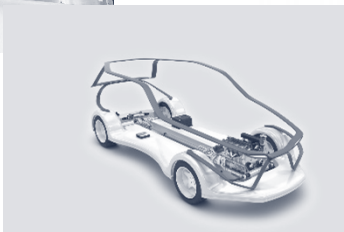
Institut für Qualitäts- und Zuverlässigkeitsmanagement GmbH
Dr.-Ing. Andreas Braasch

BERGISCHE UNIVERSITÄT WUPPERTAL

Prof. Dr.-Ing. Arno Meyna

TECHNISCHE ZUVERLÄSSIGKEIT

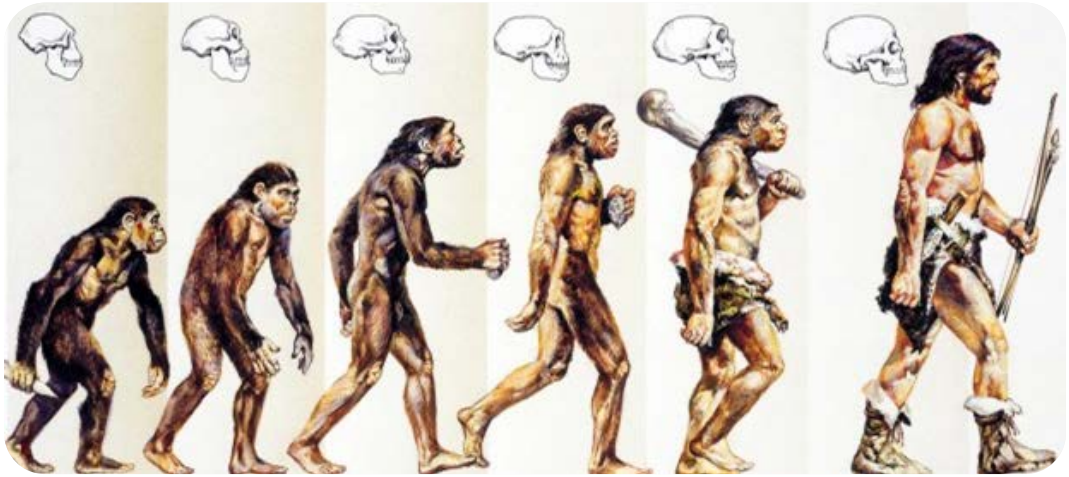
SICHERHEITSBEWERTUNG VON AUTONOMEN FAHRZEUGEN



IQZ Ihr Qualitäts-Zulieferer.

- Moderne Mensch (Homo sapiens) ca. 160.000 Jahre datiert
- Begleitfunde wie Pfeilspitze, Faustkeile etc. zeigen die enge Verbundenheit des Menschen mit der Technik
- Sicherheit und Zuverlässigkeit ist final mit der technologischen Entwicklung selbst verbunden.

„Demnach war der Mensch bei seinem Erscheinen auf der Erde sogleich Techniker. Technik ist menschliche Uranlage."
(Dessauer, Friedrich: Streit um die Technik, Verlag Josef Knecht, Frankfurt am Main, 1956)



Evolution des Menschen [http://www.welt.de/wissenschaft/article102103489/aufrechter-gang-DW-Wissenschaft-Zhenjiang-jpg.html ; 17.04.2014]

CODEX DES HAMMURABI

- Älteste bekannte Gesetzessammlung der Welt:
  Codex des Hammurabi (1700 v. Chr.) enthält u.a. Haftungs-(Straf-) Gesetze für Baumeister

  – Wenn ein Baumeister ein Haus baut für einen Mann und macht seine Konstruktion nicht stark, so dass es einstürzt und verursacht Tod des Bauherrn: dieser Baumeister soll getötet werden.

  – Wenn der Einsturz den Tod eines Sohnes des Bauherrn verursacht, so sollen sie einen Sohn des Baumeisters töten.

  – Kommt ein Knecht des Bauherrn dabei um, so gebe der Baumeister einen Knecht von gleichem Wert.

  – Wird beim Einsturz Eigentum zerstört, so stelle der Baumeister wieder her, was immer zerstört wurde; weil er das Haus nicht fest genug baute, baut er es auf eigene Kosten wieder auf.

  – Wenn ein Baumeister ein Haus baut und macht die Konstruktion nicht stark genug, so dass eine Wand einstürzt, dann soll er sie auf eigene Kosten verstärkt wieder aufbauen.

Bild: Aus dem Codex Hammurabi, Col. XX, 228 bis 233

Quelle: DIN-Mitteilungen, Nr. 10, 1978

➔ Sicherheits- und Zuverlässigkeitstechnik eng verknüpft mit den Natur- und Technikwissenschaften und deren

deterministisches Weltbild.

(u.a. Newton, Laplace – „Laplacescher Dämon“, Einstein)

Isaac Newton

[http://www.rschindler.com/newton.htm; 17.04.2014]

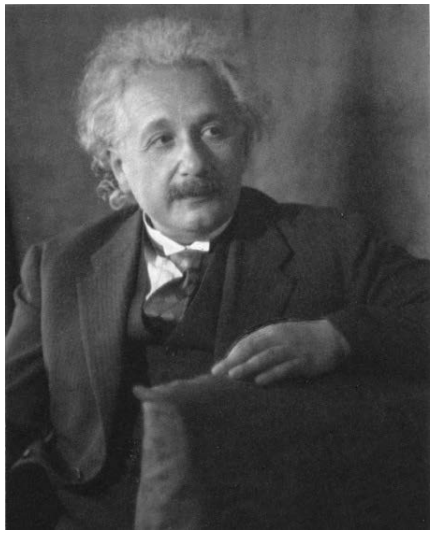
„Gegenüber jeder Aktion steht die Reaktion“

Pierre-Simon Laplace

[http://apprendre-math.info/history/photos/Laplace_3.jpeg; 23.04.2014]

„Mit dem Wort „Zufall“ gibt der Mensch nur seine Unwissenheit zum Ausdruck“

Albert Einstein



[http://de.theoriefinder.wikia.com/wiki/Albert_Einstein; 17.04.2014]

