TASTE

THE KNOWLEDGE

Jeden zweiten Donnerstag!

Automotive Software Engineering mit Expert:innen aus der Wissenschaft.

22.02.2024 15:00 – 16:30 Uhr

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

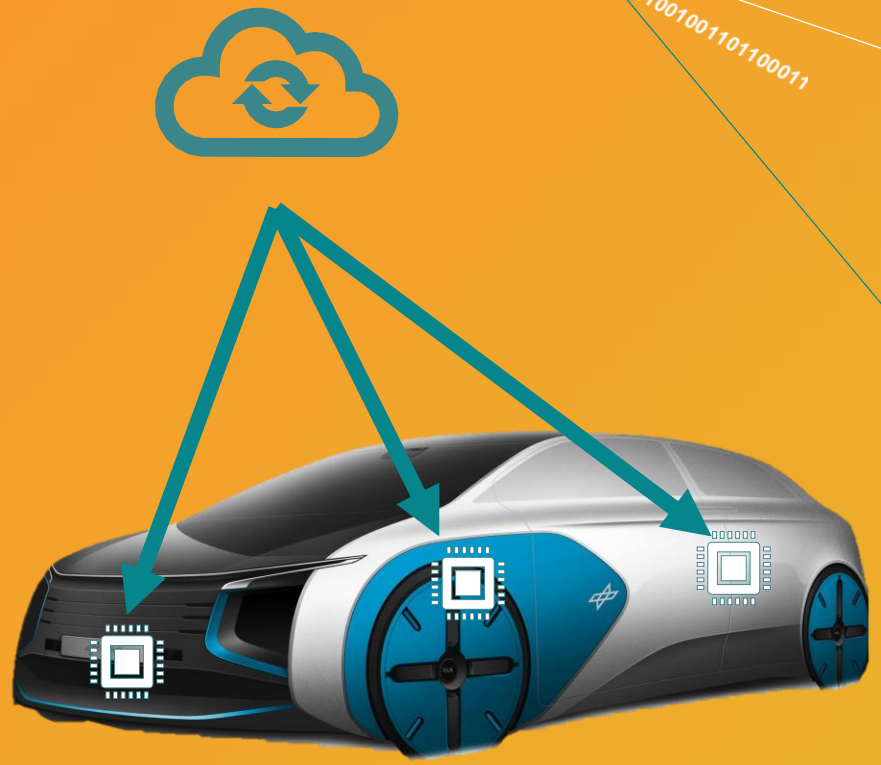
mit DLR

powered by ITS MOBILITY

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

AGENDA

1. Motivation
2. Aktuelle Herausforderungen und Perspektiven
3. Umsetzung des Update-Prozesses
4. Zusammenfassung und Ausblick



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

Henning Schlender, Björn Koopmann und Karina Rothemann
Deutsches Zentrum für Luft- und Raumfahrt e.V.

EINFÜHRUNG

Over-the-Air-Updates im Automobilbereich

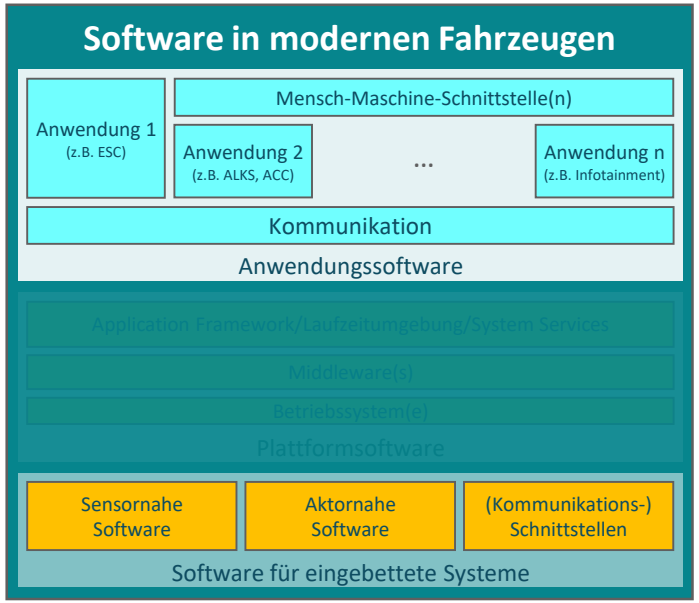
Zunehmende Relevanz von Automotive Software Updates

- 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
- Monetarisierung

Fragestellungen in diesem Vortrag

- Welche aktuellen Herausforderungen und Perspektiven ergeben sich bei der Entwicklung aktueller Fahrzeuge?
- Wie kann die korrekte und nachweisbar sichere Umsetzung von Over-the-Air-Updates gewährleistet werden?
- Welche neuen Aufgaben ergeben sich für Software-Zulieferer?
- Welche Prozessschritte übernimmt der Fahrzeughersteller?

Fahrzeug-Hersteller
Updates für Komponenten der Plattformsoftware



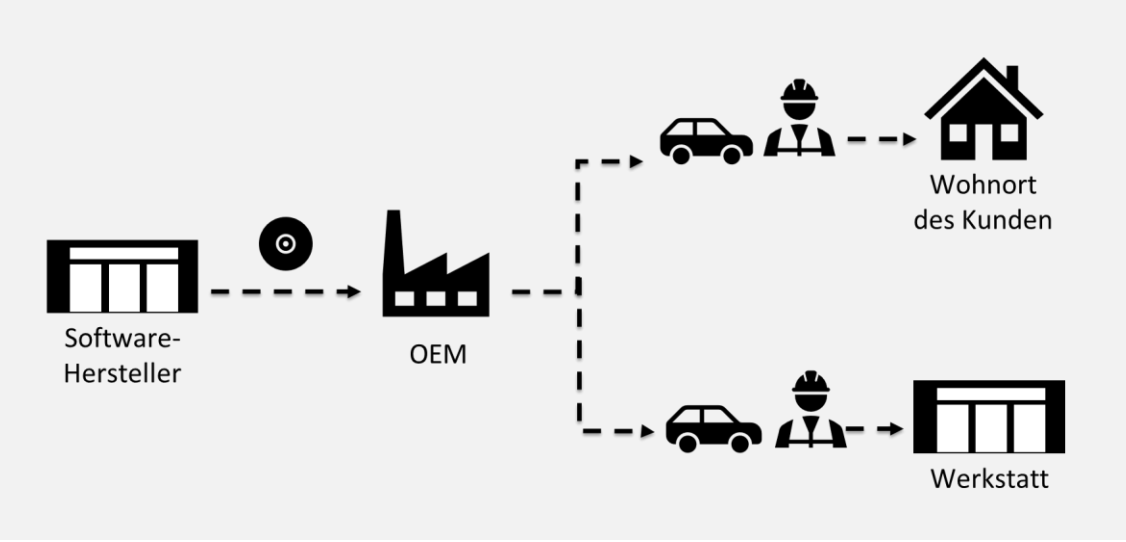
Software-Zulieferer
Updates für Anwendungs- und hardwarenahe Software

