TASTE

THE KNOWLEDGE

Automotive Software Engineering mit Expert:innen aus der Wissenschaft.

10.11.2023

AUTOMOTIVE SOFTWARE UPDATES

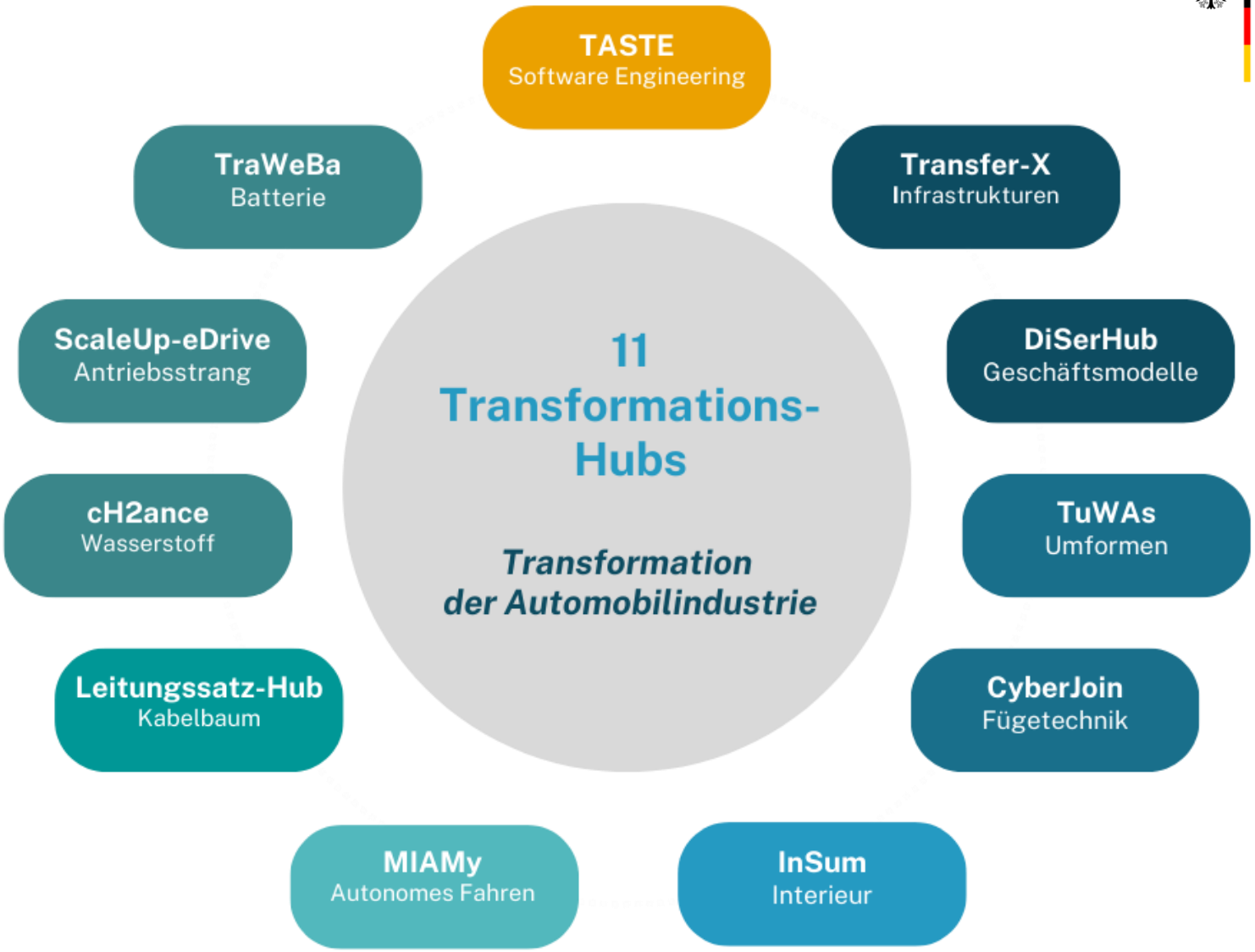
mit DLR

10.11.2023
13:00-14:30 Uhr
online

powered by ITS MOBILITY

FZI fortiss DLR Deutsches Zentrum für Luft- und Raumfahrt NFF NIEDERSÄCHSISCHES FORSCHUNGSZENTRUM FAHRZEUGTECHNIK ITS MOBILITY

TASTE


TASTE
Software Engineering
TraWeBa
Batterie
Transfer-X
Infrastrukturen
ScaleUp-eDrive
Antriebsstrang
DiSerHub
Geschäftsmodelle
11
Transformations-
Hubs
Transformation
der Automobilindustrie
cH2ance
Wasserstoff
TuWAs
Umformen
Leitungssatz-Hub
Kabelbaum
CyberJoin
Fügetechnik
MIAMy
Autonomes Fahren
InSum
Interieur

TASTE Transformations-Hub

Förderzeitraum	01.11.2022 – 30.06.2025
Budget Gesamt	3,8 Millionen Euro
Ziel	Automotive Software Engineering: Software-Zulieferkette als strategisches First Level Topic im Automobilsektor
Konsortium Konsortialführer Konsortialpartner	FZI DLR Deutsches Zentrum für Luft- und Raumfahrt NFF Niedersächsisches Forschungszentrum Fahrzeugtechnik ITS MOBILITY fortiss

TASTE
Software Engineering

ZIELE DES HUBS

Mission

Etablieren einer branchenweite Softwareentwicklungskultur in der Wertschöpfungskette der Automobilindustrie

Angebote

Vernetzung und Orientierung in der sich ändernden Softwarezulieferkette und Unterstützung beim Aufbau von Software-Engineering-Kompetenzen

Unterstützung von Unternehmen bei der Bewältigung der Herausforderungen, durch den schnell wachsenden Softwareanteil in der Zulieferkette:

- Kompetenzaufbau
- Neuausrichtung der eigenen Rolle als Unternehmen
- Eingehen von neuen Partnerschaften

INFORMATIONEN ÜBER DIE REFERIERENDEN

Kontaktdaten

1. IMPULSVORTRAG

Henning Schlender
henning.schlender@dlr.de

2. IMPULSVORTRAG

Björn Koopmann
bjoern.koopmann@dlr.de

3. IMPULSVORTRAG

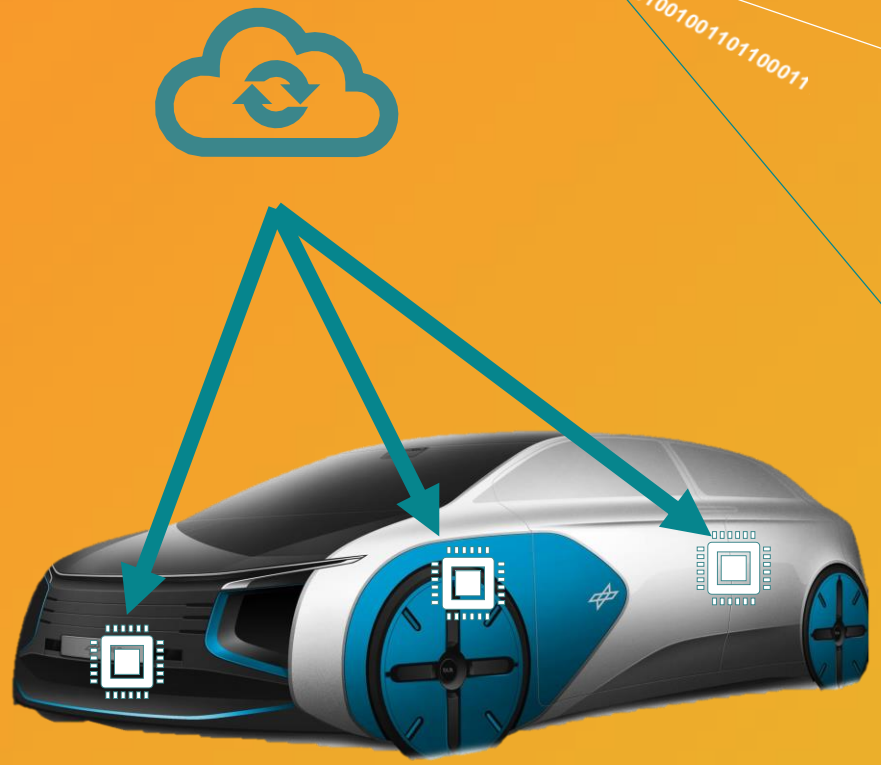
Karina Rothemann
karina.rothemann@dlr.de

AGENDA

1. Impulsvortrag – Henning Schlender
Automotive Software Updates: Herausforderungen und Perspektiven

2. Impulsvortrag – Björn Koopmann
Methoden und Techniken für sichere Over-the-Air-Updates

3. Impulsvortrag – Karina Rothemann
(Re-)Zertifizierung von Automotive Software Updates



AUTOMOTIVE SOFTWARE UPDATES: HERAUSFORDERUNGEN UND PERSPEKTIVEN

Henning Schlender (DLR)

WARUM AUTOMOTIVE SOFTWARE UPDATES?

