DHBW

Wenn die Software fährt –
Kann man der Software im Auto sein Leben anvertrauen?

Prof. Dr. Florian Leitner-Fischer

Herzlich Willkommen

Prof. Dr. Florian Leitner-Fischer

Studiengangsleiter Embedded Systems – Aerospace / Automotive Engineering

- Mehrere Jahre Erfahrung in der Entwicklung von sicherheitskritischer Automobil Software
- Forschung im Bereich Analyse von sicherheitskritischen Systemen und Software

Können wir der Software im Auto unser Leben anvertrauen?


Wer von Ihnen hat sich schon mal unwohl gefühlt als Sie nicht die Kontrolle über das Fahrzeug hatten?
Wer von Ihnen hat sich schon mal von einem Fahrerassistenzsystem unterstützen lassen?

Das letzte Auto in dem ich mich unwohl gefühlt habe …

Agenda

- Software im Automobil
- Sicherheit
- Ausblick & Diskussion

Software im Automobil

Wenn wir über Software im Automobil sprechen, sprechen wir oft von **Embedded Systems** oder **Embedded Software**

Embedded Systems

Was ist ein „Embedded System“?

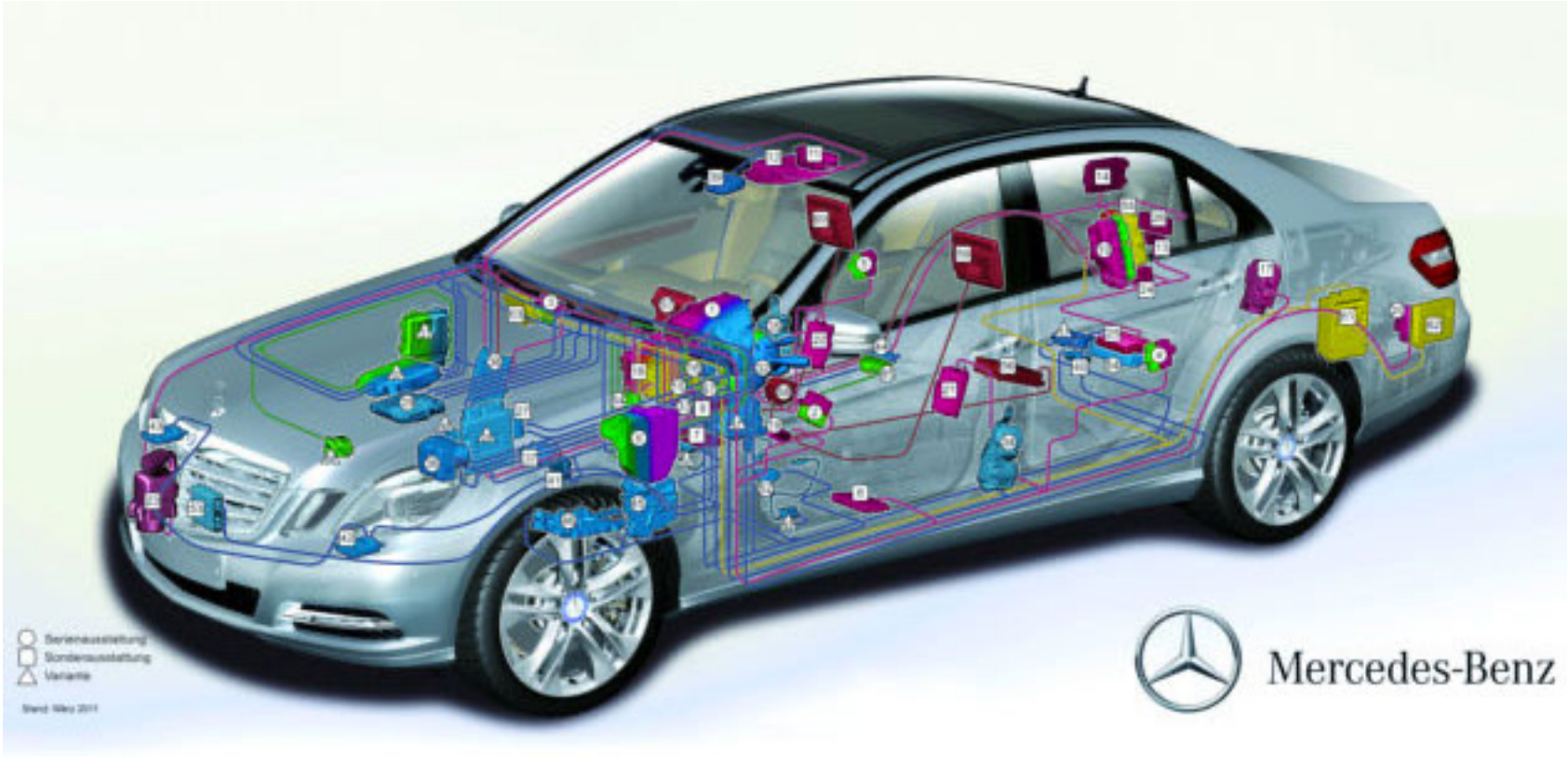
Definition: Embedded System

- Embedded Systems (engl.) = Deutsch: Eingebettete Systeme

Eingebettete Systeme sind informationsverarbeitende Systeme, die in ein größeres Produkt integriert sind, und die normalerweise nicht direkt vom Benutzer wahrgenommen werden.

