Automotive

Mehr Sicherheit.
Mehr Wert.

Fahrerassistenzsysteme im Spannungsfeld zwischen Nutzen und Risiken.

Wie werden komplexe Fehlerstrukturen beherrschbarer?

Dipl.-Phys. Udo Steininger / Dipl.-Ing. Marcus Rau / Dipl.-Ing. (FH) Bernhard Schick
Tagung Aktive Sicherheit durch Fahrerassistenzsysteme 2006

TÜV SÜD Automotive GmbH

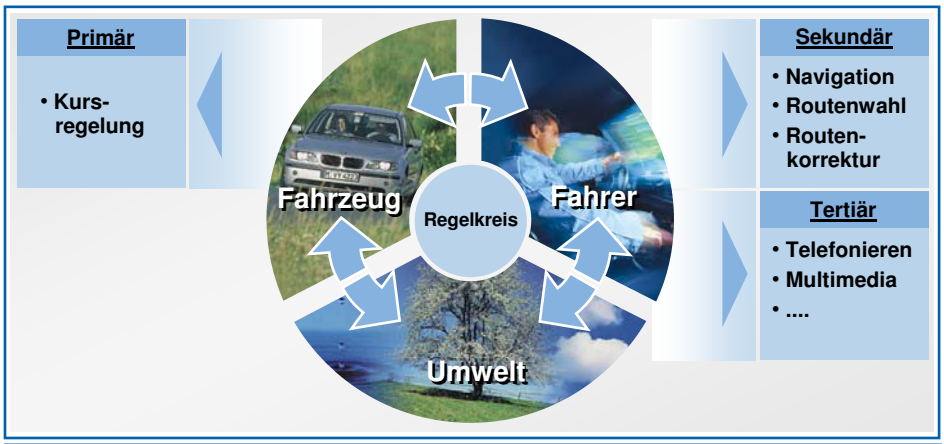
Automotive

Gliederung

1. Einleitung
2. Herausforderung
3. Funktionale Sicherheit in der Kfz-Elektronik heute
4. Globaler integrativer Ansatz
5. Zusammenfassung

1. Einleitung – Fahrerassistenzsysteme

Automotive



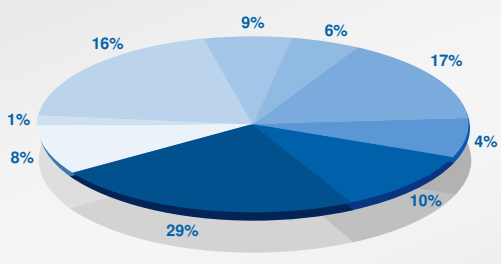
Ziel **Informieren, Empfehlen, Warnen, Intervenieren, Eingreifen**
unterstützt, entlastet und hilft dadurch dem Fahrer bei seinen drei Fahraufgaben
PLANUNG – FÜHRUNG - STABILISIERUNG

2. Herausforderung – Nutzen

Automotive

Die Motivation ein Fahrerassistenzsystem einzuführen

Unfallhäufigkeit und Unfallschwere deutlich senken



rsachen
- Unaufmerksamkeit
- Mentale Faktoren
- Unerwartetes Verhalten
- Selbstüberschätzung

Fahrerassistenzsysteme
- Lane Departure Warning
- Lane Keeping
- Adaptive Cruise Control
- Collision Warning
- Blind Spot Recognition
- Parking Assistant

Vision **Unfallfreies Fahren** sollte in ferner(?) Zukunft möglich sein!