Aktuelle Herausforderungen und Perspektiven

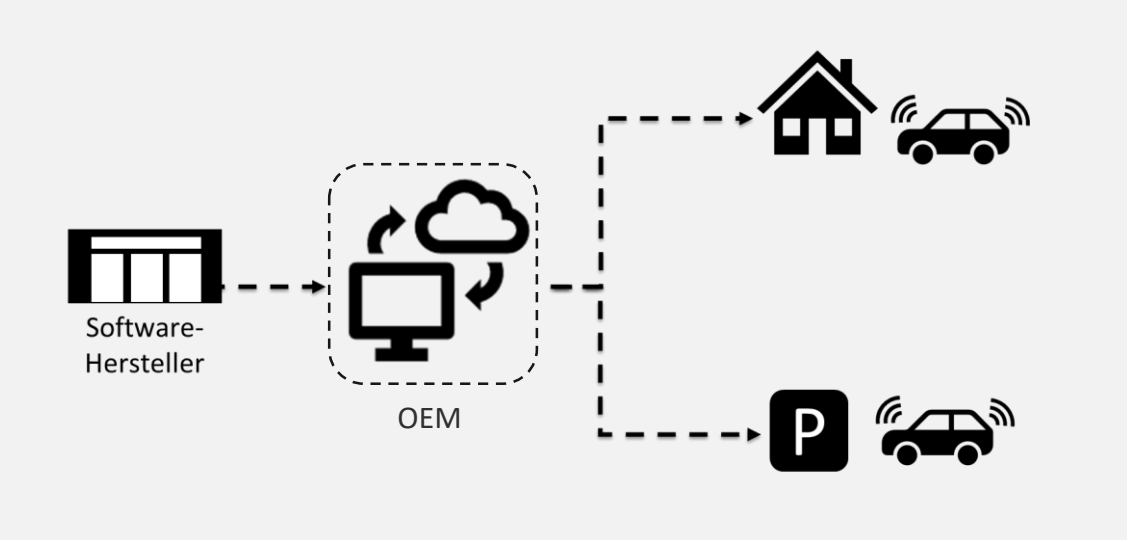
AUTOMOTIVE SOFTWARE UPDATES

Wege der Software ins Fahrzeug: Übersicht

KONVENTIONELLE UPDATES



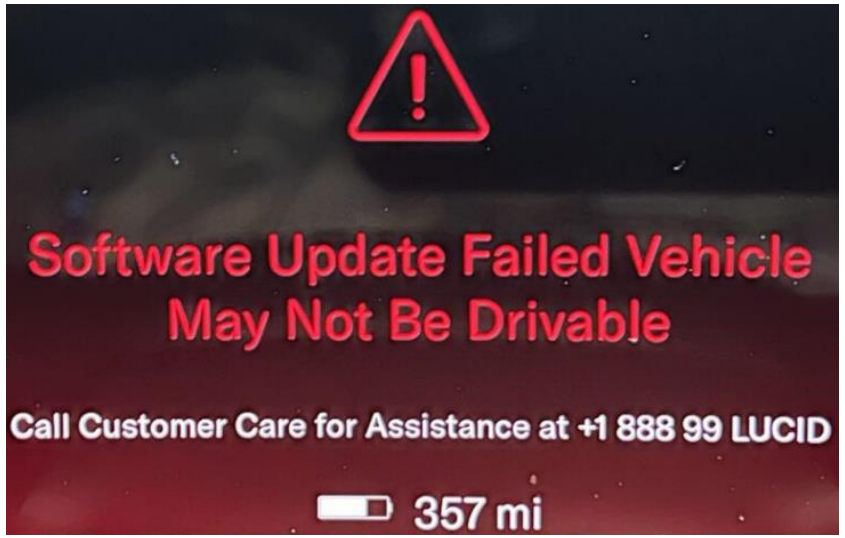
OVER-THE-AIR-UPDATES

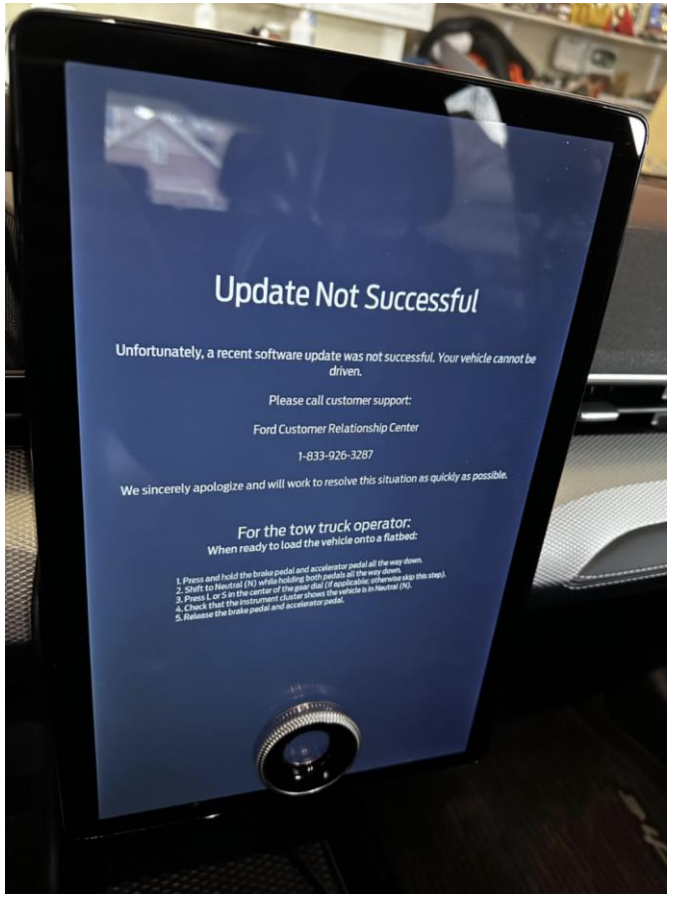


RISIKEN VON OVER-THE-AIR-UPDATES IM AUTOMOBILBEREICH

Herausforderungen bei der Entwicklung von Software-Updates

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

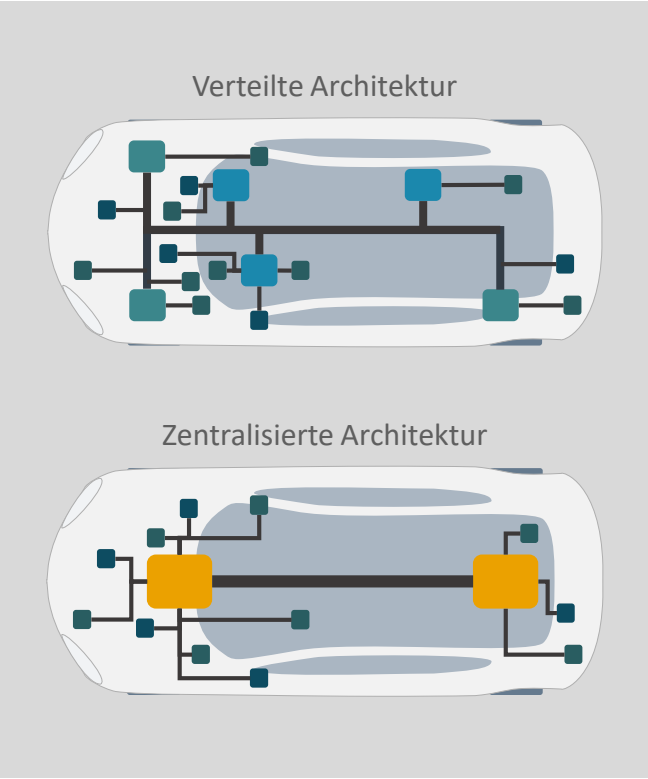