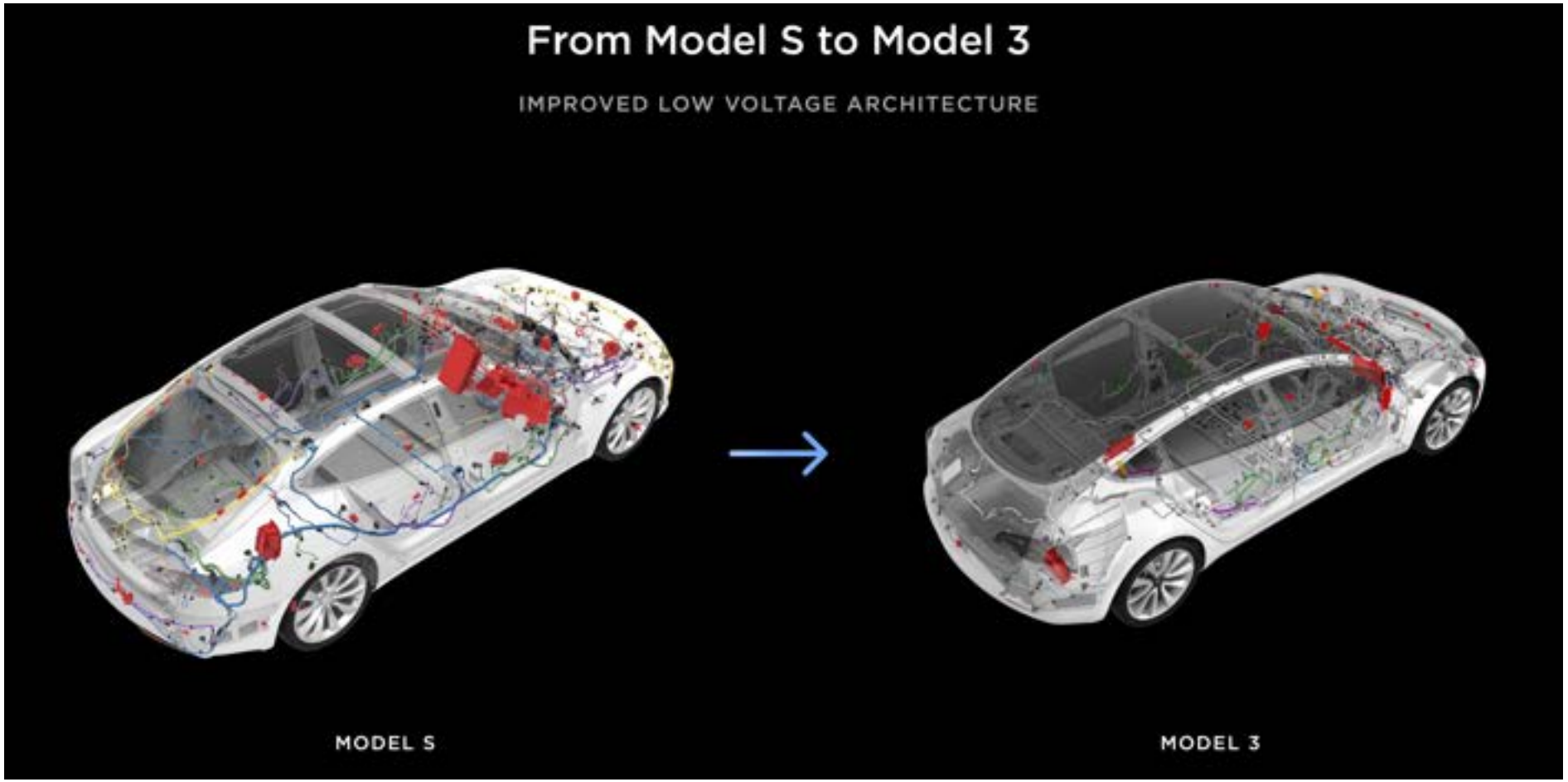
[Marwedel]

Embedded Systems im Kfz



*Mercedes Benz AG

Embedded Systems im Kfz



* Tesla Investor Day 2023. https://digitalassets.tesla.com/tesla-contents/image/upload/IR/Investor-Day-2023-Keynote

Rahmenbedingungen Kfz

Kraftfahrzeuge (Kfz) sind **komplexe** Systeme, die aus **sehr viele Teilen** aus **verschiedenen Materialien** und **Technologien** bestehen.

*Bild: Christian Bittmann, Autobild, Mercedes B-Klasse

Anforderungen (Missionprofile):

- Lebensdauer: 15 Jahre
- 300.000 km, 8000h Fahren
- Ersatzteile: 15 Jahre nach End of Production (EOP)

- Umwelteinflüsse
  - Wasser, Salz, Staub, EMV …
  - Temperatur -40 … +85 °C

Rahmenbedingungen Kfz

PKW Neuzulassungen 2022 in Deutschland

	Modell	Neuzulassungen
1	VW Golf	84.282
2	VW Tiguan	59.136
3	VW T-Roc	58.942
4	Fiat 500	52.337
5	Opel Corsa	50.191
6	Mini	40.142
7	Passat	39.261
8	Kuga	38.482
9	BMW 3er	36.231
10	Tesla Model Y	35.426

VW Golf 7: ca. 6 Millionen verkaufte Fahrzeuge (2012-2019)

* Quelle: KBA: https://www.kba.de/SharedDocs/Downloads/DE/Statistik/Fahrzeuge/FZ10/fz10_2022_12.xlsx?__blob=publicationFile&v=3

Besonderheiten Embedded Systems im Kfz

- Herausforderungen in der Automotive Entwicklung
  - Hohe Anzahl an Funktionen (von Basis Funktionen bis hin zu komplexen Fahrfunktionen)
  - Steigende Komplexität (Vielfalt an Technologien, Softwareanteil, Komplexität der Funktion)
  - Einfluss auf Sicherheit (Unfallrisiko)
  - Einfluss auf Umwelt (CO2 Emissionen)
  - Hohe Stückzahlen (mehrere Millionen)
  - Hohe Lebensdauer (mehr als 15 Jahre) / Missionsprofil
  - Einhaltung von Gesetzen (Marktabhängig)
  - Geringe Kosten (von wenigen € bis wenige 100 €)
  - Kurze Entwicklungszeiten (weniger als 2 Jahre)
  - Hohe Interaktion zwischen Kfz-Hersteller und mehreren Zulieferer (mehrere Ebenen (Tier))
  - Hohe Anforderungen an Zuverlässigkeit

Rahmenbedingungen Kfz: Toyota Unintended Acceleration

Toyota "Unintended Acceleration" Has Killed 89

A 2005 Toyota Prius, which was in an accident, is seen at a police station in Harrison, New York, Wednesday, March 10, 2010. The driver of the Toyota Prius told police that the car accelerated on its own, then lurched down a driveway, across a road and into a stone wall. (AP Photo/Seth Wenig) AP PHOTO/SETH WENIG

Unintended acceleration in Toyota vehicles may have been involved in the deaths of 89 people over the past decade, upgrading the number of deaths possibly linked to the massive recalls, the government said Tuesday.