2. Herausforderung – Nutzen

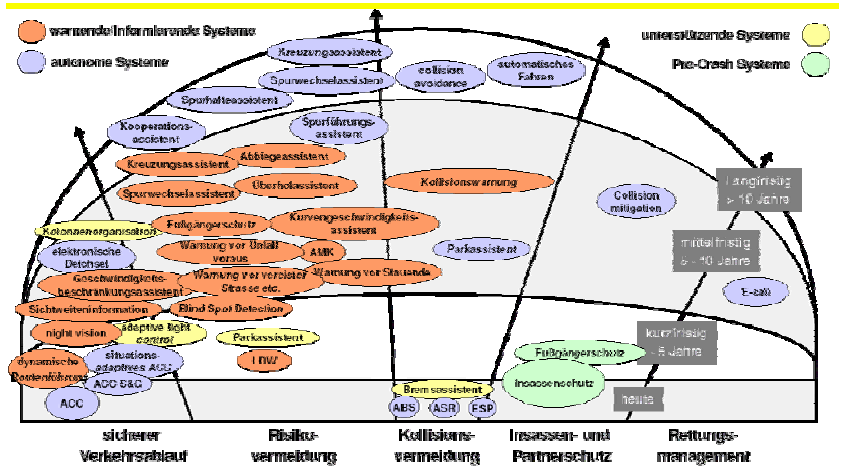
Automotive

Marktvolumen für Fahrerassistenzsysteme in Deutschland

Assistenzsysteme 2003	Assistenzsysteme 2010	Assistenzsysteme 2015
Quelle: B&D-Forecast		**3. Generation (20%)**
		• +X
		• +X
	2. Generation (30%)	**2. Generation (30%)**
	• Spurhalteassistent	• Spurhalteassistent
	• Spurwechselassistent	• Spurwechselassistent
	• Infrarot Nachtsicht	• Infrarot Nachtsicht
1. Generation (35%)	• Automatische Notbremse	• Automatische Notbremse
• ABS	• Müdigkeitserkennung	• Müdigkeitserkennung
• ESP	• Nebelsensor	• Nebelsensor
• Bremsassistent	• Unfallerkennung	• Unfallerkennung
• Reifendruckkontrolle	• Objekterkennung	• Objekterkennung
• ACC (Adaptive Cruise Control)	• +X	• +X
• Adaptives Licht	**1. Generation (80%)**	**1. Generation (100%)**
€ 900,- pro Fahrzeug	**€ 3.200,- pro Fahrzeug**	**€ 4.300,- pro Fahrzeug**

2. Herausforderung – Nutzen

Automotive



Quelle: Institut für Kraftfahrwesen Aachen

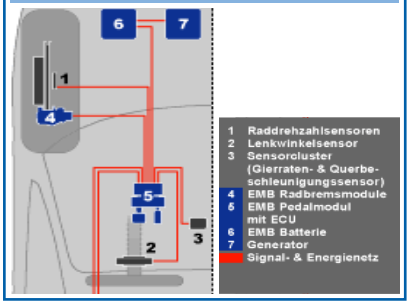
2. Herausforderung – Risiken

Automotive

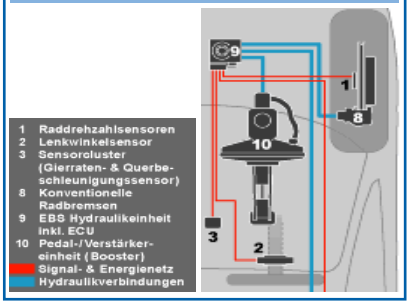
Risikopotenzial E/E/PES am Bsp. EMB

Kombination eines konventionellen Radbremsmoduls mit elektronischer Ansteuerung und Signalübertragung

