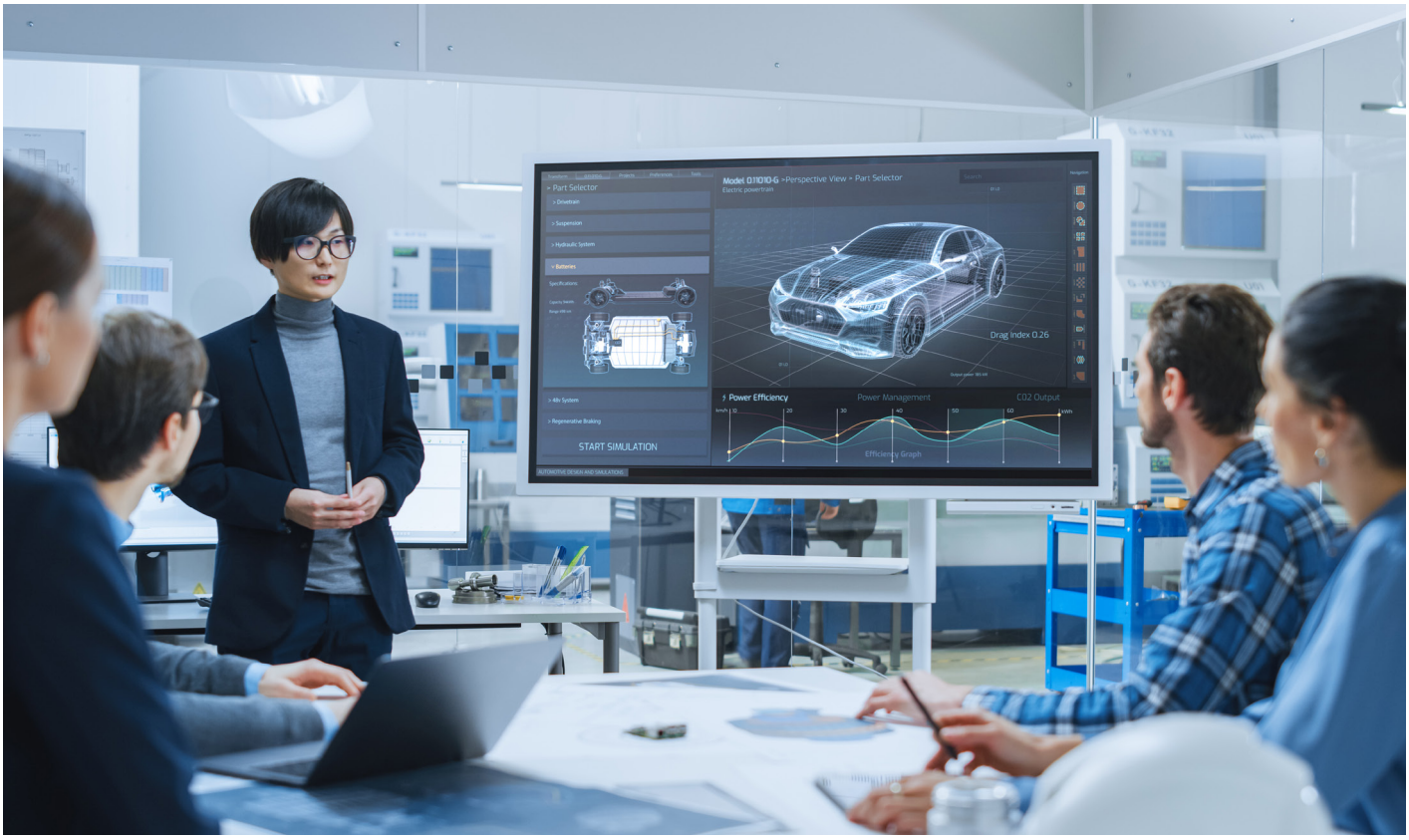
Deloitte.

