

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



powered by

ITS
MOBILITY



fortiss



Deutsches Zentrum
für Luft- und Raumfahrt



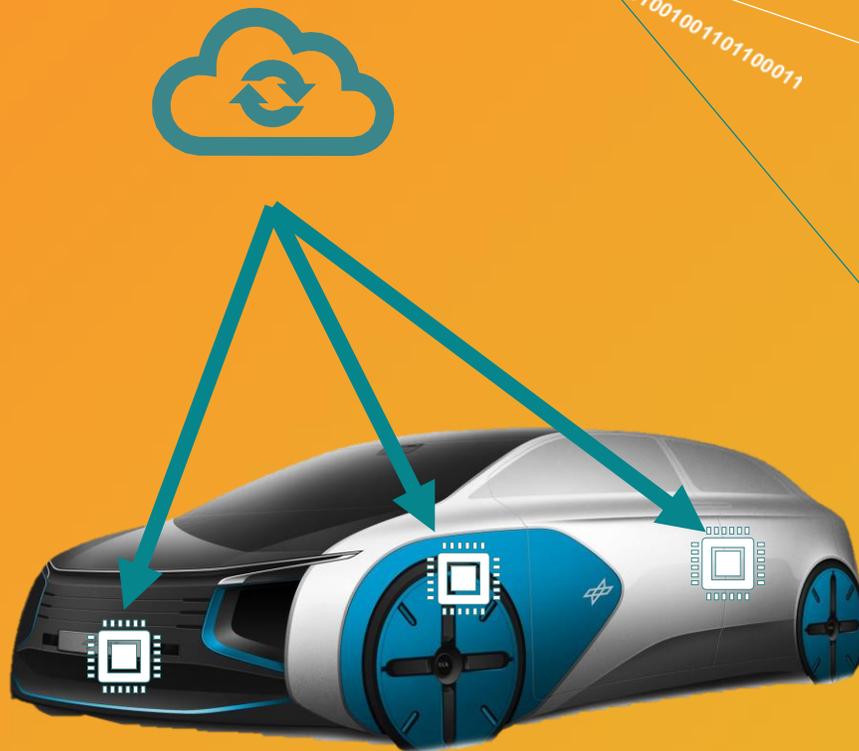
NIEDERSÄCHSISCHES
FORSCHUNGSZENTRUM
FAHRZEUGTECHNIK



AGENDA

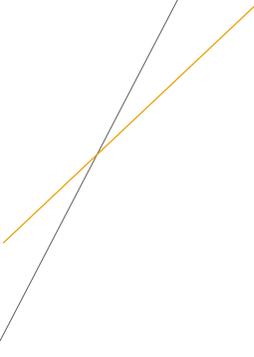
1. Motivation
2. Aktuelle Herausforderungen und Perspektiven
3. Umsetzung des Update-Prozesses
4. Zusammenfassung und Ausblick

010011110101001001101100011101001000001001111010100100110110001110100100000100111101010010011011000111010010000010011110101001011011000111010010000010011110101001011011000111010010000010



