Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

TASTE Transformations-Hub

Deployment & Updates

Automotive Updatetrends

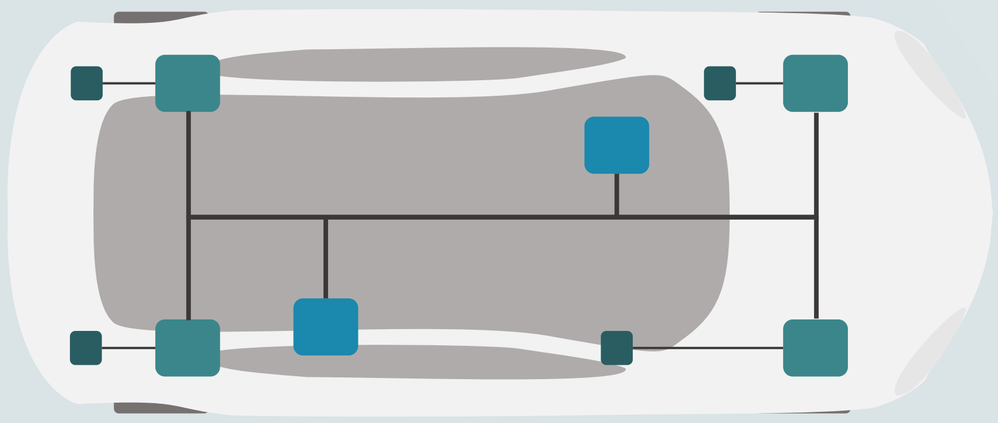
Mit einem steigenden Grad der Konnektivität von Fahrzeugfunktionen besteht eine erhöhte Notwendigkeit, die Fahrzeugsoftware auf einem aktuellen Stand zu halten. Die daraus resultierende zunehmende Relevanz von Over-the-Air-Updates stellt die Automobilbranche zukünftig vor neue Herausforderungen.

Motivation: Zunehmende Relevanz von Updates

- Das Auto als fahrender Computer: Updates für Sicherheit in der Informationstechnik (Security)
- Over-the-Air-Updates für kontinuierliche Verbesserung der Funktionalität
- Veränderte Markterwartungen: Updates als Produkt, Update-Vorgang mit geringer Beeinträchtigung