Das Fahrzeug als mobiles Endgerät: Herausforderung „Software Update Management“

UNECE R156/Software Update Management System

Die neue Regulation UNECE R156 schreibt demnächst ein Software Update Management System für alle Fahrzeuge vor. Das hat für OEMs weitreichende Implikationen. Sie müssen jetzt auch die Perspektive eines Softwareherstellers einnehmen – und langfristig Margenerwartungen in den Aftermarket verschieben.

Es ist soweit: Die Arbeitsgruppe WP.29 der Vereinten Nationen hat die UNECE-Regulierungen R155 und R156 verabschiedet. R155 fordert ein Cyber Security Management System (CSMS) für den gesamten Fahrzeug-Lebenszyklus – darauf geht der *erste Beitrag der* „Point of View“-Reihe „Trusted Software“ ein. Im Fokus des vorliegenden Beitrags steht R156.



Diese Regulierung schreibt vor, dass in naher Zukunft für sämtliche Neufahrzeuge ein normgerechtes Software Update Management System (SUMS) aufgebaut und betrieben werden muss. Die Gesetzgeber reagieren damit auf die Tatsache, dass heutzutage immer mehr Fahrzeugfunktionen digital umgesetzt werden. Spätestens wenn die Elektronik im Auto eines Tages buchstäblich das Steuer übernimmt, wird die Relevanz der Software-Thematik für die Sicherheit im Straßenverkehr deutlich, und damit auch die Bedeutung der Pflege dieser Software durch Updates, z.B. im Sinne von Bugfixes oder Security-Updates bei identifizierten Schwachstellen. Die Regulation betrifft aber weit mehr als das autonome Fahren auf Level 5 (vollautomatisiertes Fahren, ohne Fahrer). Schon heute steuert Software viele Funktionen, vom Infotainment bis zu Fahrassistenzsystemen. Gleichzeitig erhöht der Trend zur Zentralisierung und Standardisierung der Fahrzeug-IT aber die Angriffsfläche für sicherheitsrelevante Cyber-Attacken, etwa auf ein „Over the Air“-Update über die Internet-Schnittstelle des Onboardsystems. Das SUMS-Thema ist also inhaltlich eng mit dem Komplex Cyber Security / CSMS verbunden.

Die Herstellung von SUMS-Compliance ist für OEMs vor diesem Hintergrund offensichtlich von kritischer Bedeutung. Dabei ist eine langfristige Perspektive nötig, denn nun liegt eine lebenslange Verpflichtung zur Software-Pflege vor – auch und gerade jenseits des Start of Production (SOP). Das folgt einerseits aus der gesteigerten Bedeutung der Software im Fahrzeug der Zukunft für die Sicherheit im alltäglichen Betrieb, andererseits auch schon aus der Natur von Software selbst, die durch Updates laufend verbessert und an neu entstandene Risiken, Kundenwünsche und IT-Entwicklungen angepasst werden muss. Dadurch entstehen neue Kostenrisiken über den gesamten Fahrzeug-Lebenszyklus. Zugleich liegt in einem effektiven Software-Management aber auch schon der Schlüssel zur Bewältigung dieser Risiken. Denn die für das SUMS nötige Technologie und Infrastruktur schafft für den OEM gleichzeitig das Fundament für die datengestützte Geschäftsmodelle der Zukunft, indem so die Erschließung neuer Gewinnpotenziale im Aftermarket ermöglicht wird. Voraussetzung dafür ist ein grundlegend gewandeltes Mindset der Hersteller – weg von einer statischen Betrachtungsweise, die auf den SOP und den reinen Fahrzeugverkauf konzentriert ist; hin zu einem Verständnis des Fahrzeugs als Smart Device, zu einer Fokussierung auf die damit verbundenen geschäftlichen Dimensionen. Das Fahrzeug befindet sich nun lebenslang in ständiger digitaler Weiterentwicklung: Innovative Geschäftsmodelle steigern den Umsatz, neue Bezahlformen schaffen kontinuierliche Cashflow-Ströme, Margen- bzw. Kostenrisiken müssen neu betrachtet und gerechnet werden.