The National Highway Traffic Safety Administration said that from 2000 to mid-May, it had received more than 6,200 complaints involving sudden acceleration in Toyota vehicles. The reports include 89 deaths and 57 injuries over the same period. Previously, 52 deaths had been suspected of being connected to the problem. http://www.cbsnews.com/news/toyota-unintended-acceleration-has-killed-89/

- Toyota Recall ABC News: https://www.youtube.com/watch?v=uhXbl132SAA
- NASA Report: https://www.youtube.com/watch?v=TZxuVFHVvIE

„Unbeabsichtigte Beschleunigung“ in Toyota und Lexus Fahrzeugen zwischen 2000-2010

Rahmenbedingungen Kfz: Toyota Unintended Acceleration

Toyota Case: Single Bit Flip That Killed

Junko Yoshida

10/25/2013 03:35 PM EDT

During the trial, embedded systems experts who reviewed Toyota's electronic throttle source code testified that they found Toyota's source code defective, and that it contains bugs -- including bugs that can cause unintended acceleration.

"We did a few things that NASA apparently did not have time to do," Barr said. For one thing, by looking within the real-time operating system, the experts identified "unprotected critical variables." They obtained and reviewed the source code for the "sub-CPU," and they "uncovered gaps and defects in the throttle fail safes."

The experts demonstrated that "the defects we found were linked to unintended acceleration through vehicle testing," Barr said. "We also obtained and reviewed the source code for the black box and found that it can record false information about the driver's actions in the final seconds before a crash."

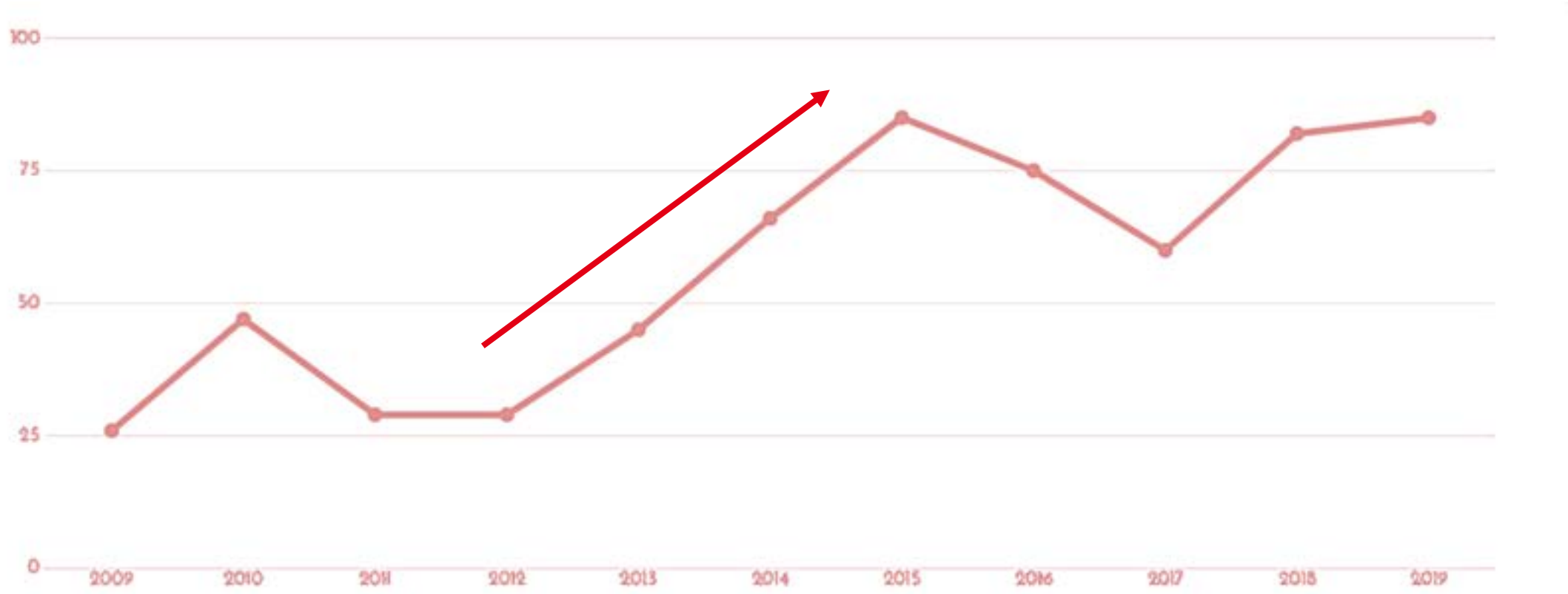
Stack overflow and software bugs led to memory corruption, he said. And it turns out that the crux of the issue was these memory corruptions, which acted "like ricocheting bullets."

Barr also said more than half the dozens of tasks' deaths studied by the experts in their experiments "were not detected by any fail safe."

Fehler (bugs) in der Software welche unbeabsichtigte Beschleunigung verursachen können

Die gefunden Fehler konnten in Fahrzeugtests unbeabsichtigte Beschleunigung verursachen

Rahmenbedingungen Kfz: Automotive Rückrufe aufgrund Software



* NHTSA Datenbank, https://www.nhtsa.gov/nhtsa-datasets-and-apis#recalls

Rückrufe

VOLKSWAGEN

Probleme mit dem Infotainment: VW Golf 8 braucht weiteres Software-Update

Anders als Tesla kann Volkswagen bislang nicht online updaten. Tausende Fahrzeuge des Golf 8 müssen für das jüngste Update darum in die Werkstatt.

Handelsblatt, 12.01.2021

AUTOPILOT

China ordnet Rückruf von Hunderttausenden Tesla-Fahrzeugen an

Probleme mit dem Tesla-Autopiloten können Unfälle verursachen, glauben chinesische Behörden und ordnen einen Rückruf von mehr als 285.000 Fahrzeugen an.

Handelsblatt, 27.06.2021

ELEKTROAUTOBAUER

Gefährlicher Autopilot: Tesla muss 362.000 Autos updaten

Wegen erhöhter Unfallgefahr bei seinem Assistenzsystem muss Tesla ein Update aufspielen. Der Rückruf ist der neueste Rückschlag für die Autopilot-Strategie, die immer mehr Behörden kritisch sehen.

Handelsblatt, 14.10.2022

AUTOBAUER

Opel ruft fast 200.000 Insignia zurück

Nach dem Dauerbrenner Corsa müssen die Rüsselsheimer auch beim auslaufenden Spitzenmodell nachbessern. Das ABS braucht ein Software-Update, Schäden sind bisher nicht bekannt.