EMB



Konventionell

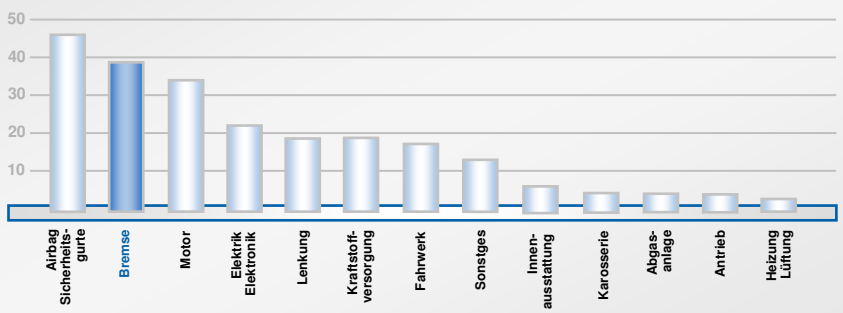


2. Herausforderung – Risiken

Automotive

Risikopotenzial E/E/PES am Bsp. EMB

Anzahl der Rückrufe nach Funktionsgruppen

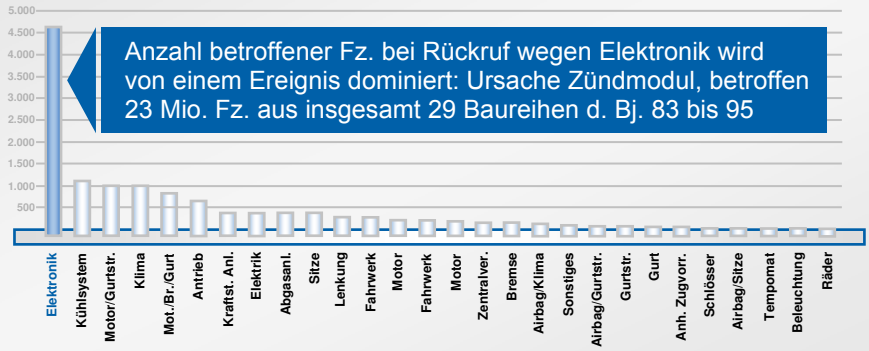


2. Herausforderung – Risiken

Automotive

Risikopotenzial E/E/PES am Bsp. EMB

Im Mittel betroffene Fahrzeuge nach Funktionsgruppen



2. Herausforderung – Risiken

Automotive

Risikopotenzial E/E/PES am Bsp. EMB

- Rückrufe nehmen insgesamt zu
- das ist insbesondere bei Einführung neuer technischer Lösungen zu beachten
- Häufige Ursache: z.B. (konventionelle) Bremse
- Großer Schadensumfang: z.B. Elektronische Bauteile
- Kombination aus Bremse und Elektronik ist hochgradig rückrufrelevant
- Fazit: Für Einführung E/E/PE Systeme ist ein wirksames Risikomanagement für das Gesamtfahrzeug erforderlich!

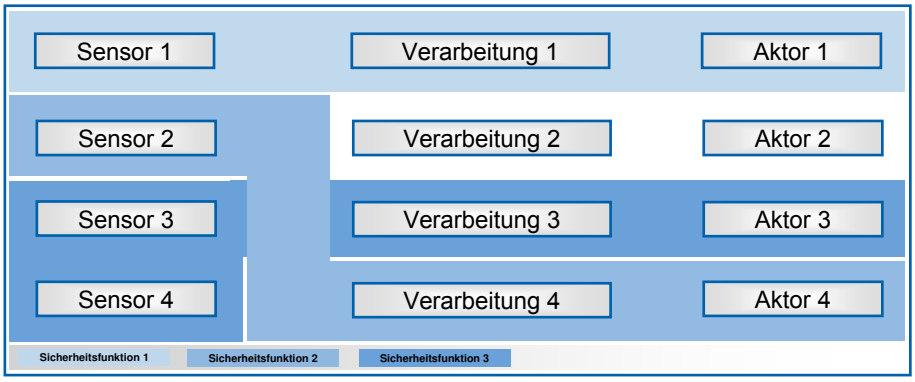
3.Funktionale Sicherheit in der KFZ-Elektronik „heute“

Automotive

„...Stand der Technik zum Zeitpunkt des Inverkehrbringens...“	
DIN V 19250/51 DIN V VDE 0801 (zurückgez. seit 10/04)	Risikobetrachtung und Realisierung von komplexen elektronischen Systemen
IEC 61508 DIN EN 61508	**Generischer Basisstandard für die Funktionale Sicherheit von elektrischen/ elektronischen Systemen**
FAKRA Normenentwurf (noch nicht verfügbar)	Applikationsnorm für die Automotive-Industrie basierend auf IEC 61508 Mitarbeit durch den TÜV SÜD

3. FS heute – Funktionaler Ansatz nach IEC 61508

Automotive



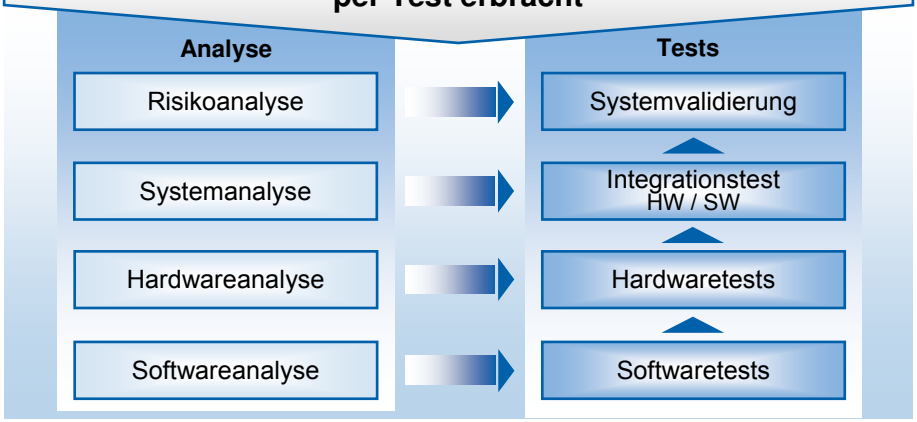
Betrachtet werden die einzelnen Sicherheitsfunktionen der Systeme im Fahrzeug:

- Funktion, die im Fehlerfall selbst zu einem Risiko werden kann (z.B. “X By Wire”)
- Funktion, die bei Anforderung sicher funktionieren muss, um ein Risiko abzuwenden (z.B. Airbag)

3. Sicherheitsnachweis der Sicherheitsfunktionen

Automotive

Für jede (einzelne) Sicherheitsfunktion werden die entsprechenden Sicherheitsnachweise analytisch und per Test erbracht



