt: $B=A(B)+A(B)$, $C=A(C)+B(C)$, $D=A(D)+C(D)$ oder $B(D)+B(D)$

Giesler, Audi

Anforderungen an Hardwareentwicklung

- Maßnahmen zur Erkennung und Vermeidung zufälliger Hardwarefehler
- Quantitative Bestimmung des Restrisikos durch single-point faults, residual faults und dual-point faults
 - **single-point fault**
 - fault in an **element** that is not covered by a **safety mechanism** and that leads directly to the violation of a **safety goal**
 - **dual-point fault**
 - individual **fault** that, in combination with another independent fault, leads to a **dual-point failure**
 - **residual fault**
 - portion of a **fault** that by itself leads to the violation of a **safety goal**, occurring in a hardware **element**, where that portion of the fault is not covered by **safety mechanisms**

硬件开发的要求

- 识别和验证最新硬件的方法
- 对单点故障、残余故障和双点故障的定量分析
- 单点故障
- 不在安全机制覆盖范围内、直接导致违反安全目标的元件故障
- 双点故障
- 与另一独立故障结合导致双点故障的单个故障
- 残余故障
- 在硬件元件中发生的、其本身导致违反安全目标的故障部分，该部分故障不在安全机制的覆盖范围内

- 选自 (B) 、C、D:

- 确定安全措施的诊断范围

- 确定硬件故障率的指标

- 如果不可能，则需要额外的安全机制

- 确定并验证目标错误率

- 通常只有通过冗余才能实现极低的错误率

Anforderungen an Hardwareentwicklung (2)

■ Ab (B), C, D:

- Diagnostic coverage von Sicherheitsmaßnahmen bestimmen
- Metriken, um Hardwarefehlerraten zu bestimmen
- Falls nicht möglich, zusätzliche Sicherheitsmechanismen
- Festlegen und Nachweisen von Ziel-Fehlerraten
 - Sehr geringe Fehlerraten häufig nur durch Redundanz möglich

ASIL	Random hardware failure target values
D	$<10^{-8} \text{ h}^{-1}$
C	$<10^{-7} \text{ h}^{-1}$
B	$<10^{-7} \text{ h}^{-1}$

NOTE The quantitative target values described in this table can be tailored as specified in [4.2](#) to fit specific uses of the item (e.g. if the item is able to violate the safety goal for durations longer than the typical use of a passenger car).