Regeln, Normen, Handlungsfelder

Aktuell geht man davon aus, dass die neue SUMS-Regelung R156 ab 2022 für alle neuen Typzulassungen gilt und ab 2024 für alle Neufahrzeuge. Alle drei Jahre muss das SUMS auditiert werden. Ohne ein zertifiziertes SUMS ist die Typzulassung für ein Fahrzeug gefährdet, Fehler beim Update Management können auch nachträglich zu einem Verlust der Zulassung führen. Für OEMs ist es jetzt daher höchste Zeit, sich mit dem SUMS zu beschäftigen – auch wenn längst noch nicht alle regulatorischen Details festgezurrt sind. So ist die Ausgestaltung der Norm ISO 24089 noch nicht abgeschlossen, die eine wichtige Referenz für die Zertifizierung nach R156 darstellt. Die Situation wird aktuell durch den Umstand verschärft, dass der Zeitplan für R156 kurzfristig vorgezogen wurde und nun analog zu dem für UNECE R155 gilt. Die Experten von Deloitte beteiligen sich an der Gremienarbeit und richten ihr Augenmerk dabei verstärkt auf die technische Dimension. Derzeit startet auch das Kraftfahrt-Bundesamt (KBA) mit den ersten Typzulassungen. Parallel sind nun die OEMs gefordert, die existierenden Übergangsphasen zu nutzen und vorbereitende Maßnahmen zu treffen.

Bei der Entwicklung der Software und dem Release Management ist die Nachverfolgbarkeit (Traceability) aller Versionen ein zentraler Aspekt. Dafür ist u.a. auch eine saubere Handhabung der RXSWIN-Nummerierung, als ein möglicher eindeutigen Identifier, notwendig, durch die eine spezifische Software für ein System mit Typzulassung mit Bezug auf eine Regulation X identifiziert wird. Generell stehen OEMs nun vor der Herausforderung, den Schritt vom Hardware- zum Software-Hersteller bewusst zu vollziehen, was ein Umdenken in vielen Bereichen erforderlich macht. Allzu oft wird Software noch wie Hardware behandelt, dem Steuergerät zugeordnet und nicht unter dem Aspekt software-spezifischer Merkmale betrachtet, z.B. in der Beschaffung. Dabei weist sie ganz eigene Charakteristika auf, etwa im Hinblick auf die spezifische Qualitätsprüfung, Logistik und Skalierungsweise im Vergleich zu Hardware. Entsprechende spezifische Kennzahlen und KPIs sind folgerichtig auch software-spezifisch aufzubauen. Die Update-Thematik kompliziert sich noch weiter, wenn es sich um dringende Maßnahmen handelt. Insbesondere bei schweren Zwischenfällen oder Sicherheitslücken muss gegebenenfalls rasch mit Updates reagiert werden – hierfür müssen priorisierte Prozesse eingerichtet werden. Es darf dabei nicht unterschätzt werden, wie personalintensiv die Entwicklung von Software ist. Bei einem typischen großen traditionellen OEM können z.B. allein für den Bereich Infotainment zwischen 2000-3000 Mitarbeiter tätig sein. Anders sieht das teilweise bei neuen Wettbewerbern aus, die von vorneherein digital aufgestellt sind, keine Legacy-Systeme berücksichtigen müssen, einer echten Software-Zentrierung folgen und daher auf ihr Entwicklungsziel hinarbeiten können. Diese Wettbewerber stellen Referenzen im Bereich der Software-Entwicklung dar. Der Grad der eigenen Software-Zentrierung ist daher idealerweise zu erhöhen.