3. FS heute – Risikoanalyse

Automotive

Risikobetrachtung je Funktion

- Ermittlung der relvanten Sicherheitsfunktion(en)
- Ermittlung der erforderlichen Zuverlässigkeit je Sicherheitsfunktion
- Häufige Ursache: z.B. (konventionelle) Bremse
- Bedingte Darstellung von Wechselwirkungen zwischen den Sicherheitsfunktionen

3. FS heute – Sicherheitsnachweis auf Systemebene

Automotive

Bewertung der Systemarchitektur entsprechend der vorgegebenen Sicherheitseinstufung **je Sicherheitsfunktion**

Beispiel: Architekturanforderungen aus IEC 61508:

Safe Failure Fraction		Hardware Fehlertoleranz N		
Typ A	**Typ B**	**N = 0**	**N = 1**	**N = 2**
---	0%...< 60%	---	SIL1	SIL2
0%...< 60%	60%...< 90%	SIL1	SIL2	SIL3
60%...< 90%	90%...< 99%	SIL2	SIL3	SIL4
≥ 90%	≥ 99%	SIL3	SIL4	SIL5

IEC 61508 Teil 2, Kap. 7.4.3.1.1 / Tab. 2&3

3. FS heute – Sicherheitsnachweis auf NW-Ebene

Automotive

Bestimmung des Ausfallgrenzwertes (PFD/PFH) **je Sicherheitsfunktion**

Formeln aus IEC 61508-6:

- Abhängig von der Architektur eines Teilsystems werden Formeln zur Bestimmung der PFD/PFH angegeben.
- z.B. für ein 2-kanaliges System (1 oo 2)

$$PFH_G = 2\left((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right)^2 t_{CE} + \beta_D\lambda_{DD} + \beta\lambda_{DU}$$

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

Markov Analyse

- Mathematische Modellierung der Systemzustände und deren Übergänge
- Bewertung der Zustände und Übergänge mit Fehlerraten (λ-Werte)

3. FS heute – Sicherheitsnachweis der Software

Automotive

Für jede Sicherheitsfunktion ist nachzuweisen:

- Bewertung der eingestzten Tools und Programmiersprachen
- Identifizierung der sicherheitsrelevanten Softwarefunktionen
- Untersuchung des Einflusses möglicher Software-Fehlfunktionen auf die Systemsicherheit
- Festlegung entsprechender Softwaretests

3. Funktionale Sicherheit – heute

Automotive

Fazit

Nach aktuellem Stand der Technik werden überwiegend die Sicherheitsfunktionen isoliert betrachtet.

Die Wechselwirkungen der einzelnen Funktionen werden in den meisten Fällen, bedingt durch die entstehende Komplexität überhaupt nicht bzw. nur unzureichend betrachtet.

4. Globaler integrativer Ansatz

Automotive

Risikomanagement

Methoden der Risikoanalyse und -bewertung und Vorgehensweisen des Risikomanagements wurden entwickelt in

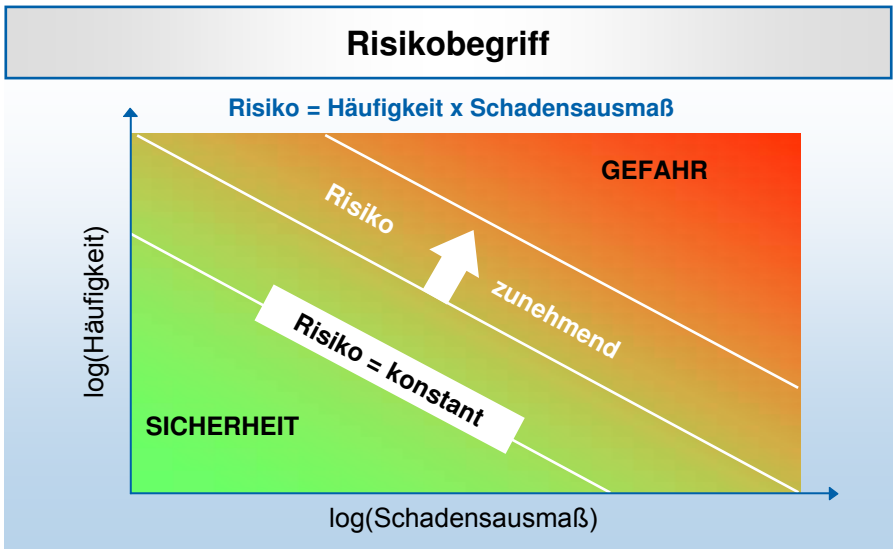
- Kerntechnik
- Luft- und Raumfahrt
- Eisenbahnbetrieb

... weitestgehend auf Automobilindustrie übertragbar!