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

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

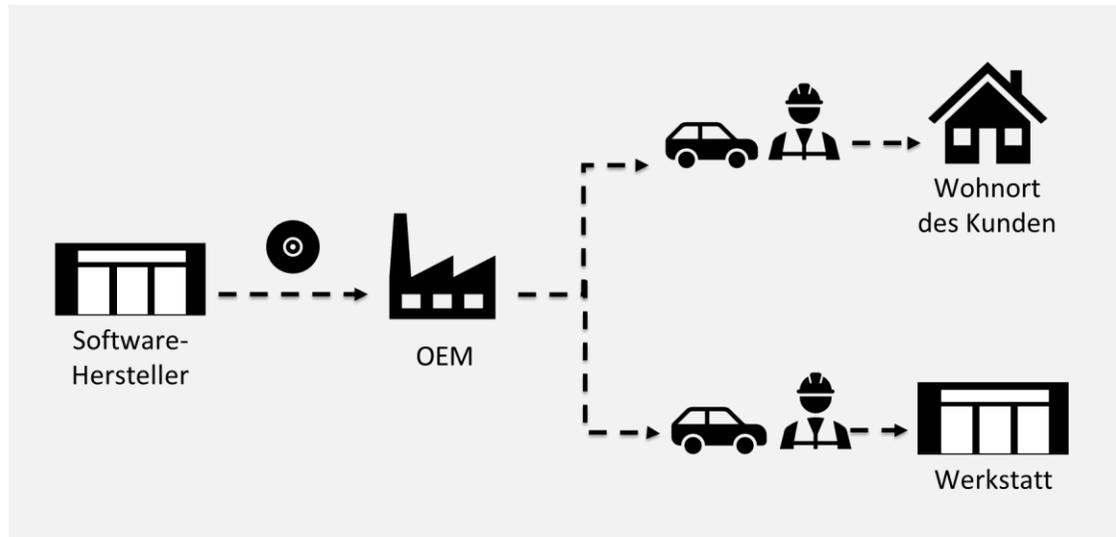


Aktuelle Herausforderungen und Perspektiven

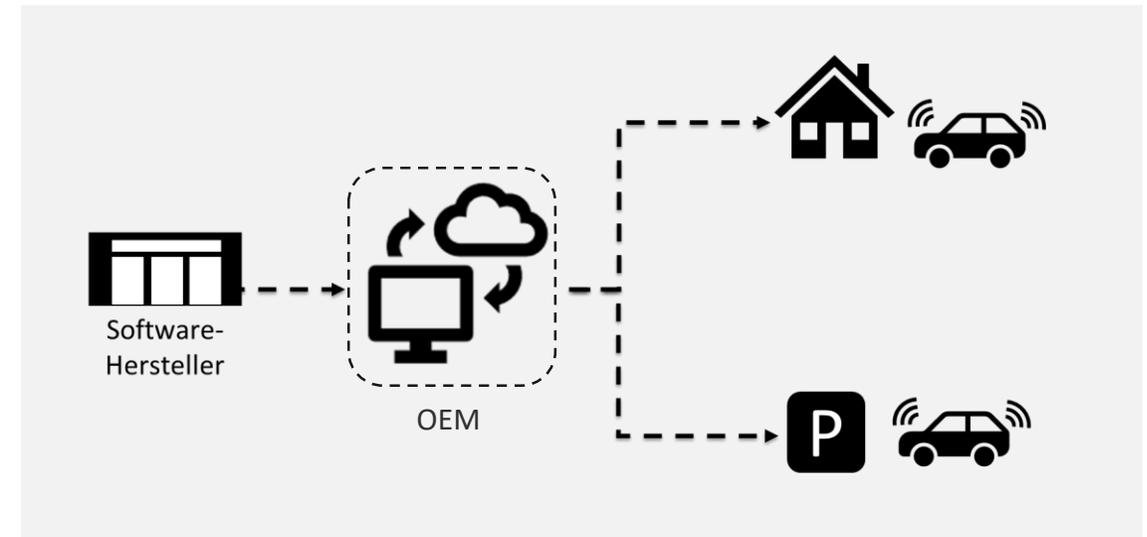
AUTOMOTIVE SOFTWARE UPDATES

Wege der Software ins Fahrzeug: Übersicht

KONVENTIONELLE UPDATES