REGULARIEN

- ISO 26262, ISO 21448, A-SPICE
- Road Vehicles Cyber Security
  - UNECE R155
  - ISO/SAE 21434
  - SAE J3061
  - NHTSA (USA)
- Road Vehicles SW Updates
  - ISO 24089
  - UNECE R156
  - AUTOSAR CP R20-11
  - GB201-5 (China)

KONTINUIERLICHE VERBESSERUNGEN

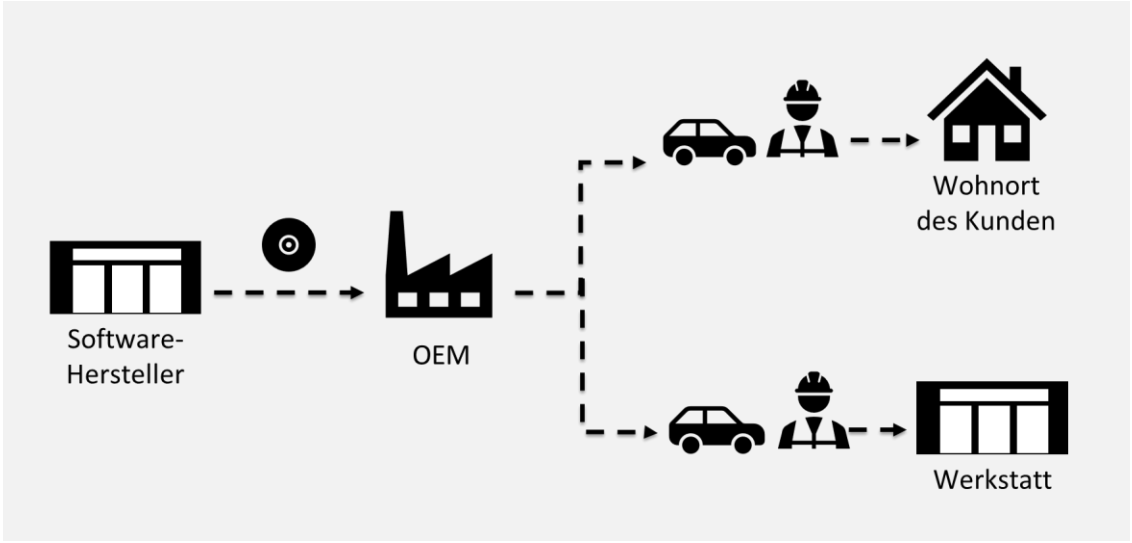
- Fehlerbehebung
- Sicherheitsupdates
- Funktionserweiterung
- Leistungssteigerung

MONETARISIERUNG

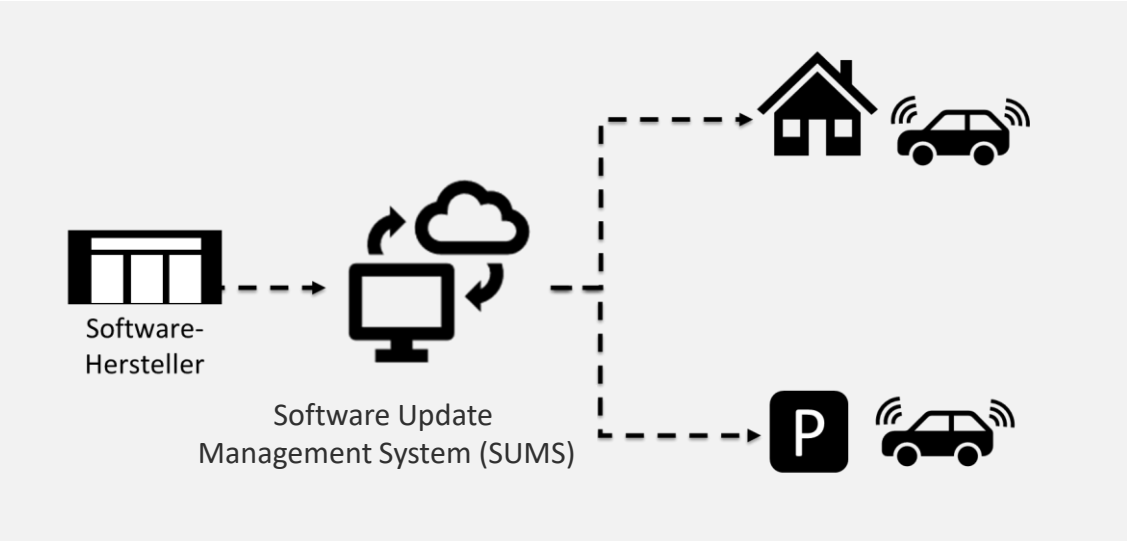
- Erweiterte Einstellmöglichkeiten für den Kunden
- Zusätzliche Funktionen
- Bsp: „Functions on Demand“ Audi