SUMS hat auch erhebliche Auswirkungen auf das Management der Lieferkette. Der Einkaufsbereich sollte angesichts des zunehmenden Softwareanteils an der Fahrzeug-Wertschöpfung eine neue Perspektive einnehmen, etwa bei der Lieferantenauswahl für Software. Ist der jeweilige Zulieferer überhaupt in der Lage, regulatorisch konform zu arbeiten? Da die Verantwortung für zugekaufte Software beim OEM liegt, muss die SUMS-Compliance der Zulieferer gründlich und kontinuierlich kontrolliert werden. Ein Vertragspassus allein ist hier nicht ausreichend, es sind spezifische Maßnahmen und Nachweise zu vereinbaren und festzulegen. Auch im Hinblick auf Bugfixes und reguläre Software-Updates ist in der Supply Chain durch den Software-Fokus eine wesentlich engere prozessuale Verzahnung zwischen OEMs und der Kaskade der Lieferkette erforderlich. Komplementär dazu müssen sich auch die Zulieferer proaktiv auf die Erfordernisse des SUMS vorbereiten, wenn sie im Sinne der Regulatorik sicher lieferfähig bleiben und vor allem ihre Produktentwicklung mit einem hohen Differenzierungsgrad für eine breite Kundenlandschaft wirksam steuern wollen. Wenn mehrere OEMs beliefert werden, macht das eventuell komplexe Differenzierungen nötig. Entwicklungsprozesse bei Zulieferern müssen agiler werden und einer schnelleren Taktung folgen; bei Verstößen z.B. bei Lieferterminen (auch bei Updates) drohen Strafzahlungen. Umso wichtiger ist eine klare Definition von Rollen und Verantwortlichkeiten vor allem während der Betriebsphase, wenn Software-Updates in der Flotte nach SOP zur Regel werden.

Die zu bearbeitenden Handlungsfelder für das SUMS sind vielfältig und anspruchsvoll. Beispielsweise sind das Vorhalten eines Verzeichnisses verbauter Hardware und installierter Software jedes Fahrzeugs (Asset Management) und die Möglichkeit Software-Updates vor Freigabe umfassend abzusichern (z.B. anhand eines digitalen Zwillings) wesentliche Voraussetzungen für ein zuverlässiges SUMS. Damit ein SUMS überhaupt in der Lage ist, zeitnah die Behebung von Fehlern oder Sicherheitslücken zu unterstützen, ist eine umfassende und permanente Überwachung der Fahrzeugflotte erforderlich. Ohne diese Voraussetzung verliert ein SUMS viel des Nutzens und der Sicherheit für die Fahrzeug-Nutzer. Ein weiterer Beitrag zur Komplexität ist die Tatsache, dass OEMs meist nur einen Bruchteil der Software im Fahrzeug selbst entwickelt haben, d.h. ohne Lieferanten auch keine Updates zu Verfügung stellen können. Hier muss die Lieferfähigkeit der betreffenden Lieferanten vertraglich und organisatorisch gesichert werden.

Es wäre falsch, die nötigen Maßnahmen lediglich als lästige Pflicht einzuordnen. Im Gegenteil - Unternehmen sollten den geforderten Aufbau von SUMS-Prozessen sowie einer komplexen Infrastruktur unmittelbar für produktive Zwecke nutzen und so aus der „Not“ eine Tugend machen. So kann beispielsweise ohne SUMS kein zuverlässiges Level bei der Cyber Security von Fahrzeugen erzielt werden. Effizienteres Lizenz-Tracking (Asset-Management) unterstützt außerdem die Kosteneinsparung, etwa bei Veränderungen im Status von Free Ware oder Open Source Code, deren Lizenz nun kostenpflichtig wurde oder anderweitig die Lizenzbedingungen angepasst wurden. Ein umfassendes und robustes Safety-Konzept ist die Basis für eine positive Bewertung bzgl. Haftungsrisiken für den Hersteller. Ebenso ist es möglich den Zollwert eines Fahrzeuges mittels des „digitalen Zwillings“ und dem für SUMS notwendigen Asset Managements und der damit verbundenen Nachweisbarkeit der Software- und Hardware-Konfiguration zuverlässig zu berechnen.