„…des Geheimnis des Alten bringt sie uns kaum näher. Jedenfalls bin ich überzeugt, daß der nicht würfelt.“
(zur Quantenmechanik)

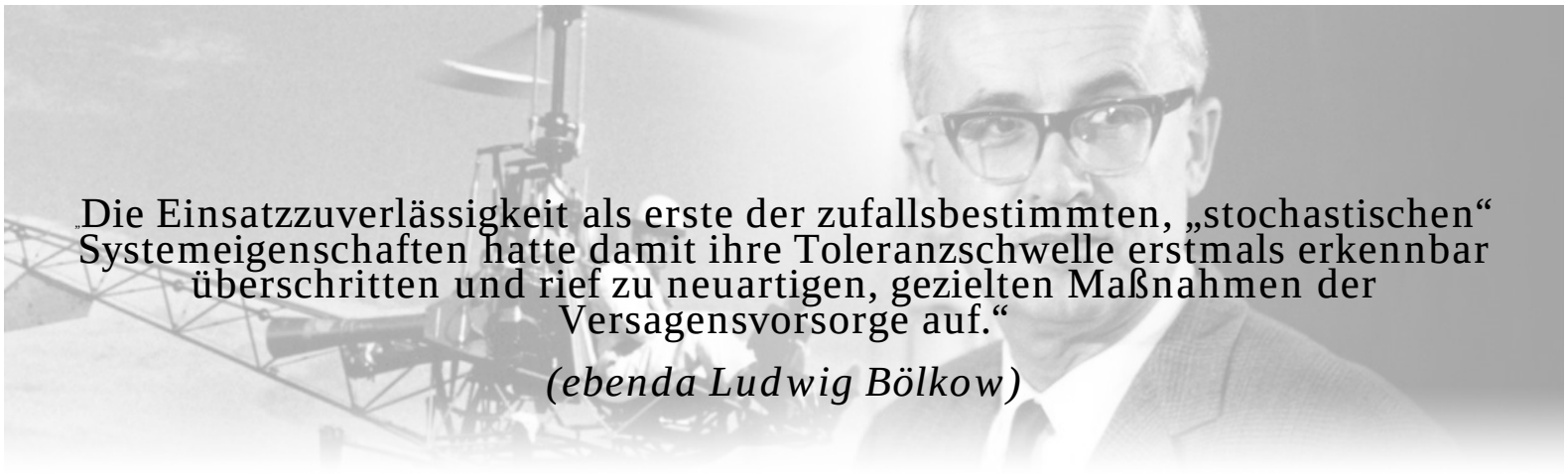
„Vor fast genau 40 Jahren, bei der Erprobung des selbstgesteuerten Fluggeräts Fi 103, das unter der Bezeichnung „V 1“ bekannt wurde, trat erstmals ein Problem ins technische Bewußtsein, das sich als eines der Schlüsselprobleme der Zukunft erweisen sollte. Trotz aller Qualitätskontrollen und auch nach Beseitigung der üblichen, an ihrer Häufung erkennbaren Anfangsfehler, war eine Erfolgsquote von 15% bis 20% nicht zu übertreffen.“

(Ludwig Bölkow: Systemtechnik heißt Verhalten vorhersehen, VDInachrichten Nr. 26, 1982)

Abschussrampe der V1 [https://www.flickr.com/photos; 17.04.2014]

Ansatz des Projektleiters Robert Lusser:
Umfangreiche Versuche („Kette ist so stark wie ihr schwächstes
Glied“); es ergeben sich jedoch keine Fehlermuster, die auf weitere Schwachstellen hinweisen.
➔ Ansatz erfolglos, da jeweils andere Bauteile versagten

https://walkingpapers.wordpress.com/tag/robert-lusser/; 17.04.2014]



„Die Einsatzzuverlässigkeit als erste der zufallsbestimmten, „stochastischen“ Systemeigenschaften hatte damit ihre Toleranzschwelle erstmals erkennbar überschritten und rief zu neuartigen, gezielten Maßnahmen der Versagensvorsorge auf.“

(ebenda Ludwig Bölkow)

Zuverlässigkeitsmodell der Fi 103 von Pieruschka

➔ Neuer stochastischer Ansatz als „Systemdenken“ durch den Projektmathematiker Erich Pieruschka.

Modell:

p1 p2 pi pn

(p = Überlebenswahrscheinlichkeit der Komponenten)

Überlebenswahrscheinlichkeit des Systems:

$$R_s(\underline{p}) = \prod_{i=1}^{n} p_i$$

Ansatz: Exponentialverteilung $R_s(t) = e^{-t\cdot\sum_{i=1}^{n}\lambda_i}$

Näherung:

mittlere Ausfallrate: $\overline{\lambda} \approx 10^{-5}\, Ausfälle/h$

Anzahl der Elemente: $n \approx 10^5$

Einsatzdauer: $t \geq 1{,}5h$

Ergebnis: $R_s(t) = e^{-n\cdot\overline{\lambda}\cdot t} \leq 0{,}2$

D.h. 20 von 100 „Marschflugkörper“ waren erfolgreich gestartet.

„Eine Kette ist schwächer als das schwächste Glied.“

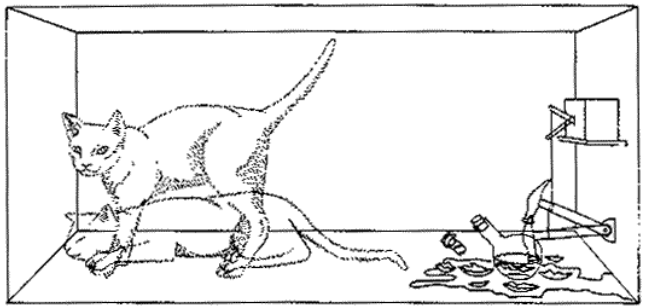
→ Sicherheits- und Zuverlässigkeitstechnik sind eng verknüpft mit den Natur- und Technikwissenschaften und deren

indeterministischen Weltbild

d.h. die Nichtbestimmtheit der Ursachen bei physikalischen Vorgängen – Zukunft ist nur durch stochastische Modellbildung (Zufalls-Prozess) bestimmbar.