Handelsblatt, 16.02.2023

ELEKTROAUTO

Softwareprobleme beim Taycan: Porsche ruft weltweit 43.000 E-Sportwagen zurück

Porsche muss die Software der Motorsteuerung beim Modell Taycan aktualisieren. Dafür müssen weltweit rund 43.000 Fahrzeuge in die Werkstatt.

Handelsblatt, 02.07.2021

Besonderheiten Embedded Systems im Kfz

- Sehr hohes Produktions- / Marktvolumen

- Oft Sicherheitskritisches System

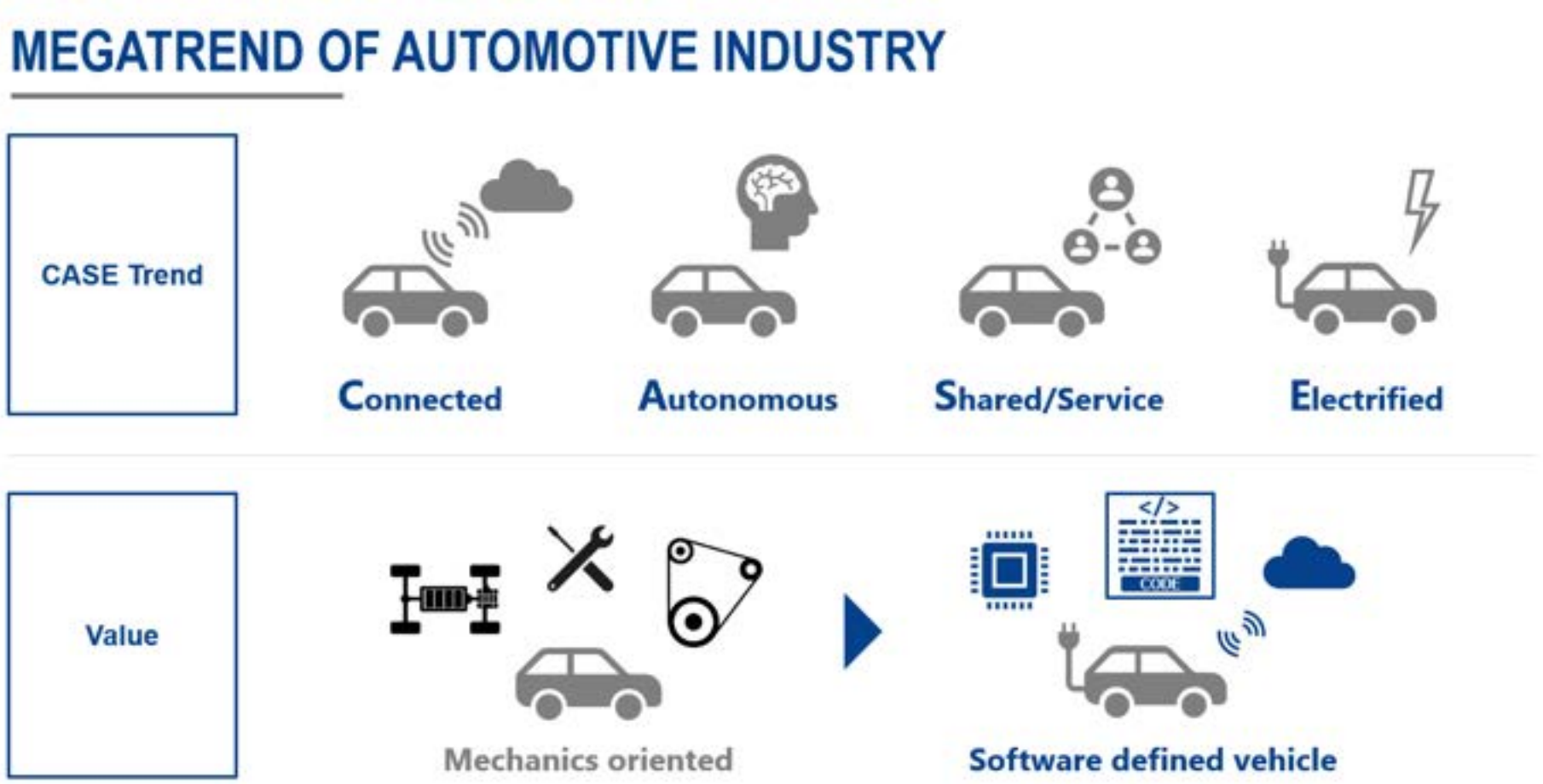
> Sicherheitskritisches System: Ein System, bei dem eine Fehlerwirkung oder Fehlfunktion zum Tod oder ernsthafter Verletzung von Personen führen kann, oder zum Verlust oder schwerem Schaden von Gerätschaften, oder zu Umweltschäden. [ISTQB Glossary]

- Oder reguliertes System (Abgasskandal)

Ergebnis: Hohe Anforderungen an Qualität und Funktion

* [ISTQB Glossary]: https://glossary.istqb.org/de/term/sicherheitskritisches-system

Automotive Mega Trends



* Renesas (https://www.renesas.com/kr/en/blogs/overview-renesas-automotive-business-strategy)

Embedded Systems im Kfz

Die Bedeutung von Elektronik und Software im Auto nimmt rasant zu. Die Kosten für elektronische Komponenten pro Fahrzeug sollen **bis 2025** voraussichtlich **von rund 3.000 auf circa 7.000 US-Dollar steigen**. Das ist das zentrale Ergebnis der Studie "Computer on Wheels/Disruption in Automotive Electronics and Semiconductors" der Unternehmensberatung Roland Berger. **Autonomes Fahren, vollständige Vernetzung und die Elektromobilität sollen diese Entwicklung forcieren**.