ENTWICKLUNG DER UPDATE-METHODIK

KONVENTIONELLE UPDATES

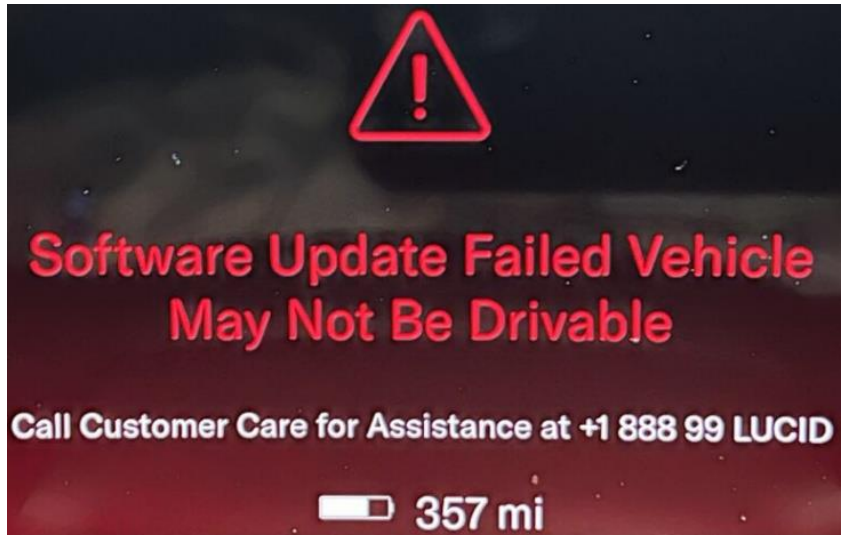


UPDATES IN ZUKUNFT



RISIKEN VON OTA-UPDATES

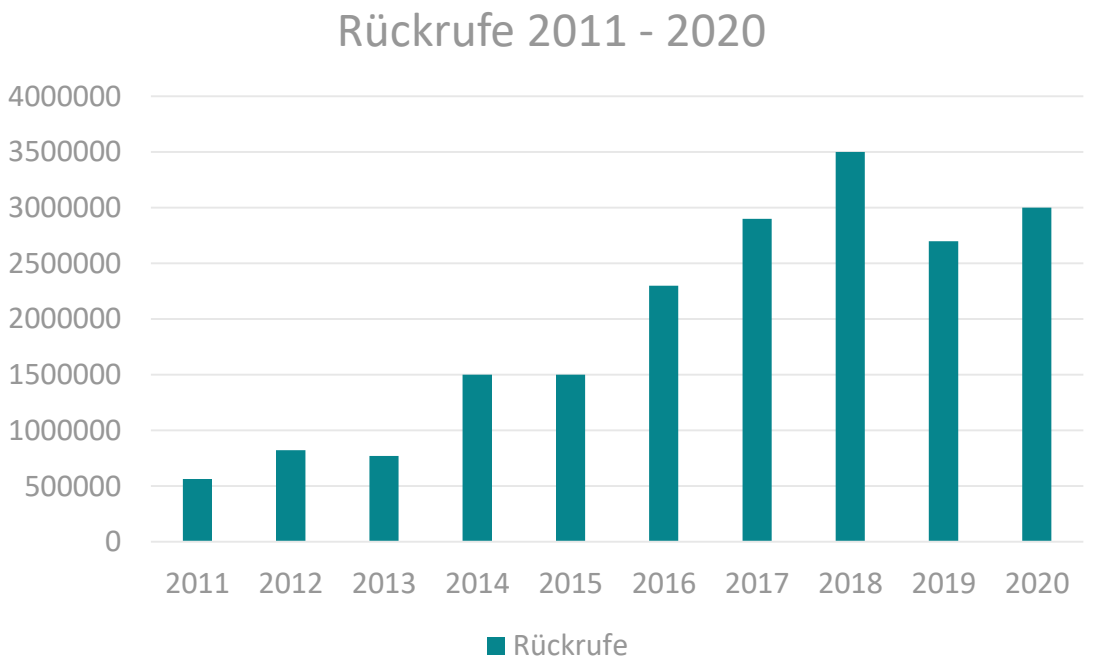
- Performance Probleme
- Einschränkung anderer Funktionen
- Beeinträchtigung der Fahrtüchtigkeit des Fahrzeugs



Quelle: Lucid Air briefly “bricked” after failed over-the-air software update - TopCarNews

RÜCKRUFAKTIONEN

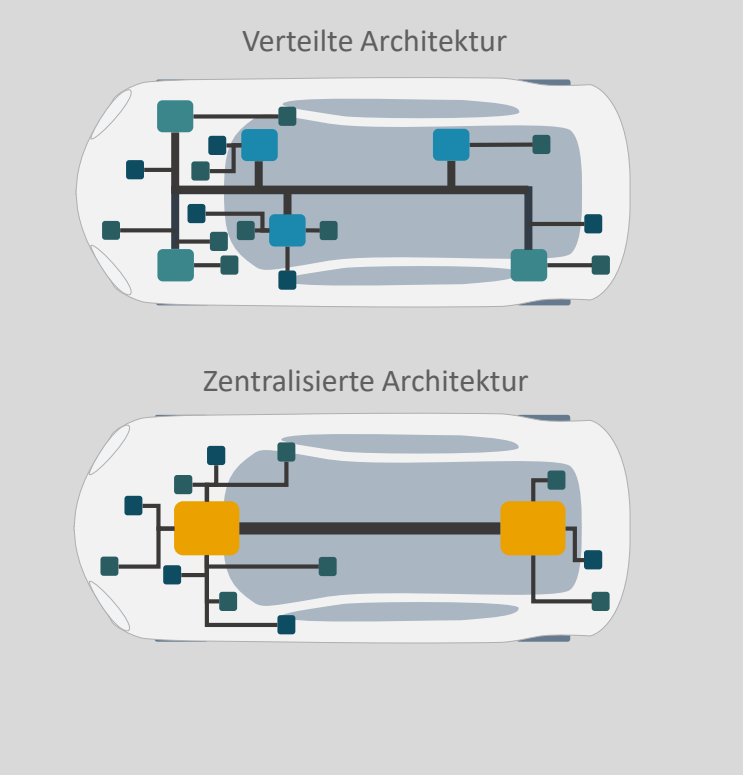
- Steigende Anzahl an Rückrufen bedingt durch SW erwartet
- Häufigere Werkstattbesuche sind den Kunden nicht zumutbar
- Kosteneinsparung



Quelle: https://www.bild.de/auto/auto-news/auto-news/kfz-rueckrufe-seit-2011-versechsfacht-werden-autos-immer-schlechter-78329254.bild.html

TREND ZUR ZENTRALISIERUNG

Zentralisierte Architektur / Zone ECUs



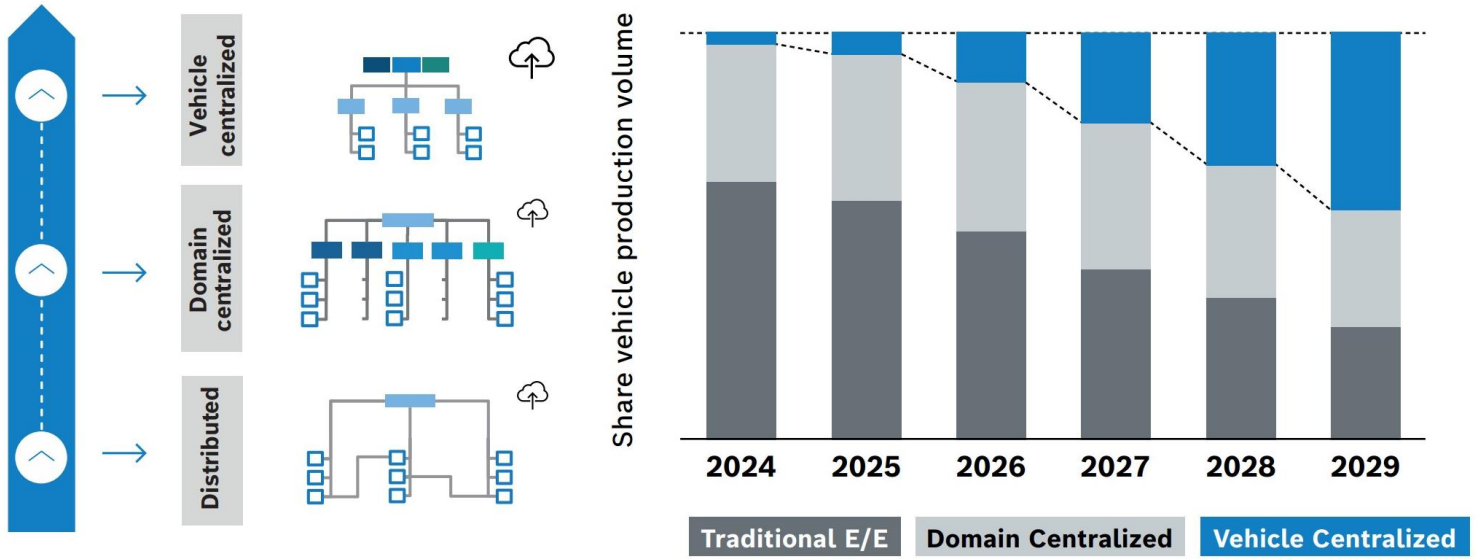


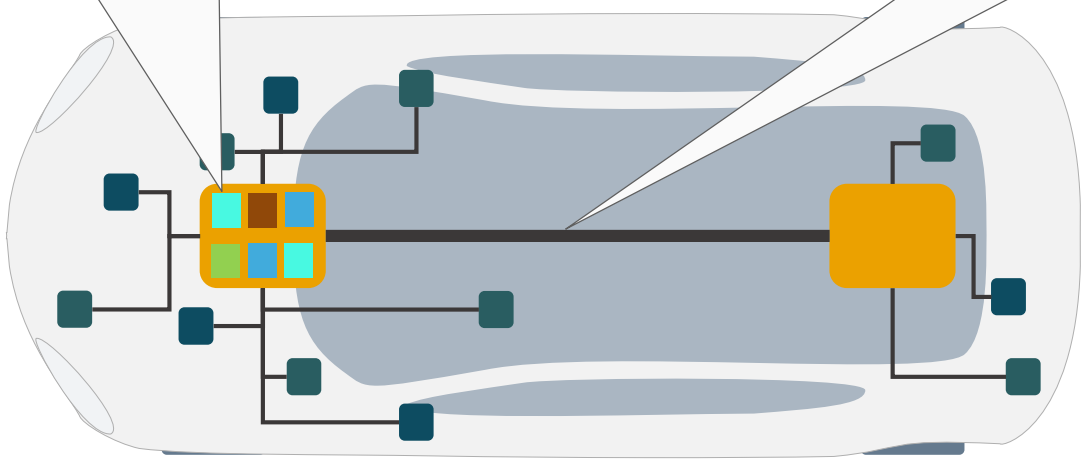
Figure 1: OEMs are ramping up new vehicle-centralized architectures and gradually replace prior architectural patterns.

