TECHNISCHE UNIVERSITÄT WIEN

# Diplomarbeit

## UNECE Regelung 156 zu Software-Update Managementsystemen: Integration der Anforderungen in einem Prüfkatalog und die Bedeutung für die Kunden-Lieferanten Schnittstelle.

ausgeführt zum Zwecke der Erlangung des akademischen Grades eines

## Diplom-Ingenieurs

unter der Leitung von

**Univ.-Prof. Dr.-Ing. Dipl.-Ing. Sebastian Schlund**
(E330 Institut für Managementwissenschaften, Bereich: Betriebstechnik und Systemplanung)

**Univ.-Ass. Dipl.-Ing. Fabian Holly B.Sc.**
(E330 Institut für Managementwissenschaften, Bereich: Betriebstechnik und Systemplanung, Fraunhofer Austria Research GmbH)

eingereicht an der Technischen Universität Wien

**Fakultät für Maschinenwesen und Betriebswissenschaften**

von

**Daniel Breschan**

01461402

[redacted]

[redacted]

Wien, im Februar 2022

Daniel Breschan

Ich habe zur Kenntnis genommen, dass ich zur Drucklegung meiner Arbeit unter der Bezeichnung

# Diplomarbeit

nur mit Bewilligung der Prüfungskommission berechtigt bin.

Ich erkläre weiters Eides statt, dass ich meine Diplomarbeit nach den anerkannten Grundsätzen für wissenschaftliche Abhandlungen selbstständig ausgeführt habe und alle verwendeten Hilfsmittel, insbesondere die zugrunde gelegte Literatur, genannt habe.

Weiters erkläre ich, dass ich dieses Diplomarbeitsthema bisher weder im In- noch Ausland (einer Beurteilerin/einem Beurteiler zur Begutachtung) in irgendeiner Form als Prüfungsarbeit vorgelegt habe und dass diese Arbeit mit der vom Begutachter beurteilten Arbeit übereinstimmt.

Wien, im Februar 2022

Daniel Breschan

# Danksagung

An dieser Stelle möchte ich mich bei all denjenigen bedanken, die mich im Laufe der vergangenen Monate unterstützt und damit zur Fertigstellung dieser Diplomarbeit beigetragen haben.

Bedanken will ich mich zunächst bei Univ.-Prof. Dr.-Ing. Dipl.-Ing. Sebastian Schlund vom Institut für Managementwissenschaften der TU Wien dafür, dass ich diese Arbeit in seinem Fachbereich für Betriebstechnik und Systemplanung verfassen durfte.

Bei Univ.-Ass. Dipl.-Ing. Fabian Holly bedanke ich mich für die hervorragende Betreuung der Arbeit. Seine Anregungen und seine konstruktive Kritik waren bei der Erstellung dieser Arbeit stets hilfreich.

Ein besonderer Dank gebührt zudem Dr.-Ing. Wolfgang Walter von der EFS Unternehmensberatung GmbH. Ohne seine fortlaufende Unterstützung wäre diese Arbeit nie zustande gekommen. Im Zuge dessen möchte ich mich auch bei allen weiteren Kollegen der EFS Unternehmensberatung GmbH für ihre Unterstützung beim Verfassen dieser Arbeit bedanken, insbesondere bei Herrn Michael Bereczuk.

Ebenfalls bedanke ich mich bei meiner Freundin und allen Freunden für den starken Rückhalt über die Dauer meines gesamten Studiums.

Abschließend möchte ich mich bei meinen Eltern bedanken, die mir mein Studium durch ihre Unterstützung ermöglicht haben und stets ein offenes Ohr für mich hatten.

# Gender Erklärung

Aus Gründen der besseren Lesbarkeit wird in dieser Diplomarbeit die Sprachform des generischen Maskulinums angewendet. Es wird an dieser Stelle darauf hingewiesen, dass die ausschließliche Verwendung der männlichen Form geschlechtsunabhängig verstanden werden soll.