Computer on wheels

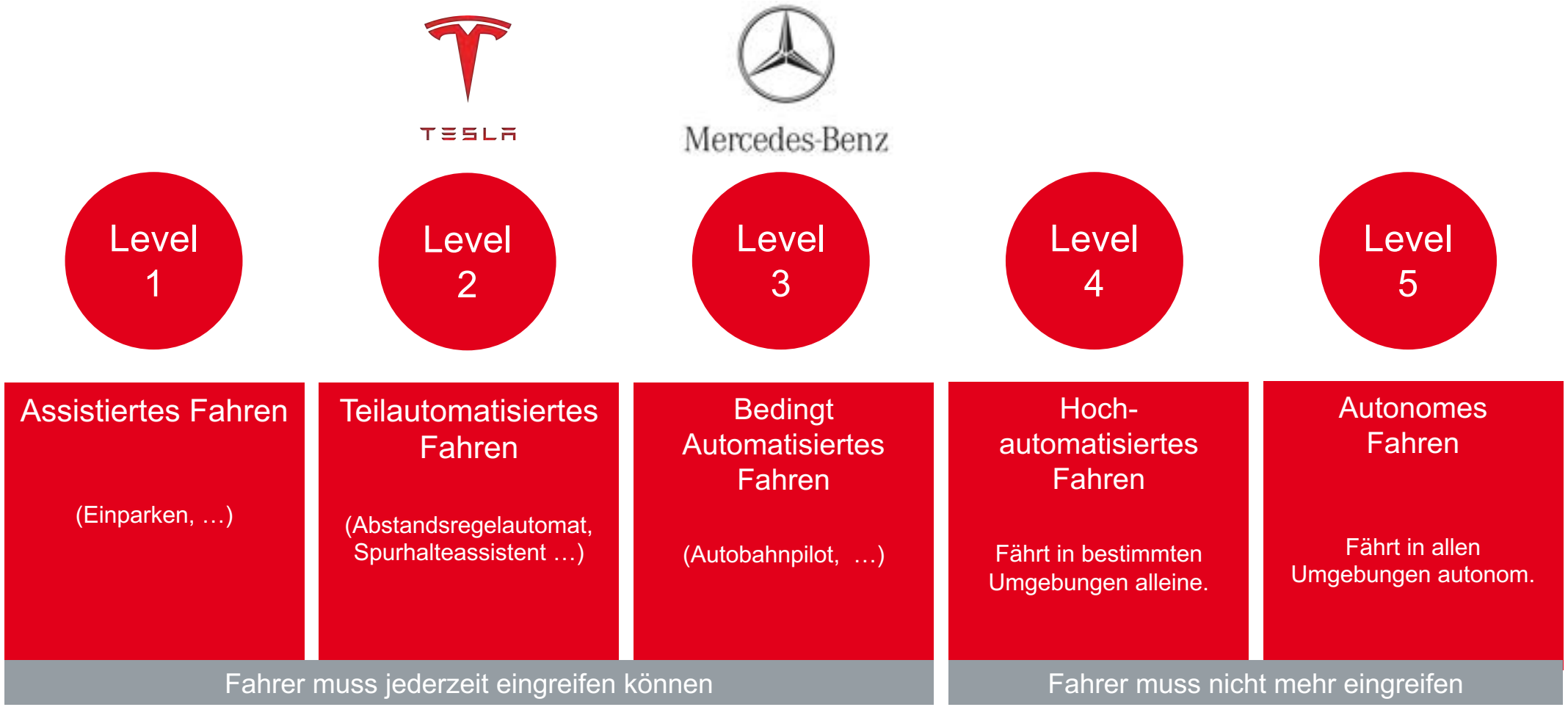
The importance of electronic components and software in vehicles is steadily increasing

Roland Berger

Bezieht sich auf Hardwarekosten hinzu kommt Wertschöpfung durch Software

* https://www.springerprofessional.de/automobilelektronik---software/mobilitaetskonzepte/bedeutung-von-elektronik-und-software-im-auto-nimmt-rasant-zu/17573872
https://www.rolandberger.com/en/Insights/Publications/The-car-will-become-a-computer-on-wheels.html

Die 5-Stufen des Autonomen Fahren



Software übernimmt im Fahrzeug immer mehr **sicherheitskritische Funktionen**.

Was ist Sicherheit für Sie?

Was ist Sicherheit?

- Betriebssicherheit (safety)
  - Sicherheit der Situation, die vom System geschaffen wird
  - Das System verhält sich entsprechend der Spezifikation fehlerfrei und gefährdet die Benutzerin / den Benutzer nicht
  - Annahme: Keine externen Akteure, keine Manipulation
  - z.B. Notausgangstüre

- Angriffssicherheit (security)
  - Sicherheit in Bezug auf äußere Manipulation
  - Nicht nur wahrscheinliche Fehlerszenarien müssen betrachtet werden
  - z.B. Türschloss

Funktionale Sicherheit: Definition

- Funktionale Sicherheit
  Kein inakzeptables Risiko aufgrund von Gefahren, die durch fehlerhaftes Verhalten von Elektronisch / Elektrischen -Systemen verursacht werden
  - Beispiele
    - Airbag löst unbeabsichtigt aus (ohne Aufprall)
    - Airbag-Auslösung im Falle eines Unfalls sicherstellen
    - Unbeabsichtigtes Bremsen durch Fahrerassistenzsystem ausgelöst
    - Destabilisierung des Fahrzeugs durch ESC-ausgelöste Bremssteuerung

... und die Herausforderung
das System so auszulegen, dass gefährliche Ausfälle vermieden oder kontrolliert werden, wenn sie auftreten

Norm: ISO 26262 Road Vehicles - Functional Safety

Funktionale Sicherheit: der "risikobasierte Ansatz"

Restrisiko	≤	Von der Gesellschaft akzeptiertes Risiko

Ziel: Vermeidung von systematischen Ausfällen und Kontrolle von systematischen und zufälligen Ausfällen, um das zu erwartende Risiko auf ein akzeptables Maß zu reduzieren

Akzeptables Restrisiko?

Welches Restrisiko ist für uns als Gesellschaft akzeptabel?