(u.a. Planck, Heisenberg, Schrödinger)

- Die stochastische Modellbildung kann allerdings eine deterministisch orientierte Zuverlässigkeits- und Sicherheitstechnik nicht ersetzen, sondern ermöglicht a priori eine Bewertung technischer Systeme in einem frühen Entwicklungsstadium
- Es zeigt sich, dass die Paradigmen der Zuverlässigkeits- und Sicherheitstechnik durch den Nexus von Determinismus und Indeterminismus geprägt sind.



http://killmonotony.net

- Realität u.a. durch Modellierung hinreichend und genau beschreiben und falsifizierbare Vorhersagen (Prognosen) für die Zukunft ermöglichen, konsistent und überprüfbar sein
- eine Theorie soll möglichst einfach (Ockhams Rasiermesser), nicht zu kompliziert, praktikabel, widerspruchsfrei, verifizierbar, extensiv u.a. sein
- andere Theorien nicht widersprechen
- u.a.

(siehe hierzu Aristoteles, Kant, Popper, etc.)

➔ Stochastische Zuverlässigkeitstheorie als eine neue Wissenschaftsdisziplin

http://static.neatoshop.com/images/product/68/468/Occams-Razor_1896-l.jpg; 17.04.2014

- stürmische theoretische und praktische Entwicklungen seit der 50er Jahre des letzten Jahrhunderts

  - 1950 erster Zuverlässigkeitsbericht (TR 75: A study of methods for...)
  - 1952 Komitee AGREE in der USA gegründet (**A**dvisory **G**roup on the **R**eliability of **E**lectronic **E**quipment)
  - 1954 1. National Symposium on Reliability and Quality Control der IEEE in den USA (**I**nstitute of **E**letrical and **E**lectronics **E**ngineers)
  - 1961 1. Tagung über Zuverlässigkeit in Deutschland , Nürnberg, danach alle zwei Jahre regelmäßig

- Heute Nutzung der Erkenntnisse der Zuverlässigkeitstheorie - ausgehend vom Bereich der Luft- und Raumfahrttechnik - in fast allen Industriezweigen
  ➔ seit den 70er Jahren auch im Bereich der Automobilindustrie

(*Reliability Methods, Ford, 1972; N.A.A.O. Reliability Office; umfangreiches Handbuch bestehend aus 30 Modulen*)

Determinismus

- Kausale Bestimmtheit allen Geschehens durch Naturgesetze (klassische Physik, Newton)
- Zukunft ist durch die Gegenwart (Anfangsbedingungen) eindeutig bestimmt

Indeterminismus

- Nichtbestimmbarkeit der Ursachen bei physikalischen Vorgängen (stoch. Physik, Planck, Heisenberg, Schrödinger)
- Zukunft nur durch stochastische Modellbildung (Zufalls-Prozesse) bestimmbar

Funktionszuverlässigkeits- und Sicherheitsprozess

- Ganzheitliche Betrachtung zur Schadens- und Risikovorsorge
- Optimierung des RAMS – Prozesses unter Berücksichtigung der LCC
- ....

BERGISCHE UNIVERSITÄT WUPPERTAL

Deutsche Flugsicherung

Automotive

Luftfahrt

Energie- und kerntechnische Anlagen

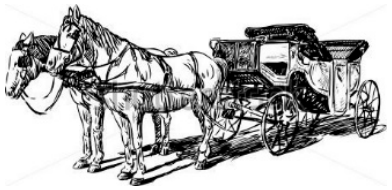
Neue Herausforderung – Autonomes Fahrzeug und Fahren

- Erfordert die Entwicklung von fehlertoleranten Architekturen, Notfallsystemen und -strategien sowie die Überführung des Fahrzeuges in den jeweiligen risikominimalen Zustand
- Modellierung von Umsetzungsszenarien und deren Risikobewertung im Sinne einer ganzheitlichen Betrachtung
- Untersuchung der Auswirkungen und Bewertung der Funktionseinschränkung (degradierte Zustände) je nach Automatisierungsgrad des automatisierten Fahrens und Straßentyps auf das System Straße – Fahrzeug (aktiv und passive Sicherheit) – Mensch (Verkehrsteilnehmer)
- Besondere Herausforderung Modellierung und Bewertung der zeitlichen Aufenthaltsdauern in den einzelnen Systemzuständen und der Verhaltensentscheidung und Überwachung des Fahrers (Mensch-Maschine-Interaktion)

Rückschritt

Fortschritt

gestern



http://de.clipartlogo.com/premium/detail/carriage-with-horses_117126268.html; 23.04.2014

„Pferdeintelligenz“

heute

http://www.mayser-schaumstofftechnik.de/branchen/automobil; 23.04.2014

„Fehlende kognitive Fähigkeiten“

morgen

http://www.sueddeutsche.de/auto/autonomes-fahren-fahrplan-in-die-zukunft-1.1864972; 23.04.2014

„Kognitives Automobil“

Ausblick:

- ➔ Zuverlässigkeitsplanung:
  Gezielte Weiterentwicklung der Methoden insbesondere der „Dynamischen Zuverlässigkeit“ und des Verhaltensmodells Fahrzeug – Fahrer – Straße zur Bestimmung der Systemsicherheit und -zuverlässigkeit im Sinne einer ganzheitlichen Systembetrachtung; u.a.
- ➔ Zuverlässigkeitsprüfung:
  Gezielte Weiterentwicklung der Methoden zur Zuverlässigkeitsprognose insbesondere Versuch versus Feld; u.a.
- ➔ Etablierung einer „Zuverlässigkeitskultur Automotive“

http://www.silber.de/forum/userpix/1714_lukrativewirtschaftlichkeit_edithaitzinger_1.jpg; 23.04.2014

Mobilität Im Spannungsfeld der Gesellschaft

Mobilitätsnachfrage steigt
Güterverkehr 32% (1999-2011)
Güterbeförderung 4,5 Mrd. t (2014)

Ausgaben für Verkehr und digitale Infrastruktur
22,86 Mrd. € (2014)

PKW –Zulassungen
43,85Mio. (2014)

Erwerbstätige Verkehr
2 Mio. (2010)

Anteil Verkehr an der Bruttowertschöpfung
3,9% ≙ 88 Mrd.€

(Quelle: Statistisches Bundesamt)

Klimabeeinflussung

Energie Ressourcen

Emissionen
(CO, HC, NO_X, PM etc.)