Regulatorischer Prozess und praktische Umsetzung

Für die erfolgreiche Zertifizierung des SUMS und die Durchführung von Software-Updates ist eine umfassende Dokumentation aller Maßnahmen notwendig. Dabei muss fortlaufend sichergestellt werden, dass Dokumentation und Implementierung übereinstimmen. Der regulatorische Prozess folgt einer strikten Logik: Der OEM baut ein zertifiziertes SUMS auf, das eine Qualitätskontrolle, eine zuverlässige Ausführung der Updates und ausreichende Cyber Security gewährleistet. Bei einem neuen Update beurteilt der OEM, ob Zertifizierungskriterien des SUMS oder der Typzulassung des betroffenen Fahrzeugtyps berührt sind. Abhängig davon muss u.U. eine Ausweitung der Zertifizierung des SUMS oder der Typzulassung durch die Zulassungsbehörde erfolgen, bevor der OEM die Sicherheit des Updates verifiziert (Safety und Security) und dann das Update bereitstellt. Da Fahrzeuge in Regionen mit unterschiedlichen Anforderungen und Verfahren für die Typzulassungen unterwegs sind, sind entsprechende Überprüfungen für alle betroffenen Regionen weltweit erforderlich und – für Fälle späterer Nachfragen oder Untersuchungen – umfassend zu dokumentieren.

Bei der Umsetzungsplanung des SUMS macht sich eine umfassende Betrachtung bezahlt, bei der entlang der Zeitachse die Interaktion mit der Lieferkette und Update-Verpflichtungen jenseits des SOP ebenso wie die dadurch ermöglichten neuen Geschäftsmodelle gestaltet werden.

Schon beim Architekturdesign muss die Update-Fähigkeit berücksichtigt – d.h. technische SUMS-Compliance sichergestellt werden. Standardisierte Hardware-Plattformen erleichtern dies und schaffen zugleich die Voraussetzungen für das Ausrollen digitaler Geschäftsmodelle. Das Konzept des digitalen Zwillings unterstützt

Schon beim Architekturdesign muss die Update-Fähigkeit, d.h. technische SUMS-Compliance sichergestellt werden.

die Testbarkeit und Wartbarkeit von Software. Die Qualitätssicherung in der Entwicklung von Software wird durch weitere Maßnahmen unterstützt: Code Audits, eine Testdatenbank, ein Software-Repository (mit getesteten und für die Entwicklung freigegebenen Software-Artefakten) und License Checks sind Ansätze dafür. Dabei kommen auch spezielle digitale Tools zum Einsatz. Deloitte hat z.B. für das License Testing einen Scanner entwickelt und bietet automatisiertes Testen von Quellcode als managed Service an.

Für Updates nach dem SOP erfordert das SUMS ein umfassendes Vehicle Asset Management, in dem erfasst wird, welche Hardware und Software im jeweiligen Fahrzeug vorhanden sind bzw. sein sollten, sowie ein kontinuierliches Fleet Monitoring der gesamten Flotte im Feld. Der aus der Entwicklung vordefinierte Rahmen für das Asset Management wird in der Produktion jedes einzelnen Fahrzeugs mit den (Stamm) Daten zu dessen Hard- und Software-Ausstattung befüllt und im weiteren Verlauf des Fahrzeug-Lebenszyklus inhaltlich fortgeführt und aktuell gehalten. Die fortwährende Analyse von (Bewegungs)Daten aus den im Betrieb befindlichen Fahrzeugen, dem Backend und externen Daten (z.B. aus Internet und Social Media) ergibt – intelligent zusammengeführt - ein Bild zur aktuellen Cyber-Bedrohungslage einzelner Fahrzeuge, Fahrzeugtypen und in der weiteren Analyse der gesamten Flotte. Bei definierten Triggern löst das Monitoring dann einen sogenannten Cyber-Incident aus und veranlasst entsprechende Analysen und die Einleitung geeigneter Maßnahmen. Die Datenanalysen können aber auch Hinweise auf Hard- oder Software-Probleme in Fahrzeugen liefern, die nicht auf Cyber Security Incidents zurückzuführen sind, sondern auf Qualitätsprobleme (einzelner Fahrzeuge, bestimmter Teile-Chargen oder Software-Versionen etc.) hinweisen. Auf diesen Informationen kann eine vorausschauende Wartung der Fahrzeugflotte aufgebaut werden, die darauf ausgerichtet ist, Qualitätsprobleme (und Kosten) rasch zu beseitigen oder erst gar nicht entstehen zu lassen.

