AQI | Automotive Quality Institute

Over-The-Air Updates

Eine vorwettbewerbliche Systematisierung

Projektnummer	9810007
Projektlaufzeit	01.12.2016 – 30.09.2017

Autoren	Jonas Römer (AQI) Dr. Danny Kreyenberg (AQI) Dr. Jürgen Großmann (Fraunhofer FOKUS)
Kontakt	jonas.roemer@aqigmbh.de

Datum	26.01.2018

Diese Veröffentlichung basiert auf dem Expertenwissen aus dem AQI und wissenschaftlicher Partner. Sie stellt einen konsolidierten Standpunkt zum entsprechenden Themenkomplex dar.

Executive Summary

Im Rahmen des AQI-Projekts „Over-The-Air-Updates“ haben das AQI und beteiligte Partner eine erste Bestandsaufnahme zu den Prozessen für Software-Updates Over-The-Air (OTA) in der Automobilindustrie durchgeführt. Die initiale Recherche zu OTA-Updates zeigte, dass viele verschiedenen Stakeholder sich mit der Thematik auseinandersetzen – aber zumeist nur mit einzelnen Teilaspekten. Forschungsinstitute beschäftigen sich wissenschaftlich mit OTA-Updates, nationale und internationale Gremien arbeiten mit behördlicher und rechtlicher Sichtweise an deren Auswirkungen und verschiedene Firmen der Automobilindustrie bereiten den Einsatz von OTA-Updates entweder vor oder bieten bereits Lösungen an. Verschiedenste Quellen wurden daraufhin geprüft, Interviews mit Experten geführt und die Inhalte strukturiert, um eine ganzheitlich Sichtweise auf den OTA-Update-Prozess zu entwickeln.

Ergebnis dieser Ist-Analyse ist ein idealisierter OTA-Prozess, der in einem Workshop mit benannten Experten diskutiert wurde. Es werden die einzelnen Aktivitäten, mögliche IT-Systeme, Informationsobjekte, Entscheidungsknoten und vor allem die Schnittstellen zwischen den verschiedenen Stakeholdern dargestellt. Der hohe Abstraktionsgrad des Prozesses ermöglicht den verschiedenen Adressaten, ihre spezifische Darstellung mit dem idealisierten Prozess zu verknüpfen. Vertiefend wird aufgezeigt, wie durch eine Klassifizierung des Updates der Prozess effizienter gestaltet werden könnte.

Die systematische Analyse des Prozesses und der Vergleich zum aktuell durchgeführten Werkstattprozess zeigen neue Herausforderungen und Aufgaben für die interne Qualitätssicherung, aber auch unternehmensübergreifend für die verschiedenen Stakeholder. Hierbei zeigt sich – wie auch in dem Workshop und den verschiedenen Gesprächen mit den Vertretern der Automobilindustrie –, dass die Regeln im Umgang mit OTA-Updates unklar sind. Regularien und Standards sind gewünscht, um den Anwendern von OTA-Updates durch adäquates Führen bzw. Lenken und Kontrolle des Update-Prozesses Sicherheit zu geben. Denn ohne diese (Rechts-)Sicherheit kann kein konformes Update durchgeführt werden.

Dieser Bericht beschreibt die abzusichernden Bereiche beim Einsatz von OTA-Updates. Aufgezeigt werden auch Probleme, Handlungsbedarf und vorwettbewerbliche Fragestellungen, die aus Sicht der Qualität zu adressieren sind. Empfohlen wird, die Ergebnisse mittels mehrerer Szenarien in einem Folgeprojekt zu verproben und ausgewählte Bereiche, in denen Unsicherheit in den Unternehmen herrscht, in einem Arbeitskreis zu diskutieren.

Inhaltsverzeichnis

Abbildungsverzeichnis

1 MOTIVATION UND ZIELSETZUNG

In der IT sind regelmäßige Software-Updates fester Bestandteil des Servicekonzepts. Firmen wie Microsoft, Apple oder Adobe bieten turnusmäßig Software-Updates (englisch Patches) an, um ihre Produkte sicherer und attraktiver zu machen. Diese Updates werden – zum Teil – an zuvor festgelegten Terminen konsolidiert angeboten, sodass sich Nutzer und Administratoren weltweit darauf einstellen können. Der wohl bekannteste dieser Tage ist der sog. Microsoft Patch-Day, an dem das Unternehmen Microsoft seine Software-Updates veröffentlicht.

In der Mobilfunkwelt werden Updates teilweise noch häufiger durchgeführt und dies mit sehr hohen Akzeptanzraten bei den Nutzern. Unter anderem deshalb, weil die Software bzw. die Apps i. d. R. besser, schneller und leistungsfähigerer werden. So geben laut einer Studie von Tomorrow Focus Media 33,4 Prozent der Befragten an, sofort ein Update bei Verfügbarkeit auszuführen. Nur 7 Prozent geben an, nie ein Update wahrzunehmen.

In der Automobilbranche haben sich Software-Updates inzwischen ebenfalls etabliert. Seit langem installieren Werkstätten neue Software, sei es für die Motor- und Getriebesteuerung oder die zahlreichen Fahrerassistenzsysteme. Im Vergleich zur IT-Welt sind die Häufigkeit und der Umfang der Software-Updates relativ gering. Dies liegt zum einen daran, dass die gesamte Softwarearchitektur komplex ist und nicht für diese Art von Aktualisierung konzipiert wurde. Zum anderen handelt es sich bei einem Fahrzeug zusätzlich um ein sicherheitskritisches System, für das besonders hohe Qualitäts- und Prüfansprüche gelten, die durch ein Software-Update nicht verletzt werden dürfen.

Software-Updates über eine Luftschnittstelle (englisch Over-The-Air [OTA]) ist die moderne, drahtlose Variante, mit der auf eine Vorführung des Wagens in eine Werkstatt und damit auf die entsprechende Ausrüstung und den Personalaufwand des Werkstattmitarbeiters verzichtet werden kann. Technologische Grundlage hierfür sind die vom Hersteller eingebauten Smart Antennas, das WIFI-Modul und / oder das Gateway (etc.). Grundsätzlich ist davon auszugehen, dass der Umfang von Software-Updates in zukünftigen, vollvernetzten Fahrzeugen deutlich zunehmen wird. Dies liegt insbesondere daran, dass die Vernetzung OTA-Updates erst möglich macht und somit ein Kanal zur Verfügung steht, Software im Fahrzeug effizient zu pflegen. Darüber hinaus wird man aber bei einem vernetzten Fahrzeug – allein schon aus Gründen der IT-Sicherheit – nicht mehr auf die flexible und rasche Bereitstellung von Software-Updates verzichten können. Technisch, organisatorisch wie auch regulatorisch stellen kontinuierliche und sichere Software-Updates eine Herausforderung für die Automobilindustrie dar.

Vor diesem Hintergrund ist es das Ziel dieses Berichts, die Thematik ganzheitlich zu strukturieren, zu analysieren und vorwettbewerblichen Fragestellungen zu OTA-Updates in der Automobilindustrie aufzuzeigen. Hierzu erarbeitet der Bericht Grundlagen, die in Folgeprojekten dazu genutzt werden können Best Practices, Maßnahmen und Kriterien, die robuste OTA-Updates ermöglichen, zu identifizieren und auf VDA-Ebene entsprechend verbindlich zu dokumentieren.

2 UMFELDANALYSE

In diesem Kapitel werden zwei Fragestellungen untersucht. Zum einen sollen die aktuellen Anwendungsszenarien und die beteiligten Stakeholder rund um OTA-Updates in der Automobilindustrie identifiziert sowie ihre Abhängigkeiten skizziert und systematisiert werden, um daraus Schnittstellen sowie notwendige Aktivitäten für OTA-Updates abzuleiten. Die hier erarbeitete Systematisierung wird im Weiteren dazu genutzt, detaillierte Prozessschemata für OTA-Updates zu entwickeln.

Zum anderen werden Initiativen und Konsortien, die sich die Standardisierung und industrielle Umsetzung von OTA-Updates in der Automobilindustrie zum Ziel gesetzt haben, in diesem Kapitel vorgestellt. Neben den Standardisierungsgremien bei der UN, ITU und ISO sind dies insbesondere Industriekonsortien, die sich speziell um Softwarearchitekturen für Telematik- und Entertainmentsysteme kümmern. In diesen Bereichen finden sich IT-Systeme mit hoher Konnektivität und – aufgrund der raschen Entwicklung – relativ kurzen Lebenszyklen.

2.1 Einsatz in der Automobilindustrie

Durch die zunehmende Vernetzung der Fahrzeuge und dem Wunsch der Kunden, auch während der Nutzungsphase neue bzw. verbesserte Funktionen zu erhalten, steigt der Druck auf die Automobilindustrie Software-Updates anzubieten. Zudem steigt die Anzahl softwarebedingter Rückrufe. 2015 wurden bereits 11,5 Prozent aller Rückrufe in den Vereinigten Staaten softwarebedingt ausgelöst, während diese Kennzahl im Jahr 2000 nur bei rund 0,5 Prozent lag. Derzeit haben die Programme eines Oberklassefahrzeugs bis zu 100 Millionen Zeilen Quelltext – Tendenz steigend. Mit Blick auf die weitere Vernetzung sowie die Einführung des hochautomatisierten Fahrens wird der Softwareanteil noch einmal deutlich zunehmen. Ferner wird in der Zukunft die Notwendigkeit bestehen, auch sicherheitsrelevante Software zu pflegen und Sicherheitslücken zu schließen. Würden in Zukunft alle Software-Updates in Fachwerkstätten durchgeführt werden, würde das zu hohen Kosten und langen Umsetzungszeiten führen.

Als Alternative zu den herkömmlichen Updates durch die Werkstätten kann die Verteilung von Software-Updates über die Luftschnittstelle „Over-The-Air“ (OTA) die Durchlaufzeit verkürzen, die Kosten reduzieren und die Kundenzufriedenheit steigern. Für die OEMs sind OTA-Updates darüber hinaus ein Instrument, kosteneffizient, zuverlässig und schnell Softwarefehler zu beseitigen. Voraussetzung ist, dass Automobilhersteller, Zulieferer und Telekommunikationsanbieter eine Infrastruktur aufbauen, mit der sich Software-Updates sicher und effizient auf die Fahrzeuge im Feld verteilen lassen.

Von den deutschen Automobilherstellern Daimler, BMW und Audi werden derzeit vor allem Apps mitsamt Internet-Browser, das Telefonmodul sowie Navigationskarten über die Luftschnittstelle aktualisiert. Bei dem Browser und den Telefonmodulen gelangen die Updates zum Teil automatisch ins Fahrzeug und können vom Kunden nicht abgelehnt werden. Apps und Navigationskarten müssen allerdings schon heute vom Kunden ausgewählt und installiert werden.

Wenn zukünftig mehr Software-Updates eingespielt werden müssen und sogar neue Funktionen nachgerüstet werden, sind Grundsatzfragen zu klären. Wie bei den Smartphones ist festzulegen, wer welche Updates erhält. In der Android-Welt hängt dies vom Hersteller und vom jeweiligen Modell ab. Ältere Geräte werden oftmals nicht mehr mit Updates versorgt, selbst bei den eigentlich unabdingbaren Sicherheits-Patches. Was wann und wie implementiert wird, ist undurchsichtig. Anders ist es in der Apple-Welt: Ein einziges iOS-Betriebssystem wird all jenen Geräten bereitgestellt, die hinreichend leistungsfähig sind.

Überträgt man das Smartphone-Beispiel auf Autos, heißt der Apple unter den Herstellern Tesla: Die Amerikaner verfolgen den Gedanken, dass alle Modellvarianten mit einem einzigen Betriebssystem fahren. Mit ihren fortwährenden Software-Aktualisierungen werden dabei Charakteristika des Fahrzeugs verändert: von den Assistenzsystemen über die Fahrwerksabstimmung und die Motorleistung bis hin zum strittigen Autopiloten. Unterschieden wird allein zwischen der ersten Hardware-Plattform bis Oktober 2016 und der Folgeplattform. Stets wird die neue Software über das eingebaute Mobilfunkmodul in den Tesla geladen. Der Besitzer des Fahrzeugs kann indes eine Aktualisierung ablehnen oder den Ladevorgang beschleunigen, indem er sein Auto in ein WLAN einwählt.

Wenn mit einem Software-Update wichtige Eigenschaften des Autos verändert werden, kann die Betriebsgenehmigung erlöschen. Im Tesla S wurden die Kamera hinter der Windschutzscheibe, der Radarsensor und zwölf Ultraschallsensoren für die Abstandsregelung und die Spurhalteassistenz genehmigt. Mit der Software vom Herbst 2015 konnte dann das Fahrzeug dank einem Teil dieser Sensoren teilautonom fahren.

Übergeordnet lassen sich drei Anwendungsszenarien für OTA-Updates identifizieren. OTA-Updates werden eingesetzt …

1) … zur Nachrüstung von Steuergeräten oder Systemen in Fahrzeugen, um technische Fehlfunktionen zu beheben. Dies spart Kosten und Zeit, z. B. bei Rückrufen;

2) … zum Schließen einer Sicherheitslücke, die durch Angreifer ausgenutzt werden könnte. OTA-Updates stellen hier die Reaktionssicherheit sicher;

3) … zur Verbesserung existierender Funktionen oder zum Hinzufügen neuer Funktionalitäten. So werden neue Geschäftsmodelle möglich bzw. der Nutzen für die Kunden und damit die Kundenbindung wird erhöht.

Erst durch Software-Updates Over-The-Air können die Marktteilnehmer die Chancen steigender Digitalisierung und Vernetzung von Fahrzeugen nutzen und deren Schwachstellen absichern.

2.2 Stakeholder des OTA-Update Prozesses

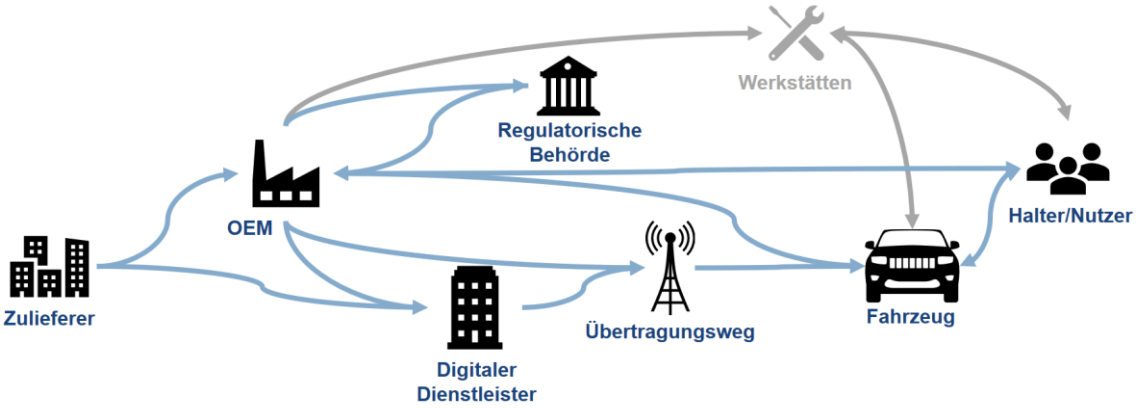


Abbildung 1: Stakeholder im OTA-Update-Prozess

Abbildung 1 zeigt schematisch die Beteiligten und deren Schnittstellen am Over-The-Air Updateprozess. Während die Werkstätten nur noch als Rückfallebene dienen, müssen insbesondere der Übertragungsweg und die Umsetzung im Fahrzeug berücksichtigt werden. Darüber hinaus erstrecken sich weitere neue Herausforderungen über alle Stakeholder und die neu entstehenden Schnittstellen.

Die Zulieferer entwickeln die Software-Updates unter ggf. neuen Gesichtspunkten der Ressourceneffizienz und zeitlicher Anforderungen, z. B. bei Aktualisierungen, die schnell zur Verfügung stehen müssen, um Sicherheitslücken zu schließen. OEM koordinieren die Updates, entwickeln diese mit bevor sie diese testen und abschließend freigeben. Die Übertragung zum Fahrzeug erfolgt entweder durch den OEM selbst oder mit Unterstützung neuer Dienstleister. Die Aufgabenteilung zwischen beiden Parteien kann dabei weitgefächert sein oder nur einzelne Aufgabenpakete betreffen.

Neue digitale Dienstleister beschäftigen sich direkt mit den Herausforderungen von OTA-Updates und bieten entsprechende Lösungen hierfür an. Zu den digitalen Dienstleistern zählen

Firmen wie Airbiquity, Blackberry, Delphi/Movimento, EnGIS Technologies, Excelforce, Harman, Wind River oder die in Berlin ansässige Firma Advanced Telematic Systems (ATS). Beispielsweise hat ATS einen OTA-Cloud-Service entwickelt, der skalierbar einsetzbar ist und das Security-Framework ‚Uptane' unterstützt. Als Mitglied des VDA ist die Firma auch in verschiedenen Gremien vertreten, um offene und industrieweite Standards zu etablieren.

Im Fahrzeug selbst findet u. a. der Empfang, die Validierung des Updatepaketes und die Installation statt. Darüber hinaus muss das Fahrzeug permanent gegen Angriffe von außen geschützt sein, denen sich das Fahrzeug mit der neuen OTA-Schnittstelle hin öffnet. Optional hilft das Fahrzeug bei der Analyse von Fehlern bzw. der Identifikation von zu aktualisierenden Fahrzeugen mittels der Übertragung von Fahrzeugkonfigurationen oder Fahrzeugdaten aus dem Feld. Die Rolle des Halters bzw. des Nutzers verändert sich ebenfalls, vor allem hinsichtlich der Information über das Update sowie der Autorisierung des Updates.

Zu betrachten ist auch die Rolle der regulatorischen Behörde und deren Flexibilität sich an ggf. dynamischere Prozesse anzupassen. OTA-Updates sind ein wichtiges Instrument, um Rückrufaktionen zu beschleunigen. Der auch für den Kunden hohe Aufwand, das Fahrzeug in die Werkstatt zu bringen, entfällt bzw. ist nur noch bei fehlgeschlagenen Updates notwendig.

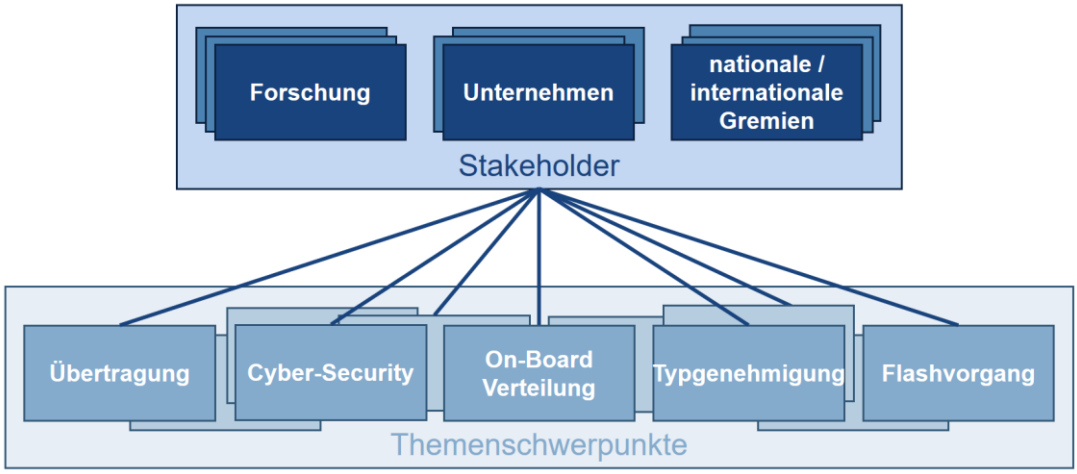


Abbildung 2: Skizze der inhaltlichen Schwerpunkte von OTA-Stakeholdern

Neben der Kategorie der Unternehmen gibt es noch weitere Stakeholder, die sich mit Software-Updates Over-The-Air auseinandersetzen. Weltweit arbeiten verschiedene Forschungsinstitute und internationale bzw. nationale Gremien an verschiedenen Teilaspekten der Thematik. Themenschwerpunkte sind dabei die Übertragung der Updates, die Cyber-Security, die On-Board-Verteilung, der Flashvorgang usw. Das Betrachtungsspektrum variiert dabei: es reicht von Berichten über Übersetzungen einzelner Prozessbausteine in Programmiersprachen, hin zu ganzen Software-Frameworks oder übergeordneten organisatorischen Fragestellungen, wie der Einfluss auf die Typgenehmigung. Zwischen den verschiedenen Gremien gibt es zum Teil große inhaltliche Schnittmengen und verschiedene Ansätze. Einzig eine ganzheitliche Betrachtung mit Berücksichtigung aller Aspekte oder zumindest Aufdeckung dieser fehlt.