Peak of Oil

Verkehrsunfälle
2,4 Mio. (2014)
Getötete: 3.378 (2014)
Verletzte: 389.407 (2014)

Staus
475.00 Staus mit einer Gesamtlänge von 960.000km (2014, ADAC)

Ziel: kognitives Auto

Unfälle verhindern
vision zero

Energieeffizientes Fahren

Emissionen vermeiden
vision emission

Staus vermeiden

Digitale Natives:
Entspannt reisen, Freiräume schaffen, Kommunikation und Arbeit

Demographischer Wandel/Handicaps mobil gestalten
(Ageing society)

Wirtschaftsstandort Deutschland sichern

Chronik autonomes Fahren (ab 1980 erste Erfolge, Auszug)

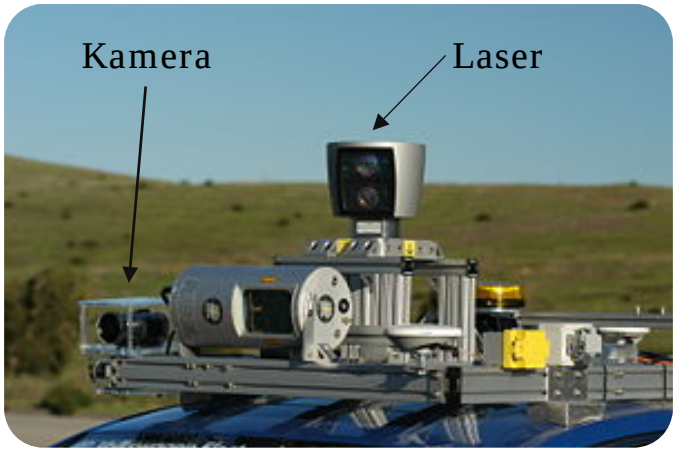
Jahr	Ereignisse
1980	Roboterauto (Prof. Dickmann) → Mercedestransporter, Autobahn, v ≤ 96 km/h, Orientierung an Gegenständen
1994	EU-Projekt EUREKA Prometheus Mercedes 500 SEL (VaMP, VITA-3) → s > 10 km auf der Autobahn (nach Paris, v ≥ 130 km/h)
1995	Mercedes SEL (Prof. Dickmann) → s ≥ 1.600 km, v ≤ 180 km/h
2004, 2005, 2007	DARPA Grand Challenge
2010	Stadtprojekt, autonomes Fahren in städtischer Umgebung (Team Institut für Regelungstechnik (Prof. Schumacher, Prof. Maurer) TU-Braunschweig; Institut für Verkehrssystemtechnik (Prof. Lemmer) DLR Braunschweig)
2011	Google-Testflotte autonom s > 1.600 km (2013 → s > 0,5 Mio. km)
2013	Daimler, historische Bertha-Benz-Strecke
heute	Fast alle großen Automobilzulieferer und Premium-Hersteller verfügen über autonom agierende Fahrzeuge und testen diese

DARPA GRAND CHALLENGE (OFFROAD)

(Defense Advanced Research Projects Agency)

Jahr	Ereignisse
2004	Kein Fahrzeug von 15 erreicht das Ziel Auslobung: 1 Mio.
2005	Fünf von 23 Fahrzeugen erreichen das Ziel max. 132 Meilen (vier unter der Maximalzeit von 10h) Auslobung: 2 Mio. Dollar Gewinner: VW Touareg Stanley, Stanford University (Prof. Truhn)
2007	Spezieller Parcour in < 6h durchfahren (Victorvill, George Air Force Base) Gewinner: 1. Tartan Racing Team, Carnegie Mellon University (2 Mio. Dollar „Boss“) 2. Stanford Racing Team, Stanford University (1 Mio. Dollar „Junior“) 3. Team Victor Tango (500.00 Dollar)

Autonomes Fahrzeug Junior (Factsheet) der Stanford University – Bild: S. Thrun, Stanford University



Junior: Dach-Sensoren

BERGISCHE UNIVERSITÄT WUPPERTAL

Automatisches Fahren – Herausforderungen

Gebrauchs-Sicherheit	Kein Einsatz der Systeme entgegen Herstellerangaben	
Bedien-Sicherheit	Kontrollierbarkeit, Mode Awareness, HMI*	
Aktive Sicherheit	Notmanöver: Bremsen, ausweichen, anhalten	
Verifikation	Freigabetest, Simulation	
Daten-Verfügbarkeit	Digitale Karten, V-2-Server, EDR*, Datenschutz	
Systemarchitektur	Redundanzen, Ausfälle	
Rechts-Sicherheit	Wiener Übereinkommen, StVO, ECE-R79	

HMI: HUMAN-MASHINE-INTERFACE
EDR: ENHANCED DATA RATE

(VDA, BARTELS, 2014)