Verträge mit Lieferanten – insbesondere für Fahrzeug-Software - als auch Verträge mit Kunden müssen den neuen Pflichten und Geschäftschancen im Aftermarket Rechnung tragen und neu ausgestaltet werden. Auf der Lieferantenseite ist insbesondere die Update-Verpflichtung während des gesamten Fahrzeug-Lebenszyklus in das Kalkül einzubeziehen und die Lieferfähigkeit sicherzustellen (Anpassung der Vertragslaufzeit und Ergänzung um Update-Verpflichtungen und Update-Fähigkeit sowie ggf. Reaktionszeiten im Falle eines Incidents). Updates werden in Zukunft verstärkt „over the air“ (OTA) stattfinden, dennoch bleibt der OEM für Updates weiterhin auch auf eine Zusammenarbeit mit Werkstätten angewiesen.

Auf der Kundenseite sind die Update-Verpflichtungen in die bestehenden Vertrags- und Garantiebedingungen einzubetten. Hier kann über attraktive Angebote zur funktionalen Weiterentwicklung eines im Markt befindlichen Fahrzeugs auch der Grundstein für neue Geschäftsmodelle gelegt werden (z.B. über Premium-Serviceverträge, die automatisch funktionale Weiterentwicklungen enthalten). Hinweis: für verpflichtende Updates im Sinne von Bugfixes können keine Wartungsgebühren verlangt werden. Ein wesentliches Thema auf der Kunden-Vertragsseite ist der Datenschutz. Hier ist Transparenz und Offenheit gefragt: es ist immer besser, Daten im Zweifelsfall nicht/ nicht in vollem Umfang zu nutzen, als am Ende das Vertrauen der Kunden zu verlieren. Jedem Kunden muss klar sein, wie und in welchem Umfang Daten aus seinem Fahrzeug genutzt werden, inwiefern diese personalisiert sind und wie er diese Datennutzung mit seinem Einverständnis unterstützen (Consent) oder eben unterbinden kann. Es muss klar sein, welche Daten der OEM auch ohne Einverständnis (nicht personalisiert) nutzen kann, um z.B. die Aufgabe des Fleet-Monitorings erfüllen zu können und welche Vorteile Kunden haben, wenn sie weitere Daten zur Verfügung stellen. Nutzung und Weitergabe von Daten müssen klar geregelt sein und Kunden müssen mit kurzen Antwortzeiten erfahren können, welche Daten von ihnen aktuell gespeichert sind sowie welche Möglichkeiten sie haben, diese dokumentiert löschen zu lassen.

Bei all diesen Aspekten stellt sich die Frage nach der Zeitspanne für zugesicherte Updates. Hierbei könnte eine praktische Lösung darin liegen, gegenüber dem Fixpunkt „End of Life“ (EOL) einen Endtermin des gewährten Update-Servicelevels zu differenzieren („End of Service“, EOS). Vergleichbar zu den Software-Updates bei Computer- bzw. Smartphone-Betriebssystemen ist nämlich davon auszugehen, dass auch bei Fahrzeugen Software-Updates nur für eine bestimmte Zeit verfügbar gemacht werden können, da die verbaute Hardware gegebenenfalls den Anforderungen neuer Updates nicht mehr gewachsen ist und die Kosten für die weitere Aktualisierung eines alten Systems unverhältnismäßig ansteigen. Vorstellbar wären hier beispielsweise ein stufenweiser Ausstieg aus der Updateverpflichtung bei Altsystemen. Möglich wären dabei die Einführung einer jährlichen Wartungspauschale und die Beschränkung auf Updates nur noch bei großen Risiken, z.B. zeitlich zusammengefasst auf zwei Updates pro Jahr. Alternativ kommt eine (kostenpflichtige) Hardware-Aufrüstung in Frage, die eine verlängerte Wartungszusage mit sich bringt. Eine weitere Option wäre die Auslagerung der Wartung an Drittanbieter, die dann (wie von IT-Systemen bekannt) die Wartungsaufgabe gegen Entrichtung einer Wartungspauschale übernehmen. Es zeigt sich dabei, dass ein wesentlicher Gesichtspunkt der Software- und Update-Strategie die Erschließung von neuen Umsätzen sein muss, da ansonsten das gesamte Geschäftsmodell der OEMs unter den neuen digitalen Vorzeichen gefährdet sein könnte.