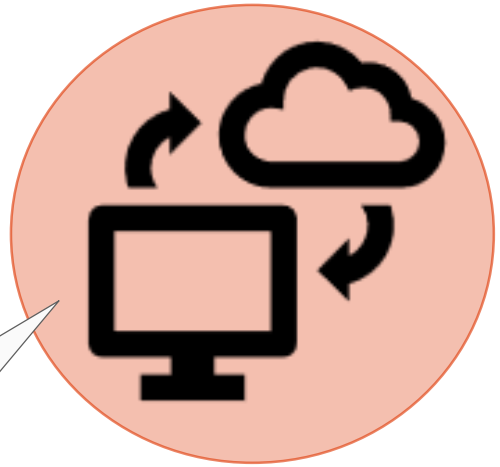
Quelle: Whitepaper The next step in E/E architectures, Bosch 2023

ZUKÜNFTIGE HERAUSFORDERUNGEN UND CHANCEN

Zone ECUs
- Betriebssystem vom OEM
- Beachtung zeitlicher und ressourcenbedingter Vorgaben
- Eingeschränkter Zugriff auf Plattform (Container)

Dynamische Verbindungen über Middlewares
- SOME/IP, Data-Distribution-Service Standard (DDS)
- Ethernet basiert
- Einsatz von Time-Sensitiv-Networks (TSN)



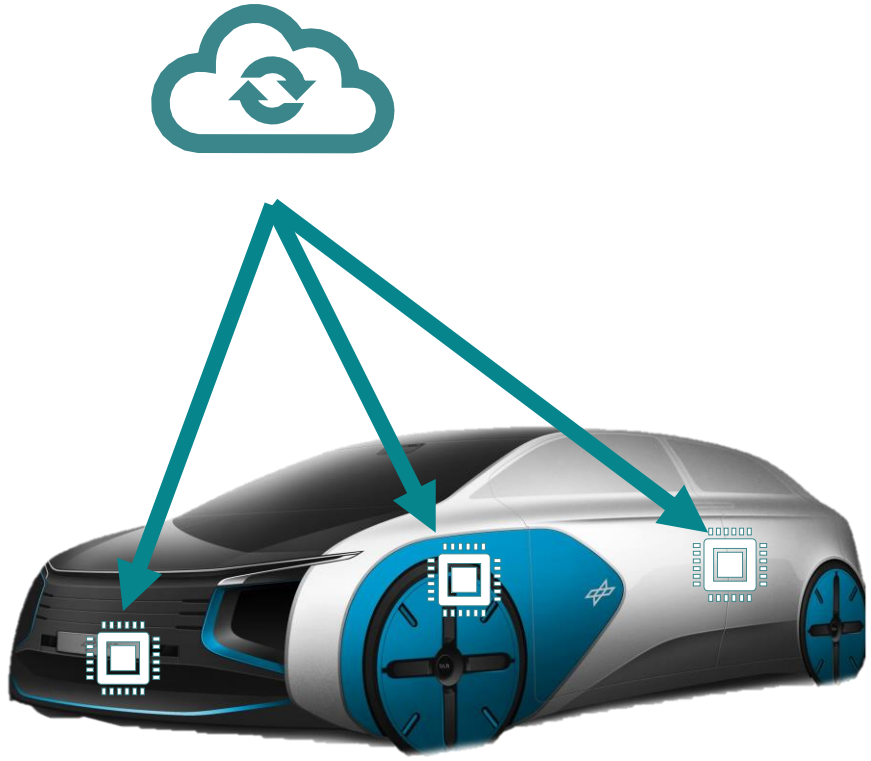


Software Update Management System (SUMS)

Änderungsmanagement / SUMS Center
- OEM muss Änderungsmanagement fest im Griff haben
- Aktualisierungen am R156-Prozess vorbei sind ein Risiko
- Enge Verzahnung des Änderungsmanagement OEM und Zulieferer notwendig

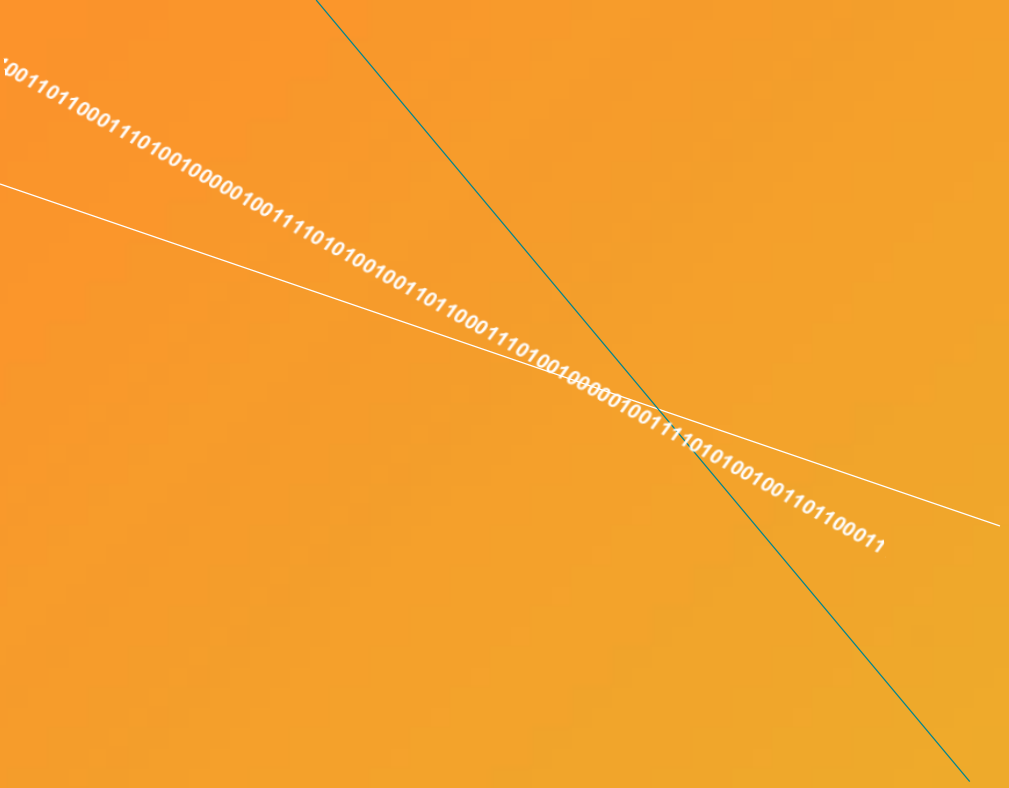
ZUSAMMENFASSUNG

- Gründe für Automotive Software Updates
- Entwicklung der Update-Methodik
- Trend zur zentralisierten Architektur
- Zukünftige Herausforderungen und Chancen



LITERATUR

- **ISO 24089:2023** Road Vehicles - Software Update Engineering
- **ISO/SAE 21434:2021**(en) Road vehicles — Cybersecurity engineering
- UNECE R155 „Approval of vehicles with regards to cyber security“
- UNECE R156 „ Software update and software update management system“
- **AUTOSAR (CP R20-11)** - Requirements on Firmware Over-The-Air
- **NHTSA** - Cybersecurity Best Practices for Modern Vehicles
- **GB201-5** - General Technical Requirements for SW Updates of Vehicles
- ROMIJN, Marcel; KMIEC, Mateusz; WEBER, Matthias. *The Ever-Changing Powertrain-How OTA Makes Powertrains Change Over Vehicle Lifetime*. SAE Technical Paper, 2022.
- Teresa Placho, Christoph Schmittner, Arndt Bonitz, Oliver Wana, Management of automotive software updates, Microprocessors and Microsystems, Volume 78, 2020
- HALDER, Subir; GHOSAL, Amrita; CONTI, Mauro. Secure ota software updates in connected vehicles: A survey. arXiv preprint arXiv:1904.00685, 2019.
- Functions on Demand | Audi Deutschland



METHODEN UND TECHNIKEN FÜR SICHERE OVER-THE-AIR-UPDATES

Björn Koopmann (DLR)