Einteilung der Fahrerassistenzsysteme

Warn/Informationssysteme

- optisch, akustisch, haptisch

Interventionssysteme

- Beeinflussung , Korrektur

Übersteuerbare	Nicht-übersteuerbare

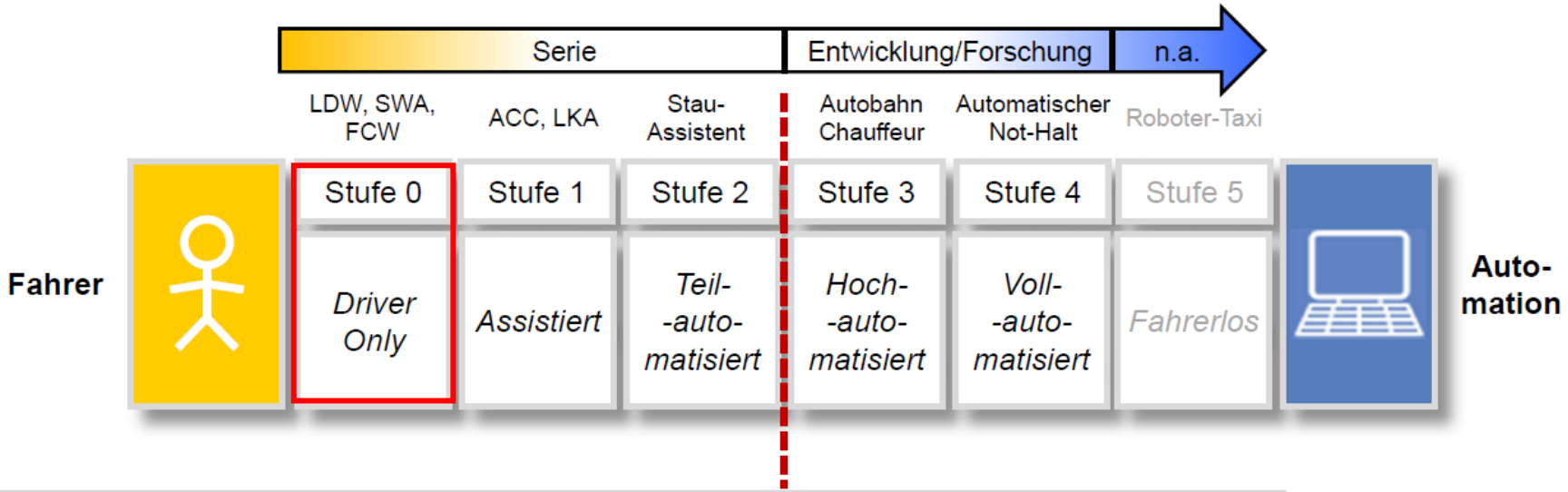
Warnungen werden an den Fahrer gegeben, die das Fahrverhalten beeinflussen sollen

Der Fahrer kann das System jederzeit übersteuern

Der Fahrer kann das System konstruktions-bedingt oder aufgrund seiner Reaktionszeit nicht übersteuern

Quelle: Küçükay

Stufen des Automatisierten Fahrens



Fahrer "in the loop"	ja (zwingend)		nein (muss nicht)	
Reaktionszeit	~ 1 s		einige s	einige min
Nebentätigkeiten	keine (verboten)		bestimmte	alle (inkl. schlafen)
Risiko min. Manöver	nein		evtl.	immer (zwingend)
von Start bis Ziel	nein (spezifische Situation und/oder bestimmte Zeit)			ja

LDW: Lane Departure Warning, SWA: Spur Wechsel Assistent, FCW: Forward Collision Warning, ACC Adaptive Cruise Control, LKA: Lane Keeping Assistance

(Ebner, 2013; in Anlehnung an Gasser et. al.)

Längsführung
DISTRONIC PLUS

Querführung
Aktiver Spurhalteassistent

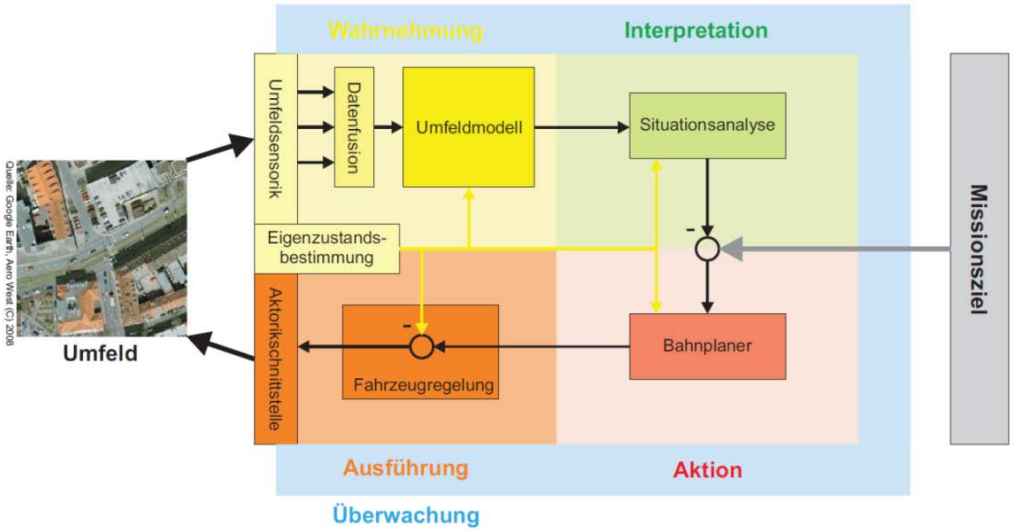
Parken, Rangieren
360° Kamera

Vorausschau
Nachtsicht Assistent Plus

Vorausschau
MAGIC BODY CONTROL

Vorausschau
Aktiver Totwinkelassistent

Quelle: Daimler



(EFFERTZ, 2009)

1. **Wahrnehmungsebene:**

   Was geschieht um mich herum und wo befinde ich mich?

2. **Interpretationsebene:**

   Welche Auswirkung hat das Umfeld auf mich und die notwendige Entscheidung zum Erreichen meines Ziels?