# Kurzfassung

Die zunehmende Anzahl an Datenschnittstellen und der große Softwareanteil in Fahrzeugen erhöhen zusehends die Angriffsfläche für sicherheitsrelevante Cyber-Attacken. Die Gesetzgeber reagieren darauf, indem neue Regularien erlassen werden. Dazu zählt die Anfang 2021 von der UNECE verabschiedete Regelung Nummer 156 zu Software-Update Managementsystemen (SUMS). Sie stellt die erste gesetzlich verpflichtende Grundlage zur Implementierung einer zentralen Kontrolleinheit für Software-Updates bei Fahrzeugherstellern dar.

Während die Regelung einen Anhaltspunkt zur Umsetzung der Anforderungen im Unternehmen bildet, bleibt sie mit ihren konkreten Ausführungen vage. Es besteht daher der Wunsch nach einer Möglichkeit zur Überprüfung der Vollständigkeit, Angemessenheit und Wirksamkeit der angestrebten Lösung. Eine solche Möglichkeit stellen Prüfkataloge dar. Sie sehen die Ausarbeitung eindeutiger und objektiv zu bewertender Prüfkriterien vor. Damit ermöglichen sie eine kosteneffiziente Vorbereitung auf Zertifizierungen.

In der vorliegenden Arbeit wird daher ein Prüfkatalog entwickelt, der Unternehmen bei der Konzeption, Implementierung und Aufrechterhaltung eines Software-Update Management Systems unterstützt. Basis für die Entwicklung des Prüfkatalogs sind einerseits verschiedene Normen, Standards und Empfehlungen mit Bezug zu Software-Updates und Informationssicherheit. Daneben bilden bereits bestehende Prüfkataloge zur Informationssicherheit die Grundlage zur Entwicklung einer Struktur und für den Aufbau des Prüfkatalogs zu SUMS.

Zur Validierung wird der entwickelte Prüfkatalog mehreren Informationssicherheits-experten der österreichischen EFS Consulting GmbH vorgelegt. Nach umfassender Prüfung des Katalogs erfolgt eine Bewertung durch die Experten mithilfe der System Usability Scale (SUS) Methode. Diese ergab eine hohe Gebrauchstauglichkeit des Prüfkatalogs für die Anwendung in Unternehmen. Die Verwendung des Prüfkatalogs ermöglicht somit eine effiziente Vorbereitung auf eine Zertifizierung gemäß UNECE Regelung Nr. 156 zu Software-Update Managementsystemen.

Die Tatsache, dass Softwaresysteme häufig von unterschiedlichen Lieferanten entwickelt und zugekauft werden, stellt eine weitere Herausforderung dar. Unter anderem mithilfe eines Experteninterviews wird daher im Rahmen der Arbeit die Bedeutung der Regelung für die Kunden-Lieferanten Schnittstelle untersucht. Dabei zeigt sich, dass zumindest jene Lieferanten zur Einhaltung der Regelung vertraglich verpflichtet werden sollten, die den Fahrzeughersteller mit sicherheitskritischen Bauteilen versorgen.

# Abstract

The growing number of data interfaces and the large amount of software in vehicles are constantly increasing the attack surface for security-related cyber incidents. Legislators are responding to this by enacting new regulations. These include Regulation number 156 on Software Update Management Systems (SUMS) which was adopted by the UNECE at the beginning of 2021. It represents the first legally binding regulation for the implementation of a central control unit for software updates at automotive manufacturers.

While the regulation provides a reference for implementing the requirements in the company, it remains vague with its concrete explanations. Companies therefore strive for a possibility to check the sufficiency, appropriateness and effectiveness of their intended solution. Such a possibility is usually represented by various test catalogs. They provide for the elaboration of unambiguous and objectively assessable test criteria and thus enable cost-efficient preparation for certifications.