4. Globaler integrativer Ansatz

Automotive

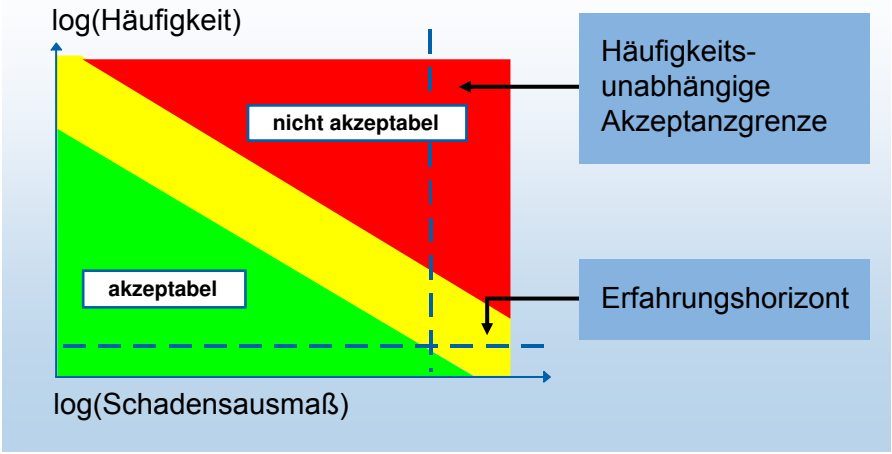
Risikobegriff



4. Globaler integrativer Ansatz

Automotive

Risikobegriff



4. Globaler integrativer Ansatz

Automotive

Risikobewertung

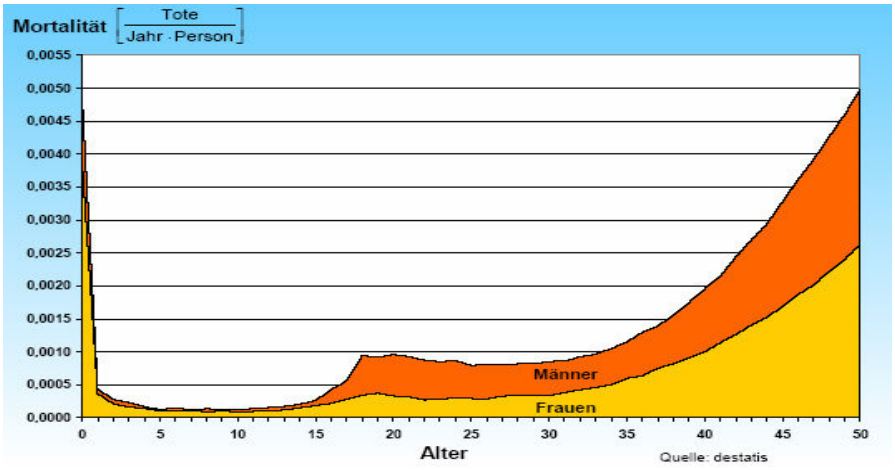
3 Konzepte zur quantitativen Bewertung von Risiken:

- MEM
- ALARP
- GAMAB

Die Ergebnisse sind bei Anwendung aller 3 Konzepte ähnlich

Automotive

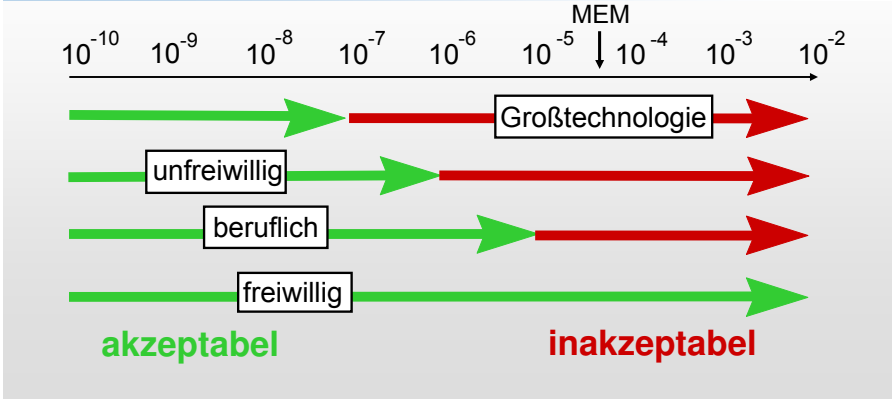
MEM: Minimale endogene Mortalität



Automotive

MEM: Minimale endogene Mortalität

Individuelles Todesfallrisiko pro Person und Jahr (Quelle: Fritzsche 1986)