Quelle links: Lucid Air briefly "bricked" after failed over-the-air software update – TopCarNews
Quelle rechts: WHAT!?! : r/MachE (reddit.com)

TREND ZUR ZENTRALISIERUNG VON FAHRZEUGARCHITEKTUREN

Zentralisierte Fahrzeugarchitekturen als Treiber der Transformation



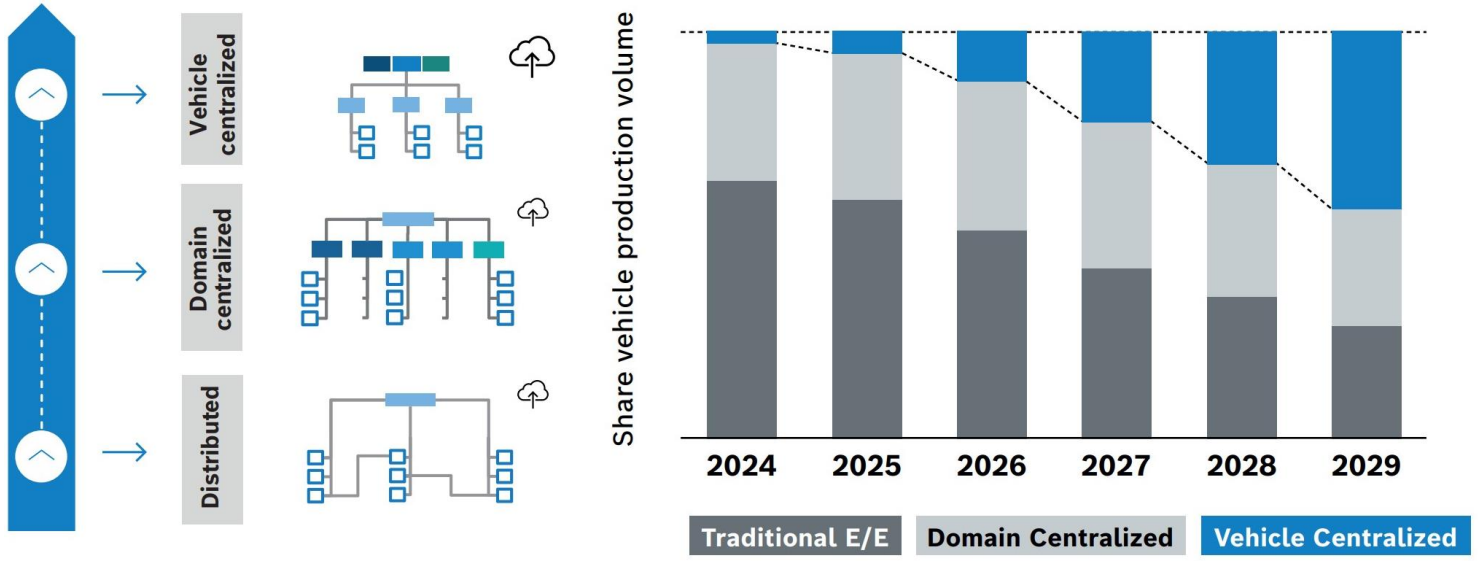


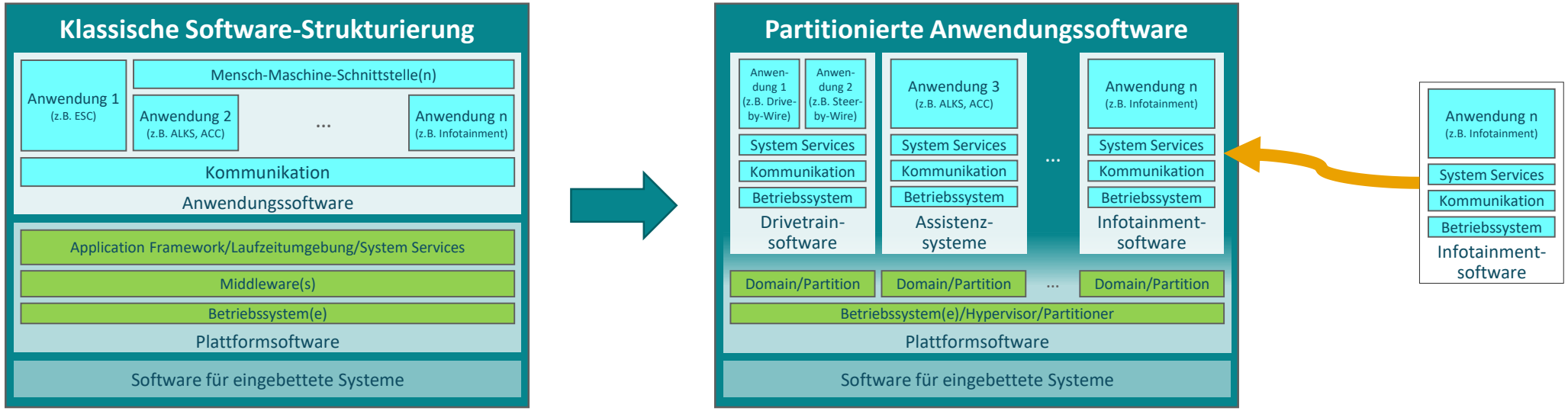
Figure 1: OEMs are ramping up new vehicle-centralized architectures and gradually replace prior architectural patterns.