In this thesis a test catalog is developed to support companies in the design, implementation and maintenance of a Software-Update Management System. The focus is on the operationalization of the requirements from the UNECE regulation. This includes the presentation of the concrete requirement goal and potential requirement proofs. The basis for the development of the test catalog are, on the one hand, various norms, standards and recommendations related to software updates and information security. On the other hand existing test catalogs for information security were used for the development of a structure of the test catalog for Software-Update Management Systems.

For validation purposes the test catalog is presented to information security experts from the Austrian company EFS Consulting GmbH. After a comprehensive review of the catalog, the experts evaluated it by using the System Usability Scale (SUS) method. The results show that the test catalog is highly suitable for the use in companies. It thus enables efficient preparation for certification in accordance with the UNECE Regulation No. 156 on Software-Update Management Systems.

The fact that software systems are often developed and purchased from different suppliers poses a further challenge. The significance of the regulation for the customer-supplier interface is therefore examined in this thesis with the help of an expert interview. The results of the analysis show that at least those suppliers who are in charge of safety-critical components should be contractually obligated to comply with the regulation.

# Inhaltsverzeichnis

# 1 Einleitung

Die Automobilindustrie befindet sich in einer Zeit radikalen technologischen Wandels. Getrieben durch die Digitalisierung rücken kundenzentrierte Mobilitätsdienste und Elektromobilität in den Fokus des Autokäufers und bestimmen zusehends den Erfolg von Automobilherstellern.[1] Bereits heute verbauen die Hersteller bis zu 150 Steuergeräte mit rund 100 Millionen Zeilen an Softwarecode je Fahrzeug. Experten gehen davon aus, dass sich diese Zahl bis 2030 auf rund 300 Millionen Zeilen verdoppeln wird.[2] Infolgedessen entwickeln sich die Automobilhersteller zu Technologieunternehmen, die digitale Dienstleistungen mit ihren Fahrzeugen bereitstellen.[3] Zusätzlich vorangetrieben wird diese Entwicklung durch die fortschreitende Autonomisierung von Fahrzeugen, deren zentrale Bestandteile Software- und Elektronikkomponenten bilden.[4]

## 1.1 Ausgangssituation und Einführung in das Themengebiet

In Anbetracht der zunehmenden Menge an Software, die in einem Auto installiert ist, nimmt auch die Bedeutung der Pflege der Software zu. Dies geschieht durch Updates, z.B. im Sinne von Bugfixes oder Security Updates bei identifizierten Schwachstellen.[5] Handelt es sich dabei um Aktualisierungen für sicherheitskritische Fahrzeugfunktionen, wie etwa jene die die Motorsteuerung betreffen, war bis dato ein Aufenthalt in der Werkstatt eines Fahrzeughändlers meist unumgänglich. Im Sinne einer verbesserten Kundenzufriedenheit und einer erheblichen Kostensenkung streben viele Automobilhersteller nach der Möglichkeit, die Updates auch Over-the-Air (OTA) anzubieten, also ohne erforderlichen Werkstattaufenthalt.[6]

Diese vernetzten, digitalen Funktionen eröffnen den Autobauern neue Pfade zu Innovation und Wachstum, die gerade in der derzeitigen Umbruchssituation der Branche von großer Bedeutung sind. Zugleich erhöhen die vielen Datenschnittstellen und der große Softwareanteil die Angriffsfläche für sicherheitsrelevante Cyber-Attacken zusätzlich.[7] Automobilhersteller müssen dementsprechend dafür sorgen, dass die Fahrzeugsicherheit nicht durch mangelnde Datensicherheit beeinträchtigt

[1] Vgl. Liu (2019), S. 38.
[2] Vgl. Burkacky et al. (2020), S. 6.
[3] Vgl. Liu (2019), S. 38f.
[4] Vgl. Burkacky et al. (2020), S. 4ff.
[5] Vgl. Herzig und Guderian (2021), S. 2.
[6] Vgl. Wind River Systems, Inc. (2017), S. 3.
[7] Vgl. Dassow, Herzig und Guderian (2021), S. 2f.