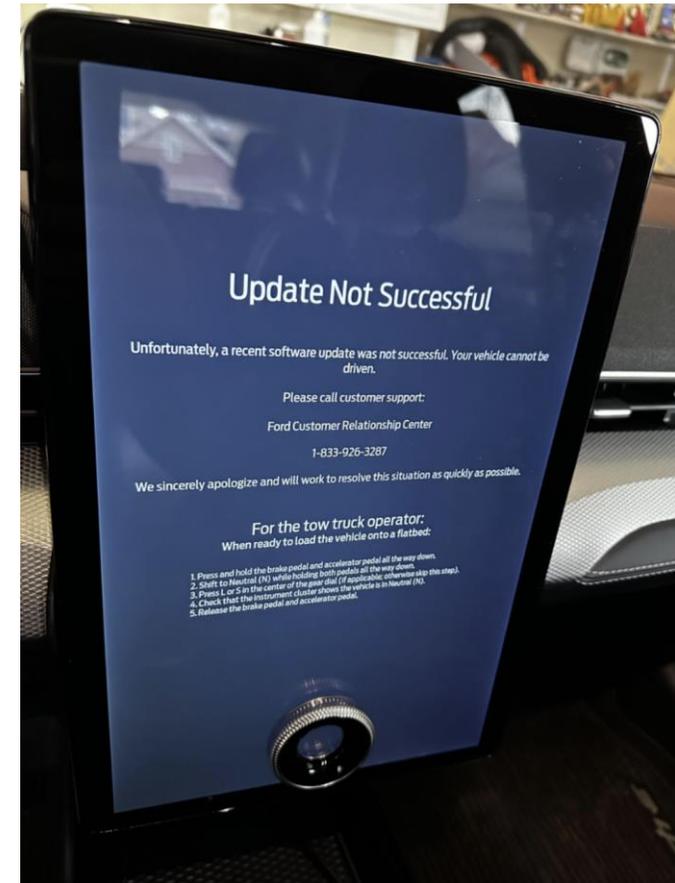
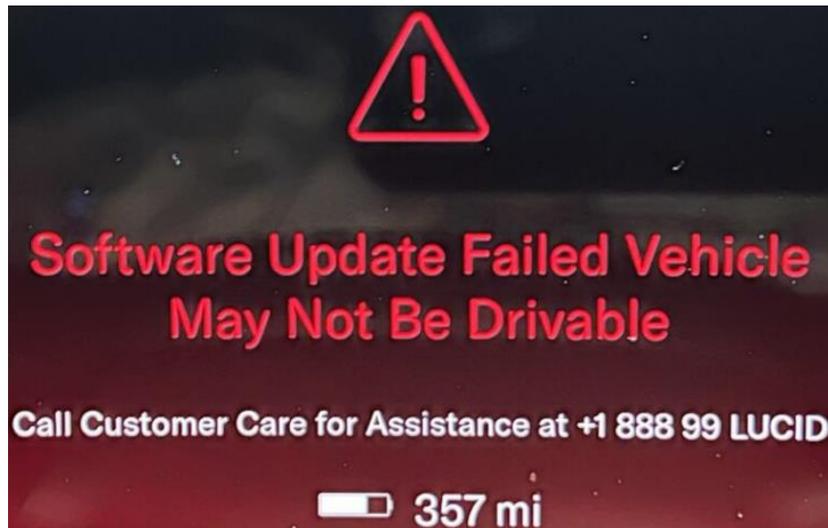
OVER-THE-AIR-UPDATES



RISIKEN VON OVER-THE-AIR-UPDATES IM AUTOMOBILBEREICH

Herausforderungen bei der Entwicklung von Software-Updates

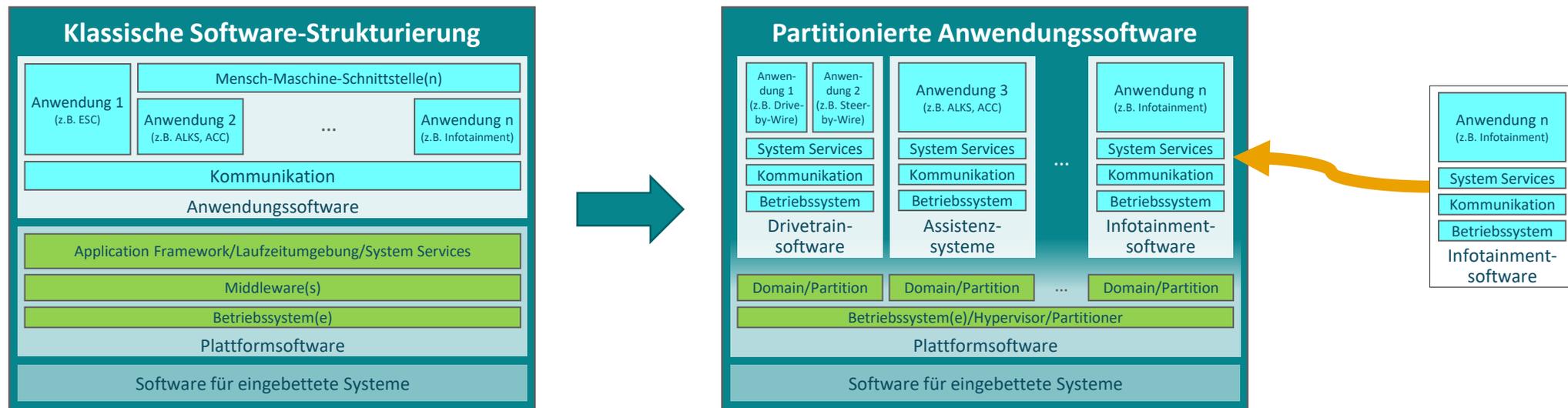
- Performance Probleme
- Einschränkung anderer Funktionen
- Beeinträchtigung der Fahrtüchtigkeit des Fahrzeugs