EINFÜHRUNG

Over-the-Air-Updates im Automobilbereich

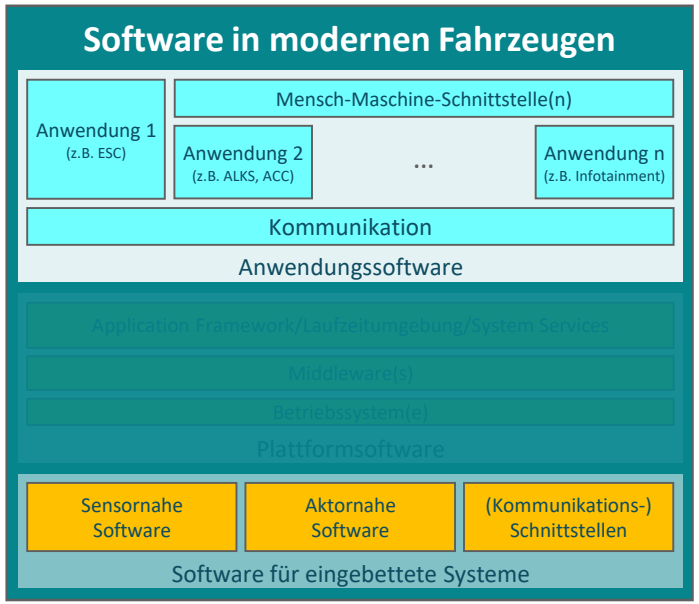
Zunehmende Relevanz von Automotive Software Updates

- Schrittweise Einführung von Over-the-Air-Updates (OTA-Updates)
  - Rechtliche Anforderungen (z.B. zur nachträglichen Fehlerkorrektur)
  - Veränderte Kundenerwartungen und neue Geschäftsmodelle
- Korrektive, perfektive und adaptive Software-Updates
- Hohe Qualitätsanforderungen an die zu aktualisierende Software, Software-Updates und den Prozess der Aktualisierung

Fragestellungen in diesem Vortrag

- Welche Änderungen ergeben sich im Entwicklungsprozess und im Software-Lebenszyklus?
- Wie kann die korrekte und nachweisbar sichere Umsetzung von Over-the-Air-Updates gewährleistet werden?
- Welche neuen Aufgaben ergeben sich für Software-Zulieferer?

Fahrzeug-Hersteller
Updates für Komponenten der Plattformsoftware

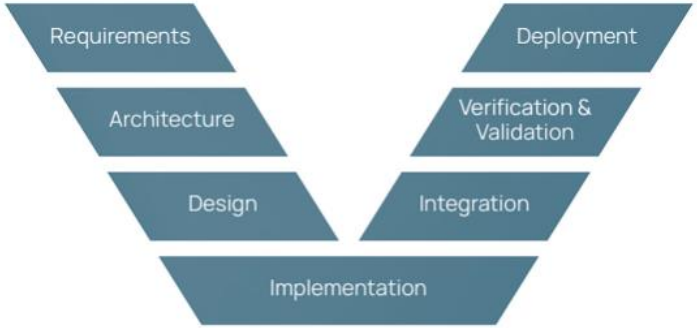


Software-Zulieferer
Updates für Anwendungs- und hardwarenahe Software

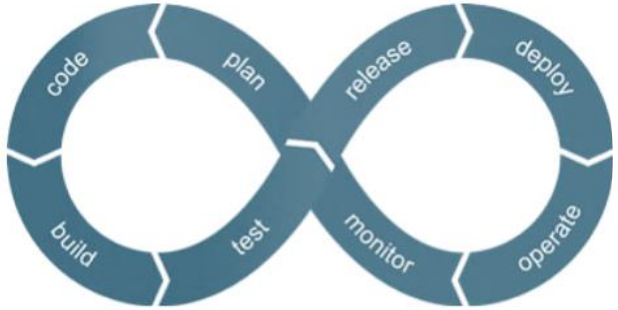
Bildquelle: ETAS GmbH (2023): *Trends Towards Software-Defined Vehicles*. Whitepaper.
URL: https://www.etas.com/en/products/trends-towards-software-defined-vehicles.php

ÄNDERUNGEN IM ENTWICKLUNGSPROZESS

Iterative Vorgehensmodelle und nachweisbare Sicherheit



V-Modell

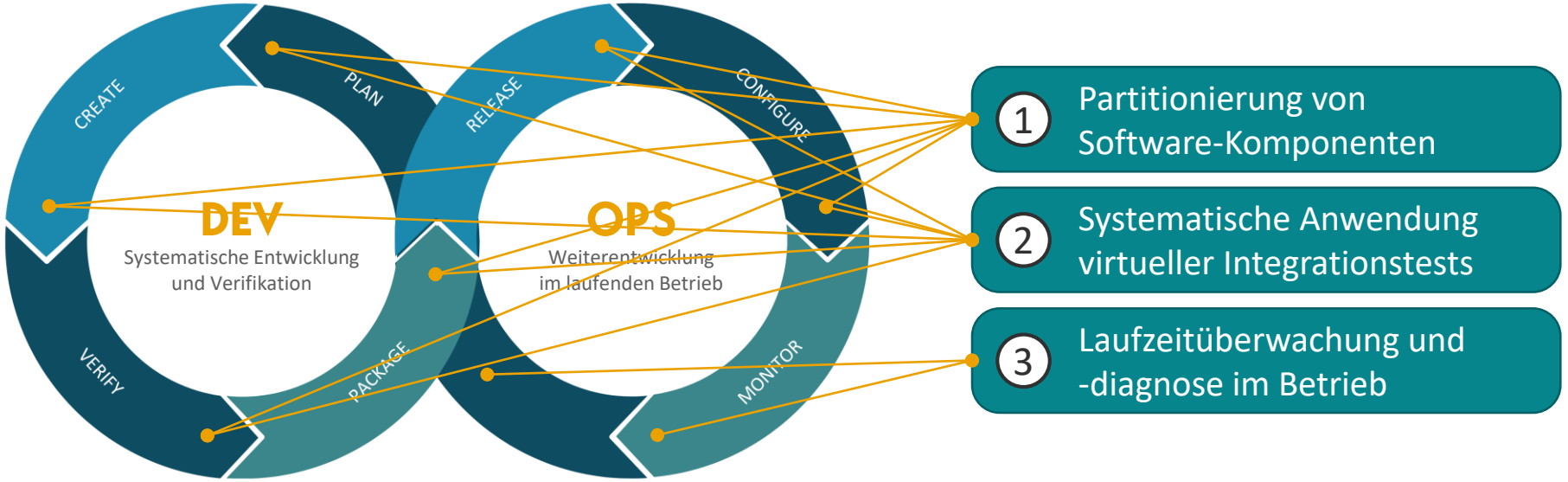


DevOps-Modell

- Zunehmender Einsatz iterativer Vorgehensmodelle (z.B. **Dev**elopment & **Op**eration**s**)
  - Starker Fokus auf die fortlaufende Optimierung durch Feedback aus der Betriebsphase
  - Software-Updates als integraler Bestandteile des Lebenszyklus zukünftiger Systeme
- Herausforderung bei der Entwicklung: Gewährleistung der korrekten und nachweisbar sicheren Funktionsfähigkeit zu aktualisierender Software-Komponenten auf geteilten Computing-Plattformen
  - Frühzeitige Spezifikation und Verhandlung nicht-funktionaler Eigenschaften (z.B. Zeit- und Speicherbudgets)
  - Enge(re) Abstimmung und Zusammenarbeit mit anderen Software-Zulieferern sowie dem Integrator/OEM
  - Nutzung virtualisierter Testumgebungen zur Qualitätssicherung vor der Integration in das Gesamtsystem
  - Laufzeitüberwachung und -diagnose in der Betriebsphase