Bildquelle: Robert Bosch GmbH (2023): *The Next Step in E/E Architectures*. Whitepaper.
URL: https://www.bosch-mobility.com/en/mobility-topics/ee-architecture/download-ee-architecture/

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)

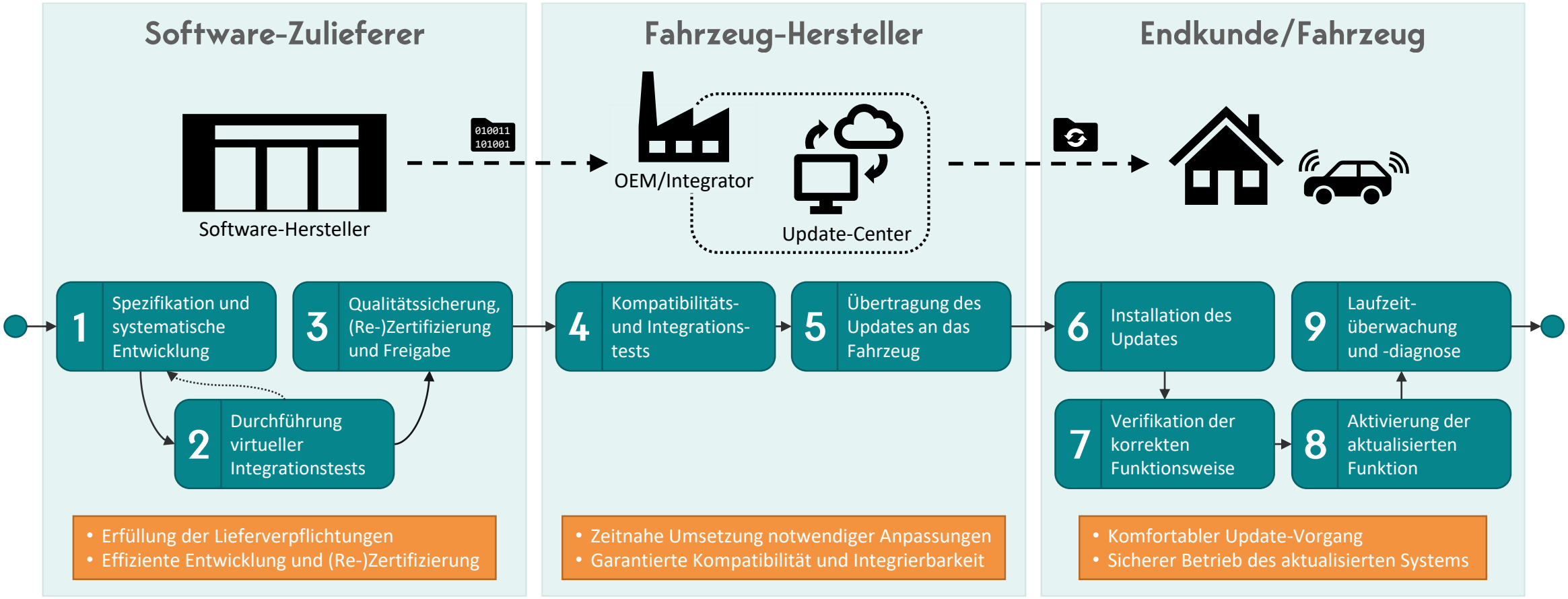


- Unabhängige Aktualisierung von Software-Komponenten unterschiedlicher Partitionen
  - „Entkopplung“ der Ausführung und des Updatevorgangs auf geteilten Computing-Plattformen
  - Erforderlicher Nachweis der Kompatibilität von Software-Updates innerhalb der jeweiligen Partition

Umsetzung des Update-Prozesses

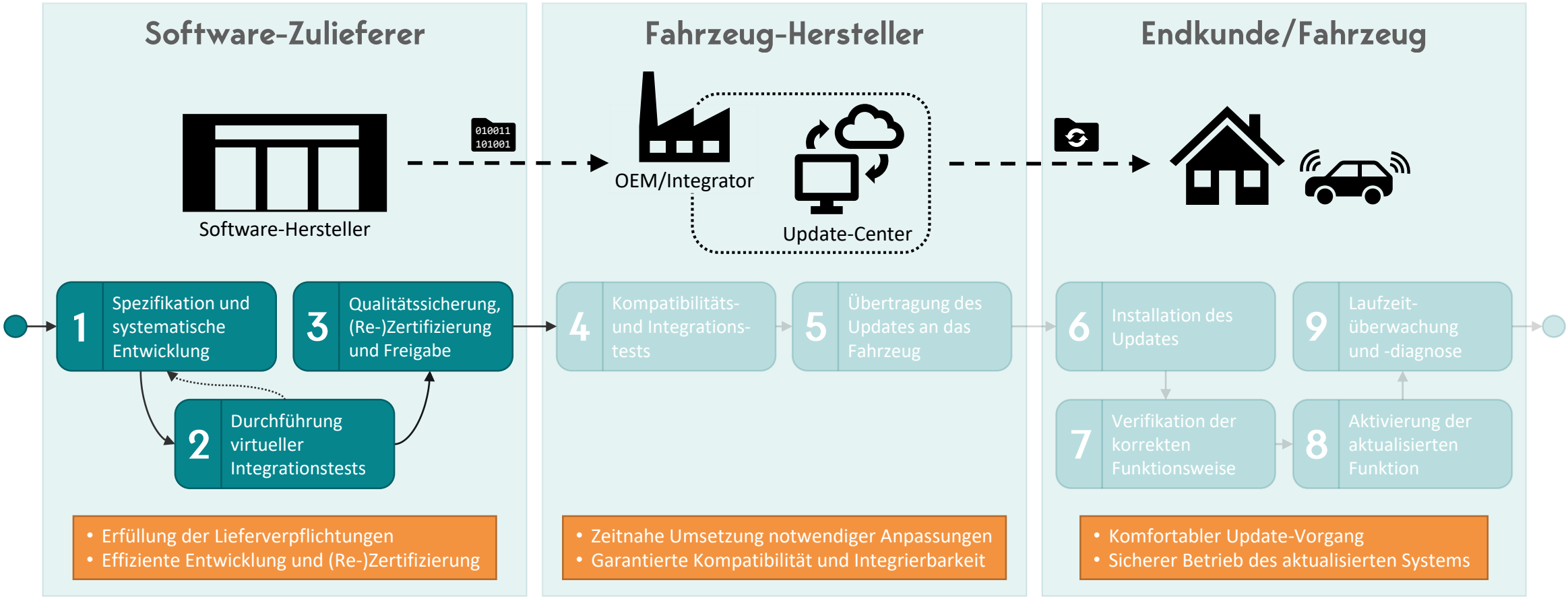
ENTWICKLUNG VON SICHEREN OVER-THE-AIR-UPDATES