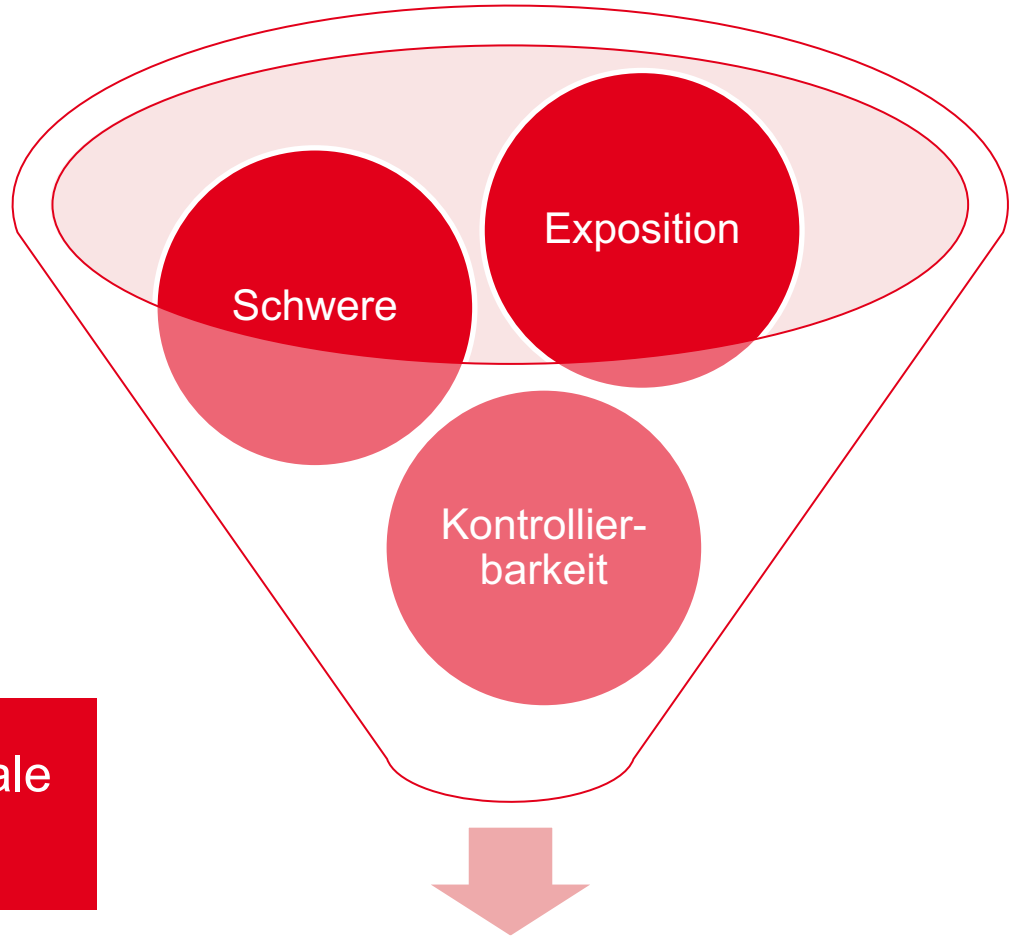
Akzeptables Restrisiko?

- Minimale endogene Mortalität
  - Wahrscheinlichkeit eines tödlichen Versagen das Systems muss kleiner der statistischen Mortalität sein ($2 * 10^{-4}$ für eine(n) europäische(n) Jugendliche(n))

- „As low as reasonably practicable“ = So niedrig wie angemessen machbar
  - Neue Technologien sollen in der Regel mindestens gleich sicher sein wie bestehende Technologien

Gefährdungsanalyse und Risikobewertung

- Gefährdungsanalyse und Risikobewertung
  - Situationsanalyse
    [Betriebssituationen, Betriebsarten,]
  - Gefahrenidentifikation und
    Klassifikation
  - Bestimmung von ASIL
    und Sicherheitsziel



Wie wirken sich Fehlfunktionen auf die funktionale Sicherheit aus?

Automotive Safety Integrity Level
ASIL A (niedrig) - ASIL D (hoch)

Sicherheit

- Funktionale Sicherheit
  - Die ISO 26262 betrachtet die Risiken, die durch **zufällige Hardwarefehler** und **systematische Fehler** entstehen.
  - **Zufällige Hardwarefehler:**
    - Für Hardware wird angenommen das diese „zufällig“ ausfällt bzw. der Ausfall von Hardware durch statistische Verteilungen vorhergesagt / abgeschätzt werden kann

    Sicherheitsnachweis durch Sicherheitsanalysen und Berechnung der Fehlerwahrscheinlichkeit

  - **Systematische Fehler:**
    - Fehler im Design (Software) / Produktion der nur durch eine Änderung behoben werden kann

    Sicherheit durch „gutes Engineering“: Methoden der Entwicklung und Tests werden je nach Sicherheitslevel (ASIL) vorgeschrieben

Software Fehler sind systematische Fehler

- Ziel: < 0,5 Fehler / 1000 Code Zeilen

- Problem:
  - Software ist diskret
  - Wenn 1 Zeile Fehlerhaft ist kann dies zu einem katastrophalen Fehler führen

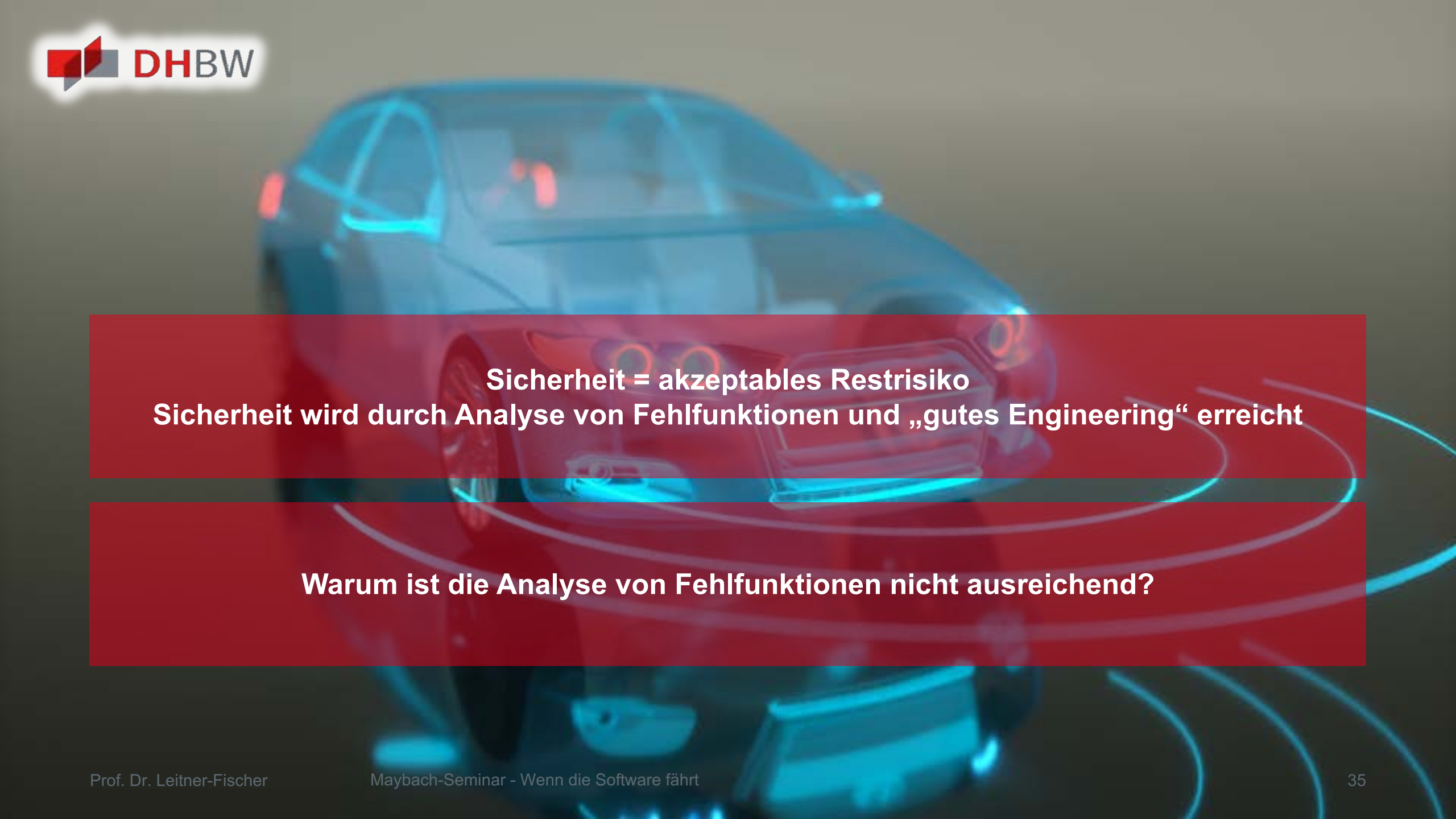
Wie findet man systematische Fehler?