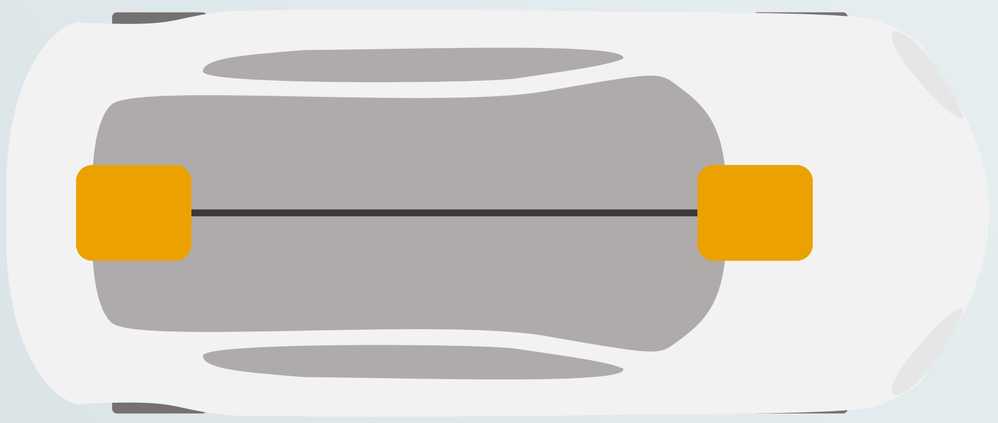
Heutige Fahrzeugarchitekturen

- Dedizierte ECUs



Zukünftige Fahrzeugarchitekturen

- Over-the-Air-Updates
- Zentralisierte ECUs

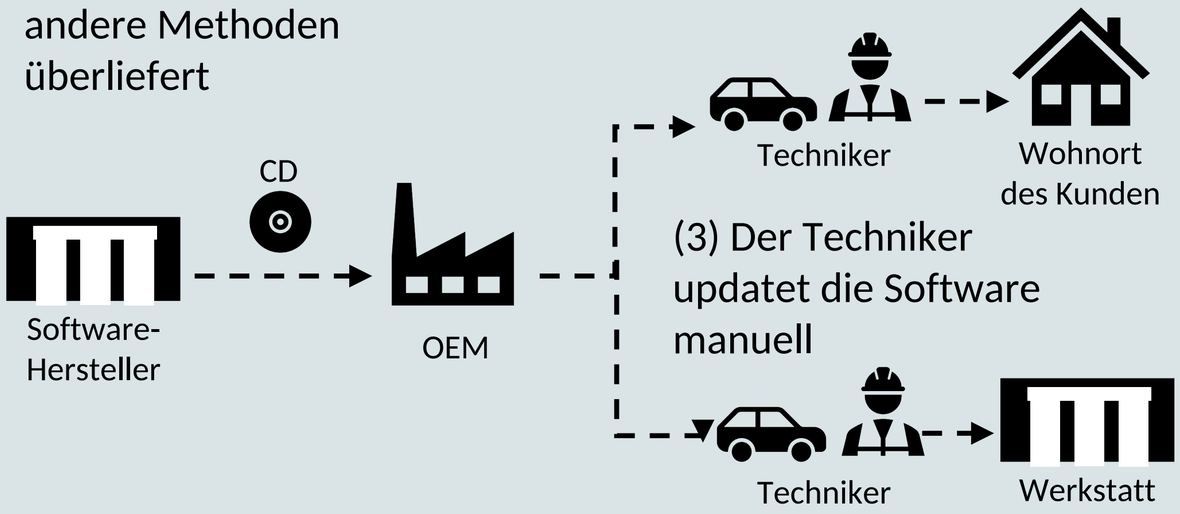


Konventionelle Update-Methode

(1) Software wird über Medien oder andere Methoden überliefert

(2) Der Kunde bringt das Auto zu einer Werkstatt oder ein Techniker kommt zu dem Kunden nach Hause

(3) Der Techniker updatet die Software manuell



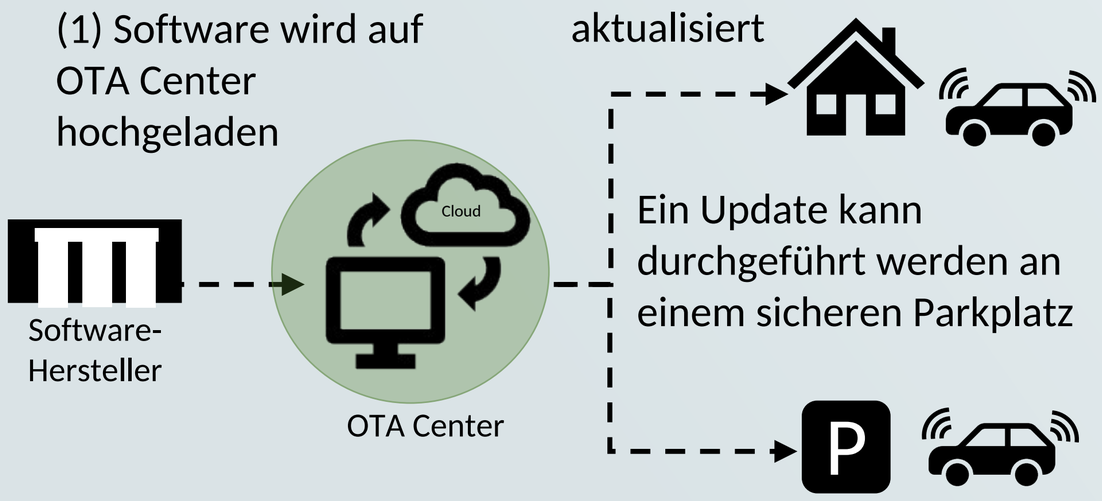
Updates in Zukunft

(1) Software wird auf OTA Center hochgeladen

(2) Software wird mit Over-the-Air-Updates verteilt

(3) Software wird automatisch aktualisiert

Ein Update kann durchgeführt werden an einem sicheren Parkplatz



Quellen:

FZI fortiss DLR Deutsches Zentrum für Luft- und Raumfahrt NFF Niedersächsisches Forschungszentrum Fahrzeugtechnik Ein Zentrum der TU Braunschweig ITS MOBILITY

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

TASTE Transformations-Hub

Deployment & Updates

Automotive Updatetrends

Die zukünftigen Updates werden zur Laufzeit in einem sensiblen Umfeld geschehen. Deshalb ist eine Sicherstellung eines korrekt durchgeführten Updates von fundamentaler Bedeutung.