4. Risikobewertung

Automotive

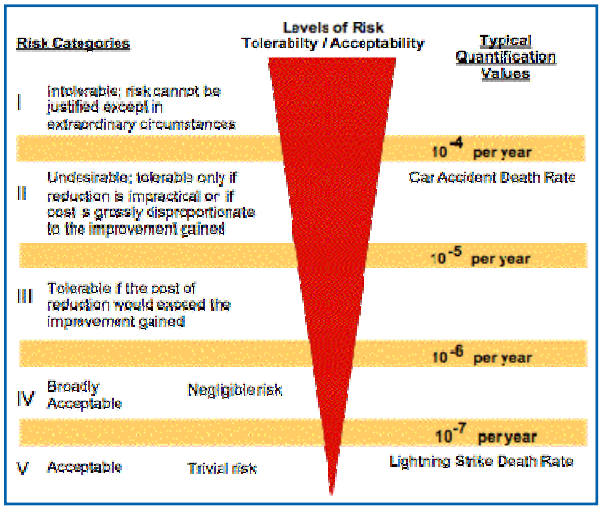
ALARP: As Low as Reasonably Practicable

- The two key levels seem to lie around road death statistics and the chances of being struck by lightning.
- If we believe something is more dangerous than driving a car then the risk is unacceptable (about one chance in 10,000 per year), but that if it about as likely as being struck by lightning (about one chance in 10 million per year), then it is probably so low that we don't expect anyone to do anything about it.
- In the range between these two figures cost benefit studies to reduce the risk to as low as reasonably practicable is appropriate.

(Quelle: Risk & Reliability Associates)

4. Risikobewertung

Automotive



Risk Levels for Individuals in a Critically Exposed Group

Diagram (without quantification) appears in IEC 61508

4. Risikobewertung

Automotive

GAMAB: Globalement Au Moins Aussi Bon

- Neue Systeme müssen das gleiche Niveau des Globalrisikos aufweisen, wie vergleichbare bereits existierende Systeme
- Bereits existierendes System ist das konventionelle Fz. ohne ACC (Grenzen sind fließend - z.B. ABS, ESP)
- Das Risiko eines Fz. mit ACC darf nur so hoch sein, wie beim konventionellen Fz.

Zu beantwortende Fragen:
- Wie werden Risiken beim konventionelle Fz. durch ACC reduziert?
- Welche neuen Risikobeiträge liefert ACC?

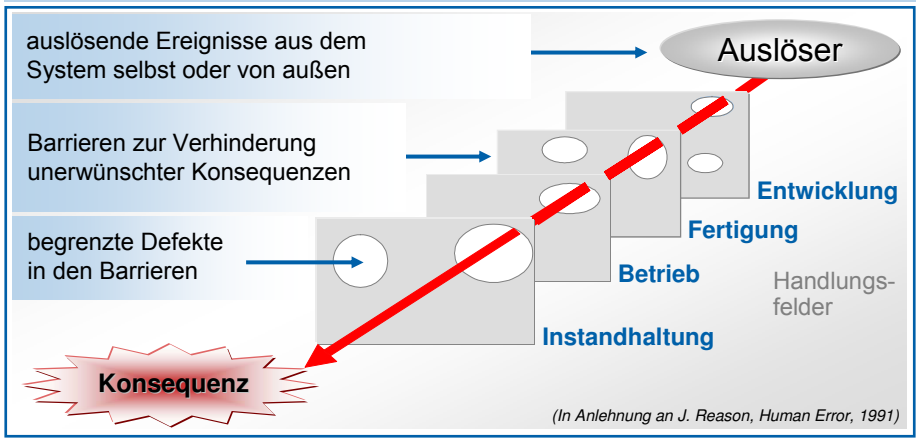
Unterschiedliche Interessenten: Kunden, Politik ←→ Zulassungsbehörden

- Aufrechnung Risikozunahme vs. Risikoreduktion möglich, aber in diesem Kontext wahrscheinlich nicht zielführend
- Besser: Neue Risikobeiträge sollten gegenüber Globalrisiko beim konventionellen Fz. vernachlässigbar sein

4. Festlegung relevanter Szenarien

Automotive

Entstehung unerwünschter Konsequenzen



4. Festlegung relevanter Szenarien

Automotive

1. Welche unerwünschten Konsequenzen können auftreten?

Fehler in Längs- und / oder Querführung

Folge: Eigenes Fz. kollidiert mit

- vorausfahrenden / stehenden Fz.
- folgenden Fz.
- entgegenkommenden Fz.
- parkenden Fz. od. Infrastrukturelementen
- querenden Verkehrsteilnehmern
- Personen und Objekten außerhalb von Fz. (Panne, Wildwechsel etc.)