Nachfolgend werden exemplarisch verschiedene Initiativen aus der Forschung und der Gremienarbeit vorgestellt.

2.3 (Inter-)nationale Gremien

Die Arbeit verschiedener internationaler und nationaler Gremien zielt auf mögliche Standardisierung im Umfeld von OTA-Updates.

2.3.1 UN Task Force on Cyber Security and OTA issues

Die Task Force wurde Ende des Jahres 2016 als Teil der Arbeitsgruppe für intelligente Verkehrssysteme / automatisiertes Fahren (IWG on IST / AD) von WP.29 gegründet. Die Arbeitsgruppe beschäftigt sich vornehmlich mit Cyber-Security und Datenschutz für Fahrzeuge und adressiert Over-The-Air-Software-Updates als ein effektives Mittel zur Behebung von Sicherheitslücken. Basierend auf einer ersten Sammlung von Cyber-Sicherheitsrisiken werden Empfehlungen erarbeitet, wie Regulierungsbehörden Cyber-Sicherheitsrisiken und Bedrohungen im Zusammenhang mit den jeweiligen Fahrzeugsystemen regulieren und verringern können. Es wird erwartet, dass die Task Force bereits innerhalb eines Jahres Empfehlungen oder Bestimmungen über Cyber-Security, Over-The-Air-Updates und Datenschutz bereitstellen kann.

2.3.2 ITU-T X.1373 (X.itssec-1)

ITU-T X.1373 definiert sichere Software-Update-Verfahren für Intelligent Transportation Systems (ITS). Der Standard beschreibt die Interaktion zwischen Software-Update-Server und Fahrzeugen sowie die notwendigen Absicherungsmaßnahmen zur Durchführung sicherer Updates. Zur Beschreibung gehört ein grundlegendes Modell des Software-Update-Prozesses, eine Bedrohungs- und Risikoanalyse, Sicherheitsanforderungen sowie die Spezifikation der abstrakten Datenformate für die Update-Kommunikation. Das Verfahren soll auf ITS-Kommunikationsgeräten in ITS-Fahrzeugen unter Verwendung der Fahrzeug-zu-Infrastruktur-Kommunikation (V2I) mittels Internet und / oder dedizierten ITS-Protokollen angewendet werden können. Verfahren und Datenformate zur Verteilung der Software im Fahrzeug gehören nicht zum Spezifikationsumfang. Der Standard wird von der Arbeitsgruppe ITU-T SG17 im Rahmen einer neuen Standardisierungsinitiative erarbeitet, mit dem Ziel die Entwicklung von Sicherheitsstandards für intelligente Verkehrssysteme (ITS) voranzubringen und zu koordinieren.

2.3.3 JasPar

Die Organisation ‚Japan Automotive Software Platform and Architecture' (JasPar) hat eine eigene Working Group zum Thema Over-The-Air Updates gegründet. Im Auftrag des Japanischen Automobilverbandes setzen sich verschiedene Gruppen von Spezialisten mit den unterschiedlichen Ebenen von OTA-Updates (Organisatorisches, Technik, Security, etc.) auseinander. Eine Veröffentlichung der Arbeitsergebnisse steht noch aus.

2.3.4 VDA

Im VDA werden OTA-Updates nur als Teil weitere Themenkomplexe behandelt. So beschäftigen sich der AK ‚Car Security', der AK ‚Daten' und der AK ‚Produktsicherheit und –konformität' in der automobilen Lieferkette bei Produktabweichungen' mit nur den Inhalten von OTA-Updates, die relevant für den jeweiligen Schwerpunkt des Arbeitskreises sind. Eine ganzheitliche Betrachtung findet nicht statt.

2.3.5 ISO/SAE AWI 21434

Die Standardisierungsgremien ISO und SAE beschäftigen sich gemeinsam in der ISO/SAE AWI 21434 ‚Road Vehicles – Cybersecurity engineering' mit der Absicherung von Straßenfahrzeuge gegenüber Cyber-Sicherheitsrisiken. Im Rahmen dieser Standardisierung wird auch das Thema OTA-Updates berücksichtigt. Der Standard ist aktuell noch in der Erarbeitung. Die Veröffentlichung ist für Oktober 2019 vorgesehen.

2.4 Forschungsergebnisse und Frameworks

Neben den erwähnten Standardisierungsaktivitäten internationaler Gremien gibt es eine Reihe interessanter Entwicklungen von Forschungseinrichtungen und Industriekonsortien, die eigene Lösungen bzw. Frameworks für OTA-Updates im Fahrzeugbereich anbieten.

2.4.1 GENIVI RVI – SOTA

Die GENIVI Alliance ist ein Industriekonsortium, das sich für die breite Einführung von Open-Source-In-Vehicle-Infotainment (IVI) -Software engagiert und eine offene Technologieplattform für das vernetzte Fahrzeug entwickelt. Im Rahmen der Arbeiten an der Technologieplattform wurde mit RVI SOTA eine Infrastruktur zum Hochladen, Verwalten, Warten, Übertragen,

Validieren und Bereitstellen von Software-Updates per Fernzugriff auf eine Fahrzeugflotte realisiert. Das Update-Framework umfasst sowohl eine Server- als auch eine Client-Komponente, die mit dem Rest des GENIVI-Systems integriert ist. RVI SOTA basiert auf offenen Standards und kann mit bestehender Logistik- und Flottenmanagement-Software als Teil einer umfassenden Update- und Security-Lösung integriert werden.

2.4.2 AGL Automotive Grade Linux

Automotive Grade Linux (AGL) ist ein Open-Source-Projekt, das, getragen von Automobilherstellern, Lieferanten und Technologieunternehmen, einen offenen Software-Stack für das vernetzte Fahrzeug entwickelt. Auf Basis von Linux entwickelt AGL eine offene Plattform, die als De-facto-Industriestandard Verwendung findet. AGL diskutiert derzeit die Integration von SOTA auf Basis von GENIVI RVI-SOTA und OSTree.

2.4.3 UPTANE / AutoTUF

Uptane ist ein neues Software-Update-Framework, das speziell auf die Sicherheitsanforderungen der Automobilindustrie abgestimmt ist und auf dem ‚The Update Framework' (TUF) basiert. TUF ist ein Sicherheitssystem, das zum Schutz von Software-Repositories, wie Microsoft Windows Update, Ubuntu, Python Package Index, etc., entwickelt wurde. Uptane ist speziell mit dem Ziel entwickelt worden, den hohen Sicherheitsanforderungen des Software-Updates in der Automobilindustrie gerecht zu werden. Uptane wurde in Zusammenarbeit mit großen Fahrzeugherstellern sowie US-Regierungsbehörden konzipiert und wird bereits von OEMs und mehreren Tier-1-Lieferanten in den USA verwendet.

2.4.4 OMA DM (Open Mobile Alliance)

Der Industriestandard der Open Mobile Alliance (OMA) beschreibt ein Verfahren und Protokolle zum Software-Update, das in den OMA Arbeitsgruppen Device Management (DM) und Data Synchronization (DS) für das Update von Software und Firmware im Telekommunikationsbereich spezifiziert worden ist. Das Protokoll basiert auf SyncML (XML) und unterstützt die Konfiguration von Geräten, das Aktivieren und Deaktivieren von Funktionen, die Bereitstellung neuer Software sowie das dafür notwendige Fehlermanagement. Der Standard ist seit 2008 in der Anwendung und hat im Jahr 2016 mit der Version 2.0 eine grundlegende Überarbeitung erfahren, die insbesondere die Nutzung internetfähiger Technologien und Architekturen erlaubt (z. B. Webbrowser zur Geräteverwaltung, Client-Server Architektur zur Verteilung der Updates).

2.4.5 Kommerzielle Technologieanbieter

Firmen wie Harman/Redbend, NXP, Elektrobit etc. bieten inzwischen alle auch eigenständige Lösungen zum Software-Over-The-Air-Update an. Die Lösungen haben einen unterschiedlichen Grad an Reife und zielen darauf ab, ausgehend vom bereits heute etablierten Lösungen für den Bereich Telematik, perspektivisch SOTA Updates für das gesamte Fahrzeug realisieren zu können.

2.5 Aktuelle Gesetzesvorhaben

Stellungnahmen zum hochautomatisierten Fahren sowie zur Cyber-Sicherheit in Fahrzeugen fordern die Verfügbarkeit rascher und unkomplizierter Software-Updates als Bestandteil der Softwarepflege und damit unumgängliche Maßnahme zur Wahrung der Cyber-Sicherheit in Fahrzeugen. Software-Updates haben darüber hinaus grundsätzlich das Potential, Herstellerzertifizierungen oder Zulassungen zuwiderzulaufen, die für die Typgenehmigung (TA) bzw. durch FMVSS und ECE gefordert sind. Entsprechende Diskussionen zur Interpretation und Revision der Zulassungs- und Zertifizierungsvoraussetzungen werden derzeit auf europäischer und internationaler Ebene diskutiert. Es ist zu erwarten, dass die ‚UN Task Force on Cyber Security and OTA Issues' (siehe Kapitel 2.3.1) im Verlauf dieses Jahres erste regulatorische Grundlagen in diesem Bereich erarbeitet. Darüber hinaus, lohnt sich ein Blick auf die Entwicklung in den Vereinigten Staaten. Die nationale Verkehrssicherheitsbehörde NHTSA setzt sich dort mit neuen Technologien und ihrer Bedeutung für die Funktionssicherheit im Fahrzeug auseinander. Im Fokus stehen hier insbesondere Software und Kommunikationstechnologien. Die NHTSA weist explizit darauf hin, dass im Falle von Sicherheitslücken in Software, allein das Vorhandensein der Sicherheitslücke einen sicherheitsrelevanten Defekt und damit ein unangemessenes Sicherheitsrisiko darstellen kann. Die NHTSA wertet Sicherheitslücken in Software im Sinne des US TREAD ACT als Meldepflichtig und erwartet von den Herstellern und Softwarelieferanten Maßnahmen mit denen sich diese Lücken schließen lassen. Inzwischen wird untersucht, ob Software-Updates Over-The-Air ein adäquates Mittel sind, dass Rückrufe ersetzen kann.

In ihrer Federal Automated Vehicles Policy stellt die NHTSA darüber hinaus fest, dass zusätzliche Maßnahmen und Werkzeuge benötigt werden, um sicherzustellen, dass die Fahrzeugnutzer und -besitzer angemessen über Software-Updates und ihre Relevanz informiert werden. Die Sicherheit der betroffenen Fahrzeuge darf nicht beeinträchtigt werden. In diesem Zusammenhang wird auf die Entwicklung neuer Qualitätssicherungsmethoden verwiesen, die u.a. simulativ die Auswirkungen eines Software-Updates auf die Fahrzeugleistung und -sicherheit ermitteln.

Grundsätzlich besitzt die NHTSA die Befugnis, den rechtlichen Rahmen für Softwareänderungen an Fahrzeugen nach dem ersten Verkauf an einen Verbraucher zu definieren. Das Potential von OTA-Updates führt nun zu einer Situation, in der die NHTSA in Betracht zieht zusätzliche Regeln und Regulierungsinstrumente zu entwickeln, die geeignet sind, Zertifizierungsanforderungen und Compliance-Prüfungen für Software-Updates nach dem Verkauf eines Fahrzeugs zu realisieren.

Für weitere Betrachtungen aktueller Gesetzeslagen und -initiativen zu OTA-Updates sei hier – mit freundlicher Genehmigung des Autors – auf den Report ‚Key Legal Issues – Automotive Over-The-Air Updates' der Firma Advanced Telematic Systems verwiesen (https://www.advancedtelematic.com/en/news/key-legal-issues-of-automotive-Over-The-Air-updates.html).

3 IST-AUFNAHME DES OTA-UPDATE-PROZESSES

In diesem Abschnitt wird der OTA-Updateprozess detailliert beschrieben. Die Beschreibung basiert auf einer Ist-Analyse anhand wissenschaftlicher Recherche, Einzelinterviews mit Vertretern der Automobilindustrie sowie einem durchgeführten Workshop am AQI mit den benannten Experten der VDA-Mitglieder. Die Darstellung des idealisierten Prozesses soll als einheitliche Diskussionsgrundlage, für gemeinsame Kommunikation sowie weitere Analysen dienen. Zunächst werden die Grenzen des Prozesses aufgezeigt, bevor die gewählte Prozessdarstellung beschrieben wird und die Prozess-Explikation selbst folgt. Im Anhang findet sich zu Vergleichszwecken eine analoge Darstellung des konventionellen Werkstatt-Prozesses (siehe Anhang: Werkstatt-Prozess).

In diesem Bericht wurde ein hoher Abstraktionsgrad gewählt, um ein gemeinsames Verständnis zwischen allen Beteiligten aufzubauen. Auf diese Weise können die verschiedenen Unternehmen ihre spezifischen Ausprägungen dem idealisierten Prozess unterordnen. Denn jede beschriebene Aktivität kann durch weitere Aktivitäten vertieft und präzisiert werden. Bei steigender Präzision ist entsprechend die Allgemeingültigkeit nicht mehr zwangsläufig gegeben, da die Unterschiede zwischen den verschiedenen Prozessen der beteiligten Mitgliedsfirmen nicht mehr berücksichtigt werden könnten. Diese Details bzw. Unterschiede begründen sich auch mit dem Wettbewerb in der Industrie der noch ‚jungen' Technologie Over-The-Air Updates. (Auf technische Ausprägungen kann innerhalb dieses Dokumentes hingewiesen werden. Unter dem Gesichtspunkt des Wettbewerbs wird jedoch darauf verzichtet, diesbezüglich Anforderungen zu beschreiben oder zu definieren.)

3.1 Prozessgrenzen

Beginn des hier dargestellten Prozesses ist die Identifikation des Software-Updatebedarfs, d.h. der beim OEM verantwortlichen Stelle für die Koordinierung eines Updates wird der Bedarf gemeldet aufgrund eines erkannten Problems. Die Meldung über den Bedarf kann dabei intern beim OEM bzw. in der Lieferkette generiert worden sein oder die Problemstellung wurde extern durch Kunden, die Presse oder andere Stakeholder an den OEM kommuniziert. Auf den

detaillierten Prozess des Erkennens von Fehlern bzw. eines Software-Updatebedarfs wird in diesem Bericht nicht eingegangen. Für die Auslösung (*Start*) des hier dargestellten OTA-Prozesses wird nur gefordert, dass ein solcher Software-Updatebedarf festgestellt worden ist.

Der Prozess *endet* nach der Rückmeldung über den Status der Installation des Updates. Diese wird entweder als erfolgreich registriert (und ggf. als erfolgreich durchgeführter Rückruf der regulatorischen Behörde gemeldet) oder bei mehrfachem Fehlschlagen der Installation erfolgt die weitere Bearbeitung im Rahmen des konventionellen Werkstattprozesses. (Der Werkstattprozess ist nicht dezidierter Teil dieser Analyse. Eine Ist-Aufnahme des gängigen Prozesses befindet sich im Anhang.)

Ferner kann bei Over-The-Air-Updates zwischen Konfigurationsupdates und Software- bzw. Firmware-Updates (sog. SOTA- bzw. FOTA-Updates) unterschieden werden. Im Folgenden wird auf alle Update-Typen als OTA-Update referenziert.

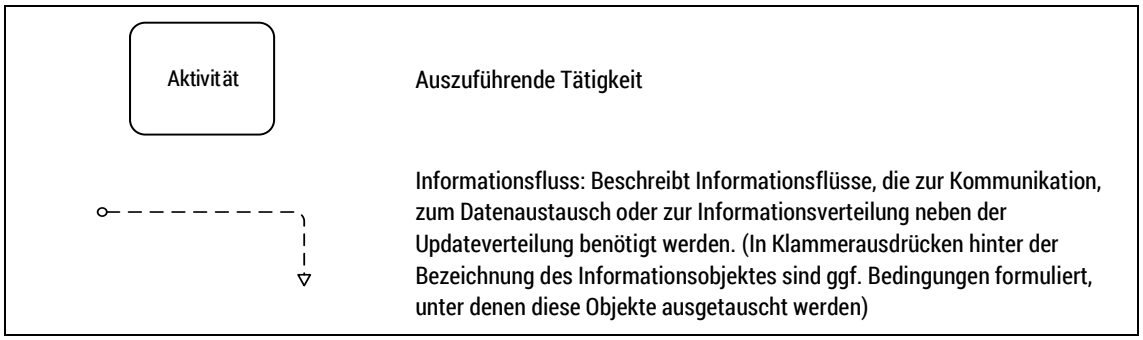
Fokus dieses Berichtes ist das OTA-Update im Sinne eines schreibenden Zugriffs auf das Fahrzeug. Vereinzelnd sind lesende Aktivitäten beschrieben, hierzu sei auf die weiteren Anforderungen beim Zugriff auf möglicherweise personenbezogene Daten hingewiesen, die ebenfalls nicht in diesem Bericht diskutiert werden.

3.2 Prozessdarstellung

Die dargestellten Prozesse werden sowohl in Prozessschreibweise als auch in Textform beschrieben. Eine genaue Erklärung und zu beachtende Aspekte bei der gewählten Darstellung werden in diesem Kapitel erläutert.