AUTOMOTIVE SOFTWARE UPDATES

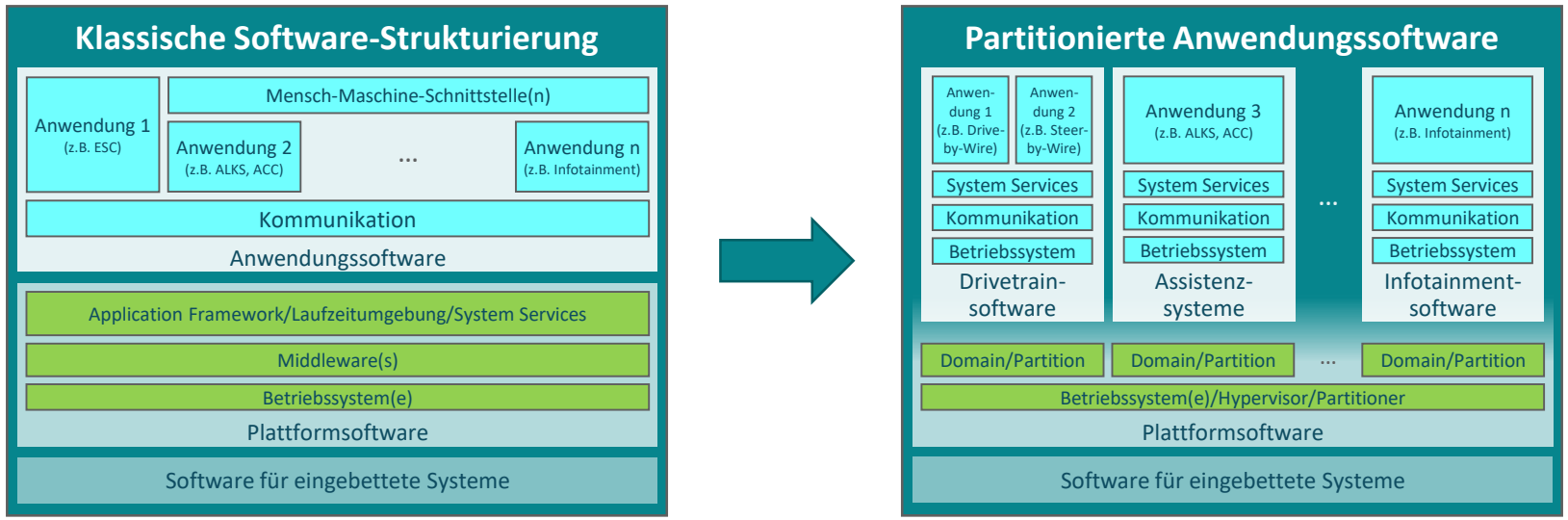
Methoden und Techniken für sichere Over-the-Air-Updates



PARTITIONIERUNG VON SOFTWARE-KOMPONENTEN

Unabhängige Ausführung gemischt-kritischer Fahrzeug-Software

- Virtuelle Partitionierung der Anwendungssoftware für zentralisierte Plattformen
  - Ziel: Minimierung gegenseitiger Beeinflussungen gemischt-kritischer Software-Komponenten
  - Herstellung garantierter Eigenschaften der Ausführungsumgebung (z.B. Verfügbarkeit zugesicherter Ressourcen)
- Unabhängige Aktualisierung von Software-Komponenten unterschiedlicher Partitionen
  - „Entkopplung“ der Ausführung und des Updatevorgangs auf geteilten Computing-Plattformen
  - Erforderlicher Nachweis der Kompatibilität von Software-Updates innerhalb der jeweiligen Partition

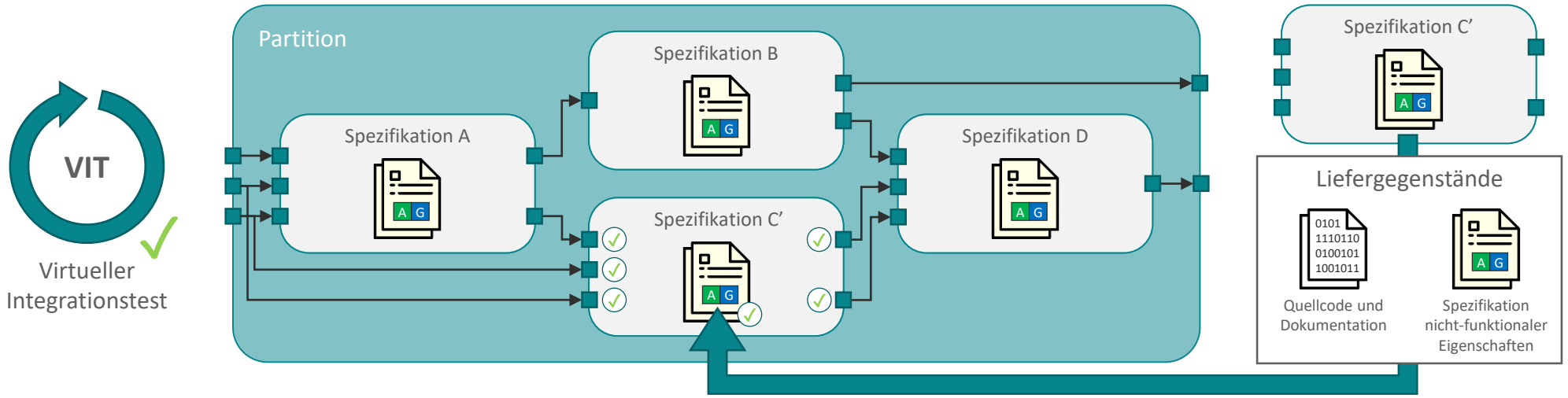


E. Böde et al. (2017): *Design Paradigms for Multi-Layer Time Coherency in ADAS and Automated Driving (MULTIC)*. In: *FAT-Schriftenreihe 302*. Forschungsvereinigung Automobiltechnik. URL: https://www.vda.de/vda/de/aktuelles/publikationen/publication/fat-schriftenreihe-302

VIRTUELLE INTEGRATIONSTESTS

Nachweis der Kompatibilität von Software-Komponenten

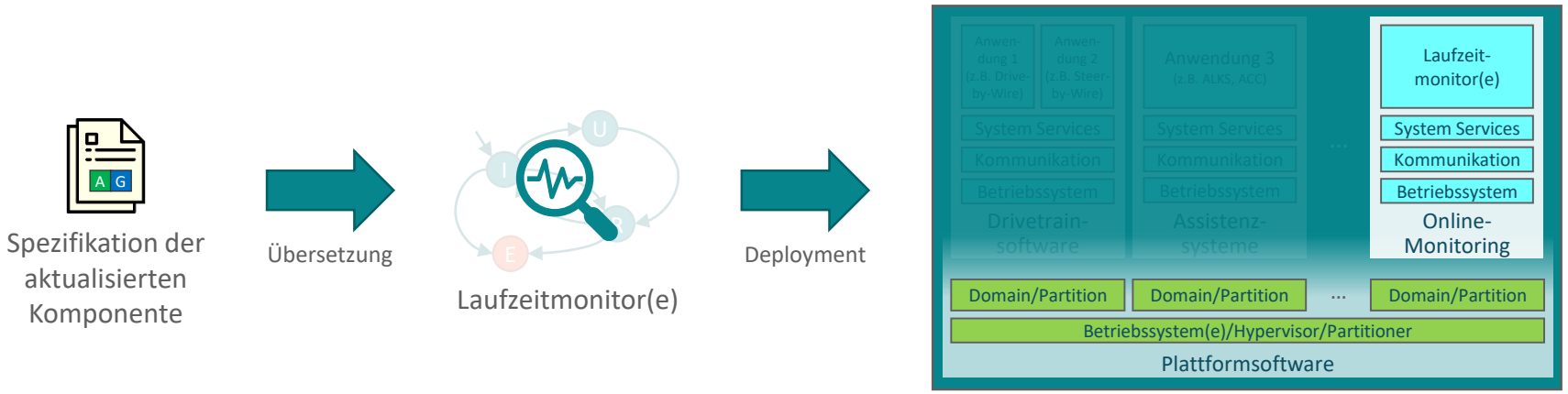
- Beschreibung des Verhaltens von Software-Komponenten in Form von Spezifikationen
  - z.B. unter Verwendung von Assume/Guarantee-Contracts für nicht-funktionale Eigenschaften
  - Ausnutzung formal definierter Kompositions- und Verfeinerungsoperationen
- Systematische Anwendung virtueller Integrationstests zum Nachweis der Kompatibilität
  - Überprüfung der Konsistenz von Software-Komponenten während der Entwurfsphase
  - Ausführung automatisierter Konsistenz- und Kompatibilitätsprüfungen im Fahrzeug



LAUFZEITÜBERWACHUNG UND -DIAGNOSE

Überwachung des Systemverhaltens während des Betriebs

- Einsatz von Techniken zur Laufzeitüberwachung und -diagnose
  - Sammlung und Auswertung von Fahrzeugdaten in der Betriebsphase
  - Erkennung von Fehlern und Überschreitungen von Ressourcenbudgets
  - Grundlage für die kontinuierliche (Weiter-)Entwicklung des Systems
- Automatisierte Generierung von Laufzeitmonitoren
  - Wiederverwendung der zuvor erstellten, nachweisbar konsistenten Spezifikationen
  - Deployment der erzeugten Laufzeitmonitore in eigener Software-Partition