4. Festlegung relevanter Szenarien

Automotive

2. Welche auslösenden Ereignisse können auftreten?

- Aktiver Fahrerfehler
- Einzelfehler HW/SW (werden i.d.R. erkannt)
- Systematische Fehler (System erkennt Situation nicht richtig → Errors of Omission / Commission)
- übergreifende Einwirkungen von Innen (EVI - z.B. Ausfall Energieversorgung)
- übergreifende Einwirkungen von Außen (EVA - z.B. regelwidriges Verhalten anderer Verkehrsteilnehmer)

4. Festlegung relevanter Szenarien

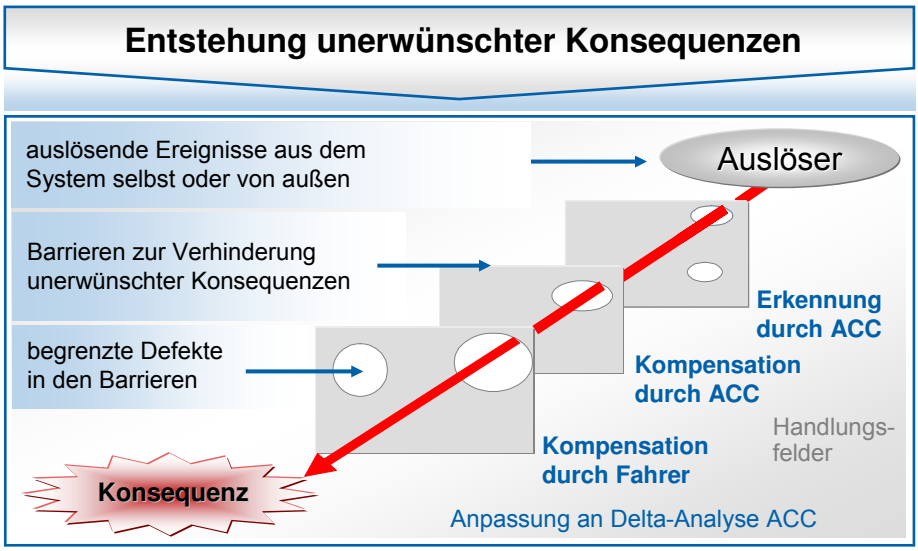
Automotive

3. Welche Barrieren zur Verhinderung unerwünschter Konsequenzen wurden geschaffen?

- Erkennung von Fahrsituationen sowie von Fehlern des Fahrers und des technischen Systems innerhalb des ACC (durch Überwachung von Bauteilen und Funktionen)
- Reaktion des ACC auf Fahrsituationen sowie auf Fehler des Fahrers und des technischen Systems (Fehlerkompensation durch ACC)
- Reaktion des Fahrers auf Fahrsituationen sowie auf Fehler des technischen Systems (Fehlerkompensation durch Fahrer)

4. Festlegung relevanter Szenarien

Automotive



4. Festlegung relevanter Szenarien

Automotive

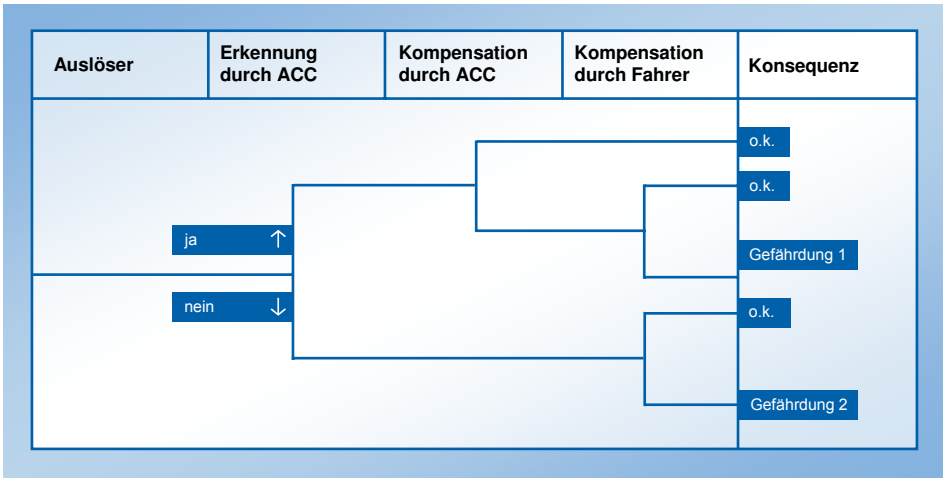
4. Welche begrenzten Defekte können vorliegen?

Ausfall, unentdeckt Bleiben oder Fehlschlagen der:

- Erkennung von Fahrsituationen sowie von Fehlern des Fahrers und des technischen Systems durch ACC
- Fehlerkompensation durch ACC
- Fehlerkompensation durch Fahrer

4. Ereignisablaufanalyse

Automotive



4. Häufigkeit und Schadensausmaß

Automotive

Die Häufigkeiten für das Eintreten der Auslöser und für das Fehlschlagen der Erkennung und Kompensation sowie das Schadensausmaß hängen ab von

- äußeren Randbedingungen (Fahrsituation, andere Verkehrsteilnehmer, Witterung etc.)
- Systemauslegung (RAMS: Reliability, Availability, Maintainability & Safety)
- Belastung und Beanspruchung des Fahrers (Kondition, Wissen, Aufmerksamkeit etc. ←→ Gestaltung HMI, zur Verfügung stehende Zeit, erforderliche Kräfte und Momente etc.)