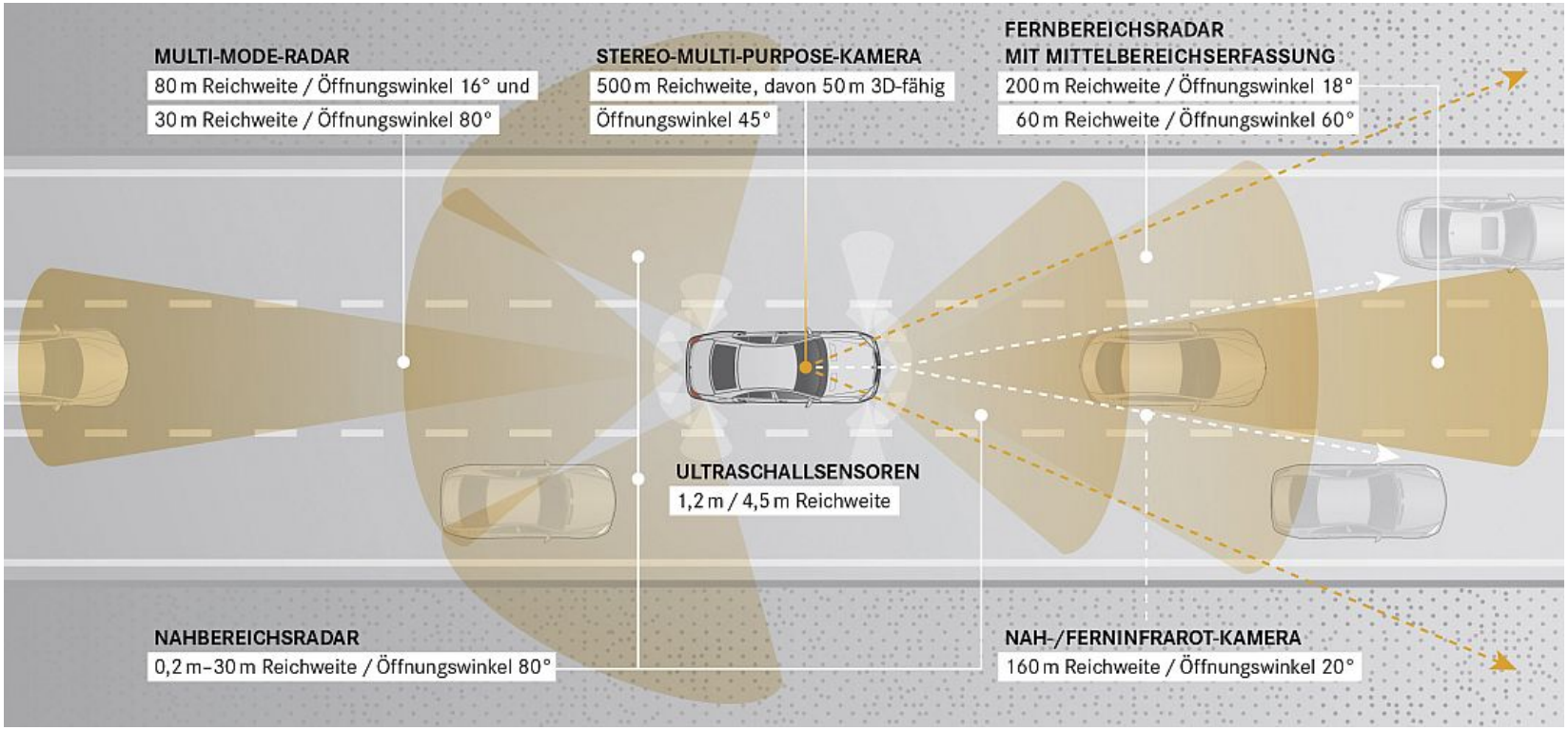
3. **Aktionsebene:**

   Welche Möglichkeiten zur Reaktion habe ich und wie setze ich diese optimiert zum Erreichen des Ziels ein?

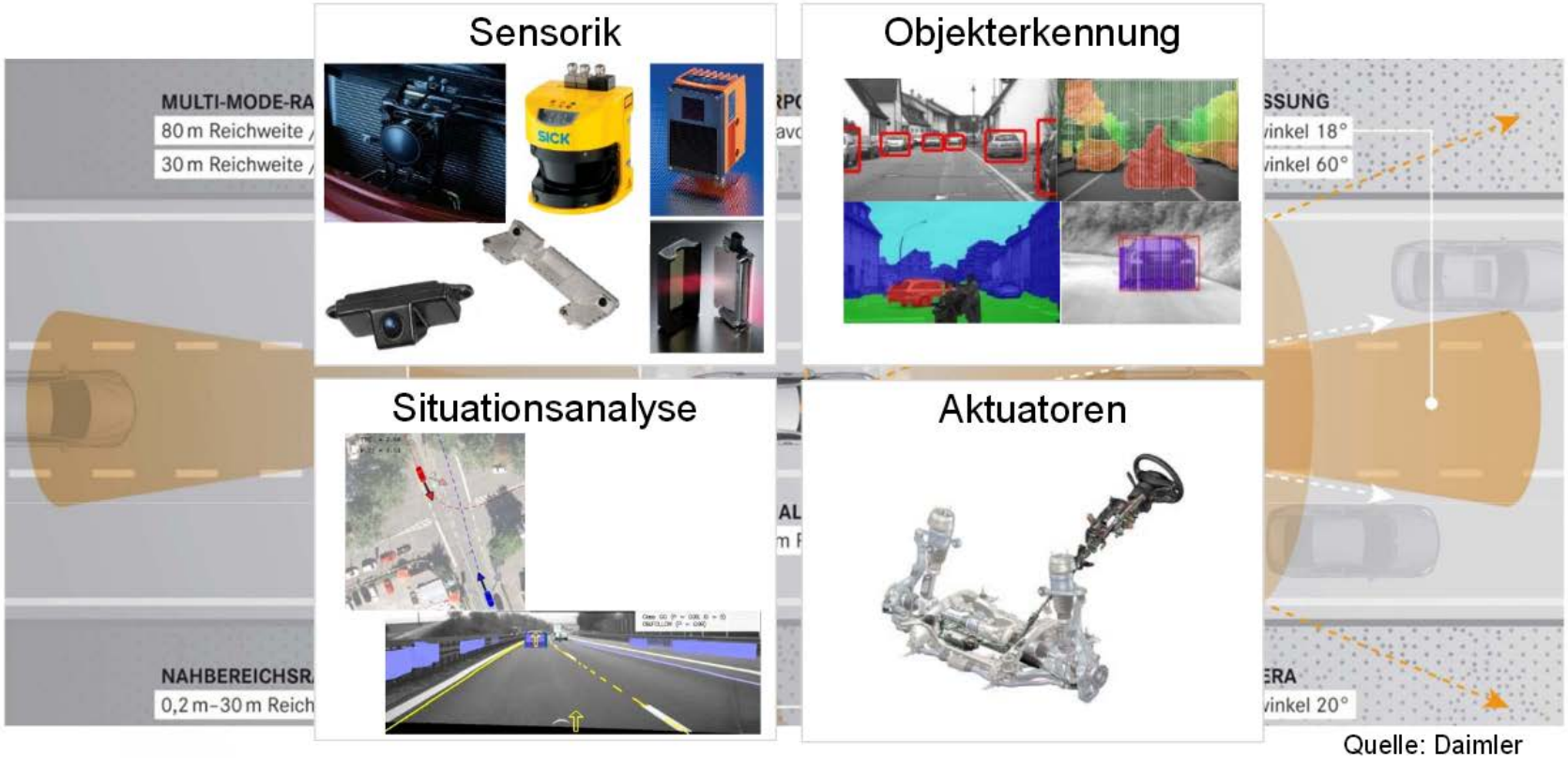
4. **Ausführungsebene:**

   Wie bediene ich die mir zur Verfügung stehenden Aktoren, um die beabsichtige Aktion korrekt auszuführen?