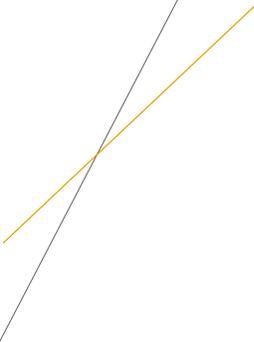
PARTITIONIERUNG VON SOFTWARE-KOMPONENTEN

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

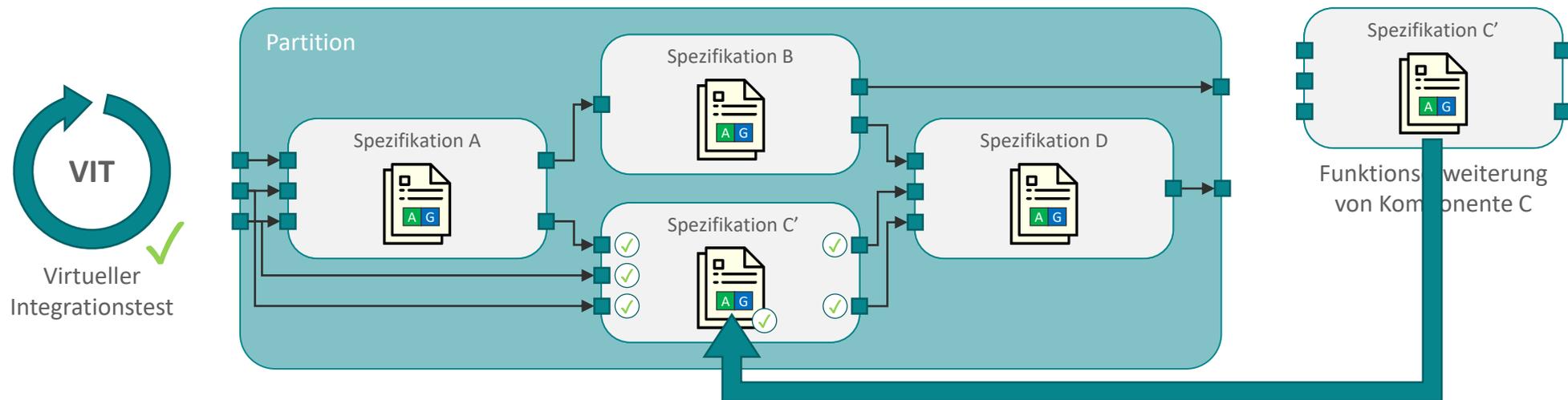
PROZESSSCHRITTE BEIM SOFTWARE-ZULIEFERER