4. Häufigkeit und Schadensausmaß

Automotive

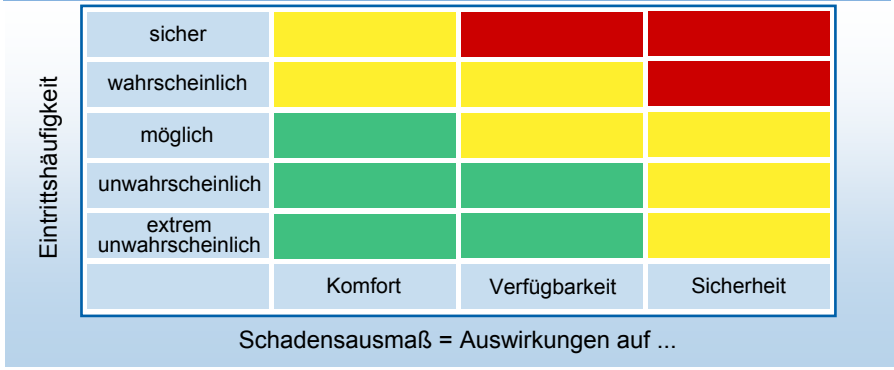
- Bestimmung der Eintrittshäufigkeiten für Auslöser und für Fehlschlagen der Erkennung und Kompensation durch ACC mittels Fehlerbaumanalyse
- Bestimmung der Wahrscheinlichkeit für das Fehlschlagen der Kompensation durch den Fahrer mittels Human Reliability Analysis (z.B. THERP)
- Bestimmung des Schadensausmaßes mittels klassischer (statistischer) Unfallanalyse → Worst Case Betrachtung
- Vorgehensweise: Semi-quantitativ

4. Ergebnis

Automotive

Risikoklassifizierung

Ergebnis: Klassifizierung von Eintrittshäufigkeit, Schadens-ausmaß und Risiko unerwünschter Ereignisse → z.B.:

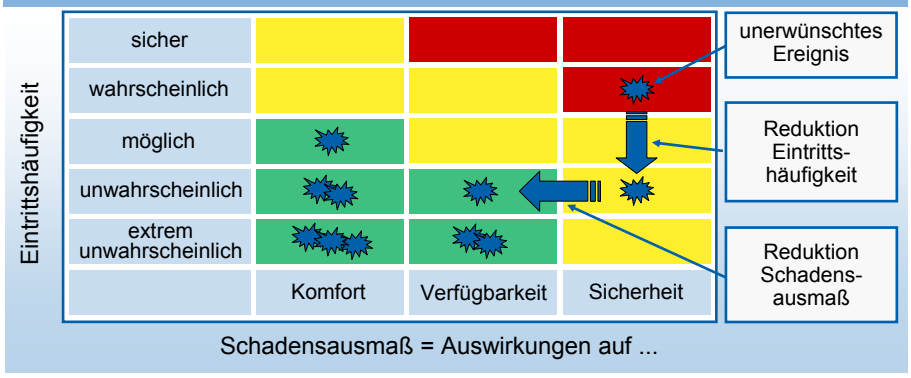


4. Ergebnis

Automotive

Maßnahmen

Handlungsbedarf erkennen → Maßnahmen identifizieren → Wirksamkeit bewerten (im Vergleich zu konvent. Fz.!)



4. Absicherung

Automotive

Absicherung

- durch Analysen und Versuche → speziell: HIL / SIL mit Simulation Fahrweg und Verkehr
- Wegen der Vielzahl der Einflussfaktoren Festlegung erforderlich, welche Einflussfaktoren in welchen Stufen zu variieren sind → Statistische Versuchsplanung (DoE)

5. Zusammenfassung

Automotive

- Vorgehen heute – isolierte Betrachtung einzelner Sicherheits-funktionen, keine Berücksichtigung der Wechselwirkungen zwischen diesen oder mit Gesamtfahrzeug
- Konzepte zur Bewertung des Gesamtfahrzeugs existieren, wurden aber bisher in diesem Bereich kaum eingesetzt
- Gesamthafte Risikoanalyse dient in erster Linie der Optimierung des Gesamtsystems
- Vorgehensweise: Projektbegleitendes Risikomanagement

Wie viel ACC braucht / will / bezahlt der Kunde?