Das Geschäft der Zukunft

Im Software Update Management müssen Unternehmen hohen Aufwand beim Aufbau des Systems betreiben und generell durch die (regulatorische) Verpflichtung zu lebenslangen Updates höhere Kostenrisiken einkalkulieren. Bei R156 und R155 handelt es sich dabei sozusagen nur um den Anfang; weitere Regulationen werden folgen. Dem steht die große Chance gegenüber, die sich mit Softwarebasierten Geschäftsmodellen im Aftermarket eröffnet. Während die Margen aus dem Fahrzeugverkauf tendenziell erodieren, beginnt in Zukunft für immer mehr OEMs das eigentliche Geschäft erst nach dem SOP bzw. nach dem Verkauf jedes einzelnen Fahrzeugs. Durch Hardwarevorhalte (Einbau von leistungsfähigerer Hardware, als im aktuellen Fahrzeug erforderlich sowie Einbau hardwareseitiger Funktionsvoraussetzungen (z.B. Zusatzdisplays oder Kameras), unabhängig davon, ob sie als Zusatzausstattung geordert wurden, oder nicht) schaffen sie die Möglichkeit späterer Upgrades und Zusatzverkäufe und sparen dabei durch diese Vereinheitlichung der Hardware-Varianten zugleich Kosten. Die oben beschriebene Daten- und SUMS-Infrastruktur wird immer effektiver zur Vermarktung datengetriebener Angebote genutzt. Unkritische Funktionen migrieren zunehmend in die Cloud, um die Rechenleistung im Fahrzeug zu optimieren. Neben einmaligen Käufen treten dabei verstärkt Abomodelle, Service-Verträge und Premium-Dienste auf. Auch Zulieferer erhalten attraktive Möglichkeiten, ihre eigenen Angebote lukrativ einzubringen, wovon dann auch der OEM als Betreiber der Plattform (des Fahrzeugs) profitiert. Dabei helfen Plattformen der Hersteller, über die z.B. auf Apps von Dritten zugegriffen werden kann. Eine digitale Community lässt auch die Kunden als entscheidende Stakeholder aktiv an den digitalen Möglichkeiten teilhaben und erhöht die Markenbindung.

Diese weitreichenden Chancen stellen potenziell viel mehr als nur eine Kompensation der neuen Kostenrisiken durch langjährige Software-Updates dar. Wenn OEMs die Software-Thematik geschickt spielen, ist eine Verbesserung von Margen und Gewinnen gegenüber dem heutigen Status quo zu erzielen. Die wichtigste Voraussetzung dafür ist aber nicht technologischer, sondern „kultureller“ Natur: ein gewandeltes Bewusstsein. Denn während Automobile ständig digitaler und flexibler werden, verändert sich zugleich das Verständnis dessen, was ein Automobil eigentlich ist: nicht mehr ein abgeschlossenes Produkt, sondern ein Smart Device, eine Plattform für Services und Produkte, die über das traditionelle Angebot der Hersteller weit hinausgehen. Wir befinden uns somit mitten in einem fundamentalen Umbruch der Sichtweise auf das Fahrzeug, dessen gezielte Gestaltung vorausschauenden OEMs ungeahnte neue Möglichkeiten eröffnet.

Während Automobile ständig digitaler und flexibler werden, verändert sich zugleich das Verständnis dessen, was ein Automobil eigentlich ist: kein abgeschlossenes Produkt sondern ein Smart Device.

Kontakte

Andreas Herzig
Partner
Automotive Lead Risk Advisory
Tel: +49 (0)711 16554 7160
aherzig@deloitte.de

Anke Guderian
Director | Risk Advisory
Automotive Software Governance
Tel: +49 (0)89 29036 6212
aguderian@deloitte.de

Deloitte.

Stand 04/2021