3.2.1 Modellierung mittels BPMN 2.0

Als Schreibweise für die Prozessdarstellung wurde BPMN 2.0 gewählt. Nachfolgende Legende beschreibt die verwendeten Elemente der Modellierungssprache:



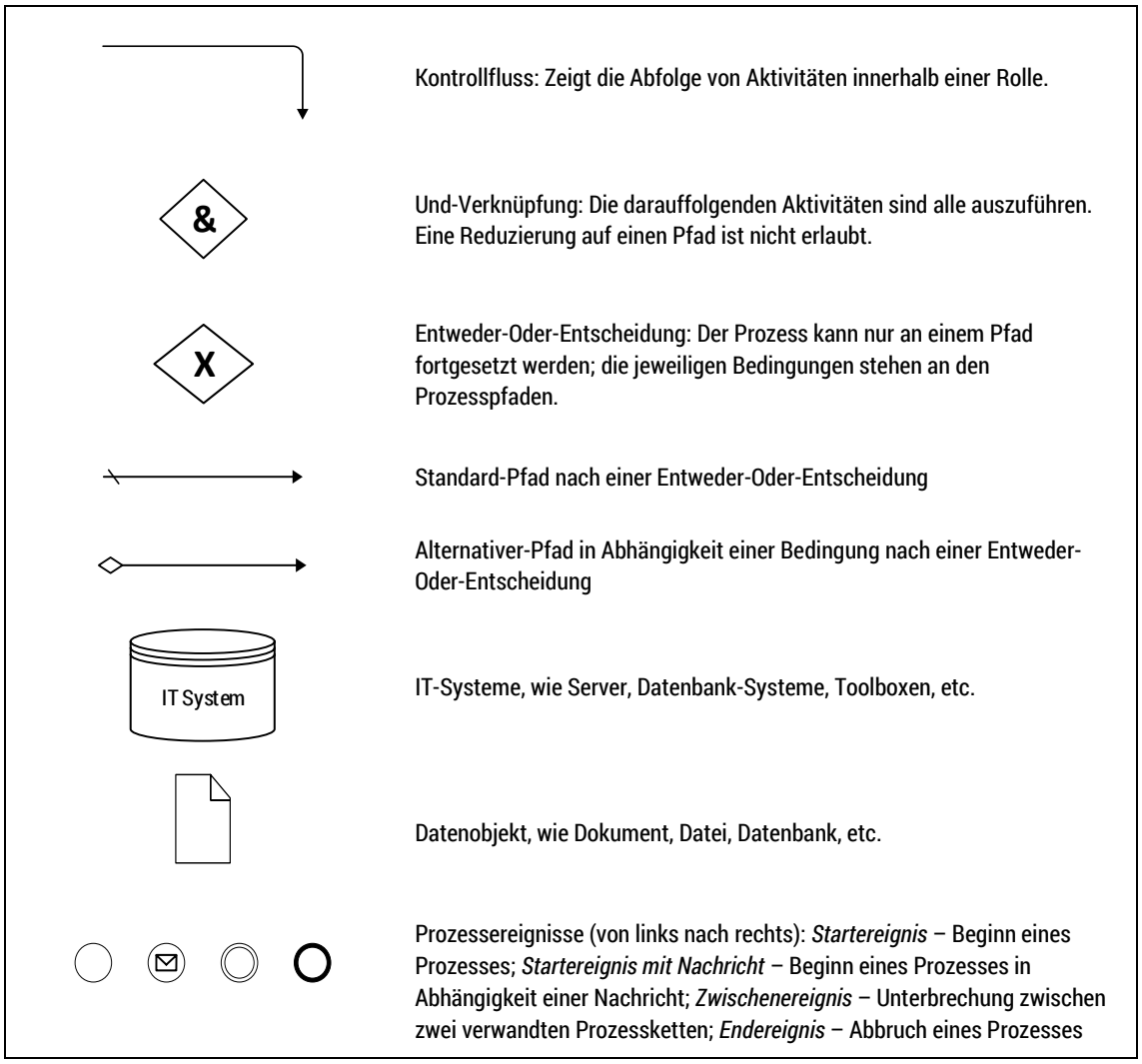


Abbildung 3: Legende der verwendeten BPMN 2.0

Alle Aktivitäten des Prozesses können durch eine eindeutige Prozess-ID identifiziert werden, auf die in dieser Dokumentation anschließend querverwiesen wird. Diese setzt sich aus drei Bestandteilen zusammen:

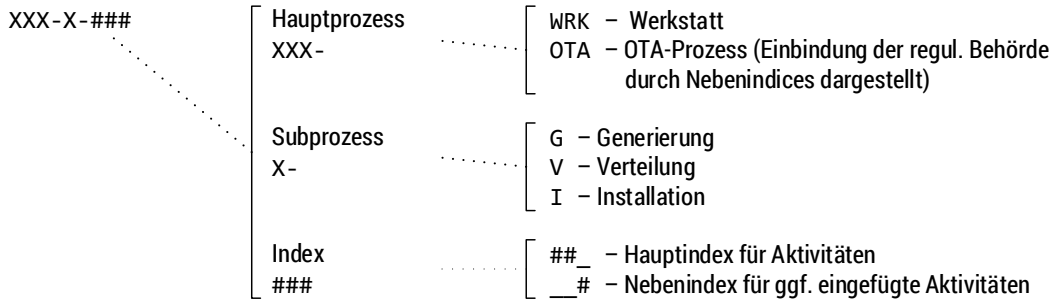


Abbildung 4: Definition der Prozess-ID

3.2.2 Textbeschreibung

Jede Aktivität ist zusätzlich in Prosa beschrieben. In ***kursiv und fett*** ist der jeweilige Verantwortliche für die Aktivität hervorgehoben. Nur in *kursiv* dargestellt sind alle weiteren Rollen, die erwähnt werden. Unterstrichen sind In- bzw. Output einer Aktivität. In der Prozesskette sind diese allerdings nur dann erwähnt, wenn Eigenschaften des Datenobjektes verändert werden oder durch Verzweigungen des Prozesses die Nachverfolgbarkeit eines Datenobjektes nicht mehr eindeutig ist. In einfacher **fetter** Schriftart hervorgehoben sind Bedingungen oder Verzweigungen, die an die Aktivität verknüpft sind. Tabelle 1 zeigt ein entsprechendes Beispiel.

Prozess-ID	Beschreibung
OTA-X-001	Input: Datenobjekt ABC ***Rolle A*** analysiert das Datenobjekt ABC und informiert *Rolle B* mittel Datenobjekt XYZ. Output: Datenobjekt XYZ
OTA-X-002	***Rolle B*** führt eine Datenabfrage gemäß der Spezifikation aus Datenobjekt XYZ durch und speichert sie auf dem Firmenserver. Ist ein Rückruf spezifiziert wird ein Dokument / ein Datenobjekt MNO an die *Regulatorische Behörde* weitergeleitet (OTA-X-003). Output: Dokument / Datenobjekt MNO
OTA-X-003	…

Tabelle 1: Beispiel einer Textbeschreibung von Prozess-Aktivitäten

3.2.3 Prozessvariationen

Während der Ist-Aufnahme wurden zwei Hauptprozesse aufgenommen: der konventionelle Werkstatt-Prozess (WRK) für Software-Updates (siehe Anlage Werkstatt-Prozess) und der Prozess, um solche Updates Over-The-Air (OTA) durchzuführen.

Aktivitäten des Werkstatt-Prozesses sind in **Schwarz** dargestellt. Finden sich diese Aktivitäten im OTA-Prozess wieder, sind sie hier ebenfalls in **Schwarz** dargestellt. In der Textvariante ist hier ein Querverweis mittels der Prozess-ID auf den identischen Prozessschritt zum Werkstatt-Prozess aufgeführt („vgl. WRK-X-###“). Alle neuen oder durch OTA-Updates veränderten Aktivitäten sind in **Blau** dargestellt.

Beide Prozesse variieren, wenn eine regulatorische Behörde eingebunden werden muss. Diese Alternationen des Prozesses sind in **Rot** hervorgehoben. Die Aktivitäten und Informationsflüsse

entfallen entsprechend, wenn die regulatorische Behörde nicht in den Updateprozess involviert wird. In der Textvariante wird mit dem Hinweis „nur bei regul. Behörde“ auf die Erweiterung der Prozesskette hingewiesen.

Abbildung 5 zeigt ein entsprechendes Beispiel.

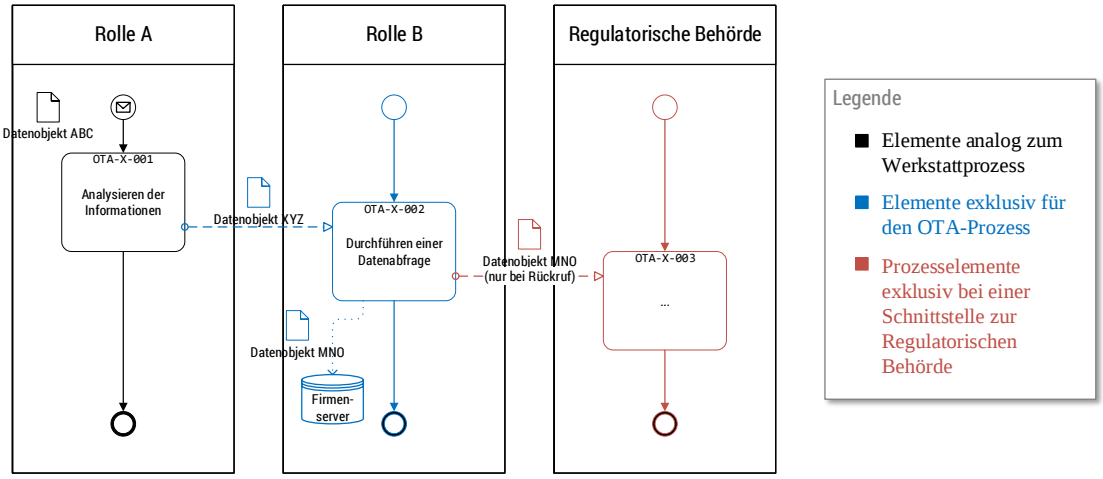


Abbildung 5: Beispiel der Darstellung von Prozessvariationen

3.2.4 Rollen im Prozess

Im Prozess werden verschiedene Rollen stellvertretend für den Bearbeiter, die Abteilung oder die Organisationseinheit in der jeweiligen spezifischen Lieferkette verwendet. Die beschriebenen Rollen können in ihrer Bezeichnung aber auch ihrem Aufgabenbereich in den verschiedenen Unternehmen variieren. Sie dienen hier zur Strukturierung der Inhalte, wurden aber praxisnah ausgesucht:

- Der *Update-Koordinator* übernimmt auf Seiten des OEM die Koordination des Software-Updates und repräsentiert den gesamtverantwortlichen Entscheider für die Behebung des identifizierten Problems.
- Der *Entwicklungsverantwortliche* verantwortet die technische Problemlösung.
- Der *Entwickler* setzt die Problemlösung um.
- Der *Digitale Dienstleister* repräsentiert die interne oder externe Abteilung / Firma, die die bei OTA hinzukommenden Aufgaben der Verteilung des Updates übernimmt. Das heißt, die ‚Lücke‘ in der Übertragung schließt, die zwischen den Servern des OEM und dem lokalen Speicher im Fahrzeug existiert.

Darüber hinaus existieren folgende Rollen:

- *Halter*
- *Fahrzeug*

- *Regulatorische Behörde*
- *Werkstatt* (nur im Werkstattprozess, siehe Anhang)

3.2.5 Prozessinhalte

Der Prozess eines OTA-Updates gliedert sich grundlegend in drei Unterprozesse, die von zwei zentralen Aufgaben begleitet werden. (Analog wurde auch der Werkstattprozess in diese drei Phasen unterteilt.)

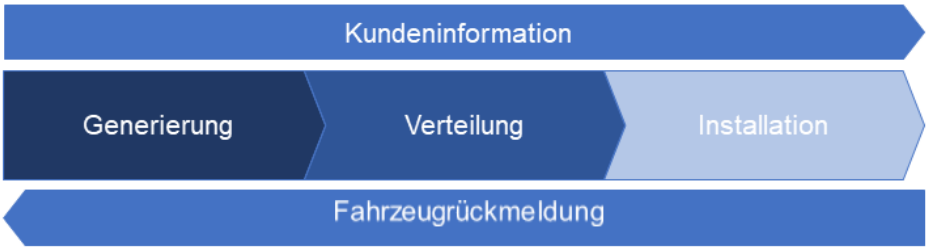


Abbildung 6: Schema des Updateprozesses

Zur **Generierung** zählen Aufgaben wie die Klassifizierung und das Kommunizieren des Updatebedarfs, die Entwicklung sowie die Qualitätskontrolle dieses Updates und eine anschließende Freigabe. Die **Verteilung** des Updates beginnt mit dem Identifizieren der betroffenen Fahrzeuge. Des Weiteren muss das Update digital zur Verfügung gestellt werden und vom Kunden bestätigt werden. Abgeschlossen wird diese Prozessphase durch das Herunterladen des Updates. Anschließend beginnt die **Installation** zunächst mit einer Verifikation des Updates bevor der Flashvorgang angestoßen wird. Nach der Durchführung der Installation ist diese zu testen und das Ergebnis zurückzumelden. Entlang der gesamten Prozesskette sind stets die **Kundeninformation** zu berücksichtigen. Kontinuierlich sind die Kunden über Updateverfügbarkeit, -inhalte und -fortschritte zu informieren. Eine begleitende **Fahrzeugrückmeldung** unterstützt das Identifizieren von Problemen und ihre anschließende Behebung für sämtliche betroffene Fahrzeuge.

3.2.6 Prozessanalyse

Nach den Inhalten der Prozesse werden tabellarisch Chancen und Risiken aufgeführt, die den Prozess begründen oder berücksichtigt werden sollten. Zwischen drei verschiedene Typen wird unterschieden:

Chancen…	…können einen positiven Einfluss auf einen der Stakeholder des OTA-Prozesses haben.

 Risiken... …können einen negativen Einfluss auf einen der Stakeholder des OTA-Prozesses haben.

 Sicherheitsrisiken... …sind Risiken, die auf eine Cyber-Security Schwachstelle zurückgeführt werden können. Diese können durch Dritte zum Schaden eines Stakeholders des OTA-Prozesses ausgenutzt werden.

Jeder Typ wird durch eine eindeutige dreistellige Kennziffer identifiziert (E###), sodass später auf diese Typen referenziert werden kann.

Die Analyse entlang der dargestellten Prozesskette basiert auf dem Vergleich zwischen Werkstatt-Prozess und OTA-Prozess, Recherchen, die zu Analysen weiterer Stakeholder führten, sowie den Experteninterviews.

3.3 Idealisierter Updateprozess Over-The-Air

Im Folgenden wird nun der OTA-Updateprozess beschrieben, dargestellt und untersucht. Jeweils für die Prozessschritte Generierung, Verteilung und Installation.

3.3.1 Generierung

Prozess-ID	Beschreibung
OTA-G-010 vgl. WRK-G-010	Input: Information über eine Fehlfunktion im Fahrzeug. Die Quelle für die Information kann unterschiedlich sein: sie kann sowohl intern durch eigene Beobachtungen oder extern durch Kommunikation mit der Regulatorischen Behörde, den Kunden, der Presse o. ä. erfolgen. Der ***Update-Koordinator*** analysiert die Informationen und identifiziert den Bedarf eines Software-Updates für ein betroffenes Bauteil / ein betroffenes System. Output: Updatebedarfsmeldung inkl. Fehlerbild und mögliche Ursache zur weiteren Nachverfolgung

OTA-G-020 vgl. WRK-G-020	Der ***Update-Koordinator*** klassifiziert das Software-Update.[1] Output: Ergänzung der Updatebedarfsmeldung um Updateklasse; ggf. Meldung an die *Regulatorische Behörde* **Konditionen: (A)** Zumindest, wenn das Update produktsicherheitsrelevant ist, ist die *Regulatorische Behörde* einzubinden (→ OTA-G-030). **(B)** Wenn das Update zu kritisch ist, um Over-The-Air verteilt zu werden, folgt hier der Abbruch und die Übergabe an den Werkstattprozess (→ WRK-G-040)
OTA-G-030 vgl. WRK-G-030 (nur bei Regul. Behörde)	Die ***Regulatorische Behörde*** registriert den Rückruf und informiert ggf. RAPEX bzgl. des Rückrufs.
OTA-G-031 vgl. WRK-G-031 (nur bei Regul. Behörde)	Ggf. wird durch die ***Regulatorische Behörde*** eine Frist bis zur Erfüllung des Rückrufs und/oder weitere Auflagen festgesetzt. Output: Anweisung
OTA-G-040 vgl. WRK-G-040	Der ***Update-Koordinator*** kommuniziert den Updatebedarf an den *Entwicklungsverantwortlichen*. Output: dokumentierte Updatebedarfsmeldung
OTA-G-050 vgl. WRK-G-050	Der ***Entwicklungsverantwortliche*** definiert das Lastenheft für das Software-Update. Output: Lastenheft für Software-Update
OTA-G-060	Input: Fahrzeugkonfiguration / Fahrzeugdaten (aus OTA-G-070) Der ***Entwicklungsverantwortliche*** beginnt die betroffenen Fahrzeuge zu identifizieren. Dies kann durch direkte Abfrage der OTA-fähigen Fahrzeuge erfolgen (‚Shoulder-Tap') oder indirekt durch Zugriff auf eine Datenbank, in welche die Fahrzeuge regelmäßig (in einem festgelegten Zeitintervall) ihre Konfiguration / weitere Eigenschaften schreiben könnten (‚Fhrzg.-DB'). Output: Datenbank mit den zu aktualisierenden Fahrzeugen (an OTA-G-080); ggf. Abfrage / ‚Shoulder-Tap' (an OTA-G-070)

[1] Klassifizierungsschemata vgl. Kapitel 4

OTA-G-070	Input: Abfrage / ‚Shoulder-Tap' oder zeitlich festgelegtes Intervall Das ***Fahrzeug*** sendet entsprechend OTA-G-060 die Fahrzeugkonfiguration (Softwareversionen, verbaute Hardware, etc.) / die Fahrzeugdaten. Zu den Fahrzeugdaten zählen dabei z. B. Diagnose-Daten oder je nach Zustimmung der Halter auch Belastungs- oder Fahrprofile. Output: Fahrzeugkonfiguration / Fahrzeugdaten (an OTA-G-060)
OTA-G-080	Input: Fahrzeugkonfiguration / Fahrzeugdaten Der ***Entwicklungsverantwortliche*** analysiert die übermittelte Fahrzeugkonfiguration / die extrahierten Fahrzeugdaten und unterstützt so ggf. den *Entwickler* mit den Ergebnissen der Analyse der übermittelten System- / Diagnosedaten zum Fahrzeugzustand. Output: Diagnoseergebnisse[2]
OTA-G-090 vgl. WRK-G-060	Input: Lastenheft, Diagnoseergebnisse Der ***Entwickler*** entwickelt das neue Software-Update. Output: Software-Update
OTA-G-100 vgl. WRK-G-070	Der ***Entwickler*** übermittelt das Software-Update an den Update-Server des OEM und informiert den *Entwicklungsverantwortlichen* über den neuen Softwarestand. Output: dem OEM verfügbares Software-Update; Mitteilung über Verfügbarkeit des Updates

[2] Die Diagnoseergebnisse können verschieden ausgeprägt sein. Basis sind Marktdaten betroffener Fahrzeuge, möglich sind auch die Fahrzeugkonfigurationen unter denen die Fehler auftreten, bis hin zu Benutzeraktivitäten bei denen die Fehler aufgetreten sind.