Herausforderungen

- Funktionale Sicherheit
- Sicherstellung der zeitlichen Grenzen
- Sicherstellung des Ressourcenbedarfs
- Regularien von außen
- Kompatibilität mit Bestandssoftware
- Herstellung einer Ausführungsumgebung mit Ressourcengarantien für das Update
- Schutz vor Angreifern
- Absicherung von Updates

Entwicklung von Over-the-Air-Updates für geteilte Computing-Plattformen

„Correct-by-Design“-Entwicklung (2)
- Prozessbegleitende Verfeinerung der Spezifikationen zur nachweisbaren Umsetzung
- Implementierung der Funktionalität unter Verwendung OEM-spezifischer Schnittstellen
- Varianten- und Konfigurationsmanagement

Systematischer Entwurfsprozess (1)
- Frühzeitige Spezifikation extrafunktionaler Eigenschaften zur Berücksichtigung strenger vertraglicher Vorgaben zu nutzbaren Ressourcen
- Requirements Engineering & Traceability
- Modellbasierte Entwicklung

Abnahme durch den Auftraggeber (5)
- Finale Integrations- und Abnahmetests durch den Fahrzeughersteller mit eigenen Testsystemen
- Überprüfung der Einhaltung vertraglicher Vorgaben zu nutzbaren Ressourcen
- Produktivsystem-unabhängige Systemtests

„Over-the-Air“-Auslieferung (6)
- Schrittweise Auslieferung der Software-Komponenten als Over-the-Air-Updates
- Fahrzeuglokale Überprüfung der Kompatibilität unterschiedlicher Software-Komponenten durch eine herstellerspezifische Update-Middleware