Beteiligte Akteure und relevante Prozessschritte



ENTWICKLUNG VON SICHEREN OVER-THE-AIR-UPDATES

Beteiligte Akteure und relevante Prozessschritte



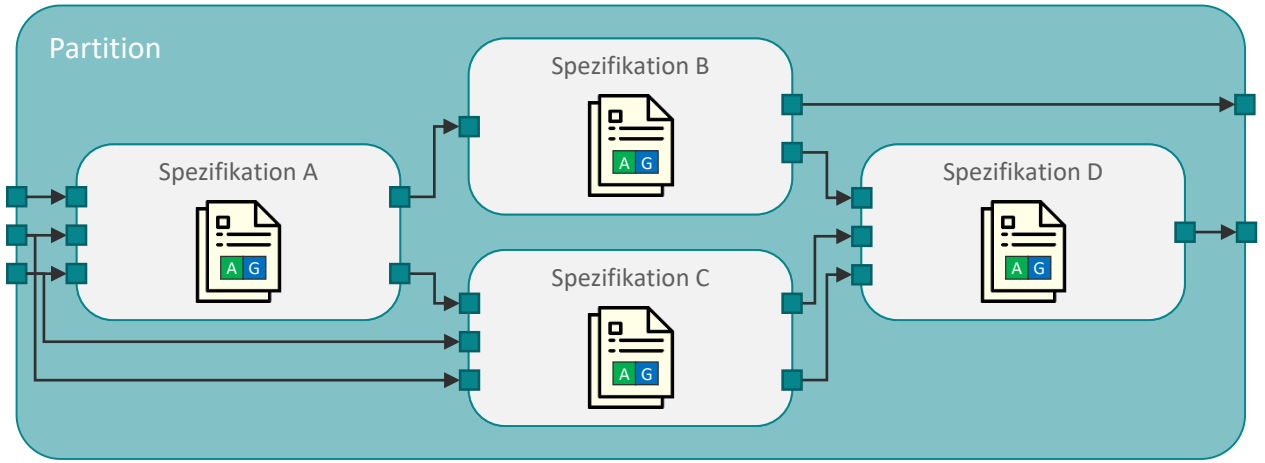
E. Böde et al. (2019): *MULTIC-Tooling*. In: *FAT-Schriftenreihe 316*. Forschungsvereinigung Automobiltechnik.
URL: https://www.vda.de/vda/de/aktuelles/publikationen/publication/fat-schriftenreihe-316

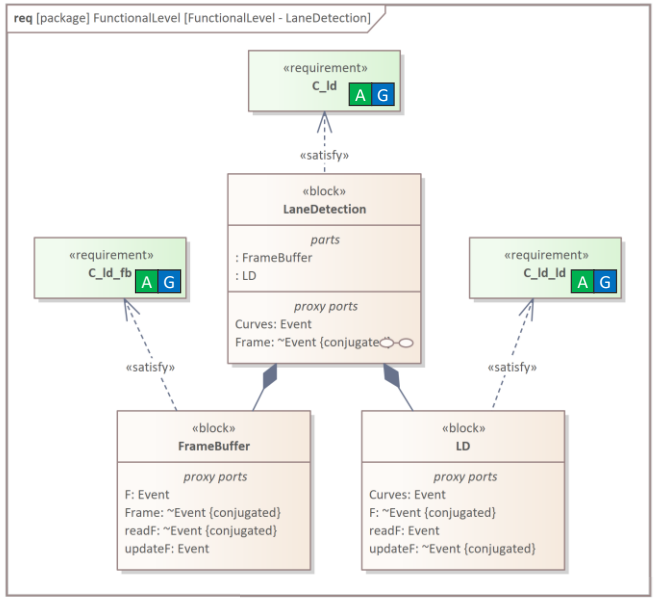
PROZESSSCHRITTE BEIM SOFTWARE-ZULIEFERER

Entwicklung neuer Funktionen und Updates

1. Systematische Entwicklung neuer Funktionen und Updates

- Spezifikation des gewünschten Verhaltens von Software-Komponenten
  - z.B. unter Verwendung von Assume/Guarantee-Contracts (u.a. für Zeit- und Speicherbudgets)
  - Ausnutzung formal definierter Kompositions- und Verfeinerungsoperationen
- Prozessbegleitende Verfeinerung der Spezifikationen





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

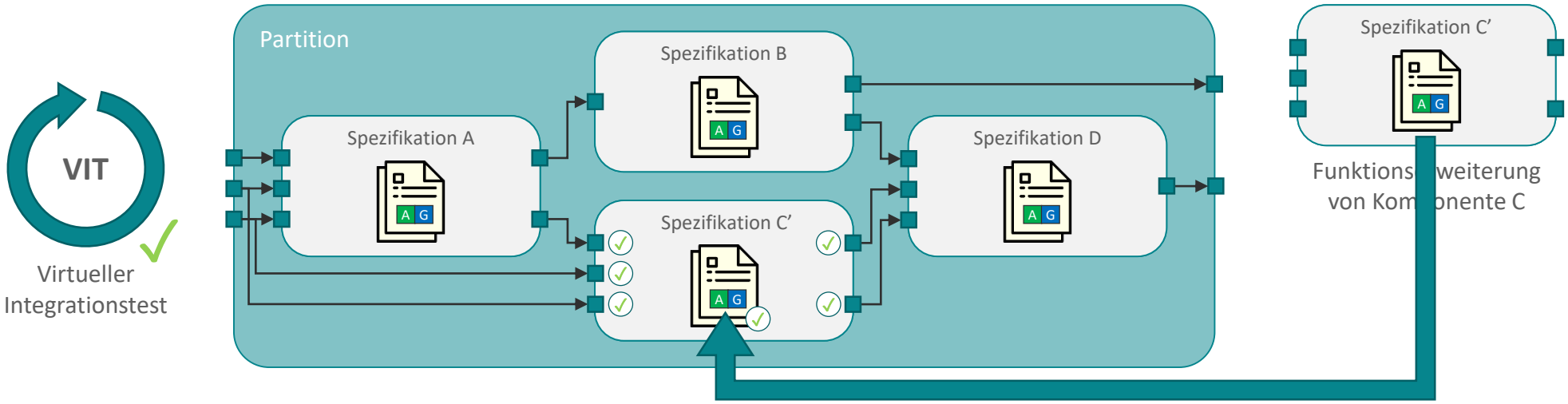
E. Böde et al. (2017): *Design Paradigms for Multi-Layer Time Coherency in ADAS and Automated Driving (MULTIC)*. In: *FAT-Schriftenreihe 302*. Forschungsvereinigung Automobiltechnik. URL: https://www.vda.de/vda/de/aktuelles/publikationen/publication/fat-schriftenreihe-302

PROZESSSCHRITTE BEIM SOFTWARE-ZULIEFERER

Durchführung virtueller Integrationstests

2. Entwicklungsbegleitende Durchführung virtueller Integrationstests

- Überprüfung der Konsistenz und Kompatibilität von Funktionen und Updates
- Anwendung klassischer Testverfahren zur Validierung der Funktionalität
- Abschließende Implementierung unter Einhaltung der verfeinerten Spezifikationen