OTA-G-110 vgl. WRK-G-080	Der ***Entwicklungsverantwortliche*** überprüft die Qualität des neuen Softwarestandes. Bei ernster Gefährdung[3] wird die gewählte Lösung dokumentiert und an die *Regulatorische Behörde* zur weiteren Prüfung weitergeleitet (→ OTA-G-120). Output: Ergebnis der Qualitätsprüfung; ggf. Dokumentation zur technischen Lösung (nur bei ernster Gefährdung) **Konditionen: (A)** das Software-Update entspricht den Anforderungen des Lastenheftes und besteht die Prüfung durch die *Regulatorische Behörde* (→ OTA-G-130). **(B)** es entspricht den Anforderungen des Lastenheftes, aber besteht die Prüfung durch die *Regulatorische Behörde* nicht. Der *Entwicklungsverantwortliche* muss das Lastenheft überarbeiten (→ OTA-G-050). **(C)** es entspricht nicht den Anforderungen des Lastenheftes. Der *Entwicklungsverantwortliche* fordert den *Entwickler* zur Nachbesserung auf (→ OTA-G-090).
OTA-G-120 vgl. WRK-G-090 (nur bei Regul. Behörde)	Nur bei ernster Gefährdung: Die ***Regulatorische Behörde*** prüft die vorgestellte Lösung auf Konformität. Output: Prüfbescheid
OTA-G-130 vgl. WRK-G-100	Der ***Entwicklungsverantwortliche*** gibt das Update intern aus technischer Sicht für den weiteren Prozess frei. Output: freigegebenes Update
OTA-G-140 vgl. WRK-G-110	Der ***Update-Koordinator*** zeichnet das Software-Update für die Umsetzung des Rückrufs an den Kundenfahrzeugen frei. Output: freigezeichnetes Update

[3] Gemäß der geltenden Auffassung der jeweiligen regulatorischen Behörde

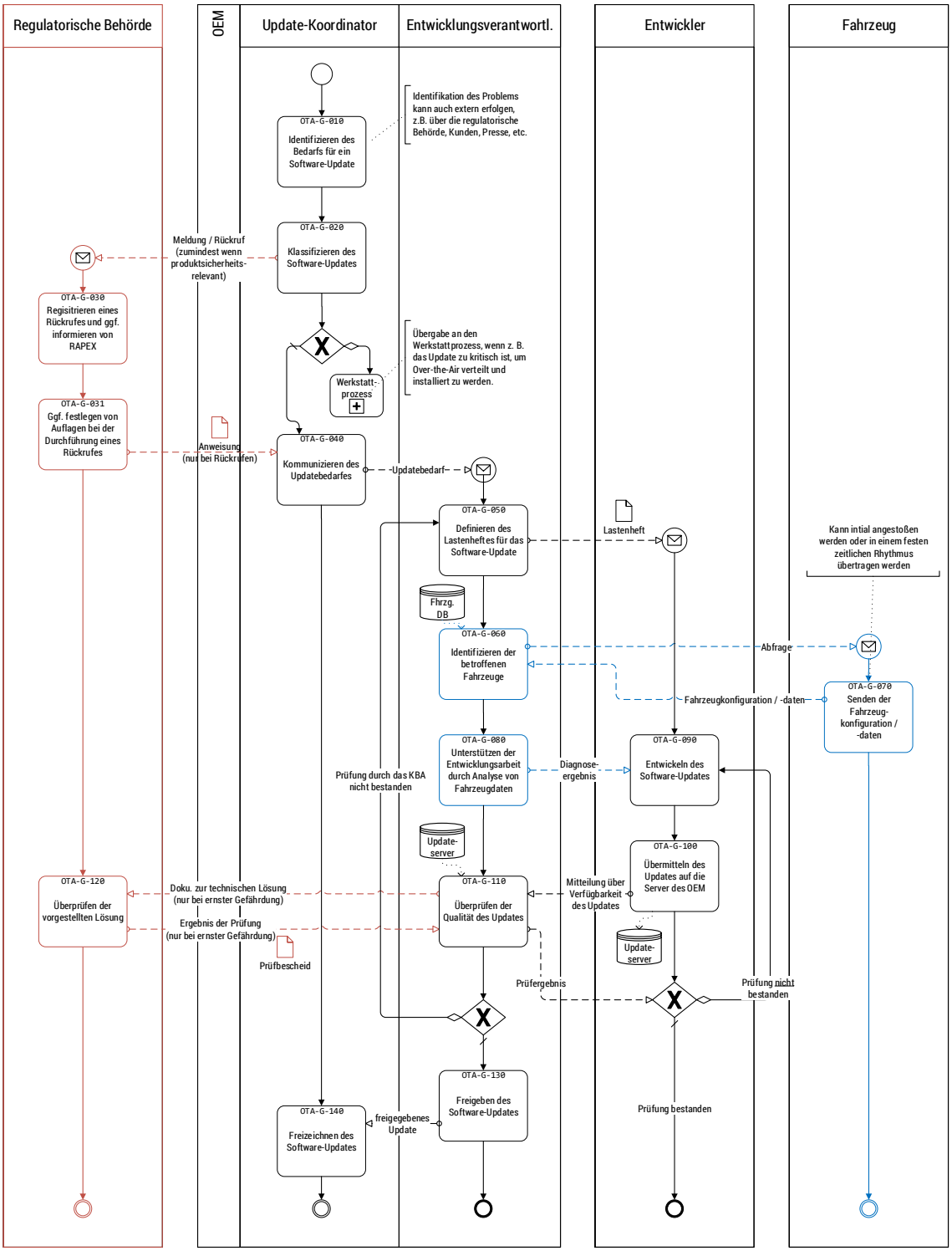


Abbildung 7: OTA-Prozess "Generierung"

ID	Typ	Prozess-ID	Beschreibung
E001		OTA-G-020	Durch das Klassifizieren von OTA-Updates und einer damit einhergehenden Variation der Prozessdurchführung in Abhängigkeit der Klassifikation, kann der Update-Prozess effizienter gestaltet werden.
E002		OTA-G-020	Eine falsche Klassifizierung kann zu einer Verletzung einer Meldepflicht bei der *Regulatorischen Behörde* führen.
E003		OTA-G-020	Eine falsche Klassifizierung kann dazu führen, dass das Update nicht ausreichend getestet wurde und es in Folge dessen zu Fehlern im Feld kommt.
E004		OTA-G-060	Durch den Fernzugriff auf die Fahrzeuge können die betroffenen Fahrzeuge zuverlässiger identifiziert und ihr aktueller Softwarestand analysiert werden. So kann vermieden werden, dass ein Update-Vorgang initiiert wird, der auf Grund fehlender Kompatibilität fehlschlagen könnte.
E005		OTA-G-070	Die Rahmenbedingungen, unter denen Daten aus den Fahrzeug abgerufen werden dürfen, sind zu klären.
E006		OTA-G-070	Das Risiko eines unautorisierten Datenzugriffs auf Unternehmens- oder personenbezogene Daten bei der Datenübermittlung besteht.
E007		OTA-G-070	Die Datenschnittstelle und/oder andere Fahrzeugelektronik werden manipuliert oder missbraucht.
E008		OTA-G-080	Der Fernzugriff auf Daten zur Unterstützung der Fehlerdiagnose und damit der Fehlerbehebung kann zu einer verbesserten Fehler-Interpretation und Lösungsfindung führen.
E009		OTA-G-080	Analog OTA-G-070 / E005 sind die Rahmenbedingungen für den Datenaustausch der Kundendaten zwischen OEM und möglichem externen *Entwickler* zu klären.
E010		OTA-G-140	Das Update ändert die Fahrzeugfunktionalität über das zugelassene Maß hinaus, sodass die Zulassung erlöschen kann.

3.3.2 Verteilung

Prozess-ID	Beschreibung
OTA-V-010	Input: freigezeichnetes Update-Paket Der ***Update-Koordinator*** leitet das freigezeichnete Update an den *Digitalen Dienstleister* weiter. Output: freigezeichnetes Update-Paket

OTA-V-020	Der ***Digitale Dienstleister*** stellt das Update auf einer entsprechenden Server-Struktur / einem Content-Delivery-Network (CDN)[4] bereit.
OTA-V-030	Input: CRM-Tool, Halterdaten (über die *Regulatorische Behörde*) Der ***Update-Koordinator*** verknüpft die identifizierten Fahrzeuge mit den entsprechenden Haltern zur korrekten Adressierung. Einerseits kommen die Daten aus dem internen CRM-Tool, andererseits erfolgt ein Abgleich mit der *Regulatorischen Behörde*. Output: Halterabfrage / FIN-Liste identifizierter Fahrzeuge
OTA-V-040 (nur bei Regul. Behörde)	Die ***Regulatorische Behörde*** übermittelt bei Bedarf die Halterdaten zu den betroffenen Fahrzeugen. Output: Halterdaten
OTA-V-050	Der ***Digitale Dienstleister*** benachrichtigt die Fahrzeuge über das verfügbare Software-Update. Entweder erfolgt dies direkt über einen ‚Shoulder-Tap' oder indirekt, indem das *Fahrzeug* in definierten Zeitintervallen überprüft, ob Updates verfügbar sind. Output: Benachrichtigung
OTA-V-060	Das ***Fahrzeug*** gleicht (erneut) die Fahrzeugkonfiguration mit den Update-Anforderungen ab (verbaute Hardware, installierte Software, etc.), falls sich inzwischen durch einen Werkstattaufenthalt (z. B. nach einem Unfall) die Fahrzeugkonfiguration verändert hat. Output: Fahrzeugkonfiguration oder -daten
OTA-V-070	Der ***Digitale Dienstleister*** aktualisiert die Fahrzeug-Datenbank entsprechend der Rückmeldung des Fahrzeuges. Output: Nachricht über aktualisierte Fahrzeugdatenbank Anm.: Wenn die Fahrzeugkonfiguration nicht kompatibel ist, das heißt, nicht den Anforderungen des Updates entspricht, entfällt das *Fahrzeug* aus dem weiteren Updateprozess. Dieser Umstand sowie dessen Ursache dafür werden vom *Digitalen Dienstleiser* dokumentiert und im Rahmen eines Update-Reports an den Auftraggeber übermittelt.

[4] Für die Verteilung des Updates an die Fahrzeuge wird eine neue Serverstruktur benötigt, die eine deutlich höhere Anzahl von Zugriffen bedienen müssen als bei der Verteilung des Updates an die Werkstätten. Gegebenenfalls ist ein Content-Delivery-Network aufzusetzen oder über einen Drittanbieter einzubinden.

OTA-V-080	Input: aktualisierte Datenbank mit Fahrzeugen korrekter Konfiguration Der ***Update-Koordinator*** schaltet das Update final frei, sodass das Ausrollen angestoßen wird. Außerdem beginnt der ***Update-Koordinator*** die *Halter* über das Update zu informieren. Output: Information an den *Fahrzeug-Halter*, Signal über die Verfügbarkeit an das *Fahrzeug* Anm.: **A)** Die Informationen über das Update kann auf verschiedenen Wegen stattfinden: per Postwurfsendung, per E-Mail, OnScreen im Fahrzeug, Smartphone-Applikation, etc. Die Updateinhalte sollten dem Kunden eindeutig und in verständlicher Sprache geschildert werden, um ihm über die Veränderungen am Fahrzeug und über die Zeit zu informieren, die das Fahrzeug dem Kunden nicht zur Verfügung steht. **B)** Bei der Information für den Kunden über ein Rückruf-Update ist eindeutig hervorzuheben, dass es sich um eine solche Rückrufmaßnahme handelt, die bis zu einem gewissen Zeitpunkt durchgeführt werden muss. Das Update darf durch den Kunden nur solange zurückgehalten werden, anschließend müsste das Fahrzeug in der Werkstatt vorgeführt werden oder das Fahrzeug verliert ggf. seine Zulassung.
OTA-V-090	Das ***Fahrzeug*** zeigt das verfügbare Update im Fahrzeug selbst an und fragt vom *Halter* die Genehmigung für das Update an. Output: Informationsscreen mit Möglichkeit zur Bestätigung / Verzögerung / Ablehnung des Updates[5]
OTA-V-100	Der ***Halter*** überprüft die ihm zur Verfügung gestellten Informationen und entscheidet, ob das Update zur Installation genehmigt wird. Output: Ergebnis des Genehmigungsprozesses **Entweder** er genehmigt das Update (→ OTA-V-110) **oder** er genehmigt das Update nicht. Im negativen Falle kann das Update bis zu x-mal wiederholt angezeigt werden. Sollte das Update auch weiterhin nicht genehmigt werden, wird der Updateprozess Over-The-Air abgebrochen und (bei Bedarf) im konventionellen Werkstattprozess weiter nachverfolgt (→ WRK-V-010). Anm.: Eine Implementation der Genehmigung des Updates aus der Ferne ist zu empfehlen. Z. B. kann anhand einer Analyse des Fahrprofils dem Eigentümer ein geeigneter Zeitpunkt vorgeschlagen werden, zu dem das Fahrzeug nicht benutzt wird und ein Update ohne Einschränkung durchgeführt werden kann.

[5] Dem Kunden sollten bei einem Update die Möglichkeiten angeboten werden, das Update durchzuführen, später erneut daran erinnert zu werden oder das Update abzulehnen.

OTA-V-110	Das ***Fahrzeug*** verwaltet den Genehmigungsprozess und leitet die Entscheidung über die Installation des Updates weiter. Output: Ergebnis des Genehmigungsprozesses **Konditionen: (A)** bei erteilter Genehmigung wird der *Update-Koordinator* entsprechend benachrichtigt. **(B)** bei nicht erfolgter Genehmigung kann das Update erneut angezeigt werden. Wird das Update endgültig abgelehnt, ist auch dies dem *Update-Koordinator* mitzuteilen.
OTA-V-120	Der ***Update-Koordinator*** verfolgt den Genehmigungsprozess des *Halters* nach. Output: ggf. Freischaltung des Fahrzeuges für Update (bei Genehmigung) Anm.: Dies kann eine automatisierte Aktivität sein. Die Überwachung bzw. die Verantwortung, dass alle Anforderungen erfüllt werden – z. B. der *Regulatorischen Behörde* – liegt beim *Update-Koordinator*. **Konditionen: (A)** bei erteilter Genehmigung wird der *Digitale Dienstleister* entsprechend benachrichtigt. **(B)** bei nicht erfolgter Genehmigung wird **entweder** der OTA-Prozess beendet – bei einem Update ohne Produktsicherheits-Relevanz) **oder** beendet und an den Werkstattprozess übergeben – bei einem Update mit Produktsicherheits-Relevanz (→WRK-V-010).
OTA-V-130	Der ***Digitale Dienstleister*** initiiert den Start des Downloads (z.B. durch Versenden einer Download-Referenz). Output: Download-Referenz Anm.: A) diese Aktivität kann auch schon direkt nach Freischaltung des Updates passieren, d.h. vor der eigentlichen Autorisierung des Updates durch den Halter. Zur Steigerung der Kundenzufriedenheit kann das Update bereits geladen werden, während die Bestätigung noch aussteht. Eine Installation kann somit verzögerungsfrei direkt nach der Bestätigung erfolgen. Dies ist jedoch mit höheren Kosten verbunden, z.B. bei einer dann nicht folgenden Autorisierung des Updates. B) Ein Update kann auch in mehreren ‚Wellen' an die Fahrzeuge verteilt werden, um die Zugriffe auf die Serverstruktur zeitlich zu verteilen.
OTA-V-140	Das ***Fahrzeug*** lädt das Update-Paket herunter. Output: lokal im *Fahrzeug* gespeichertes Update

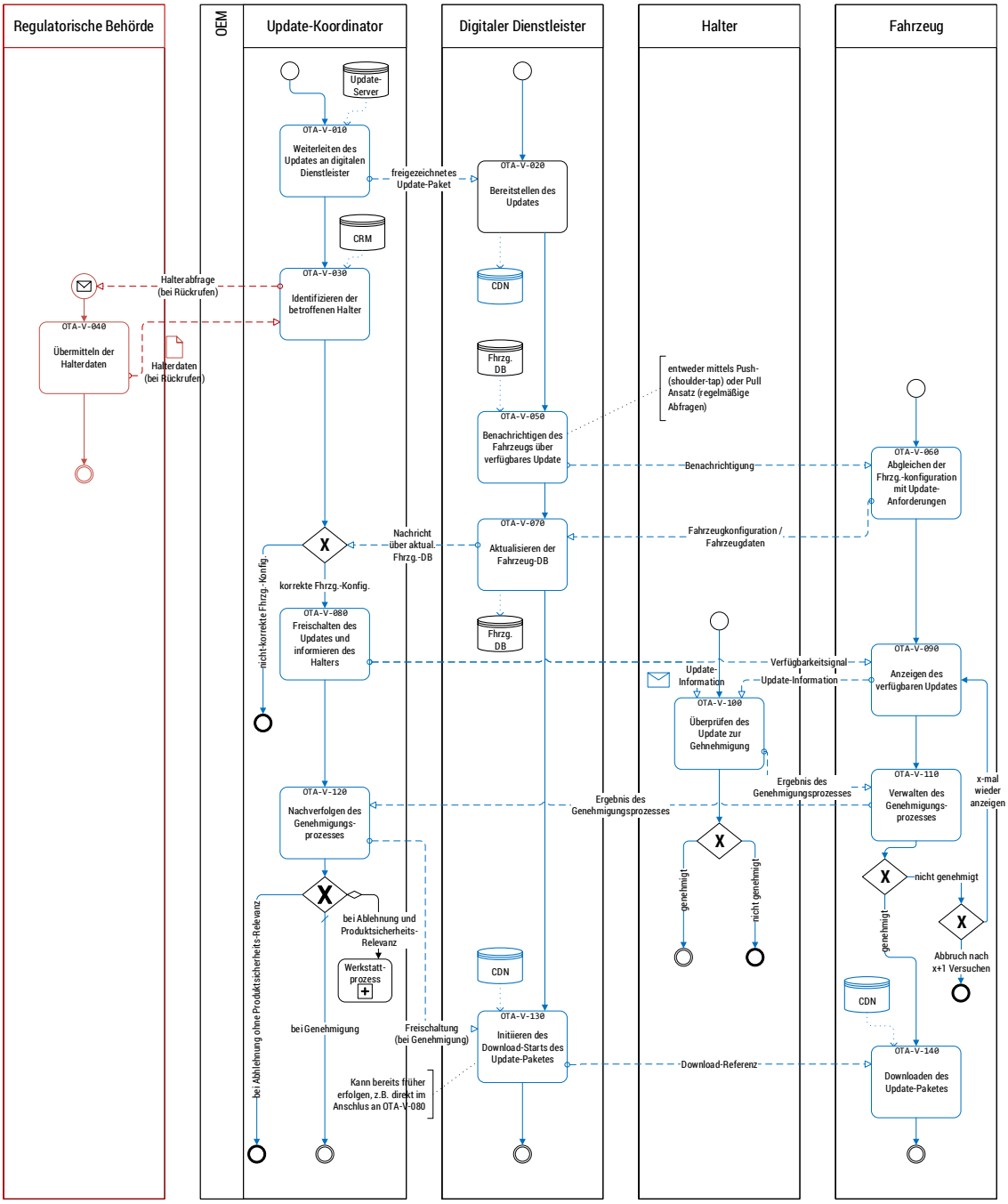


Abbildung 8: OTA-Prozess "Verteilung"

Event-ID	Event-Typ	Prozess-ID	Beschreibung
E011		OTA-V-010	Durch den Einsatz eines digitalen Dienstleisters als Intermediär ist das Update als technisches Know-How des Auftraggebers einem Sicherheitsrisiko auf fremder Infrastruktur ausgesetzt.
E012		OTA-V-020	Nicht ausreichende Sicherheiten beim digitalen Dienstleister führen zu einem entsprechenden Sicherheitsrisiko: Update-Daten können mitgelesen werden, manipuliertes Update kann aufgespielt werden, Malware kann installiert werden.
E013		OTA-V-050	Die Benachrichtigung kann so manipuliert werden, dass das Fahrzeug angewiesen wird, ein Roll-Back auf eine vorherige, möglicherweise fehlerhafte Version durchzuführen.
E014		OTA-V-060	Die Rahmenbedingungen, unter denen Daten aus den Fahrzeug abgerufen werden dürfen, sind zu klären.
E015		OTA-V-060	Die Datenschnittstelle und / oder andere Fahrzeugelektronik werden über die Datenschnittstelle manipuliert oder missbraucht.
E016		OTA-V-070	Die häufige Kommunikation mit den Fahrzeugen stellt eine stets aktuelle Datenbasis sicher.
E017		OTA-V-080	Die Möglichkeit der einfacheren und schnellen Veränderung von Software ermöglicht neue Geschäftsmodelle (z.B. Function on Demand).
E018		OTA-V-080	Durch die Durchführung des Software-Updates ohne die Partizipation einer Werkstatt sind Kostenersparnisse möglich.
E019		OTA-V-080	Bei sicherheitskritischen Updates kann eine getrennte Verteilung der Updates, die das Verhalten, das Interface oder andere sonstige kunden-wahrnehmbare Features verändern, hilfreich sein, um eine schnelle Bestätigung des Updates zu erhalten.
E020		OTA-V-080	Teilweise existieren gesetzliche Regelungen bzgl. der Verantwortung zur Wartung von Fahrzeugen für den Verkäufer und somit liegt diese Verantwortung eventuell bei der Werkstatt des Händlers anstelle beim OEM.
E021		OTA-V-080	Eine unzureichende Information des Fahrzeugeigentümers über das Software-Update könnte einen unerlaubten Eingriff in die Eigentumsrechte des Eigentümers darstellen.
E022		OTA-V-080	Ggf. ist ein Verbindungsaufbau zum Fahrzeug nicht möglich (technischer Defekt, Privacy Modus des Halters, o.ä.).
E023		OTA-V-080	Die Kommunikation des Updates zum aktuellen Halter des Fahrzeuges sind unter besonderer Berücksichtigung von Privacy-Anforderungen durchzuführen. Bei nachträglichen Funktionsfreischaltungen könnten z.B. Zahlungsdaten kompromittiert werden.
E024		OTA-V-090	Fehlerhafte Informationen über das Update (z.B. Dauer der Installation) führen zu einem negativen Erlebnis der Kunden.
E025		OTA-V-090	Die Updatefunktion kann blockiert werden, z.B. durch Denial-of-Service Attacken (Überlasten des Datennetzes oder Überlasten der

			Empfangseinheit), sodass das Fahrzeug in einem unsicheren Zustand verbleibt.
E026		OTA-V-100	OTA-Updates reduzieren den Aufwand für den Fahrzeugkunden bei Software-Updates enorm.
E027		OTA-V-100	Unautorisierte Personen genehmigen ein Update, sodass vom Eigentümer ungewollte Software / Updates im Fahrzeug installiert werden.
E028		OTA-V-100	Bei einer Ablehnung des Updates durch den Halter kann das Fahrzeug weiter in einem vielleicht sicherheitskritischen Zustand verbleiben.
E029		OTA-V-100	Bei einer Installation ohne vorliegende Einverständniserklärung kann ein unerlaubter Eingriff in die Eigentumsrechte des Eigentümers vorliegen.
E030		OTA-V-130	Durch hohen verfügbare Kapazitäten können mehr Fahrzeuge gleichzeitig adressiert und aktualisiert werden, als über die existierenden Werkstatt- und Vertriebsnetzwerke.
E031		OTA-V-140	Das Fahrzeug kann den Download nicht initiieren und das Update kann nicht geladen werden, z.B. aufgrund einer Überlastung der Serverstruktur.
E032		OTA-V-140	Das Update wird unvollständig oder fehlerhaft übertragen.
E033		OTA-V-140	Die Datenschnittstelle und/oder andere Fahrzeugelektronik werden manipuliert oder missbraucht.