Beispiel: Sensoren in der Mercedes S-Klasse



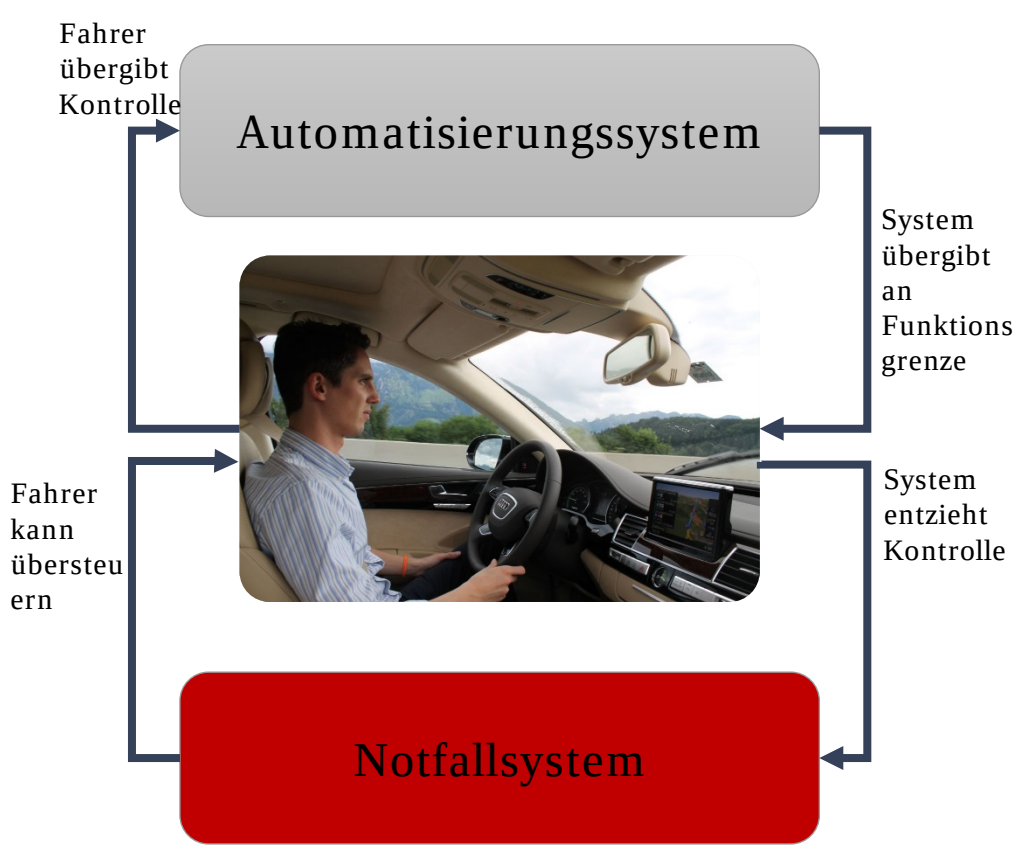
Quelle: Daimler



Quelle: Daimler

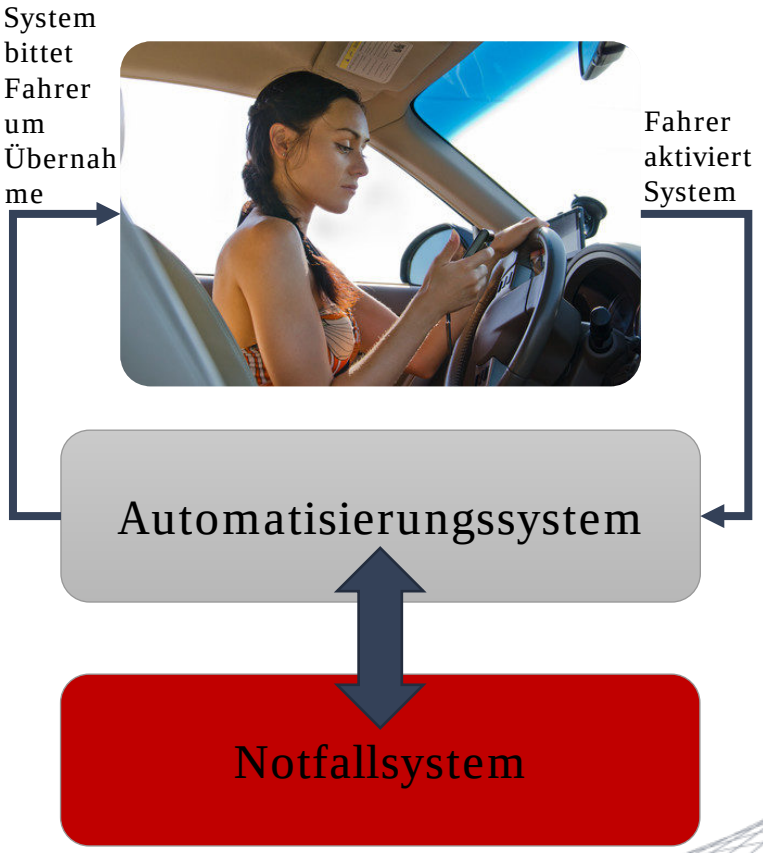
Teilautomatisiert

Driver in the Loop



Hochautomatisiert

Driver out of the Loop



Quelle: Herrtwich

Teilautomatisiert

„Forseeable Misuse“ muss vermieden sein

- Fahrer muss das System überwachen
- System muss überwachen, dass der Fahrer es überwacht

Technische Lösung der Überwachung

- Invasiv/Substitute
  - Lenkmomentsensor
  - Totmannschalter
  - Voice Challenge and Response
- Nicht invasiv
  - Fahrerkamera
  - ...