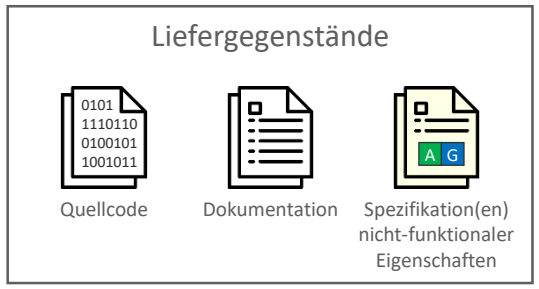


PROZESSSCHRITTE BEIM SOFTWARE-ZULIEFERER
(Re-)Zertifizierung und interne Freigabe

Software-Zulieferer	Fahrzeug-Hersteller	Endkunde/ Fahrzeug

3. Qualitätssicherung, (Re-)Zertifizierung und interne Freigabe

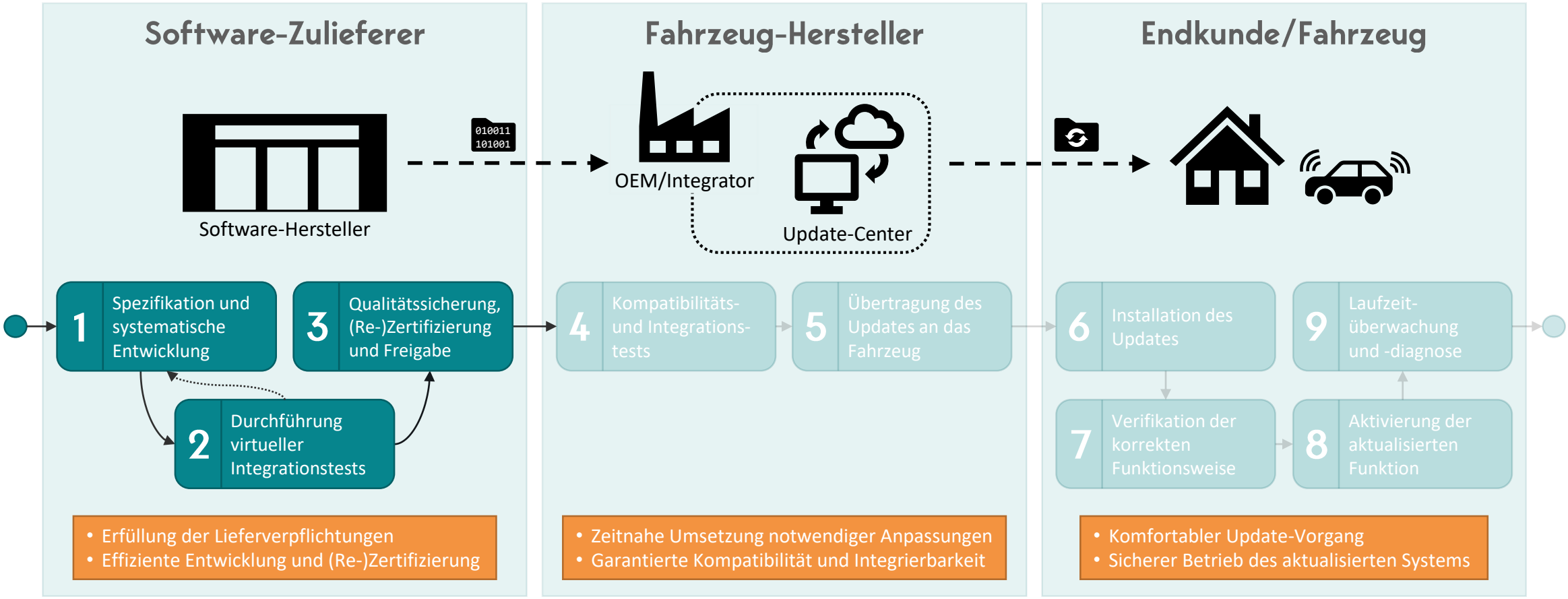
- Einsatz virtualisierter Testumgebungen zur Qualitätssicherung vor der Auslieferung
- Zertifizierung der neuen Software-Komponenten hinsichtlich relevanter Standards
  - Funktionale Sicherheit (z.B. ISO 26262)
  - Cybersecurity (z.B. ISO/SAE 21434, UNECE R155, SAE J3061)
  - Software-Updates (z.B. ISO 24089, UNECE R156)
- Übergabe der Software, Dokumentation und Spezifikationen an den Auftraggeber



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

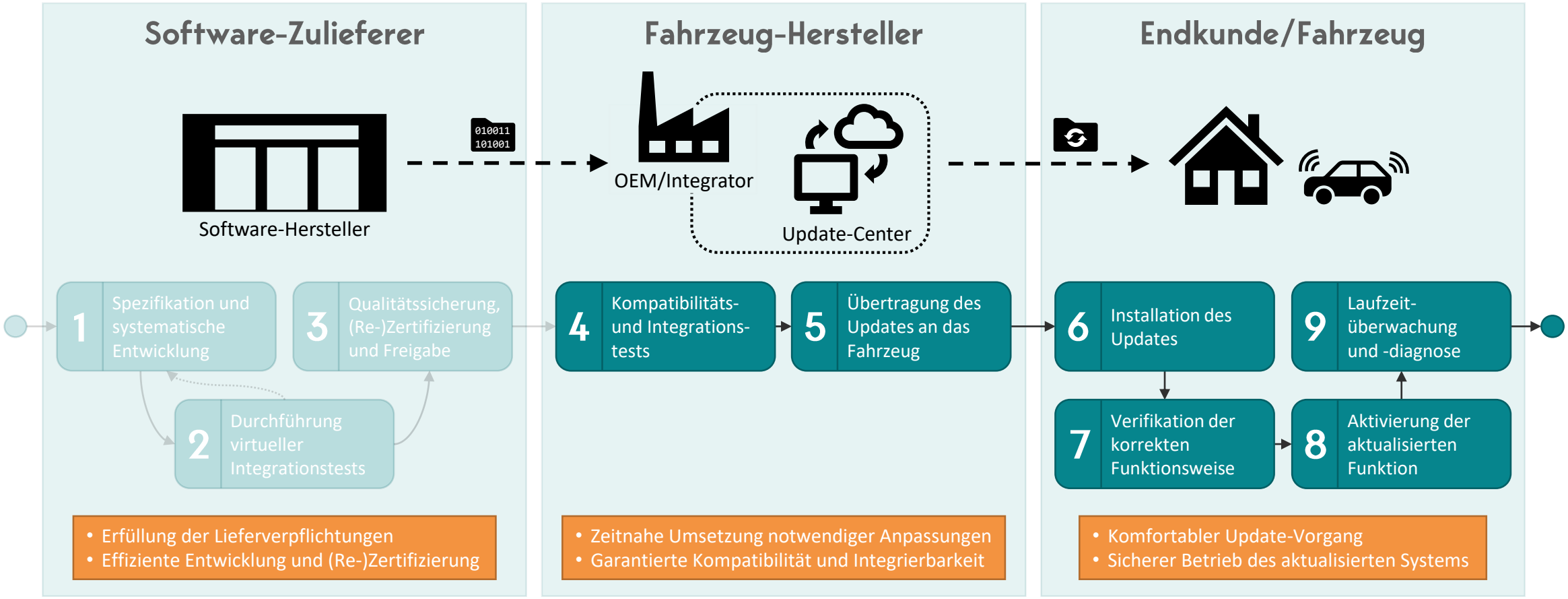
ENTWICKLUNG VON SICHEREN OVER-THE-AIR-UPDATES