Bildquelle des Symbols für Spezifikationen: Modifizierte Version eines Icons von *smalllikeart* auf Flaticon.
URL: https://www.flaticon.com/de/kostenloses-icon/dokument_888034

ZUSAMMENFASSUNG

Methoden und Techniken für sichere Over-the-Air-Updates

- Zunehmender Einsatz iterativer Vorgehensmodelle (z.B. DevOps)
- Neue Aufgaben für Software-Zulieferer:
  - Abstimmung nicht-funktionaler Eigenschaften mit anderen Software-Zulieferern und OEMs
  - Nutzung virtualisierter Testumgebungen zur Qualitätssicherung (ohne Hardwarezugriff)
  - Kompatibilitätsnachweise und Spezifikationen als mögliche Liefergegenstände
- Techniken für die Entwicklung sicherer OTA-Updates:
  - Unabhängige Ausführung gemischt-kritischer Fahrzeug-Software durch Software-Partitionen und virtualisierte Ausführungsumgebungen
  - Systematische Anwendung virtueller Integrationstests zur Gewährleistung der Kompatibilität von Software-Komponenten und -Updates
  - Laufzeitüberwachung und -diagnose in der Betriebsphase als Grundlage für die Entwicklung zukünftiger Software-Updates

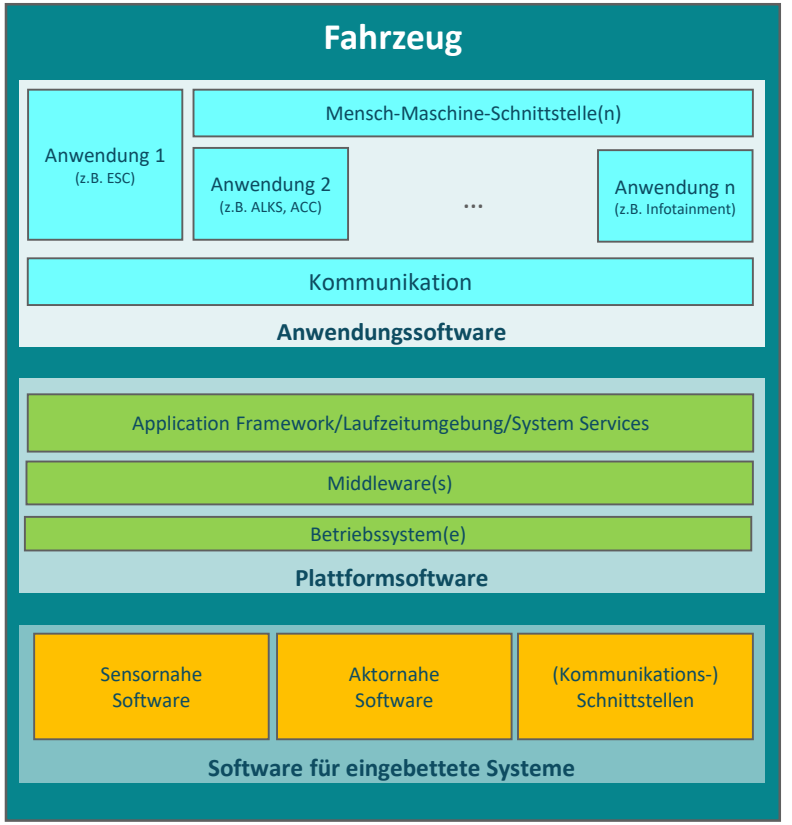
(RE-)ZERTIFIZIERUNG VON AUTOMOTIVE SOFTWARE UPDATES

Karina Rothemann (DLR)

WAS KANN ALLES EINEM UPDATE UNTERLIEGEN

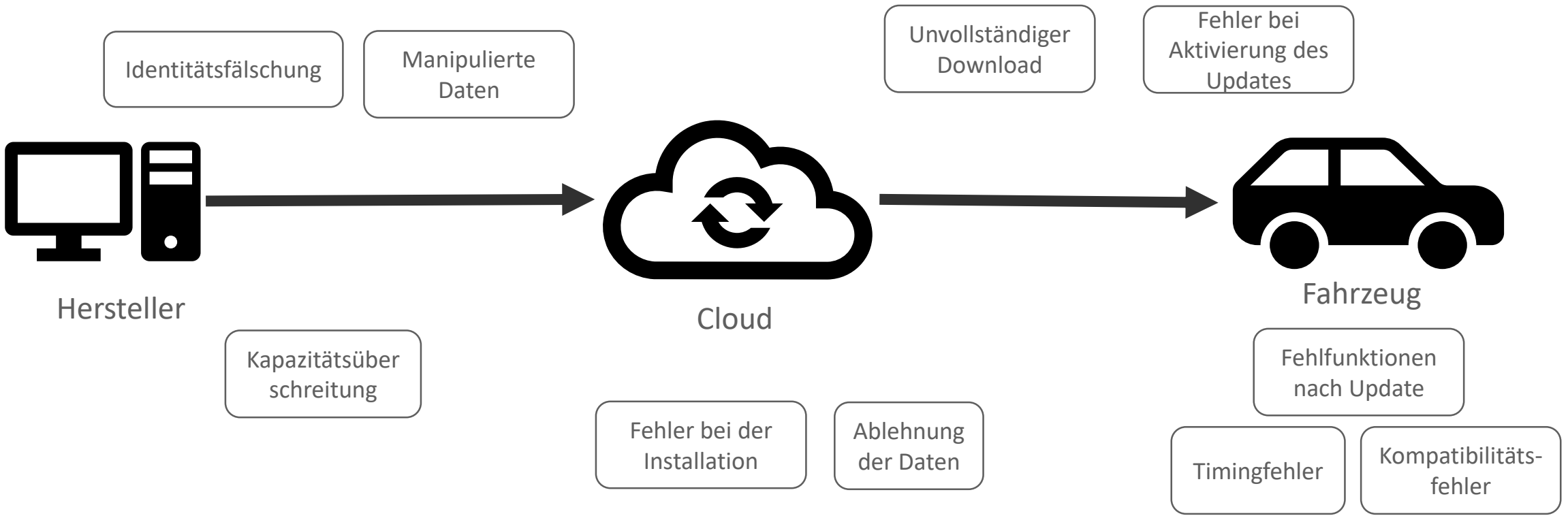
Update ist nicht gleich Update

- **Anwendungssoftware**
  - Infotainment
  - Fahrerassistenzsysteme
- **Plattformsoftware**
  - Betriebssysteme
  - Middleware
- **Software für eingebettete Systeme**
  - Sensornahe Software
  - Aktornahe Software
- **Die Software gibt vor, wie sicherheitskritisch ein Update ist.**



Bildquelle: Automotive Software Abbildung, Projekt TASTE

HERAUSFORDERUNGEN BEIM UPDATE PROZESS



NEUE REGELUNGEN FÜR CYBERSECURITY UND UPDATES

UNECE R155 und R156

UNITED NATIONS
ECONOMIC COMMISSION
FOR EUROPE

R155

- Nachweis eines funktionierenden Cyber-Security-Management-System (CSMS)
  - Risikomanagement
    - Risikoerkennung
    - Risikobewertung
    - Risikominimierung
- Berücksichtigung von Risiken durch Zulieferung
- Prozesse über gesamten Lebenszyklus
- Bestätigung durch Prüfinstitut

R156

- Nachweis eines funktionierenden Software-Update-Management-System (SUMS)
  - Einhaltung von Gesetzesvorschriften nach Update
- System soll nach Update „Safe“ und „Secure“ sein
  - Definition von „Safe & Secure“ ist nicht weiter beschrieben
  - Genaue Umsetzung eines SUMS nicht beschrieben

Bildquelle: https://www.itu.int/net4/wsis/ungis/Members/1160

NEUE REGELUNGEN FÜR UPDATES

UNECE R156 und ISO/SAE 21434 Road Vehicle – Cybersecurity Engineering

R156

- Erweiterte Regeln für Over the Air Updates:
  - Updates dürfen die Sicherheit nicht beeinträchtigen
  - Regelungen für komplexe Updates
  - Regelungen bei fehlerhaften Updates
  - Maßnahmen um Updates vollständig durchzuführen
  - Meldungen an den Fahrer über Update