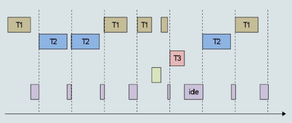
Entwicklungsteam

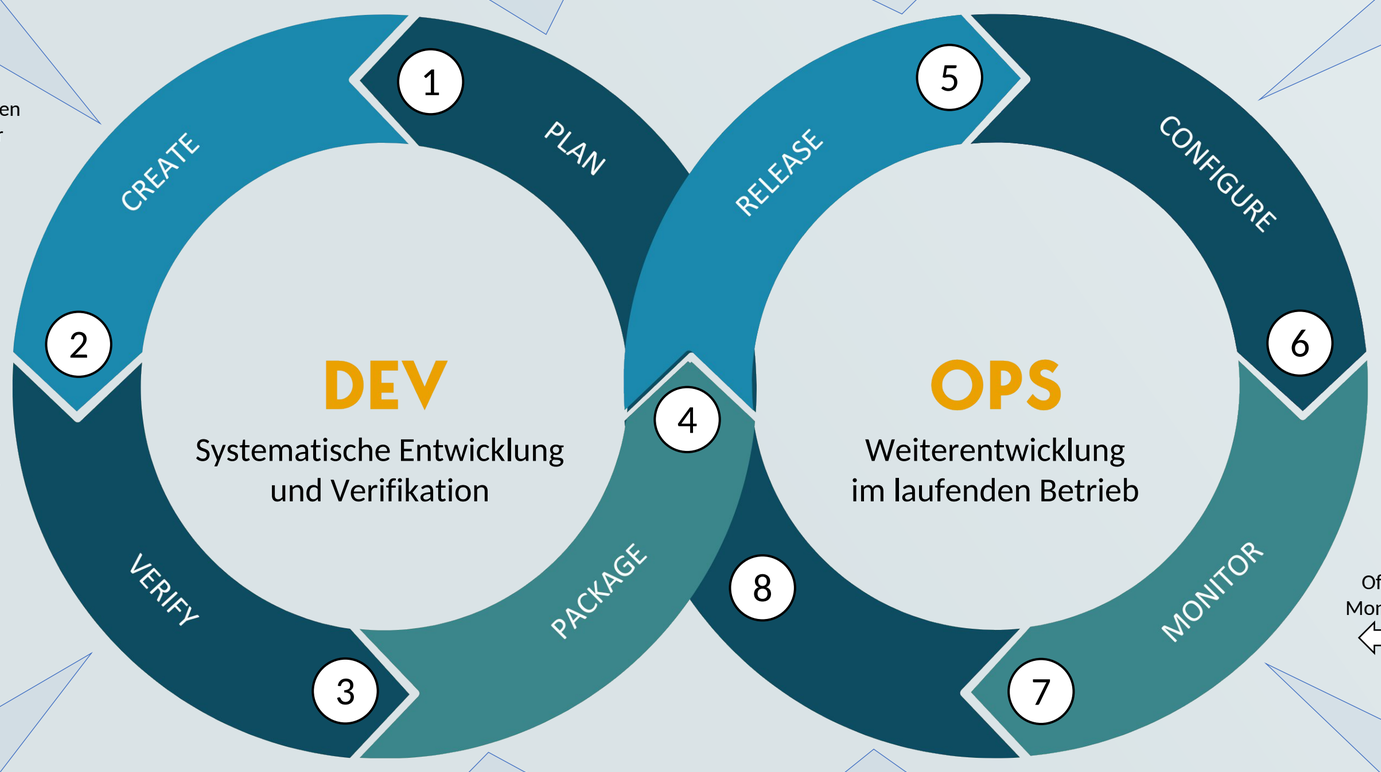
Übergabe an den Auftraggeber

Feedback zur Entwurfszeit

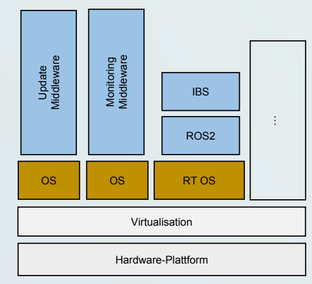
Update-Server

Werkzeugunterstützung für virtuelle Integrationstests

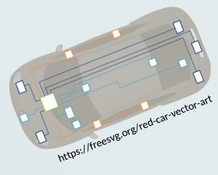




Update-Middleware



Online-Monitoring



Offline-Monitoring

Management und Analyse von Flottendaten

Verifikation & Validierung (3)
- Frühzeitige Überprüfung der Einhaltung vertraglicher Vorgaben zu nutzbaren Ressourcen
- Verifikation extrafunktionaler Eigenschaften
- Validierung der gewünschten Funktionalität
- Optimierung der Software-Komponenten

Unternehmensinterne Freigabe (4)
- Einsatz virtualisierter Testumgebungen zur Qualitätssicherung vor der Auslieferung
- Durchführung von virtuellen Integrationstests zur Absicherung der Einhaltung vertraglicher Vorgaben zu nutzbaren Ressourcen

Selbstdiagnose (8)
- Auswertung der gesammelten Flottendaten
- Ableitung und Priorisierung erforderlicher Anpassungen an den Software-Komponenten
- Planung der Umsetzung der erforderlichen Änderungen in der nächsten Prozessiteration

Selbstüberwachung (7)
- Dynamische Validierung von Sicherheits-eigenschaften während der Betriebsphase
- Laufzeitüberwachung zur Identifikation von Fehlern und Ressourcenkonflikten
- Aufnahme und Vorverarbeitung von Flottendaten

Deutsches Zentrum für Luft und Raumfahrt e. V. (DLR)

Das Oldenburger DLR-Institut „Systems Engineering für zukünftige Mobilität“ erforscht Methoden zur Entwicklung und Absicherung automatisierter und autonomer Verkehrssysteme der Zukunft. Im Fokus stehen die Entwicklung neuer effizienter Systems-Engineering-Methoden und -Werkzeuge für den Nachweis von Funktionalität (Verifikation) und Praxistauglichkeit (Validierung) sowie die Weiterentwicklung vertrauenswürdiger Systeme.

Quellen:
UP2DATE: Intelligent software-UPDATE technologies for safe and secure mixed-criticality and high performance cyber physical systems (H2020)

FZI fortiss DLR Deutsches Zentrum für Luft- und Raumfahrt NFF Niedersächsisches Forschungszentrum Fahrzeugtechnik Ein Zentrum der TU Braunschweig ITS MOBILITY