Durchführung virtueller Integrationstests



2. Entwicklungsbegleitende Durchführung virtueller Integrationstests

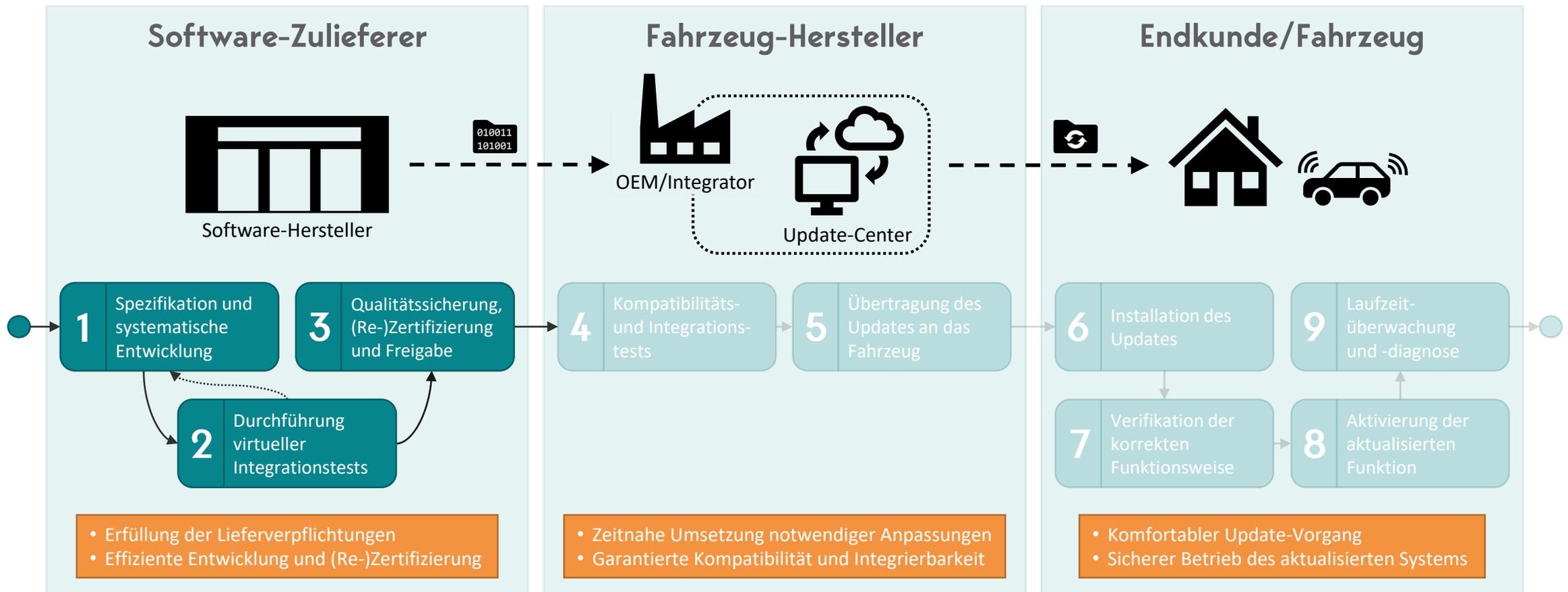
- Überprüfung der Konsistenz und Kompatibilität von Funktionen und Updates
- Anwendung klassischer Testverfahren zur Validierung der Funktionalität
- Abschließende Implementierung unter Einhaltung der verfeinerten Spezifikationen



0010011110101001001101100011101001000001001111010100100110110001110100100000100111101010010011011000111010010000010011110101001011011000111010010000010011110101001011011000111010010000010