3.3.3 Installation

Prozess-ID	Beschreibung
OTA-I-010	Input: lokal im Fahrzeug gespeichertes Update Das ***Fahrzeug*** führt eine Routine durch, um den benötigten Fahrzeugzustand abzusichern (z.B. Batteriestatus, Zündung, Fensterposition, Gang, Parkposition, etc.). Wird ein Kriterium nicht erfüllt, wird dies dem Fahrzeugführer kommuniziert und nach Bestätigung erneut geprüft. **Entweder** der benötigte Fahrzeugzustand kann erfolgreich hergestellt werden (→ OTA-I-020) **oder** die Routine ist nicht erfolgreich. Bei negativen Ausgang wird eine Fehlermeldung an das Backend gesandt (→ OTA-I-060).
OTA-I-020	Das ***Fahrzeug*** überprüft, ob es die Anforderungen an das Update erfüllt (Speicherplatz, Batterie-Ladestand, etc.), und es überprüft die Authentizität des Updates. **Entweder** werden die Anforderungen erfüllt (→ OTA-I-030) **oder** die Überprüfung schlägt fehl. Bei negativen Ausgang wird eine Fehlermeldung an das Backend gesendet (→ OTA-I-060).
OTA-I-030	Das ***Fahrzeug*** entschlüsselt, entpackt und installiert selbstständig das Update.

OTA-I-040	Das ***Fahrzeug*** prüft / testet, ob die Installation erfolgreich war. Entsprechende Testmechanismen sind zu implementieren, die die Installationsroutine und ggf. anschließend die veränderte Funktionalität überprüfen. **Entweder** die Installation war erfolgreich **oder** die Installation schlug fehl. Bei einem Fehler kann zunächst versucht werden, die Installationsroutine zu wiederholen (→ OTA-I-010). Schlägt die Installation mehrfach fehl, wird eine Fehlermeldung erstellt (→ OTA-I-060). Anm.: Bei einer fehlerhaften Installation sollte das Fahrzeug selbstständig versuchen die Installation zu wiederholen, bis sie erfolgreich durchgeführt wurde (Anzahl der Versuche ist zu definieren). Schlägt die Installation weiterhin fehl, ist das Fahrzeug in einen funktionierenden Betriebszustand zurückzuführen (Fall-Back-Ebene). Anschließend ist die Aktualisierung der Software im Werkstattprozess weiterzuverfolgen.
OTA-I-050	Das ***Fahrzeug*** sendet eine Bestätigung über die erfolgreiche Installation an die Fahrzeug-Datenbank / das Backend. Output: Bestätigung (z. B. aktualisierter Datenbankeintrag)
OTA-I-060	Das ***Fahrzeug*** sendet eine Fehlermeldung über das fehlgeschlagene Update an die Fahrzeug-Datenbank / das Backend. Output: Fehlermeldung (z. B. aktualisierter Datenbankeintrag)
OTA-I-070	Das ***Fahrzeug*** versucht einen sicheren Zustand wiederherzustellen und kommuniziert dies und das Ergebnis des Versuchs an den *Fahrer* / *Halter*. Output: Rückmeldung an den *Digitalen Dienstleister* und den *Fahrer* / *Halter* Anm.: Ziel ist es, die Einschränkungen für den Kunden so gering zu möglich zu halten und möglichst alle Funktionalitäten wieder bereitzustellen. Zu überlegen ist, ob bei sicherheitsrelevanten Fehlern, deren Behebung fehlgeschlagen ist, die entsprechende Funktion zu deaktivieren. Minimalziel ist es, das Fahrzeug in einen fahrbereiten Zustand zu versetzen.
OTA-I-080	Der ***Digitale Dienstleister*** beobachtet den Fortschritt des Updateprozesses. Hierzu zählen die Überwachung des prozessualen Ablaufs in der gesamten Verteilung als auch die Überwachung der Installationsroutine und der Umgang / die Eskalation mit möglichen Fehlermeldungen einzelner Fahrzeuge. Hier wird primär versucht, das Update erneut auszurollen. Bei mehrfachem Abbruch ist dies dem Update-Koordinator zu kommunizieren. Output: Status des gesamten Prozesses / einfacher Fehler

OTA-I-090	Der ***Update-Koordinator*** überwacht den Update-Prozess und koordiniert die Eskalation möglicher Fehler im Ablauf. Output: Statusbericht (nur bei Rückrufen) **Konditionen: (A)** ggf. ist das Update im Werkstattprozess weiterzuverfolgen (→ WRK-V-010). **(B)** ggf. weist das Update einen systematischen Fehler auf. In diesem Fall muss die Verteilung gestoppt und ein aktualisiertes Update generiert werden (→ OTA-G-050). **(C)** Bei einem laufenden Rückruf leitet der *Update-Koordinator* in vereinbarten Zeitintervallen einen Statusbericht an die *Regulierende Behörde* weiter.
OTA-I-100 (nur bei Regul. Behörde)	Die ***Regulatorische Behörde*** aktualisiert die Rückruf-Datenbank und schließt gegebenenfalls den Rückruf entsprechend ihrer jeweiligen Vorgehensweise ab.

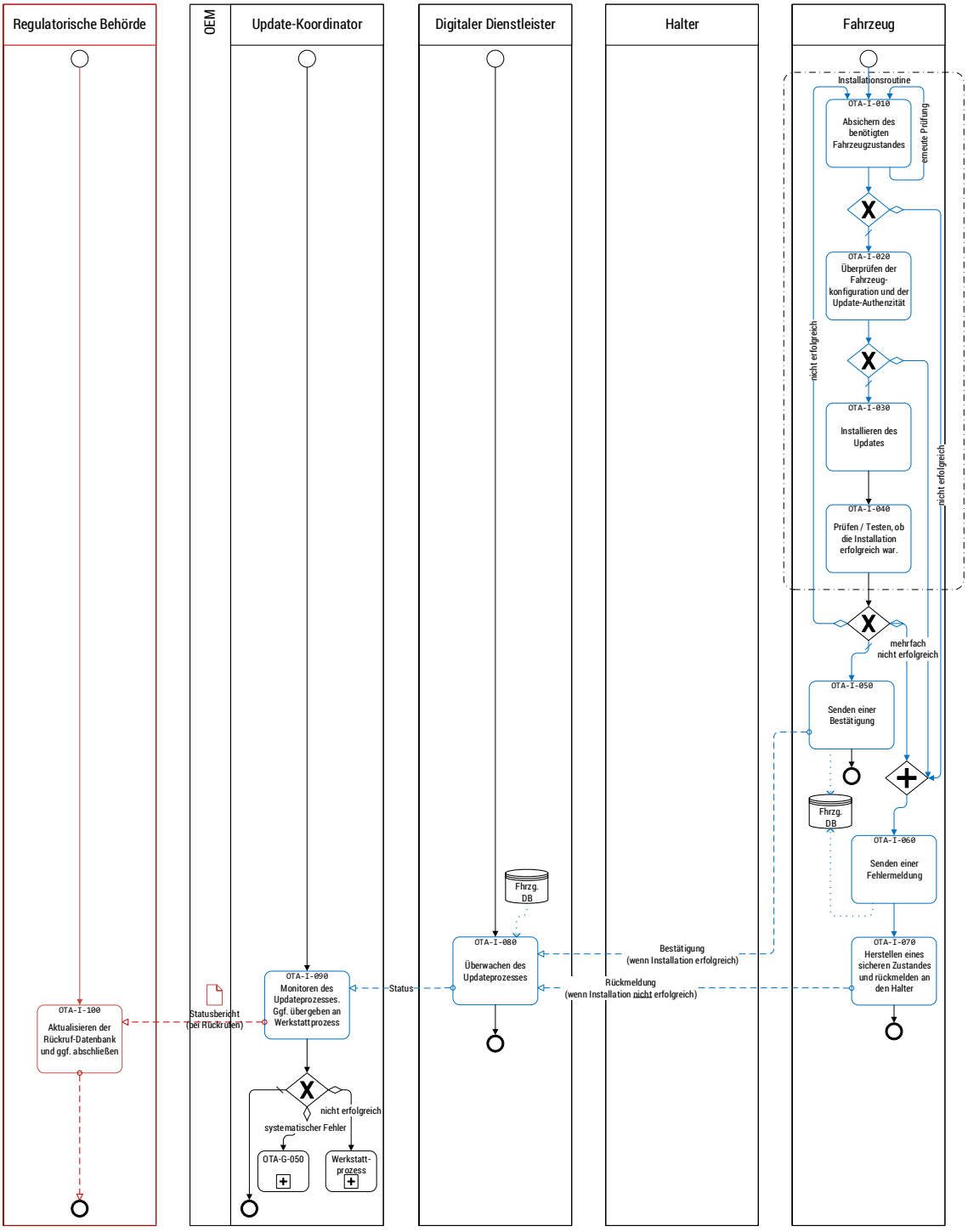


Abbildung 9: OTA-Prozess "Installation"

Event-ID	Event-Typ	Prozess-ID	Beschreibung
E034		OTA-I-020	Ein Software-Update wird aufgespielt, das nicht mit dem Fahrzeug kompatibel ist, sodass es zu Funktionalitätsverlusten kommt.
E035		OTA-I-020	Das Update kann aufgrund fehlender Betriebsressourcen nicht aufgespielt werden oder es bricht während der Installation ab, sodass das Fahrzeug in einem nicht gewünschten Zustand verbleibt.
E036		OTA-I-020	Es wird unautorisierte, manipulierte oder gefälschte Software zur Installation freigegeben.
E037		OTA-I-030	Die Installation findet selbstständig ohne notwendiges Personal und ohne entsprechende Kosten statt.
E038		OTA-I-030	Die Installation bricht ab (z.B. durch eine Veränderung des Fahrzeugzustandes) und das Fahrzeug verbleibt in einem ungewünschten Systemzustand.
E039		OTA-I-030	Nach der Entschlüsselung des Updates auf dem Gateway, kann das Update und damit Know-How – z.B. auf dem CAN-BUS mitgelesen werden.
E040		OTA-I-040	Nach der Installation oder einem Abbruch der Installation wird ein Fehler festgestellt, sodass das Fahrzeug nicht mehr fahrbereit ist. Eine Rückführung in einen fahrbereiten Zustand ist vorzunehmen.
E041		OTA-I-050	Die Veränderung am Fahrzeug wird nicht dokumentiert, sodass es bei der Benutzung oder bei dem Weiterverkauf des Fahrzeuges zu einem negativen Kundenerlebnis kommt.
E042		OTA-I-050	Das erfolgreich durchgeführte Update wird abgestritten (z.B. kann dies bei Zusatz-Features zu einem Ausfall von Zahlungen führen.)
E043		OTA-I-050	Durch eine nicht erfolgte Rückmeldung über den Erfolg des Updates kann ein Verkauf einer Dienstleistung oder ein Rückruf nicht abgeschlossen werden.
E044		OTA-I-080	(Systematische) Fehler können erst bei den Kunden im Feld auftreten, ohne dass eine direkte Betreuung durch einen Werkstattmitarbeiter möglich wäre. Hier kann es zu hohen Einschränkungen durch den Kunden kommen.

4 KLASSIFIZIERUNG

Im Weiteren wird die Möglichkeit einer Klassifizierung von OTA-Updates diskutiert und drei verschiedene Klassifizierungsarten von OTA-Updates vorgestellt. Generell ermöglicht eine Klassifizierung, die Prozesskette entsprechend den Anforderungen der verschiedenen Update-Klassen an die Aktivitäten abzustufen und zu variieren. Hierdurch entstehen den Firmen bei der Durchführung der Prozesse Freiheitsgrade, durch die die internen Abläufe beschleunigt werden können, da die Klassifizierung eine Priorisierung und Anpassung des Arbeitsaufwandes ermöglicht. Die Anforderungen an die verschiedenen Update-Klassen kann auch einer Qualifizierung von Anbietern dienen, indem deren Angebot mit dem Anforderungskatalog abgeglichen wird, sodass für die Anbieter festgelegt werden kann, welche Update-Klasse sie durchführen können.

4.1 Klassifizierung nach dem Update-Ziel

In Abhängigkeit des Zwecks eines Updates kann sich der regulatorische Aufwand, sowie der Informationsaufwand gegenüber den Kunden verändern. Unterschieden werden kann zwischen Updates der Softwarepflege, der Security- oder Privacy-Eigenschaften, zur Fehlerbehebung und zur Funktionsänderung (Veränderung einer existierenden Funktion, Hinzufügen einer neuen Funktion).

Wird eine **Softwarepflege** am Fahrzeug durchgeführt, zum Beispiel als präventive Sicherheitsmaßnahme (Austausch von Verschlüsselungs-Keys), zur Steigerung der Performance oder zum Optimieren des Programmcodes, werden Eigenschaften des Fahrzeuges perfektioniert, aber im Sinne der Gesetzgebung oder aus Sicht des Kunden nicht verändert. Eine Anzeige gegenüber der regulierenden Behörde wäre nicht notwendig, genauso wenig wie eine detaillierte Information des Kunden.

Ein zweites Ziel von Updates kann das Schließen einer entdeckten **Security**- oder **Privacy-Lücke** sein. Auch wenn aus Sicht der Kunden, wie bei der Software-Pflege, keine Eigenschaft des Fahrzeuges weitreichend verändert wurde, stellt ein solches Update weitreichendere Anforderungen: Die Dringlichkeit eine solche Lücke zu schließen kann höher sein. Sie könnte

auch vom Gesetzgeber eingefordert werden, sollte eine Gefahr für die Umwelt aus einer solchen Lücke resultieren, z.B. durch Hacker-Angriffe. Über Sicherheitslücken können auch die persönlichen Daten der Fahrzeugnutzer (zurückgelegte Routen, Fahrprofil, Bezahldaten, etc.) zu deren Nachteil nicht ausreichend vor unerlaubten Zugriffen geschützt sein. Entsprechende Maßnahmen sind zu berücksichtigen.

Eine korrektive oder präventive Maßnahme zur **Fehlerbehebung** kann im Sinne der aktuellen Gesetzgebung als Rückruf der regulierenden Behörde ausgelegt werden, da es sich um eine Behebung eines systematischen Mangels an einem Serienfahrzeug handeln kann. Jeder Rückruf ist meldepflichtig bei der regulatorischen Behörde (z.B. in Deutschland beim KBA). Der Hersteller ist verpflichtet, den Fahrzeug-Halter im Falle eines Rückrufes mindestens einmal per Post anzuschreiben und über den Rückruf zu informieren. Außerdem erweitert sich der Prozess um die Schnittstelle zu der regulierenden Behörde, die über den Umfang und Inhalt der Fehlerbehebung informiert werden muss. Gegebenenfalls wird auch eine Frist zur vollständigen Durchführung der Maßnahme durch die regulatorische Behörde festgesetzt. Entsprechend muss der Kunde über den Rückruf und mögliche Konsequenzen bei ausbleibender Autorisierung des Updates informiert werden.

Kommt es zu **Funktionsänderungen, -erweiterungen oder -ergänzungen** durch ein Software-Update, müssen vor allem drei Faktoren berücksichtigt werden: A) Verändert ein solches Update das Eigentum tiefgreifender als die Updates zuvor? Mitunter muss die Kommunikation mit den Kunden entsprechend angepasst werden und eine Autorisierung muss vom Halter des Fahrzeuges eingeholt werden. Zudem muss nachhaltig die Veränderung am Fahrzeug dokumentiert werden, da Funktionen eventuell so verändert werden, dass die Bedienung nicht mehr der ausgewiesenen Handhabung in der Dokumentation entspricht. B) Eine solche Veränderung könnte typgenehmigungsrelevant sein, was entsprechend abgesichert werden muss. C) Weitreichende Funktionsänderungen haben meist verschiedenste Schnittstellen, die betrachtet werden müssen. Für solche Updates bedarf es erweiterter Funktionstests in der Entwicklungsphase. Solche Änderungen an Funktionen sind entweder additiv und fügen neue Funktionen hinzu oder adaptiv, wenn die Funktion – z. B. – an neue Rahmenbedingungen der Technik oder der Umwelt angepasst werden.

4.2 Klassifizierung nach Funktionsbereichen im Fahrzeug

Die Unterscheidung zwischen Updates verschiedener Funktionsbereiche adressiert die verschiedenen Techniken an Bord eines Fahrzeuges. Ursachen für mögliche Funktionsbeeinträchtigungen dieser können dabei mechanisch oder softwareseitig sein. Unterschieden werden kann zwischen Infotainment-, Karosserie- / Komfort- oder Fahrfunktionen. Eine Klassifizierung zwischen diesen Funktionen zielt darauf ab – v. a. unter

Berücksichtigung der möglichen Gefährdung für Insassen und Umwelt als Konsequenz eines Fehlers der Funktion – für die verschiedenen Funktionstypen das richtige Maß der Absicherung festzulegen. Neben der richtigen Qualitätsabsicherung für die jeweilige Funktion (wie könnte ein fehlerhaftes Update zu einer Gefährdung führen?) ist der OTA-Update-Prozess auch hinsichtlich der (Reaktions-)Zeit (wie schnell muss eine mögliche Gefährdung im Feld berichtigt werden?) und hinsichtlich – eines möglicherweise nicht notwendigen – Mehraufwandes für die unterschiedlichen Funktionen zu optimieren (z. B. wie kann der Testaufwand für Infotainment-Updates reduziert werden?).

Die Unterscheidung ermöglicht es, verschiedene Anforderungen an den Prozess in Abhängigkeit der Systeme im Fahrzeug zu stellen (verschiedene Sicherheitszonen mit verschiedenen Anforderungen bzgl. Security Maßnahmen, etc.) sowie organisatorische Anforderungen z.B. bzgl. des Zeitmanagements, der durchzuführenden Testverfahren (auch nach der Installation im Fahrzeug) oder der Einbindung der regulierenden Behörde zu definieren. Nachfolgend werden die drei verschiedenen Stufen beschrieben:

Updates des **Infotainment**-Systems sind hauptsächlich Programm- bzw. Applikations-Updates ohne Verbindung zu mechanischen Komponenten. Ein Manipulieren einer solchen Funktion, die beispielsweise über den MOST-BUS kommuniziert, wirkt sich während der Fahrt störend auf den Fahrer aus, z.B. durch nicht mehr funktionierende Infotainment-Anwendungen, fehlerhafte Lautstärkesteuerung, etc., oder kann auf die Kompromittierung von Nutzerdaten (Zahlungsinformationen, Fahrprofile, etc.) abzielen. Eine physische Gefährdung für die Insassen oder die Umwelt besteht zumeist nicht.