Beteiligte Akteure und relevante Prozessschritte



ENTWICKLUNG VON SICHEREN OVER-THE-AIR-UPDATES

Beteiligte Akteure und relevante Prozessschritte



PROZESSSCHRITTE BEIM FAHRZEUG-HERSTELLER

Abnahme und Übertragung

Software-Zulieferer	Fahrzeug-Hersteller	Endkunde/ Fahrzeug

4. Kompatibilitäts- und Integrationstests zur Abnahme

- Prüfung des Update-Paketes auf Kompatibilität
- Durchführung von Integrationstests
  - Contract-basierte virtuelle Integrationstest → Prüfen von Contract Verletzungen
  - Inkrementelle Integrationstest → Gezieltes Testen der betroffenen, geupdateten Komponenten
- Prüfung von weiteren Nachweisen

→ Nach erfolgreicher Überprüfung, Freigabe für Fahrzeug

5. Übertragung des Update an das Fahrzeug

- Übertragung des Update-Pakets an Update-Center
  - Wichtig: Identitätsstempel von Fahrzeughersteller
  - Paket steht zum Download zur Verfügung
- Herunterladen des Update-Paketes auf das Fahrzeug
  - Sicherstellung des vollständigen Downloads
  - Metadatencheck
  - Einhalten von Nebenbedingungen

UNECE R155
Cyber Security Management System (CSMS)

UNECE R156
Software Update Management System (SUMS)

PROZESSSCHRITTE IM FAHRZEUG

Installation und Verifikation

Software-Zulieferer | Fahrzeug-Hersteller | **Endkunde/ Fahrzeug**

6. Installation des Updates

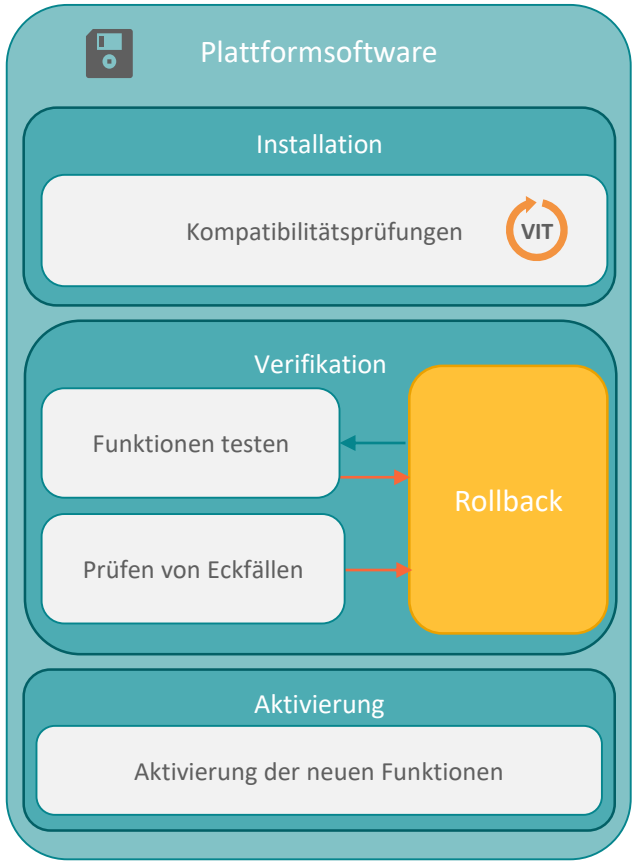
- Plattformsoftware erhält Update-Paket
- Extrahieren des Update-Pakets und lokale Speicherung der Daten
- Erneute Prüfung der Kompatibilität
  - Durchführung verschiedener Tests, basierend auf dem System und der Spezifikationen der betroffenen Komponente
  - Prüfung System erwarteter Zustand

7. Verifikation der korrekten Funktionsweise

- Dynamische Online-Prüfungen mit Rollback:
  - Aktualisierte Funktionen werden mit Testdaten angeregt
  - Prüfen von vordefinierten Eckfällen
- Paralleler und überwachter Betrieb im Quarantänemodus

8. Aktivierung der aktualisierten Funktionen

- Alte Funktionen und Monitore werden abgeschaltet
- Funktionen und die entsprechenden Monitore werden aktualisiert