Hochautomatisiert

Rückfallebene Fahrer unzuverlässig

- Fahrer darf Nebentätigkeiten durchführen
- Rückfallebene Fahrer existiert für eine gewisse Zeit nicht (neue ASIL-Bewertung)

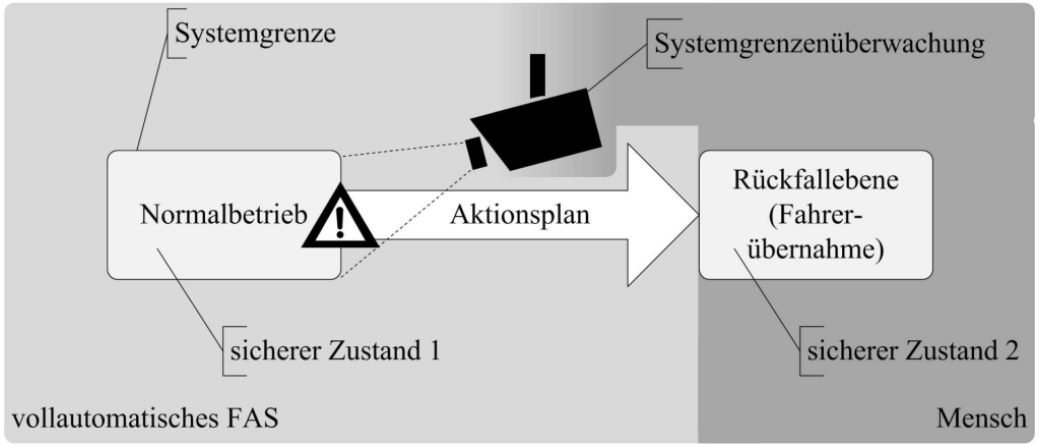
Notwendige Neubetrachtung der Aktorik

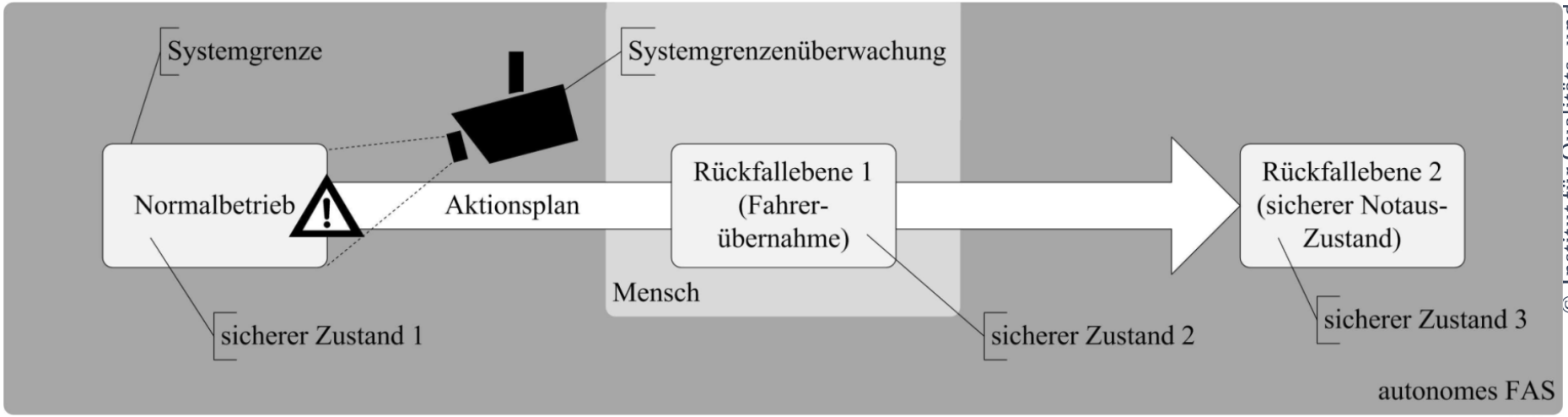
- Lenkung
- Bremse

Technik der Überwachung und Auslegung der Aktorik bestimmt Freiheit des Fahrers

Quelle: Herrtwich

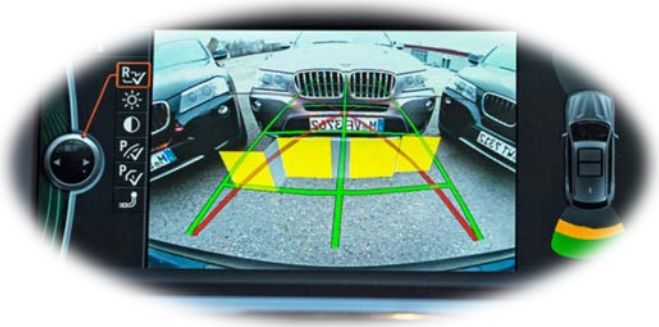
ÜBERGEORDNETE STRATEGIEN





(HÖRWICK, 2011)

DAS FAHRZEUG DER ZUKUNFT…



…lernt sehen
Kameratechnologie

…lernt mit anderen Fahrzeugen zu reden
drahtlose, mobile Kommunikation

…spricht uns an
digitale Darstellung
digitale Sprache

…lernt seine Umgebung zu verstehen
Erfassen von Trajektorien

Quelle: Text nach Leohold

WIR FREUEN UNS AUF IHRE FRAGEN!

Prof. Dr.-Ing. Arno Meyna

Leiter des Fachgebiets
Sicherheitstheorie und
Verkehrstechnik

Bergische Universität Wuppertal

Mail: meyna@uni-wuppertal.de

www.sitheorie.uni-wuppertal.de

Dr.-Ing. Andreas Braasch

Geschäftsführender Gesellschafter

IQZ GmbH

Mail: braasch@iqz-wuppertal.de

Tel.: +49 (0)202 – 515 616 90

Fax: +49 (0)202 – 515 616 89

www.iqz-wuppertal.de