Karosserie- / Komfortfunktionen sind solche Funktion, die z. B. zu dem Body-Netzwerk (Türen, Fenster, Klima, etc.) eines Fahrzeugs gehören. Sie kommunizieren über den Low-Speed-CAN oder LIN-BUS miteinander. Zu diesen Funktionen zählen zum Beispiel die Scheibenwischanlage, die elektronischen Fensterheber oder die Ansteuerung von Scheinwerfern. Nicht gewünschte Funktionszustände können den Fahrer stark von der Fahrzeugführung ablenken. Die Möglichkeit, das Fahrzeug sicher abzustellen, ist gegeben, eine Gefährdung durch Ablenkung durch die Funktionsstörung ist nicht auszuschließen.

Sind **Fahrfunktionen** oder Funktionen der dynamischen Fahrzeugkontrolle betroffen, adressieren Updates Funktionen von denen eine hohe Gefährdung für die Fahrzeuginsassen und die Fahrzeugumwelt ausgehen kann. Hierzu zählen Steering-by-Wire Systeme, Fahrfunktionen, die auf das Gas- oder Bremspedal zugreifen, regelnde Fahrerassistenzsysteme usw. Ein resultierender Fehler könnte ein nicht mehr zu kontrollierende Fahrsituation hervorrufen oder einem Dritten ermöglichen, durch einen Sicherheitsfehler auf solch eine Funktion zuzugreifen und entsprechend zu manipulieren. Beide Szenarien haben ein hohes Gefährdungspotential. (Ein Ergebnis dieser Einstufung in diese Kategorie könnte auch sein, dass das Update nicht Over-The-Air durchgeführt werden kann, weil es zu hohe Anforderungen an das Testen und Verifizieren der Installation stellt, für die mitunter weiterhin ein Service-Mitarbeiter einer Werkstatt benötigt wird.)

Abbildung 10 zeigt beispielhaft welche Auswirkung eine Klassifizierung nach den Funktionsbereichen im Fahrzeug auf die Prozesskette haben kann. Für die Prozesskette sind beispielhaft Anforderungen in den roten Kästen dargestellt. Die in fetter Schriftart hervorgehoben Anforderungen sind entsprechend den drei Klassen (in blau dargestellt) in der Matrix variiert worden. Eine solche Variation kann ebenfalls für die weiteren Anforderungen als auch die weiteren Klassifikationsarten vorgenommen werden.

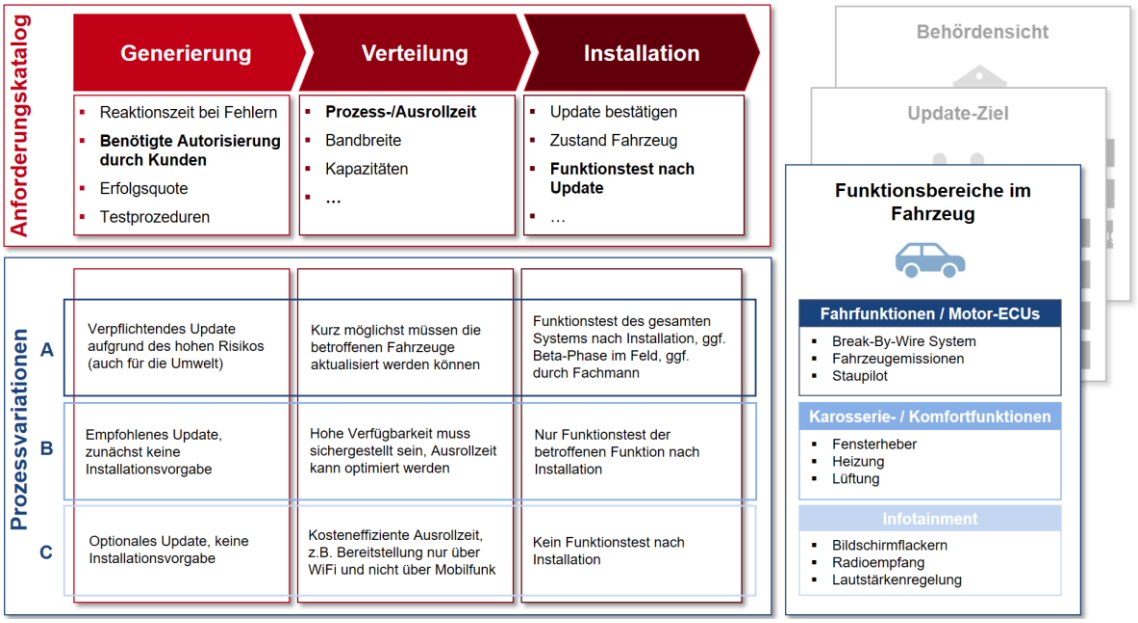


Abbildung 10: Beispielhafte Prozessvariation in Abhängigkeit des Funktionsbereichs

4.3 Klassifizierung nach der Behördensicht

Die dritte Klassifizierung unterscheidet darin, welcher Mehraufwand durch regulatorische Ansprüche an das Update entsteht, z.B. wenn die Typgenehmigung[6] betroffen ist. Für OTA-Updates ergeben sich drei verschiedene Fälle:

1. OTA-Updates **ohne Typgenehmigungsrelevanz** (z. B. Infotainment- und Komfort-Funktionen)
2. OTA-Updates **mit Typgenehmigungsrelevanz** (z. B. X-by-Wire-Aktualisierungen, Sicherheitsupdates)

[6] Die Typgenehmigung ist eine Erlaubnis zur Herstellung eines Fahrzeuges in Übereinstimmung mit den für die Herstellung einschlägigen technischen Anforderungen (Certificate of Conformity). Sie wird durch die regulatorische Behörde erteilt.

3. OTA-Updates **mit Typgenehmigungs- und Zulassungsrelevanz** (z. B. Leistungssteigerung)

4.4 Klassifizierung nach der Kritikalität

Eine vierte Variante einer Klassifizierung wäre eine Kombination der drei vorhergehenden. Kombiniert man diese miteinander könnte ein Schema entwickelt werden, welches, zum Beispiel, die Updates in drei Kategorien der Kritikalität einstuft (niedrig, mittel, hoch). So wäre möglicherweise eine Softwarepflege eines Fahrfunktion-relevanten Systems ohne Beeinträchtigung der Typgenehmigung ein Update niedriger Kritikalität. Ein Privacy / Security-Fehler im Infotainment durch den die Bezahldaten der Kundendaten durch eine App kompromittiert werden könnte, könnte durch ein Update mittlerer Kritikalität behoben werden. Wird durch eine Funktionsänderung an einem Motor-Steuergerät die Leistung des Fahrzeugs gesteigert, kann dies ein Update hoher Kritikalität sein, welches entsprechend nach der Installation auf Funktionalität geprüft werden muss und das eine Relevanz für die Typgenehmigung und die Zulassung haben könnte.

Dieses Schema einer Klassifizierung zu entwickeln und zu verproben, ist Bestandteil des Folgeprojektes OTA II.

4.5 Zusammenfassung Klassifizierung

Die Qualitätssicherung kann nach den hier vorgeschlagenen Klassifizierungsarten eine Einstufung von OTA-Updates in verschiedene Update-Kategorien unterschiedlicher Risikoklassen vornehmen. Darauf aufbauend könnten einheitliche Standards in Abhängigkeit der Update-Klasse geschaffen werden. An den Aktivitäten, Datenobjekten und Schnittstellen in der Prozesskette können Anforderungen, Unterprozesse und / oder (Mindest-)Standards definiert werden, die die Qualität und Robustheit von OTA-Updates entlang der gesamten Prozesskette und zwischen allen beteiligten Akteuren erhöht.

5 HANDLUNGSOPTIONEN ZUR NUTZUNG DER CHANCEN UND VERRINGERUNG DER RISIKEN VON OTA-UPDATES

OTA-Updates besitzen ein hohes Potential, Kosten und Zeit einzusparen. Sie bieten nicht nur einen Mehrwert für den OEM, sondern auch für den Kunden. Demgegenüber stehen höhere Risiken, da im Vergleich zu konventionellen Software-Updates durch Werkstätten neue Schnittstellen benötigt werden sowie ein höherer Grad an Automatisierung notwendig ist. Risiken resultieren aus der hohen Komplexität automatisierter Prozesse und möglicher Cyber-Security-Incidents, die aufgrund der größeren Angriffsoberfläche der Luftschnittstelle wahrscheinlicher werden. Gegenüber dem konventionellen Werkstattprozess können resultierende Fehler im OTA-Update-Prozess schwerer erkannt und behoben werden. In diesem Kapitel werden Handlungsoptionen dargestellt, die es erlauben die Chancen zu nutzen und die Risiken zu adressieren.

5.1 Chancen nutzen

Im Vergleich zum Werkstattprozess haben OTA-Updates das Potential den Softwarewartungsprozess durch den vereinfachten und automatisierten Workflow zu beschleunigen. Hierdurch können die Wartungsprozesse kostengünstiger gestaltet und die Produktqualität langfristig gesteigert werden. Zusätzlich können die OEMs schneller auf Security Incidents reagieren und den Kunden neue Funktionen oder Geschäftsmodelle anbieten. Letztlich können erst durch Software-Updates Over-The-Air die Chancen der steigenden Digitalisierung und Vernetzung von Fahrzeugen in Gänze genutzt werden und deren Schwachstellen abgesichert werden.

Vorteile für den Automobilhersteller ergeben sich insbesondere dadurch, dass A) der Update-Prozess hochgradig automatisiert über die Luftschnittstelle realisiert wird, B) der Mehrwert für den Kunden zum Kaufgrund von Fahrzeugen mit OTA-Update-Fähigkeit werden könnte und C)

die Möglichkeit besteht Fehler und Security-Lücken schnell und unkompliziert beseitigen zu können.

A) Kostenreduktion und neue Geschäftsmodelle

Es ist zu erwarten, dass sich durch den Wegfall der Werkstattaufenthalte bei Software-Updates OTA langfristige Kosteneinsparungen ergeben, die die Investitionen in die neue Technologie rechtfertigen. Diese Kosteneinsparungen können sowohl vor als auch nach der Zulassung realisiert werden:

i) Vor der Zulassung

- Am Ende der Produktion wird üblicherweise die Fahrzeugsoftware konfiguriert und auf den neuesten Stand gebracht. Durch Nutzung von OTA-Technologie lässt sich dieser Prozess flexibler gestalten, sodass der Einsatz von Personal reduziert und Wartezeiten vermieden werden.
- Neufahrzeuge können auch bei längeren Standzeiten beim Händler einfach auf den neusten Softwarestand gebracht werden.
- Um den Anforderungen umfänglicher Software-Updates im Fahrzeug gerecht zu werden, ist davon auszugehen, dass sich zukünftig flexiblere Software- und Steuergerätearchitekturen und standardisierte Middleware durchsetzen werden (siehe Adaptive AUTOSAR, GENIVI etc.). Aufwände für Spezifikation und Entwicklung werden im Rahmen großer Konsortien realisiert und so zwischen verschiedenen Partnern geteilt.

ii) Nach der Zulassung

- Da bei OTA-Updates der Werkstattbesuch entfällt und kein Techniker vor Ort mit eingebunden werden muss, sondern das Update hochautomatisiert installiert wird, ergeben sich auch unter Berücksichtigung des Aufwandes für die OTA-Technik deutliche Kostenersparnisse (E018, E037).
- Der automatisierte Workflow mit weniger Aufwand für den Kunden erlaubt es, Software-Updates häufiger, zielgerichteter und umfassender durchzuführen. Der OEM kann kontinuierlich Softwarepflege betrieben, was insgesamt die Wartbarkeit des Produkts steigert und der Produktqualität zugutekommt. Darüber hinaus kann der OEM jederzeit neue Funktionalitäten im Fahrzeug anbieten. (E026)
- Rückrufe können einfacher, schneller und mit einer höheren Erfolgsquote abgeschlossen werden (sofern ein robuster Update-Prozess implementiert wurde). Vorgaben der Regulierungsbehörden können so einfacher und kosteneffizienter umgesetzt werden. (E030)

- Durch die Möglichkeit dem Kunden auch nach der Fahrzeugzulassung neue Funktionalität zur Verfügung zu stellen, ergeben sich neue Geschäftsmodelle, wie z.B. die kostenpflichtige Erweiterung von Funktionalität. Insgesamt wird die Zeit für die Markteinführung und die zur Bereitstellung neuer Funktionen deutlich verkürzt und durch die Möglichkeit erweitert, auch bereits verkaufte Fahrzeuge mit einzubeziehen. (E017)
- Moderne Fahrassistenz- und Telematik-Systeme sind vermehrt darauf angewiesen, dass auch der lokal im Fahrzeug verfügbare Informationspool (Karten etc.) kontinuierlich aktualisiert wird. Ohne OTA-Update Funktionalität wird das nicht realisierbar sein. (E017)
- Durch die neue Luftschnittstelle am Fahrzeug ergeben sich neben OTA-Updates auch noch zusätzliche Chancen, die in einer Kosten-Nutzen-Bewertung als Opportunitätskosten berücksichtigt werden können. So kann vor allem der lesende Zugriff die Datenbasis bei der Ursachenbegründung von Fehlern verbessern. Nicht nur ist so die Fahrzeugdatenbank stets aktuell, sondern auch Diagnosedaten können aus dem Fahrzeug ausgelesen und analysiert werden.[7] (E004, E008, E016)

B) **Kundenmehrwert**

OTA-Updates können zum Wettbewerbsvorteil werden und zur Kundenbindung beitragen:

- Es ergibt sich eine deutliche Zeitersparnis für den Kunden. Durch OTA-Updates ist der Kunde nicht mehr von einem Termin einer Werkstatt abhängig und muss hier sein Fahrzeug während der Öffnungszeiten nicht mehr vorführen und abholen. Stattdessen beschränken sich die Aufgaben des Kunden auf das Autorisieren des Updates in einem für ihn optimalen Zeitfenster sowie im Einrichten des benötigten Fahrzeugzustandes zum Durchführen des Updates.
- Die Funktionen des Kunden können stets aktuell gehalten werden. Sofern es die technische Basis der Kundenfahrzeuge zulässt, können die Funktionen auch im Feld regelmäßig weiter verbessert, an die Innovationen neuer Modelle angeglichen oder mit veränderten Rahmenbedingungen abgeglichen werden. Der letzte Aspekt besitzt besondere Relevanz sollte sich die Gesetzgebung für (hoch-)automatisierte Fahrfunktionen während ihres Einsatzes ändern, sodass gegebenenfalls Parameter dieser Funktionen über ein OTA-Update schnell an die aktuelle Gesetzeslage angepasst werden können.
- Neue digitale Dienste und Geschäftsmodelle können dem Kunden zur Verfügung gestellt werden. Bei der Einführung neuer Konzepte im Rahmen der

[7] Hier sei nur auf diese Möglichkeiten im Kontext von OTA-Updates verwiesen, die Auseinandersetzung mit diesem Thema ist nicht Inhalt dieses Berichtes.

Digitalisierung kann durch OTA-Updates nicht nur auf die Neufahrzeugflotte zurückgegriffen werden, sondern auch die aktuell im Feld befindliche Flotte adressiert werden, um auf diese Weise mehr potentielle Kunden zu erreichen.

C) Car-Security

Durch OTA-Updates können Fehler und Security-Lücken schneller geschlossen werden als bei einem Werkstattrückruf. Im Kontext der zunehmenden Digitalisierung und Vernetzung unterliegen die komplexen Software-Produkte einem beschleunigten Alterungsprozess und benötigen eine entsprechende Wartung. Andererseits besteht durch die Automatisierung und die damit einhergehende Übertragung kritischer Funktionalitäten an Softwarealgorithmen ein erhöhtes Sicherheitsrisiko für die Insassen und Umwelt sollte eine der (hoch-)automatisierten Fahrfunktionen nicht wie gewünscht funktionieren bzw. manipulierbar sein.

5.2 Risiken absichern

Den Chancen gegenüber stehen Risiken, die sich konkret auf die Nutzung von OTA-Updates zurückführen lassen. Durch neue Schnittstellen sowie die komplexen, technischen Abläufe, erhöht sich die Wahrscheinlichkeit von Fehlern sowie die Möglichkeit, dass Sicherheitslücken von Angreifern mit verschiedenen Motivationen ausgenutzt werden können. Im OTA-Prozess entstehen neue Schnittstellen zu neuen Marktteilnehmer, der regulatorischen Behörde und den Kunden. Außerdem machen die Automatisierung und die fehlende Betreuung durch einen Werkstattmitarbeiter den Prozess technisch komplexer und damit insgesamt anfälliger für Fehler. Es bedarf entsprechender Regelalgorithmen, um den Prozess zu monitoren, Störungen abzufangen und eine fehlerfreie Installation abzusichern. Insgesamt ist ein robuster Prozess notwendig, um Risiken ausreichend abzusichern und Vertrauen gegenüber Gesetzgeber und Kunden zu erlangen.

Im Folgenden sind aus den identifizierten Risiken (siehe Kapitel 3.3) Aufgaben für die zuständigen Unternehmen abgeleitet worden. Diese unterteilen sich in drei Bereiche: regulatorische Risiken absichern, prozessuale Risiken absichern und technische Risiken absichern. Die Aufgaben sind zusätzlich entweder als individuell lösbar gekennzeichnet („→Individuell“), wenn jeder OEM einen eigenen Umgang mit dem Risiko finden muss. Für einige dieser Aufgaben bietet es sich an, Lösungen branchenübergreifend zu diskutieren. Diese sind als gemeinschaftlich lösbar gekennzeichnet („→Alle“).

5.2.1 Regulatorische Risiken absichern

- **Die Rahmenbedingungen für den lesenden Zugriff auf Fahrzeugdaten und der Umgang mit solchen sind zu definieren.[8] → Alle**
  Der Zugriff auf Fahrzeugdaten hat einen großen Einfluss auf die Möglichkeiten, die sich durch OTA-Updates ergeben. Fehlende Informationen können den Prozess verlangsamen. Zu den Daten können nicht nur die Daten über die Fahrzeugkonfiguration zählen (verbaute Steuergeräte, Softwareversionen, etc.), sondern auch die Diagnosedaten solcher Steuergeräte. Grundsätzlich ist zu klären, auf welche Daten der OEM im Rahmen eines OTA-Update Prozesses zugreifen darf und welche Daten als personenbezogenen Daten einer besonderen Regulierung unterliegen. Darüber hinaus sind die rechtlichen Rahmenbedingungen zur Weitergabe von Daten an den Digitalen Dienstleister abzuklären. (E005, E009, E014, E023)

- **Die Möglichkeiten, Rückrufe durch OTA-Update zu optimieren, sind zu untersuchen. → Alle**
  Rückrufe durch OTA-Updates zu realisieren, bietet die Möglichkeit kosteneffizient und schnell Fehler beseitigen zu können. Für die Überprüfung, inwiefern bei festgestellten Produktabweichungen Behörden gemäß landesspezifisch geltender Gesetze eingebunden werden müssen, ist zu klären. Hierzu sei an dieser Stelle auf den VDA Gelb-Band „Produktsicherheit und -konformität in der automobilen Lieferkette bei Produktabweichungen“ verwiesen.

5.2.2 Prozessuale Risiken absichern

- **Ein gemeinsames Prozessverständnis ist aufzubauen. → Alle**
  Durch die Verteilung von Software Over-The-Air entstehen neue Prozesse mit neuen Marktteilnehmern. Zum Erlangen eines gemeinsamen Prozessverständnisses bedarf es einer gemeinsamen Plattform, auf der ohne den Austausch Wettbewerbs-relevanter Daten diskutiert werden und Probleme und Lösungen verortet werden können, sodass eine vorwettbewerbliche Harmonisierung von Prozessessen, Schnittstellen und Mindeststandards erreicht werden kann. Ansonsten besteht das Risiko, dass die Herausforderungen von OTA-Updates nur als Randaspekte weiterer aktueller Themen betrachtet werden.