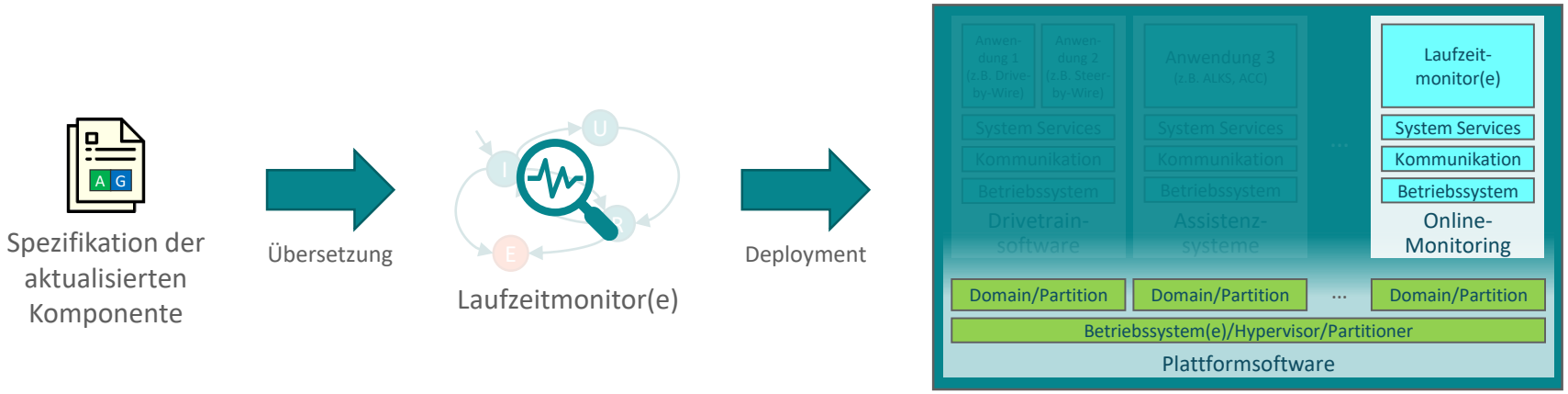
LAUFZEITÜBERWACHUNG UND -DIAGNOSE

Überwachung des Systemverhaltens während des Betriebs

Software-Zulieferer | Fahrzeug-Hersteller | **Endkunde/ Fahrzeug**

9. Laufzeitüberwachung und -diagnose

- 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

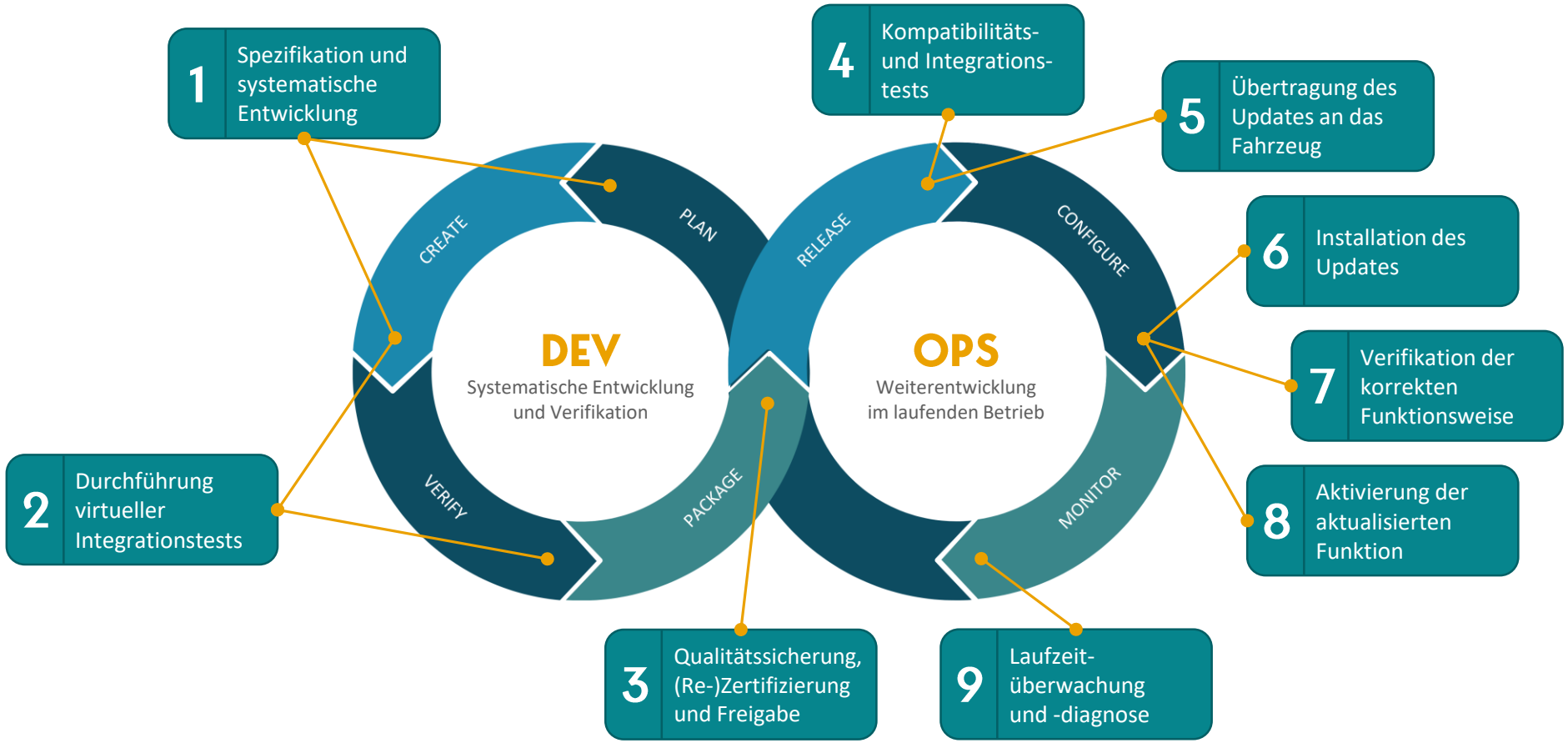


Bildquelle des Symbols für Spezifikationen: Modifizierte Version eines Icons von *smalllikeart* auf Flaticon.
URL: https://www.flaticon.com/de/kostenloses-icon/dokument_888034

Zusammenfassung und Ausblick

ENTWICKLUNG VON SICHEREN OVER-THE-AIR-UPDATES

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



ENTWICKLUNG VON SICHEREN OVER-THE-AIR-UPDATES

Aktuelle Forschungsprojekte

Step-Up!CPS

„Software-Methoden und Technologien für modulare Updates von cyber-physischen Systemen“

Laufzeit: **10/2018** bis **09/2021**
Budget: **4,0 Mio. €**

Gefördert durch das Bundesministerium für Bildung und Forschung (BMBF)

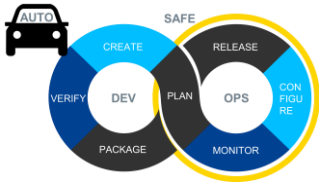
UP2DATE

„Sichere Software-Updates für gemischt-kritische cyber-physische Systeme“

Laufzeit: **01/2020** bis **12/2022**
Budget: **3,8 Mio. €**

Gefördert durch das „Horizon 2020“-Programm der Europäischen Union

AutoDevSafeOps



„Integrierte Entwicklung und Betrieb von sicheren Automotive-Systemen”

Laufzeit: **10/2022** bis **09/2025**
Budget: **11,7 Mio. €**

Gefördert durch das Bundesministerium für Bildung und Forschung (BMBF)

Weitere interne und Drittmittel-finanzierte Projekte (z.B. V&V4NGC, EcoMobility)

ZUSAMMENFASSUNG

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

Zukünftige Herausforderungen bei der Entwicklung von Software-Updates

- „Over-the-Air“-Auslieferung von sicherheitskritischen Aktualisierungen
- Zunehmender Einsatz zentralisierter Fahrzeugarchitekturen

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

Methoden und Techniken für die Entwicklung sicherer Over-the-Air-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

Q&A SESSION

Vielen Dank für Ihre Aufmerksamkeit!

TASTE
THE KNOWLEDGE

Jeden zweiten Donnerstag!

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

TASTE
THE KNOWLEDGE

NÄCHSTER TERMIN

Jeden zweiten Donnerstag!

07.03.2024 15:00-16:30 Uhr

Vertiefung – Systems Engineering mit dem NFF

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