wird und dass das Fahrzeug vor Manipulation geschützt ist.[8] Darüber hinaus gilt es Haftungsrisiken zu minimieren, Reputationsschäden zu vermeiden und das Ausrollen neuer Daten-getriebener Geschäftsmodelle nicht zu gefährden.[9] Technisch, organisatorisch wie auch regulatorisch stellen kontinuierliche und sichere Software-Updates eine Herausforderung für die Automobilindustrie dar.[10]

## 1.2 Motivation und Problemstellung

Die Tatsache, dass immer mehr Fahrzeugfunktionen digital umgesetzt werden, macht die Relevanz der Software-Thematik für die Sicherheit im Straßenverkehr deutlich. Die Gesetzgeber reagieren darauf, indem neue Regularien erlassen werden. Anfang 2021 hat eine Arbeitsgruppe der Vereinten Nationen die UNECE-Regulierungen R155 und R156 verabschiedet. Während R155 ein Cyber Security Management System (CSMS) für den gesamten Fahrzeug-Lebenszyklus fordert, schreibt die Regulierung R156 den Aufbau und Betrieb eines zertifizierten Software Update Management System (SUMS) vor. Verpflichtend sind die Vorgaben ab Juli 2022 für alle neuen Fahrzeugtypen, ab Juli 2024 dann für sämtliche Neufahrzeuge, die in den knapp 60 Mitgliedsstaaten der UNECE zugelassen werden. Viele Fahrzeughersteller sind auf diese Neuerungen noch nicht ausreichend vorbereitet. Insofern besteht akuter Handlungsbedarf, um regulatorische Compliance zu gewährleisten.[11]

Gegenstand dieser Arbeit ist die UNECE Regelung R156 (SUMS). Sie sieht einheitliche Bestimmungen für die Genehmigung von Kraftfahrzeugen hinsichtlich der Softwareaktualisierung und des Softwareaktualisierungsmanagementsystems vor.[12] Während die Regelung der UNECE einen ersten organisatorischen Rahmen festlegt, bleibt sie mit ihren konkreten Anforderungen dennoch vage. Abgesehen von allgemein verfassten Mindestanforderungen an die Automobilhersteller bietet sie keine detaillierte Anleitung für die betrieblichen Praktiken innerhalb des Unternehmens.[13] Insbesondere die derzeit (November 2021) noch ausstehende Ausgestaltung der Norm ISO/SAE 24089 (Road vehicles – Software update engineering), die eine wichtige Referenz für Zertifizierungen nach R156 darstellt, verschärft die Situation weiter.[14] Im Zuge dieser Arbeit soll daher ein Prüfkatalog entwickelt werden, der Unternehmen bei der Konzeption, Implementierung und Aufrechterhaltung eines Software-Update Managementsystems unterstützt.

[8] Vgl. https://www.embeddedcomputing.com/application/automotive/automotive-ecus-architecture-considerations-to-implement-secure-software-updates-over-the-air (Gelesen am: 01.10.2021)
[9] Vgl. Dassow, Herzig und Guderian (2021), S. 3.
[10] Vgl. Römer, Kreyenberg und Großmann (2018), S. 6.
[11] Vgl. Dassow, Herzig und Guderian (2021), S. 2f.
[12] Vgl. Herzig und Guderian (2021), S. 4.
[13] Vgl. Burkacky et al. (2020), S. 13.
[14] Vgl. Herzig und Guderian (2021), S. 3.