- **Neue Stakeholder sind zu integrieren. → Alle**
  Die Integration von OTA-Updateprozessen ermöglicht – u. a. durch die bereits existierende OTA-Technik in anderen Industrien – neuen Firmen den Markteintritt (Telekommunikationsanbieter, digitale Dienstleister, Cloud-Speicher-Anbieter, etc.). Diese sind in die Lieferkette zu integrieren, die verschiedensten

[8] Hier sei nur auf diese Möglichkeiten im Kontext von OTA-Updates verwiesen, die Auseinandersetzung mit diesem Thema ist nicht Inhalt dieses Berichtes.

Zusammenarbeitsmodelle, die mit diesen Anbietern existieren, sind zu homologieren und eine Qualifikation dieser Anbieter ist anzustreben (z.B. unter Berücksichtigung folgender Faktoren: Car-SIR-Fähigkeit, Datensicherheit, Leistungsfähigkeit, etc.). Risiken bestehen bei Qualitätsmängeln möglicher neuer Marktteilnehmer. Dies kann letztlich dazu führen, dass ein Update nicht richtig aufgespielt wird und zu einer negativen Wahrnehmung bei Gesetzgeber und Kunden führt. Darüber hinaus besteht durch die Einbindung externer Serverstrukturen ein Sicherheitsrisiko bezogen auf die Daten der Kunden und die Daten des Updates. Dieses könnte ausgelesen, manipuliert oder um eine Malware erweitert werden. (E011, E013)

- **Die Prozesslaufzeit ist zu optimieren. → Individuell**
  Um die Reaktionsfähigkeit nachhaltig sicherzustellen, müssen die Anforderungen an die Prozessaktivitäten angepasst werden. Ein Ansatz hierfür ist die Einführung einer Klassifizierung von OTA-Updates. Ziel muss es sein, Prozesse entlang der Klassifizierung optimieren zu können, sodass Fehler innerhalb kürzester Zeit abgestellt werden können.

- **Es ist eine branchenübergreifende Klassifizierung zu definieren. → Alle**
  Eine Klassifizierung hilft den OTA-Prozess effizienter durchzuführen und sämtliche Potentiale abzurufen. Es empfiehlt sich, eine Klassifizierung auf breitem Expertenwissen zu basieren und ein Klassifizierungsschema zu entwickeln, das eine Vielzahl von Szenarien berücksichtigt und auch gegenüber regulatorischen Behörden kommuniziert werden kann. (E002, E003, E010)

- **Die Schnittstellen zwischen OEM und Händler-Netzwerk ist ggf. neu zu definieren. → Individuell**
  Regulatorische Vorgaben können die Verteilung von OTA-Updates durch den OEM einschränken. Z. B. haben in den USA vereinzelte Bundesstaaten die Wartungstätigkeiten an Fahrzeugen gesetzlich den Händlern zugeschrieben. Ein direktes Software-Update durch den OEM ohne Einbindung der Händler ist somit momentan in diesen Bundesstaaten nicht möglich. (E020)

- **Die Bestätigung des Updates durch den Kunden ist rechtssicher zu gestalten. → Alle**
  Bisher wurde ein Software-Update durch einen Werkstattauftrag mit der Unterschrift des Halters autorisiert. Bei OTA-Updates erfolgt eine Autorisierung i. d. R. vom Fahrer / Nutzer im Fahrzeug bzw. über das Webportal des Herstellers. Um sicherzustellen, dass keine unbefugte Person ein Update auslöst oder ablehnt, muss sich der Fahrer / Nutzer durch einen mehrstufigen Prozess registrieren und gegenüber dem OEM autorisieren. Folgende Punkte wurden für die Autorisierung von OTA-Updates als kritisch identifiziert (E021, E029):

    - Diskrepanz zwischen Fahrer / Nutzer und Halter. Ohne zusätzliche Absicherung kann ein Fahrer / Nutzer aktuell ein Update annehmen oder ablehnen, ohne dass der Halter, der am Ende in der Rechtspflicht steht, darauf einwirken kann. Der

OEM muss eine informationstechnische Lösung bereitstellen, um dem Halter zu ermöglichen, Updates rechtssicher durchzuführen. Delegation an weitere Personen in Onlineportalen sind als weitere technische Maßnahme möglich. Offen bleibt jedoch eine Reihe weiterer Fragen, die bisher nicht einheitlich geregelt sind (z. B. Kann der Nutzer ein OTA-Update vor seiner Fahrt ablehnen / abbrechen? Sind für bestimmte Updates Vorabautorisierungen möglich? Wie werden diese erteilt und beschrieben, sodass sie von allen Parteien anerkannt und als rechtssicher beurteilt werden?). (E027)

- Die Hersteller sollten Möglichkeiten bereitstellen, ein Software-Update über die Ferne zu starten. Dieses ist vor allem bei Flotten- und Leasingfahrzeugen (ein Halter, mehrere Nutzer) von Interesse, um sicherzustellen, dass alle Fahrzeuge den gewünschten Softwarestand erhalten.
- Langfristig ist davon auszugehen, dass Software-Updates notwendige Voraussetzung für den Weiterbetrieb eines Fahrzeugs darstellen, weil die Updates sicherheitsrelevante Fehler korrigieren oder Gefahren für die Umwelt verringern (E028). In einem solchen Fall stellen sich u.a. folgende Fragen:
  - Sind solche Updates verpflichtend? (z.B. könnte dies eine Option für Korrekturen hoch-automatisierter Fahrfunktionen sein. Einem Eingriff in die Eigentumsrechte des Kunden ist hier vorzubeugen.)
  - Wer überprüft die Durchführung der Updates?
  - Ist eine Remote-Sperrung des Fahrzeugs möglich? Szenarien, bei denen in die Fahrzeugnutzung eingegriffen werden könnte, sind z. B. ein nicht durchgeführtes Security-Update, ein leerer AdBlue-Tank oder eine nicht gezahlte Leasing-Rate für die Batterie.

- **Eine Fall-Back-Ebene für den Fall fehlgeschlagener Updates ist einzuführen. → Alle** Eine Installation in einer unkontrollierten Umgebung sowie zu einem unkontrollierten Zeitpunkt oder das Installieren falscher Software kann zu Unterbrechungen des Updatevorgangs bzw. zu einem inkonsistenten Softwarestand führen. Dadurch, dass das Update nicht mehr in der Fachwerkstatt durchgeführt und der Vorgang von Experten überwacht wird, besteht die Gefahr, dass ein solcher inkonsistenter Softwarestand nicht entdeckt bzw. nicht behoben werden kann. Es entstehen folgende Risiken beim Kunden (E032, E034, E035, E038, E040):
  - Fehlerhafte Funktionsausführung von Fahrfunktionen und Fahrzeuganwendungen;
  - Nicht startende ECUs oder ECUs, die sich in einer endlosen Reboot-Schleife befinden;
  - Nicht korrekt startende Programme.

Für fehlgeschlagene Updates ist sicherzustellen, dass das Fahrzeug …

- … in den alten aber konsistenten Zustand vor dem Update zurückversetzt wird. Ein dafür notwendiges Backup kann in einem zweiten Flashspeicher in der ECU, im Gateway oder in einem Cloudspeicher gesichert werden.
- … notfalls mit einem reduzierten aber betriebssicheren Funktionsumfang wieder fahrbereit gemacht wird, um wenigstens die Mobilität des Kunden herzustellen (Fall-Back-Ebene).
- … schlimmstenfalls stillgelegt wird, wenn die Betriebssicherheit gefährdet ist.

- **Die Fahrzeugrückmeldung ist zuverlässig zu gestalten. → Individuell**
  Sowohl bei einer korrekten als auch abgebrochenen Installation bedarf es einer zuverlässigen Rückmeldung an die Systeme des OEMs. Eine anderweitige Nachverfolgung wäre mit einem sehr großen Aufwand verbunden. Für die Erfüllung von Rückrufen wie auch zur Abrechnung zugekaufter Funktionen ist eine solche Rückmeldung essentiell, um die Vorgänge rechtssicher abzuschließen zu können. (E043)
- **Die Veränderungen am Fahrzeug sind nachhaltig zu dokumentieren. → Alle**
  Durch OTA-Updates können Eigenschaften, Funktionen oder Verhalten des Fahrzeuges dauerhaft verändert werden (z. B. eine veränderte Bedienoberfläche, Funktionserweiterungen, etc.). Bei solchen Eingriffen veraltet das Bordhandbuch, welches damit nicht mehr den technischen Stand des Fahrzeugs widerspiegelt. Der Halter bzw. Fahrer/Nutzer muss dabei (1) über die geplanten Änderungen informiert werden und (2) eine vollständige und aktuelle Dokumentation der installierten Technik seines Fahrzeuges zur Verfügung gestellt bekommen. Für beide Fälle ist derzeit noch keine herstellerüberreifende Regelung gefunden. (E041)
- **Eine Option zum Löschen personenbezogener Daten ist zu implementieren. → Alle**
  Fallen beim Aufspielen von Software-Updates personenbezogene Daten an (z.B. Bezahldaten), so muss sichergestellt sein, dass diese Daten vor dem Weiterverkauf des Fahrzeuges gelöscht werden können. Bei Smartphones existiert zu diesem Zweck die Funktion „Auf Werkszustand zurücksetzen“.
- **Der Kunde ist detailliert über den Umfang des Updates zu informieren. → Alle**
  Der Halter eines Fahrzeugs muss prinzipiell einem Update zustimmen. Vor dem Einholen dieser Zustimmung ist der Halter ausführlich über den Inhalt, die Rahmenbedingungen und die Dauer des Updates zu informieren. Welche Informationen hier kommuniziert werden sollten und welche Kanäle hierzu zu wählen sind, ist abzustimmen. Besonders bei sicherheitskritischen Updates ist eine weitreichende Aufklärung des Kunden sicherzustellen, damit diese Updates zeitnah installiert werden. Die Angaben zur Dauer des Updates sollten präzise sein, damit es zu keinem negativen Kundenerlebnis kommt. (E024)

Ferner sollte die Abfolge des Update-Verlaufes dem Kunden transparent sein. Eine gängige Abfolge ist z. B. Bestätigung des OTA-Updates im Fahrzeug, benötigter Zustand des Fahrzeugs, eventuelle Aufforderung das Fahrzeug zu verlassen, etc.

Bei der Übergabe an den Werkstattprozess ist bei einer Rückrufmaßnahme zwingend die Zeit bis zum Erlöschen der Betriebserlaubnis zu berücksichtigen. Dem Kunden muss genügend Zeit zum Vorführen seines Fahrzeuges in der Werkstatt eingeräumt werden.

5.2.3 Technische Risiken absichern

- **OTA-Updates sind gegen Security-Incidents abzusichern. → Individuell**
  Cyberangriffe ermöglichen prinzipiell den Zugriff auf die Fahrzeugsoftware sowie auf personenbezogene Daten der Kunden. Neben allgemeinen Nutzerdaten, wie Name, Adresse oder Zahlungsmöglichkeiten, gehören hierzu auch Bewegungsprofile oder Tonmitschnitte, die über integrierte Mikrofone der Sprachbedienung mitgehört werden. Die Öffnung des Fahrzeuges über die Luftschnittstelle birgt das Risiko, dass Angreifer über Schwachstellen dieser Schnittstelle bzw. in der Verteilinfrastruktur auf das Fahrzeug bzw. das Software-Update zugreifen können. Bei entsprechendem Know-how der Angreifer und fehlender Absicherung könnten Daten und Software mitgelesen oder manipuliert bzw. auf Funktionen des Fahrzeuges zugegriffen werden. Angreifer könnten zudem nachträglich ein Device im Fahrzeug-Bordnetz einbauen und dadurch die interne OTA-Kommunikation mitlesen, manipulieren oder blockieren (E006, E007, E015, E023, E033).

  Im Folgenden werden beispielhaft einige Cyberangriffe aufgelistet, bei denen sich ein Zusammenhang mit OTA-Updates erkennen lässt:

  - Kompromittierte Software erlaubt den Zugriff auf Funktionen des Fahrzeuges. So wären, neben der Störung von Fahrzeugfunktionalität und der damit einhergehenden Konsequenzen für die Fahrsicherheit, zum Beispiel auch Ransomware-Attacken möglich, die Fahrzeugfunktionen blockieren bzw. eine Beschädigung des Fahrzeuges (z. B. Zerstörung der Batterie bei Zugriff auf das Batteriemanagementsystem) oder ein Eingriff in die Fahrsicherheit (Deaktivierung der Lenkung, Deaktivierung der Bremsen) androhen, um vom Halter oder OEM ein „Lösegeld“ einzufordern. (E036)
  - Bei weitreichendem Zugriff auf die Kommunikation zwischen Fahrzeug und der Verteilinfrastruktur bzw. auf die Fahrzeugsoftware selber, können betriebsrelevante oder personenbezogene Daten ausgelesen werden. Dieses ist unter anderem dann der Fall, wenn die Kommunikation zwischen dem zentralen Gateway und den Steuergeräten unzureichend verschlüsselt erfolgen sollte. (E039)
  - Das Blockieren der Datenkommunikation zwischen Fahrzeug und der Verteilinfrastruktur kann dazu führen, dass Software-Updates nicht aufgespielt

werden und damit das Beheben einer Sicherheitslücke oder eines sicherheitsrelevanten Softwarefehlers verhindert werden kann. (E025)

- Der Updateprozess kann möglicherweise so beeinflusst werden, dass ein Rollback auf einen vorherigen und damit unsichereren Versionsstand durchgeführt wird oder Update-Dateien vor der Installation ausgetauscht werden bzw. ein falsches Update aufgespielt wird, wodurch das Fahrzeug wieder in einen unsicheren Zustand überführt wird.
- Durch gezielte Manipulation kann der Updateprozess so beeinflusst werden, dass die erfolgreiche Installation und damit die positive Rückmeldung nicht erfolgt, sodass der Kunde die erfolgreiche Einspielung eines Updates abstreiten kann. Dem Unternehmen entgeht entweder Gewinn oder die Kosten für die Durchführung des Updates erhöhen sich. (E042)

- **Branchenübergreifende Qualitätsstandards sind zu definieren. → Alle**
  Zur Unterstützung der Integration der neuen Stakeholder und zur Erweiterung des Prozessverständnisses können Qualitätsstandards als branchenübliche Maßstäbe bei der Durchführung von OTA-Updates definiert werden. Dies dient einerseits als Motivation von neuen Marktteilnehmern ihr Angebot weiter zu optimieren und andererseits als Nachweis gegenüber dem Gesetzgeber, wie die Branche das Thema adressiert und deren Performance sicherstellt.

- **Der notwendige Zustand des Fahrzeuges für ein OTA-Update ist zu definieren. → Alle**
  Für die Durchführung eines OTA-Update muss sich das Fahrzeug in einem sicheren Zustand befinden. Hierzu gibt es seitens der OEM jeweils eigene Definitionen z. B. „Fahrzeug stillstehen“, „Motor aus“, „Handbremse angezogen“, „Fahrzeug verriegeln“, oder „Safe Lock ein“. Eine einheitliche Position gegenüber der regulatorischen Behörde und den Kunden ist anzustreben. Dies kann auch in Abhängigkeit der Klassifizierung erfolgen, sodass je Klasse der jeweils notwendige Zustand definiert wird, in dem ein Fahrzeug robust aktualisiert werden kann.

- **Es ist zu klären, wie bei fehlender Verbindung zum Fahrzeug, das Update übertragen werden kann. → Alle**
  Es kann verschiedene Gründe geben, die dazu führen, dass ein Update nicht an das Fahrzeug kommuniziert werden kann: der Download lässt sich – z.B. aufgrund einer Überlastung der Serverstruktur – nicht initiieren, ein technische Defekt liegt vor oder das Fahrzeug ist in einem ‚Privacy Modus‘. Für diese Fälle ist eine Strategie zu entwickeln, wie die entsprechenden Fahrzeuge bzw. ihre Halter zeitnah erreicht werden können und die Software aktualisiert werden kann. (E022, E031)

5.2.4 Zusammenfassung

Tabelle 2 fasst die identifizierten Aufgaben mit ihren jeweiligen Stakeholdern abschließend zusammen.

Aufgabe	Stakeholder
Regulatorische Risiken absichern	
Die Rahmenbedingungen für den lesenden Zugriff auf Fahrzeugdaten und der Umgang mit solchen sind zu definieren.	Alle
Die Möglichkeiten, Rückrufe durch OTA-Update zu optimieren, sind zu untersuchen.	Alle
Prozessuale Risiken absichern	
Ein gemeinsames Prozessverständnis ist aufzubauen.	Alle
Neue Stakeholder sind zu integrieren.	Alle
Die Prozesslaufzeit ist zu optimieren.	Individuell
Es ist eine branchenübergreifende Klassifizierung zu definieren.	Alle
Die Schnittstelle zwischen OEM und Händler-Netzwerk ist ggf. neu zu definieren.	Individuell
Die Bestätigung des Updates durch den Kunden ist rechtssicher zu gestalten.	Alle
Eine Fall-Back-Ebene für den Fall fehlgeschlagener Updates ist einzuführen.	Alle
Die Fahrzeugrückmeldung ist zuverlässig zu gestalten.	Individuell
Die Veränderungen am Fahrzeug sind nachhaltig zu dokumentieren.	Alle
Eine Option zum Löschen personenbezogener Daten ist zu implementieren.	Alle
Der Kunde ist detailliert über den Umfang des Updates zu informieren.	Alle
Technische Risiken absichern	
OTA-Updates sind gegen Security Incidents abzusichern.	Individuell
Branchenübergreifende Qualitätsstandards sind zu definieren.	Alle
Der notwendige Zustand des Fahrzeuges für ein OTA-Update ist zu definieren.	Alle
Es ist zu klären, wie bei fehlender Verbindung zum Fahrzeug, das Update übertragen werden kann	Alle

Tabelle 2: Handlungsoptionen zur Verringerung der Risiken von OTA-Updates

6 FAZIT

Dieser Bericht stellt einen Überblick über die notwendigen Prozesse und die abzusichernden Bereiche beim Einsatz von OTA-Updates bereit. Es werden ganzheitlich alle relevanten Aktivitäten bei der Durchführung von OTA-Updates betrachtet und die verschiedenen Inhalte der verschiedenen Stakeholder strukturiert. Dargestellt wird dies in einem generischen OTA-Prozess. Dieser Ist-Prozess ist eine systematische und herstellerübergreifende Beschreibung der OTA-Update-Aktivitäten und seiner Schnittstellen und dient als Basis für weitere Analysen und dem Vergleich zum konventionellen Werkstatt-Prozess. Entlang des Prozesses wurden neue Schnittstellen zwischen den beteiligten Rollen identifiziert und zusammen mit den einzelnen Aktivitäten auf Chancen, Risiken und Sicherheits-Schwachstellen untersucht.

Ergebnis ist – neben der ganzheitlichen Prozessdarstellung – eine Konzeption für die Klassifizierung von OTA-Updates, die Auflistung der Chancen und Risiken entlang des OTA-Prozesses sowie die Darstellung von Handlungsoptionen, wie Chancen genutzt und Risiken abgesichert werden können.

Im Rahmen des Projektes wurde festgehalten, dass es bei der Absicherung verschiedener Risiken eine Unsicherheit in der Industrie, bei den Kunden und dem Gesetzgeber gibt, wie hier rechtlich korrekt zu verfahren ist. Aufgrund dieser Unsicherheit bzw. ungenügender Rechtssicherheit kann allerdings auch kein technisch konformer OTA-Prozess etabliert werden. Eine Klärung vorwettbewerblicher rechtlicher und technischer Rahmenbedingungen – wie sie auch im Bericht identifiziert werden – wird benötigt. Ein Instrument, dieses zu adressieren, kann ein VDA Arbeitskreis sein, um Anforderungen an bzw. Maßnahmen für einen robusten OTA-Prozess zu dokumentieren und evtl. zu standardisieren.