- Testen?

> “Program testing can be used to show the presence of bugs, but never to show their absence!”
>
> — Edsger W. Dijkstra

Wie findet man systematische Fehler?

- Problem beim Testen:



Sicherheit = akzeptables Restrisiko
Sicherheit wird durch Analyse von Fehlfunktionen und „gutes Engineering“ erreicht

Warum ist die Analyse von Fehlfunktionen nicht ausreichend?

Und dann kam der Kunde …

* Tesla Motors Club

Und die Umgebung ...

Tesla-Auto

Tödlicher Unfall mit Autopilot

Wie sicher sind autonom fahrende Autos? Diese Frage hat eine neue Brisanz bekommen. Zum ersten Mal starb ein Autofahrer in einem Wagen, der vom Computer gelenkt wurde. Das Fahrassistenz-System eines Tesla-Autos hatte offenbar im hellen Licht einen weißen LKW-Anhänger nicht erkannt.

01.07.2016

Sicherheit ist mehr als die Vermeidung von Fehlfunktionen

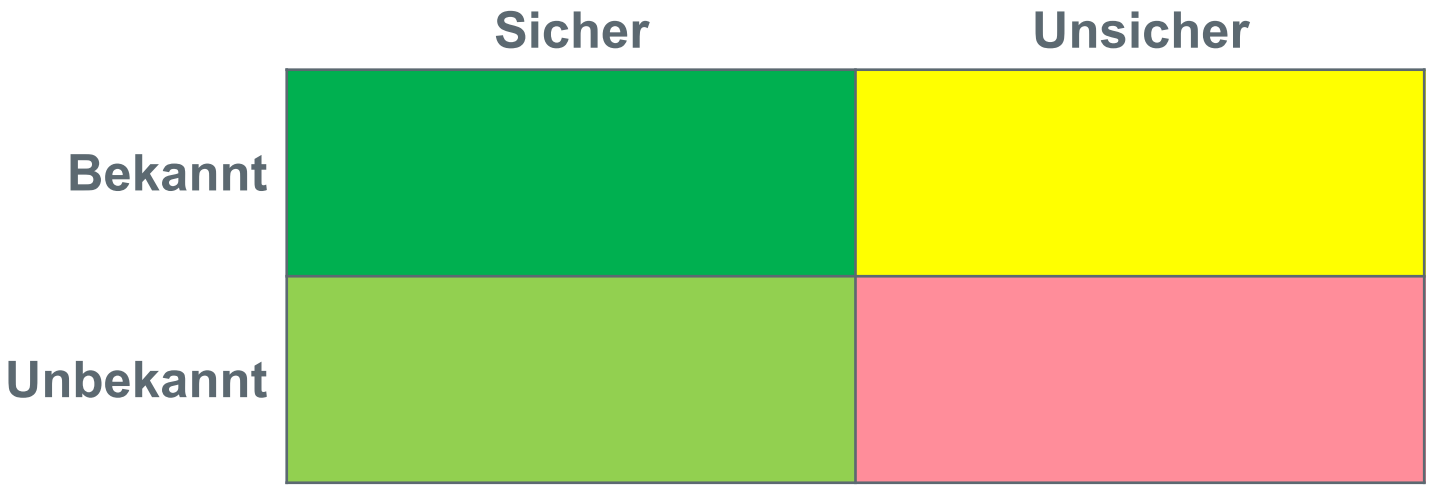
Sicherheit bedeutet auch, dass die eigentliche Funktion so funktioniert wie sie soll …

- Safety of the Intendend Function (SOTIF)
  - Die Beabsichtigte Funktion (zum Beispiel Fahrerassistenzsyteme) sollen sicher sein

Safety of the Intendend Function (SOTIF)

- Welche Grenzen hat das eingesetzte System?
  - Verarbeitungsgeschwindigkeit, Erkennungsfähigkeit, Schmutz auf Sensoren …
- Wie wirkt es sich aus, wenn das System außerhalb der spezifizierten Grenzen der Sollfunktion arbeitet?
  - Für Autobahnverkehr entwickelt, in der Stadt genutzt
- Wie kann der Fahrer ein Assistenzsystem fehlerhaft nutzen?
  - Vorhersehbarer Fehlgebrauch
- Welche Verifikations- und Validierungsmaßnahmen sind zu ergreifen, um die Sollfunktion zu prüfen?
  - Wie viel reale Fahrkilometer, …
- Ist die Bedienung des Systems für den Fahrer klar und eindeutig?