Neben diesem grundsätzlich bestehenden Problem stellt die Tatsache, dass Softwaresysteme häufig von unterschiedlichen Lieferanten entwickelt und zugekauft werden, eine weitere große Herausforderung dar.[15] Die Verantwortung für zugekaufte Software liegt beim Original Equipment Manufacturer (OEM), angesichts dessen muss die SUMS-Compliance der Zulieferer gründlich und kontinuierlich geprüft werden.[16] Die konkrete Bedeutung der Regelung für die Kunden-Lieferanten Schnittstelle ist vielen Unternehmen allerdings nach wie vor unklar und soll deswegen ebenfalls in dieser Arbeit diskutiert werden.

## 1.3 Aufbau und Struktur der Arbeit

Die Entwicklung und Gestaltung des Prüfkatalogs erfordern ein methodisch-strukturiertes Vorgehen. Dazu bieten sich verschiedene Forschungsmodelle aus dem Bereich der sogenannten Design Science Research an. Diese Modelle zielen darauf ab, neue Ergebnisse durch einen praxisnahen Forschungsansatz zu entwickeln und nutzbar zu machen. In den vergangenen Jahren sind eine Reihe dieser Leitlinien entwickelt worden, die alle zum Ziel haben, Wissenschaftler beim gestaltungsorientieren Forschungsprozess zu unterstützen. Zu diesen zählt auch ein vierstufiger Erkenntnisprozess von Österle und Otto, der sich durch seine leichte Verständlichkeit sowie Umsetzbarkeit auszeichnet und deswegen in dieser Arbeit zur Anwendung kommt.[17]

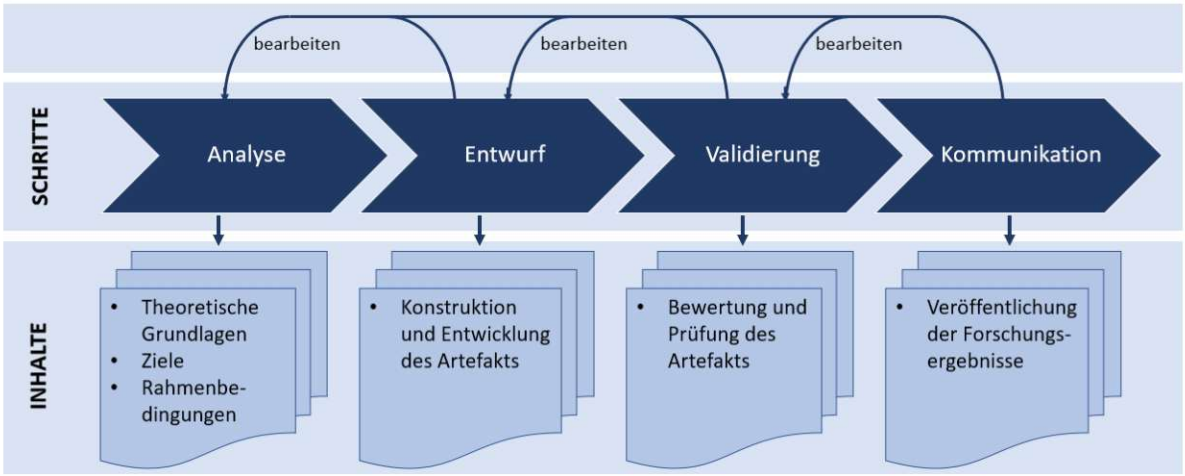



**Abbildung 1: Vierstufige Forschungsmethode[18]**

Vorrangiges Ziel der designorientierten Forschungsmethode von Österle und Otto ist es, wissenschaftlich fundierte und praktisch relevante Ergebnisse zu liefern. Sie folgen dazu dem in Abbildung 1 dargestellten Vier-Phasenmodell. Anstelle der Evaluation

[15] Vgl. Wind River Systems, Inc. (2017), S. 3.
[16] Vgl. Herzig und Guderian (2021), S. 3.
[17] Vgl. Brenner-Wickner, Kneuper und Schlömer (2020), S. 4ff.
[18] Quelle: Eigene Darstellung in Anlehnung an Brenner-Wickner, Kneuper und Schlömer (2020), S. 6.

findet in dieser Diplomarbeit in der dritten Phase die Validierung des entwickelten Prüfkatalogs statt. Angesichts des begrenzten Zeitraums für die Erstellung der Arbeit wird zudem Phase 4 – Diffusion – durch Kommunikation der Forschungsergebnisse ersetzt. Diese erfolgt im Rahmen der Präsentation der Diplomarbeit.