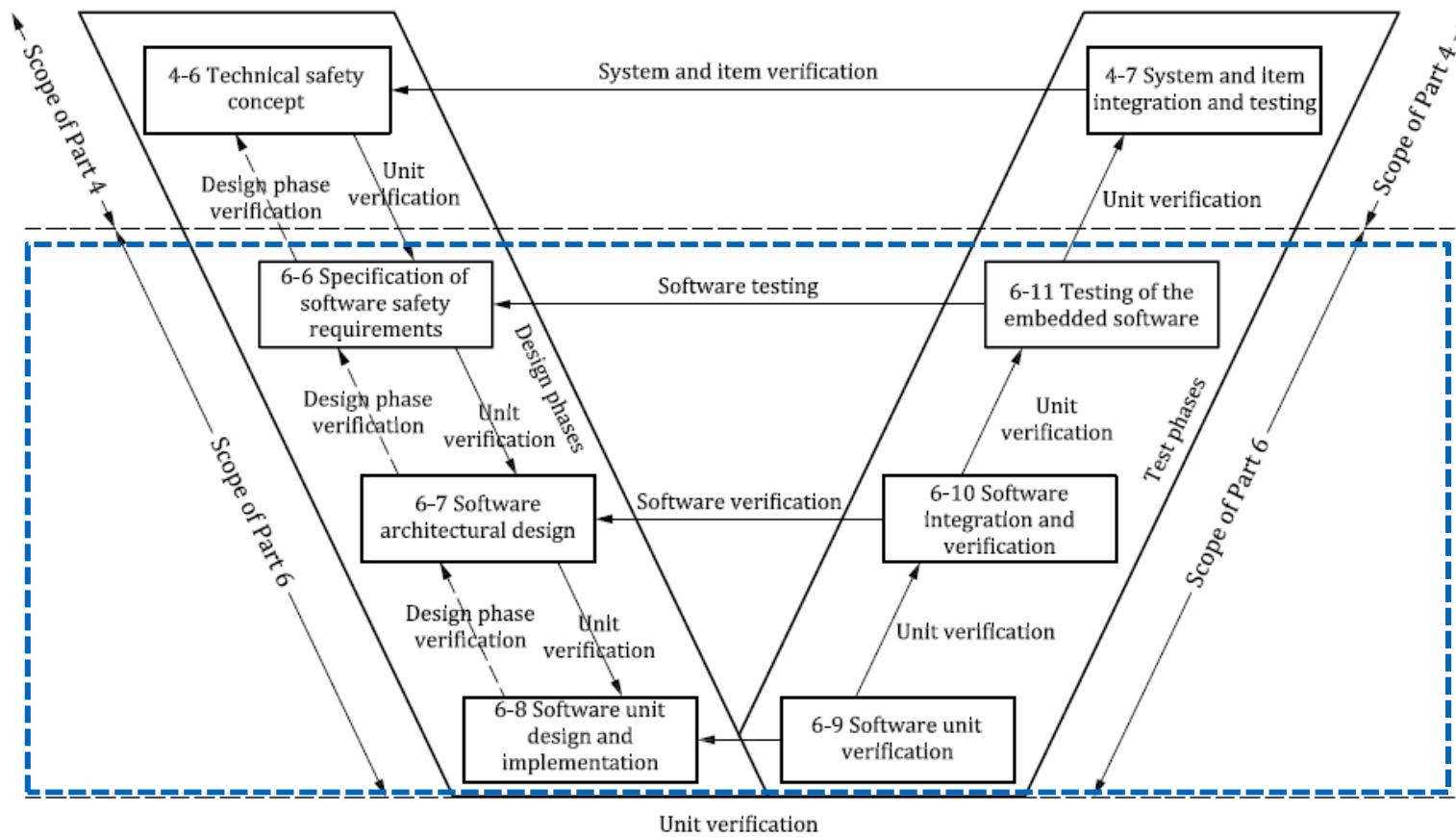
Fehlerraten

- ASIL-D: $10^{-8} \frac{1}{h} = \textcircled{10 \text{ FIT}}$ (Failure in Time, $\textcircled{1 \text{ FIT}} = 10^{-9} \frac{1}{h}$)
- Bei Reihenschaltung von Komponenten werden Fehlerraten der Komponenten addiert → Gesamtsystem schlechter als die schlechteste Komponente
- Sehr geringe Fehlerraten nur durch Redundanz zu erreichen

如果元件串联，则元件的误差率相加 总系统比最差的元件差
- 只有通过冗余才能实现极低的误差率

Produktentwicklung auf Softwareebene

Überblick



- 开发符合软件（安全）要求的软件设计。
- 证明软件设计能够满足 ASIL 安全要求。
- 支持软件实施。

主要涉及以下几点:

- 关于软件符号的建议

- 关于软件结构原则的建议

- 错误检测机制（范围检查、可信度检查……）。

- 错误控制机制（优美降级、多样化冗余……）。

- 软件设计验证方法建议

Produktentwicklung auf Softwareebene

Beispiel: 6-7 Software architectural design

Ziel:

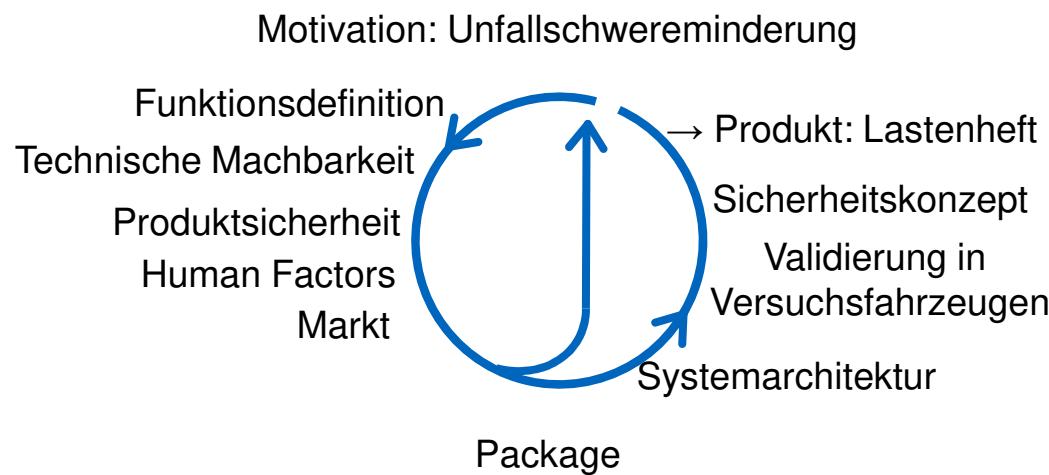
- Entwicklung eines Softwaredesigns, welches die (Sicherheits-) Anforderungen an die Software einhält.
- Zeigen, dass das Softwaredesign in der Lage ist die ASIL Sicherheitsanforderungen zu erfüllen.
- Unterstützung der Softwareimplementierung.

Dazu werden unter anderem folgende Punkte adressiert:

- Empfehlungen zur Software Notation
- Empfehlungen zu Prinzipien der Software Architektur
- Mechanismen zur Fehlererkennung (range checks, plausibility checks, ...)
- Mechanismen zur Fehlerbeherrschung (graceful degradation, diverse redundancy, ...)
- Empfehlung von Methoden zur Verifikation des Softwaredesigns

Zusammenfassung der Leitfragen

- Wie ist der Entwicklungsprozess nach Maurer aufgebaut? Wie können prototypische Konzepte für die durchlaufenen Teilschritte bewertet und entwickelt werden?



Zusammenfassung der Leitfragen

- Was bedeutet "Sicherheit" und in welche Teilbereiche kann sie untergliedert werden?
 - „Safety: absence of unreasonable risk“
 - Teilaspekte:
 - Funktionale Sicherheit: ISO 26262
 - Gebrauchssicherheit – Safety of the intended functionality (SOTIF): ISO/PAS 21448
 - Angriffssicherheit (Cyber Security): ISO/SAE 21434
- Womit beschäftigt sich die ISO 26262 und was sind ihre Kernelemente?
 - Thema: Funktionale Sicherheit von E/E-Komponenten in Serienfahrzeugen
 - Spezifiziert Entwicklungsprozesse und Anforderungen → für alle Serienfahrerassistenzsysteme relevant!

Zusammenfassung der Leitfragen

- Wie kann ein System entsprechend der G&R-Analyse nach ISO 26262 analysiert und bewertet werden?
 1. Item Definition
 2. Identifizieren aller Betriebszustände und -modi des Gesamtsystems
 3. Identifizieren aller Betriebssituationen
 4. Systematische Identifikation aller Fehlfunktionen
 5. Gefährliche Situationen = Kombination aus Fehlfunktion und Betriebssituation
 6. Klassifizierung des gefährlichen Events: Bewertung der Schwere, Exposition und Kontrollierbarkeit
 7. Bestimmung der ASIL für jedes gefährliche Ereignis
 8. Festlegung von Sicherheitszielen