Safety of the Intendend Function (SOTIF)

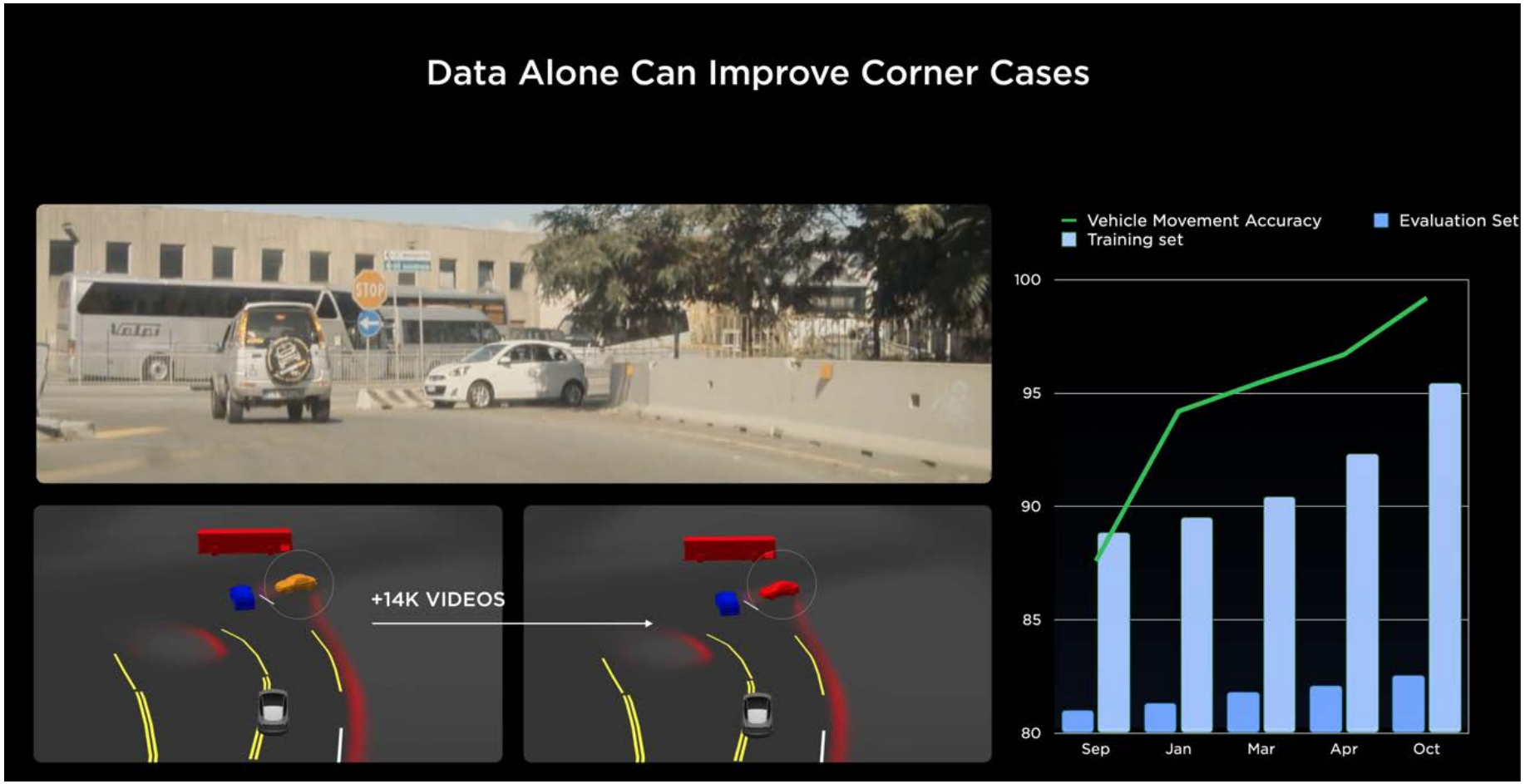


Beispiel: Tesla

- Was sehen Sie hier?

* Tesla Investor Day 2023. https://digitalassets.tesla.com/tesla-contents/image/upload/IR/Investor-Day-2023-Keynote

Beispiel: Tesla



* Tesla Investor Day 2023. https://digitalassets.tesla.com/tesla-contents/image/upload/IR/Investor-Day-2023-Keynote

Grundsätzlich wird bei SOTIF auch **vorhersehbarer Missbrauch** berücksichtigt.
Aber wo fängt dieser an und hört dieser auf?

Automotive Cyber Security

- Fahrzeuge sind heutzutage intelligente, vernetzte und Software-basierte Systeme

- Erhöhter Anteil an IT-Technologie / Vernetzung bringt die gleichen Herausforderungen mit sich wie in der IT:
  - Cloud-Dienste
  - Software als Dienstleistung

- Alle Funktionen sind ultimative Ziele für Angreifer

Security
=
Angriffssicherheit

Beispiel: Chrysler Hack

- „After Jeep Hack, Chrysler Recalls 1.4M Vehicles for Bug Fix“ (Wired, 24.07.15)
- Gravierende Sicherheitslücken im Entertainment-System
  - Fahrzeuge über Mobilfunknetz fernsteuerbar
  - Mangelhafte Angriffssicherheit kann auch Betriebssicherheit beeinträchtigen

Quelle: Andy Greenberg/Wired
Forscher: Charlie Miller
and Chris Valasek

* https://www.youtube.com/watch?v=MK0SrxBC1xs
* https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Cyber Security Management im Automotive Kontext

- **Funktionale Sicherheit (Safety)** ist die Vermeidung von Gefahren, die durch zufällige Ereignisse verursacht werden.

- **Cybersicherheit** ist die Verhinderung von Bedrohungen, die durch absichtlich böswillig induzierte Ereignisse verursacht werden.

- **Cybersicherheit**: Freiheit von unangemessenen Risiken (im Bereich Safety, Financial, Operational und Privacy) aufgrund unbefugter Handlungen an Produkten durch einen Angreifer

- **Übergeordnetes Ziel: Risiko managen**, dass ein Angreifer ein Produkt angreift, um Schaden im Bereich Safety, Financial, Operational und Privacy anzurichten

Mit der UN ECE R155 und der ISO/SAE 21434 wurde Cyber Security in Automotive Umfeld regulatorisch verankert.

Sicherheit

- Sicherheit für Software im Automobil wird durch verschiedene Aspekte erreicht

Funktionale Sicherheit (Safety)

Sicherheit der beabsichtigte Funktion (SOTIF)

Cybersicherheit (Security)


DHBW
Können wir der Software im Auto unser Leben anvertrauen?
Was meinen Sie?

Vielen Dank

Prof. Dr. Florian Leitner-Fischer

Telefon +49.7541.2077.242

leitner-fischer@dhbw-ravensburg.de

Präsentation als PDF