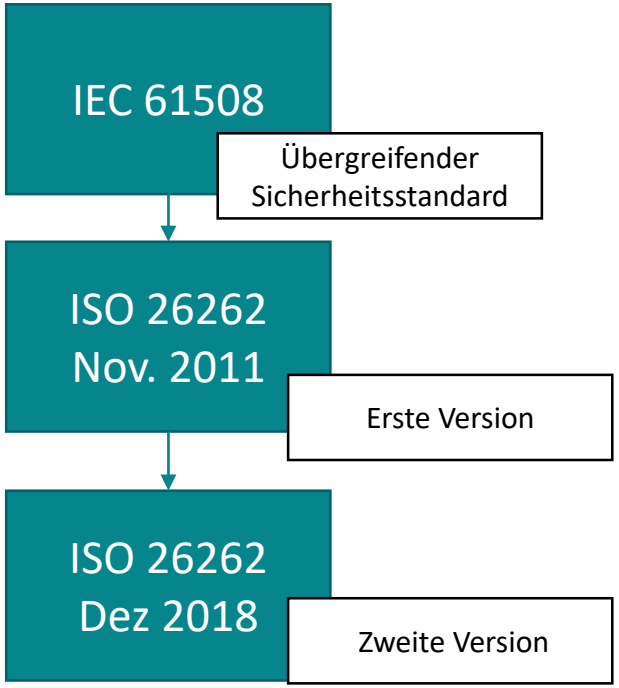
ISO/SAE 21434 Road Vehicle – Cybersecurity Engineering

- Sicherheitsanforderungen für Softwareupdates definiert
- Umfassende Risikobewertung für geplante Softwareupdates
- Mechanismen für die Authentifizierung von Softwareupdates
- Sicherstellung der Integrität

SICHERHEIT UND VORSCHRIFTEN

ISO 26262 Internationale Norm für funktionale Sicherheit in Kraftfahrzeugen

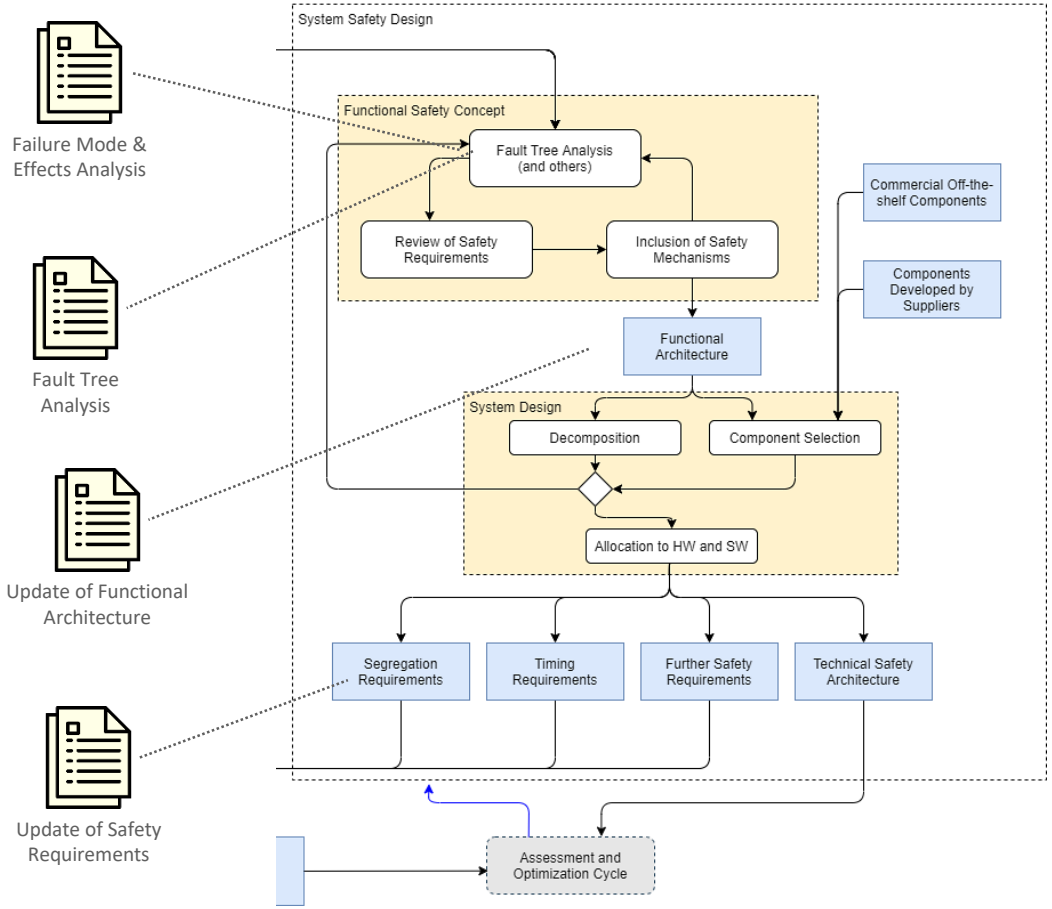
- Internationaler anerkannter Standard
- Anpassung der Norm IEC 61508 an den Automotive Bereich.
- Festlegung von Anforderungen und Prozesse um sicherzustellen, dass elektrische Systeme in Fahrzeugen sicher und zuverlässig sind.
- Nachweise sollen sicherstellen, dass die Systeme während ihres gesamten Lebenszyklus sicher und zuverlässig funktionieren.



SICHERHEIT UND VORSCHRIFTEN

ISO 26262 Internationale Norm für funktionale Sicherheit in Kraftfahrzeugen

- **Gefährdungsanalyse:**
  - Identifikation von potentiellen Schadensquellen
- **Gefährdungsklassifizierung:**
  - Art und Schwere der Gefährdung bewerten
- **Risikobewertung:**
  - Wahrscheinlichkeit des Auftretens der Gefährdung
- **Sicherheitskonzept:**
  - Festlegung von Sicherheitszielen und Maßnahmen zur Risikominimierung
- **Die Dokumentationen müssen zu jeder Zeit transparent und aktuell sein.**



Bildquelle: Design Process and Artifacts, Project Panorama

VERIFIKATION UND VALIDIERUNG

Was wird benötigt?

- **Inkrementelle Verifikation**
  - Contract- und Kompatibilitätsprüfungen
- **Dynamische Online-Prüfungen mit Rollback:**
  - Aktualisierte Funktion wird mit Testdaten angeregt
  - Prüfen von vordefinierten Eckfällen
- **Paralleler und überwachter Betrieb im Quarantänemodus:**
  - Paralleles Laufen von alter und aktualisierter Software
  - Korrekte Funktionsweise gemäß eines vorgegebenen Vertrauensniveaus
  - Prüfung während der Laufzeit

QUELLEN

- https://www.kuglermaag.de/funktionale-sicherheit/sw-ebene-iso-26262/
- Bebawy Y, Guissouma H, Maelen SV, Kroger J, Hake G, Stierand I, Franzle M, Sax E, Hahn A (2020) Incremental Contract-based Verification of Software Updates for Safety-Critical Cyber-Physical Systems 2020 International Conference on Computational Science and Computational Intelligence. CSCI 2020 : Las Vegas, Nevada, USA, 16-18 December 2020 : proceedings. IEEE, Piscataway, NJ, S 1708–1714
- Caviglia R, Gaggero GB, Vincis N, Morando O, Aceti A, Marchese M (2023 - 2023) SPAT: A Testbed for Automotive Cybersecurity Training 2023 IEEE International Conference on Cyber Security and Resilience (CSR). IEEE, S 381–386
- Costantino G, Vincenzi M de, Matteucci I (2022) In-Depth Exploration of ISO/SAE 21434 and Its Correlations with Existing Standards. IEEE Comm. Stand. Mag. 6(1):84–92. doi:10.1109/MCOMSTD.0001.2100080
- Halder S, Ghosal A, Conti M (2020) Secure over-the-air software updates in connected vehicles: A survey. Computer Networks 178:107343. doi:10.1016/j.comnet.2020.107343

TASTE
THE KNOWLEDGE

Q&A SESSION

FZI fortiss DLR Deutsches Zentrum für Luft- und Raumfahrt NFF NIEDERSÄCHSISCHES FORSCHUNGSZENTRUM FAHRZEUGTECHNIK ITS MOBILITY