Die Ergebnisse dieses Projektes können den verschiedenen Stakeholder von OTA-Updates dienen als:

- gemeinsame Kommunikationsplattform, um Inhalte entlang der Prozesskette verorten zu können.
- Unterstützung der Analyse des eigenen Prozesses, ob weitere Chancen genutzt werden können oder zusätzliche Risiken abgesichert werden müssen.
- Input zur effizienteren Gestaltung des eigenen Prozesses, z. B. durch die Klassifizierung von OTA-Updates.

Darüber hinaus bilden die Ergebnisse die Grundlage für ein Folgeprojekt im AQI. In diesem Folgeprojekt sollen die hier erarbeiteten Grundlagen genutzt werden, um eine Szenarioanalyse verschiedener OTA-Update-Typen durchzuführen. Mit den Ergebnissen dieser Analyse sollen die Klassifizierungsansätze in ein Klassifizierungsschema überführt und validiert werden. Durch die Simulation der verschiedenen Anwendungsfälle sollen ebenfalls die Prozessbeschreibung optimiert und erweitert, sowie die Risikoanalyse vertieft werden.

ANHANG

Werkstatt-Prozess

Der hier dargestellte Werkstattprozess entspricht gängiger Praxis. Dies dient als Vergleich, um aufzuzeigen, welche Aktivitäten durch ein OTA-Update hinzukommen bzw. entfallen. Abgebildet ist ebenfalls die Einbindung des KBA bei Rückrufen. Die hierfür zusätzlich anfallenden Aktivitäten. Die Darstellung des Prozesses in BPMN 2.0 befindet sich im Anhang.

Generierung

Prozess-ID	Beschreibung
WRK-G-010	Input: Information über eine Fehlfunktion im Fahrzeug. Die Quelle für die Information kann unterschiedlich sein: sie kann sowohl intern durch eigene Beobachtungen oder extern durch Kommunikation mit der Regulatorische Behörde, den Kunden, die Presse o. ä. erfolgen. Der ***Update-Koordinator*** analysiert die Informationen und identifiziert den Bedarf eines Software-Updates für ein betroffenes Bauteil / ein betroffenes System. Output: Updatebedarf inkl. Fehlerbild und mögliche Ursache zur weiteren Nachverfolgung
WRK-G-020	Der ***Update-Koordinator*** klassifiziert das Software-Update (vgl. Kapitel 4). Output: Ergänzung der Updatebedarfsmeldung um Updateklasse.; ggf. Meldung an die *Regulatorische Behörde* **Konditionen:** zumindest, wenn das Update produktsicherheitsrelevant ist, ist die *Regulatorische Behörde* einzubinden (→ WRK-G-030).
WRK-G-030 (nur bei Regul. Behörde)	Die ***Regulatorische Behörde*** registriert den Rückruf und informiert ggf. RAPEX bzgl. des Rückrufs.

WRK-G-031 (nur bei Regul. Behörde)	Ggf. wird durch die ***Regulatorische Behörde*** eine Frist bis zur Erfüllung des Rückrufs und/oder weitere Auflagen festgesetzt. Output: Anweisung
WRK-G-040	Der ***Update-Koordinator*** kommuniziert den Updatebedarf an den *Entwicklungsverantwortlichen* des Updates. Output: dokumentierter Updatebedarfsmeldung
WRK-G-050	Der ***Entwicklungsverantwortliche*** definiert das Lastenheft für das Software-Update. Output: Lastenheft für Software-Update
WRK-G-060	Der ***Entwickler*** entwickelt das neue Software-Update. Output: Software-Update
WRK-G-070	Der ***Entwickler*** übermittelt das Software-Update an den Update-Server des OEM und informiert den *Entwicklungsverantwortlichen* über den neuen Softwarestand. Output: dem OEM verfügbares Software-Update; Mitteilung über Verfügbarkeit des Updates
WRK-G-080	Der ***Entwicklungsverantwortliche*** überprüft die Qualität des neuen Softwarestandes. Bei ernster Gefährdung wird die Lösung dokumentiert und an die *Regulatorische Behörde* zur weiteren Prüfung weitergeleitet (→ WRK-G-090). Output: Ergebnis der Qualitätsprüfung; ggf. Dokumentation zur technischen Lösung (nur bei ernster Gefährdung) **Konditionen: (A)** Das Software-Update entspricht den Anforderungen des Lastenheftes und besteht die Prüfung durch die *Regulatorische Behörde* (→ WRK-G-100). **(B)** Es entspricht den Anforderungen des Lastenheftes, aber besteht die Prüfung durch die *Regulatorische Behörde* nicht. Der *Entwicklungsverantwortliche* muss das Lastenheft überarbeiten (→ WRK-G-050). **(C)** Es entspricht nicht den Anforderungen des Lastenheftes. Der *Entwicklungsverantwortliche* fordert den Entwickler zur Nachbesserung auf (→ WRK-G-060).
WRK-G-090 (nur bei Regul. Behörde)	Nur bei ernster Gefährdung: Die ***Regulatorische Behörde*** prüft die vorgestellte Lösung auf Konformität. Output: Prüfbescheid

WRK-G-100	Der ***Entwicklungsverantwortliche*** gibt das Update intern aus technischer Sicht für den weiteren Prozess frei. Output: freigegebenes Update
WRK-G-110	Der ***Update-Koordinator*** zeichnet das Software-Update für die Umsetzung des Rückrufs an den Kundenfahrzeugen frei. Output: freigezeichnetes Update

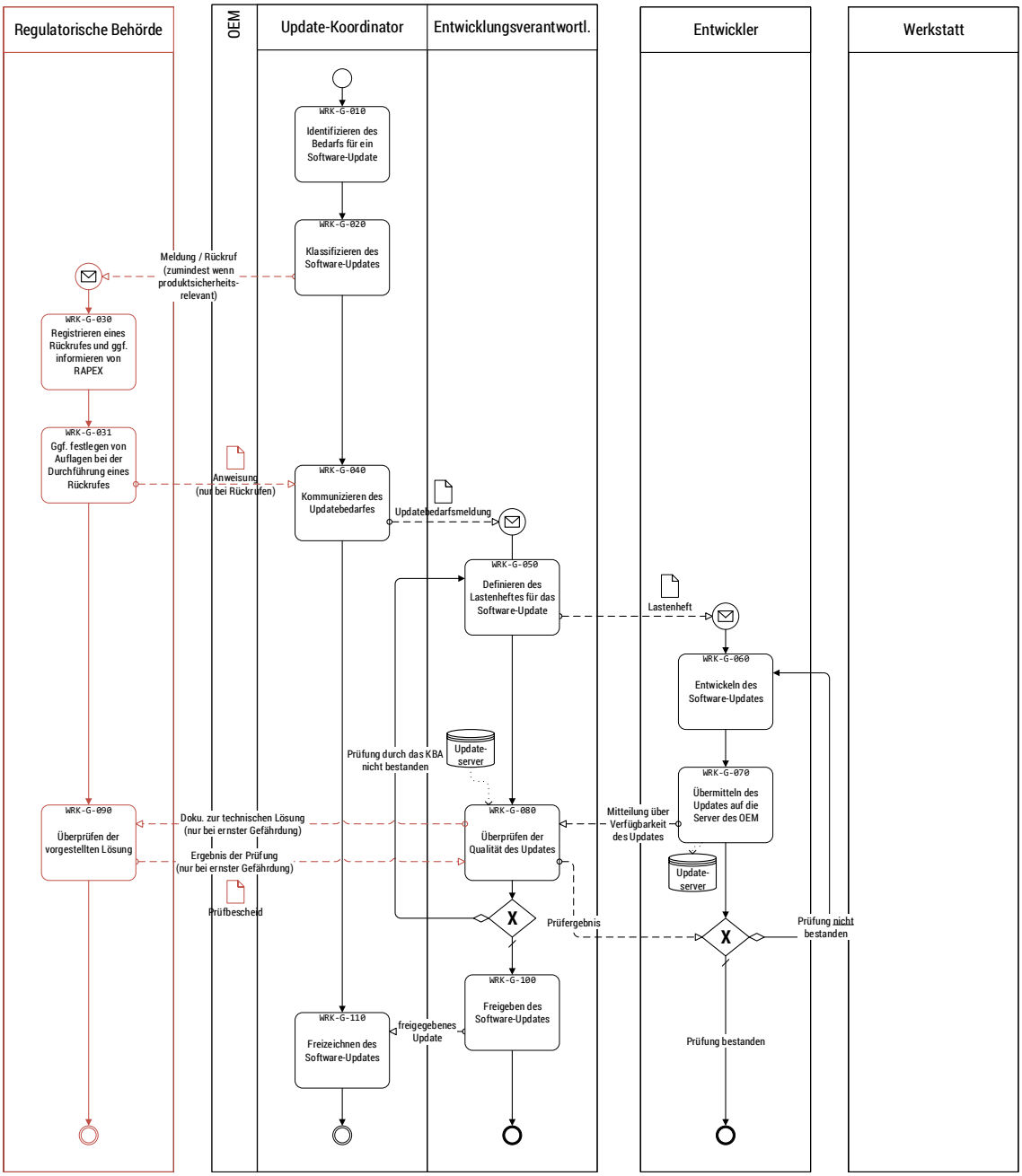


Abbildung 11: Werkstatt-Prozess "Generierung"

Verteilung

Prozess-ID	Beschreibung
WRK-V-010	Der ***Update-Koordinator*** identifiziert die betroffenen Fahrzeuge. Zur Identifikation der Halter der betroffenen Fahrzeuge kann eine Halterabfrage an die regulatorische Behörde gestellt werden. Output: Halterabfrage / FIN-Liste identifizierter Fahrzeuge
WRK-V-020 (nur bei Regul. Behörde)	Die ***Regulatorische Behörde*** übermittelt bei Bedarf die Halterdaten zu den betroffenen Fahrzeugen. Output: Halterdaten
WRK-V-030	Der ***Update-Koordinator*** verarbeitet die erhaltene Datenbank und verteilt sie an die relevanten Werkstätten, z.B. über eine CRM-Plattform. Output: Halterdaten
WRK-V-040	Input: freigezeichnetes Update-Paket Nach Erhalt der Freigabe: Die ***Werkstatt*** lädt das Updatepaket vom Updateserver auf seine lokalen Systeme herunter. Anm.: Alternativ kann die Verteilung vom OEM zu den Werkstätten auch über ein Speichermedium erfolgen.
WRK-V-050	Input: Halterdaten Die ***Werkstatt*** benachrichtigt den *Halter* über den Rückruf. Output: Informationen über das Update Anm.: A) Üblicherweise erfolgt die Kommunikation per Brief, kann aber auch über die Presse, TV- oder Radio-Werbung, Webseiten oder telefonische Kontaktaufnahme erfolgen. B) Dies kann alternativ auch direkt über die regulatorische Behörde erfolgen. C) Nicht sicherheitsrelevante Software-Rückrufe können eventuell durch den Kunden selbst durchgeführt werden. Die Update-Daten können vom Hersteller über verschiedene Medien an den Halter geschickt werden. Mit Hilfe einer Bedienungsanleitung kann das Update z. B. über eine USB-Schnittstelle durchgeführt werden.

WRK-V-060	Der ***Halter*** überprüft das Update anhand der Informationen, die er vom OEM erhalten hat. Output: ggf. Genehmigung **Konditionen: Entweder** er genehmigt das Update und setzt sich in Verbindung mit dem Hersteller **oder** er genehmigt es nicht. Anm.: Genehmigt der Halter das Update nicht, erhält der OEM nicht zwangsläufig eine Rückmeldung über diese Entscheidung. Für den OEM ist ein zusätzlicher Aufwand notwendig, um dies nachzuverfolgen und die Rückrufquote zu steigern.
WRK-V-070	Die ***Werkstatt*** koordiniert einen Termin mit dem *Halter* zur Vorführung des Fahrzeuges. Bei zeitkritischen Updates muss entsprechend die benötigte Kapazität in der *Werkstatt* vorhanden sein. Output: Terminvereinbarung
WRK-V-080	Der ***Halter*** führt das Fahrzeug in der *Werkstatt* vor und autorisiert vor Ort die Durchführung des Software-Updates mit seiner Unterschrift unter dem entsprechenden Auftrag.

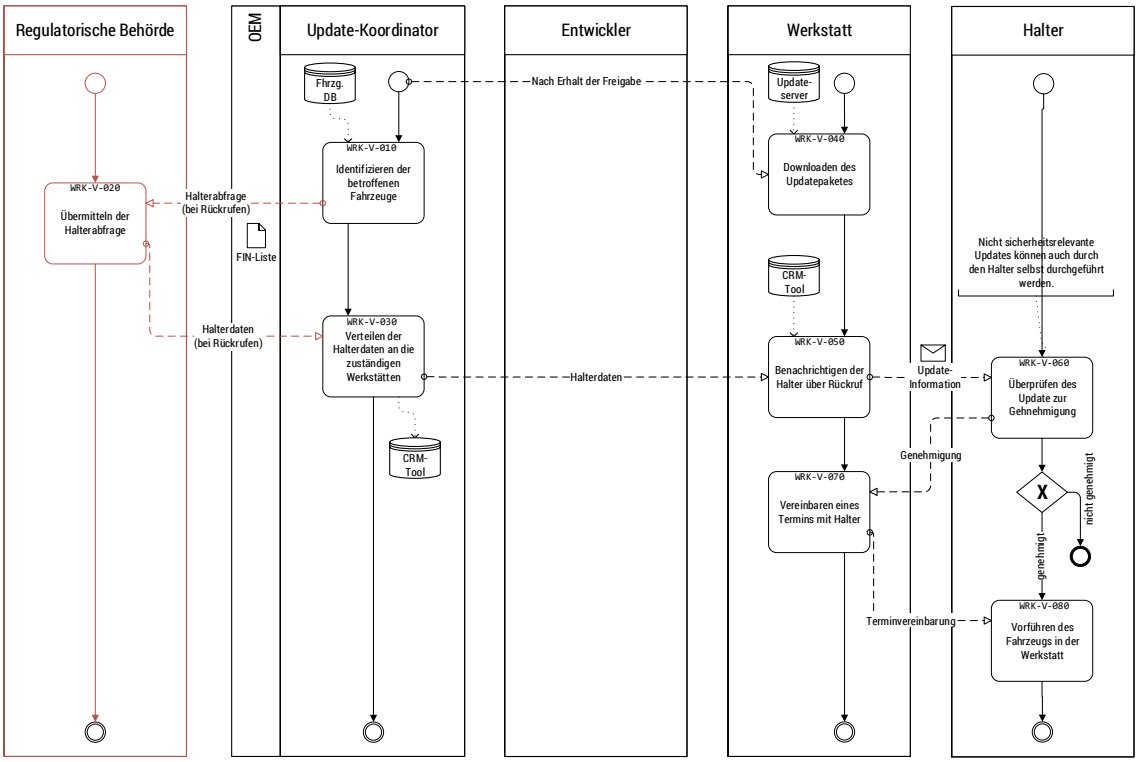


Abbildung 12: Werkstatt-Prozess "Verteilung"

Installation

Prozess-ID	Beschreibung
WRK-I-010	Die ***Werkstatt*** aktualisiert ihre Programmiertools und befähigt die Tools so, das Update durchzuführen.
WRK-I-020	Die ***Werkstatt*** überprüft die Fahrzeugkonfiguration, ob sie den Anforderungen des Updates entspricht.
WRK-I-030	Die ***Werkstatt*** spielt das Update über das an das Fahrzeug angeschlossene Programmiertool auf das System auf.
WRK-I-040	Die ***Werkstatt*** überprüft / testet, ob die Installation erfolgreich war. **Entweder** die Installation war erfolgreich **oder** die Installation schlug fehl (→ WRK-I-020).
WRK-I-050	Die ***Werkstatt*** benachrichtigt den *Halter*, dass sein Fahrzeug wieder abgeholt werden kann, und den *Update-Koordinator*, dass das Update erfolgreich aufgespielt wurde. Output: Informationsobjekte an *Halter* und *Update-Koordinator*
WRK-I-060	Der ***Halter*** bzw. ein Stellvertreter nimmt das Fahrzeug in der *Werkstatt* ab.
WRK-I-070	Der ***Update-Koordinator*** aktualisiert seine Fahrzeug-Datenbank, um das aktualisierte Fahrzeug. Bei Rückrufen wird der aktuelle Status des Rückrufes regelmäßig an die Regulatorische Behörde kommuniziert. Output: Statusbericht (bei Rückrufen)
WRK-I-080 (nur bei Regul. Behörde)	Die ***Regulatorische Behörde*** aktualisiert die Rückruf-Datenbank und schließt gegebenenfalls den Rückruf entsprechend ihrer Vorgehensweise ab.

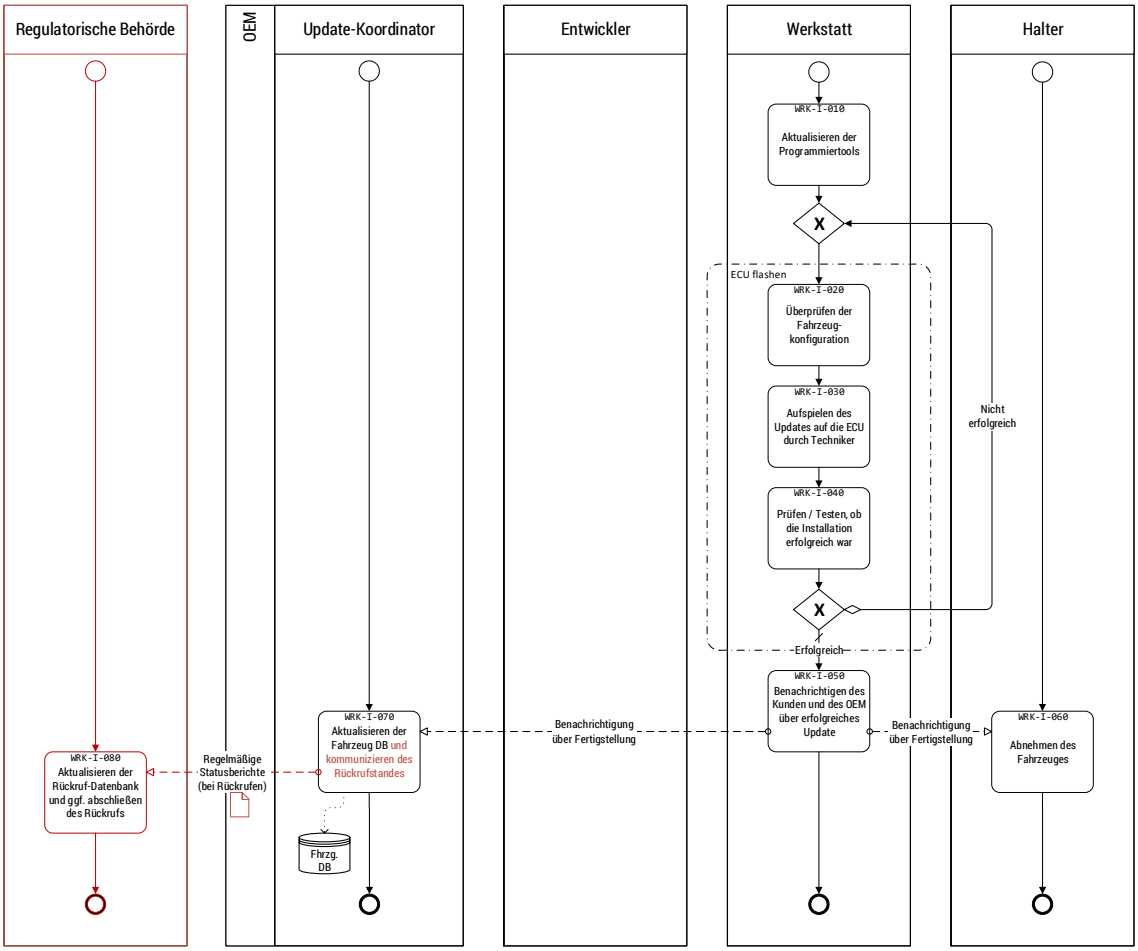


Abbildung 13: Werkstatt-Prozess "Installation"