ENTWICKLUNG VON SICHEREN OVER-THE-AIR-UPDATES

Beteiligte Akteure und relevante Prozessschritte



LAUFZEITÜBERWACHUNG UND -DIAGNOSE

Überwachung des Systemverhaltens während des Betriebs

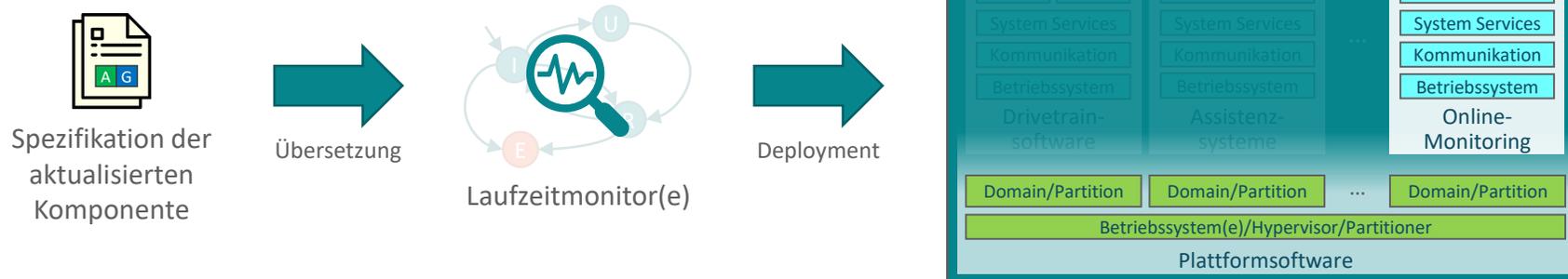
Software-
Zulieferer

Fahrzeug-
Hersteller

Endkunde/
Fahrzeug

9. Laufzeitüberwachung und -diagnose

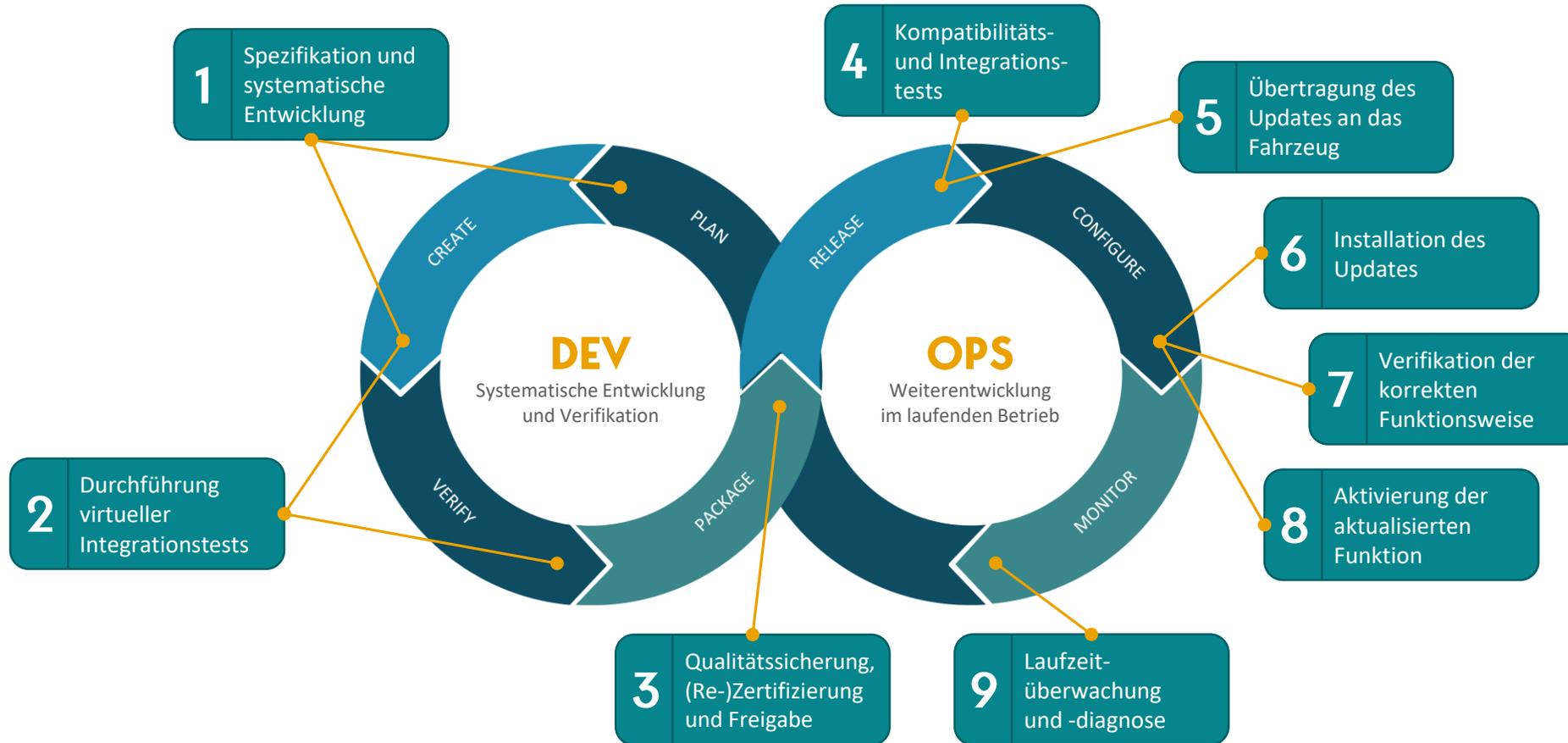
- Einsatz von Techniken zur Laufzeitüberwachung und -diagnose
 - Sammlung und Auswertung von Fahrzeugdaten in der Betriebsphase
 - Erkennung von Fehlern und Überschreitungen von Ressourcenbudgets
 - Grundlage für die kontinuierliche (Weiter-)Entwicklung des Systems
- Automatisierte Generierung von Laufzeitmonitoren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



Zusammenfassung und Ausblick

ENTWICKLUNG VON SICHEREN OVER-THE-AIR-UPDATES

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





Q&A SESSION

Vielen Dank für Ihre Aufmerksamkeit!

TASTE

THE KNOWLEDGE

Jeden zweiten Donnerstag!



fortiss



Deutsches Zentrum
für Luft- und Raumfahrt



NIEDERSÄCHSISCHES
FORSCHUNGSZENTRUM
FAHRZEUGTECHNIK





TASTE
THE KNOWLEDGE

Jeden zweiten Donnerstag!

NÄCHSTER TERMIN

07.03.2024 15:00-16:30 Uhr

Vertiefung – Systems Engineering mit dem NFF



fortiss



Deutsches Zentrum
für Luft- und Raumfahrt



NIEDERSÄCHSISCHES
FORSCHUNGSZENTRUM
FAHRZEUGTECHNIK