Die Analysephase beginnt meist mit einer ersten vagen Idee zu einem Forschungsthema und endet mit einem fundierten Überblick zu diesem Themengebiet, inklusive konkreter Definition der Ziele und Rahmenbedingungen. In der Entwurfsphase kommen bewährte Techniken für die Konstruktion und Entwicklung des Artefakts zum Einsatz. Dabei sind die Rahmenbedingungen und Ziele aus der Analyse sowie die Ergebnisse des Literaturüberblicks zu berücksichtigen. Phase 3 stellt die Validierungsphase dar. Im Zuge dessen werden die Artefakte anhand der zuvor festgelegten Forschungsziele bewertet oder, wenn Artefakte nicht geprüft werden können, Expertenbefragungen durchgeführt. Die vierte Phase – Kommunikation – folgt der Idee der Verbreitung der Forschungsergebnisse. Bei akademischen Arbeiten etwa bedeutet dies die Veröffentlichung der Ergebnisse in Büchern oder Zeitschriften. Praktische Forschungsergebnisse können wiederum in Unternehmen Anwendung finden.[19]

Wesentliche Grundlage zur Entwicklung des Prüfkataloges ist die intensive vorab durchgeführte Literaturrecherche in Kapitel 2. Dabei werden Grundkenntnisse in den Bereichen Digitalisierung, Software-Updates und Zuliefersituation in der Automobilindustrie vermittelt. Zudem werden verschiedene Normen, Standards und Regelungen der Informationssicherheit vorgestellt und der aktuelle Forschungsstand zu Prüfkatalogen im Bereich der Informationssicherheit erhoben. Dieser offenbart das Fehlen eines Prüfkatalogs, der konkret auf die neue Regelung der UNECE eingeht. Der sich dadurch ergebende Forschungsbedarf, das Ziel der Arbeit sowie die Abgrenzung der Arbeit zu anderen Themengebieten werden im nachfolgenden Kapitel 3 konkretisiert. Es folgt in Kapitel 4 mit der Konzeptionalisierung und Entwicklung des Prüfkatalogs der Kern der Arbeit. Sie basiert inhaltlich auf den eingangs erläuterten Normen, Standards und Empfehlungen sowie strukturell auf anderen bereits bestehenden Prüfkatalogen zur Informationssicherheit. Mithilfe der System Usability Scale (SUS) Methode wird der neu entwickelte Prüfkatalog anschließend in Kapitel 5 validiert. Die Beantwortung des Fragebogens erfolgt dabei durch Experten auf dem Gebiet der Informationssicherheit. Kapitel 6 befasst sich mit der Bedeutung und Auswirkung der Regelung auf die Kunden-Lieferanten Schnittstelle. Im finalen Kapitel 7 werden schließlich die zuvor erlangten Ergebnisse zusammengefasst und ein Ausblick über mögliche zukünftige Entwicklungen gegeben.

[19] Vgl. Österle und Otto (2010), S. 287ff.

# 2 Theoretische Grundlagen und Stand der Forschung

Dieses Kapitel widmet sich den theoretischen Grundlagen und dem Stand der Forschung der vorliegenden Diplomarbeit. Im Sinne von Österle's Design Science Research beginnt damit die erste Phase des vierstufigen Erkenntnisprozesses – die Analysephase. Ziel ist es, einen Überblick über die theoretischen Inhalte der Arbeit zu erlangen. Im weiteren Verlauf dient dies als Basis zur Entwicklung des Prüfkatalogs.

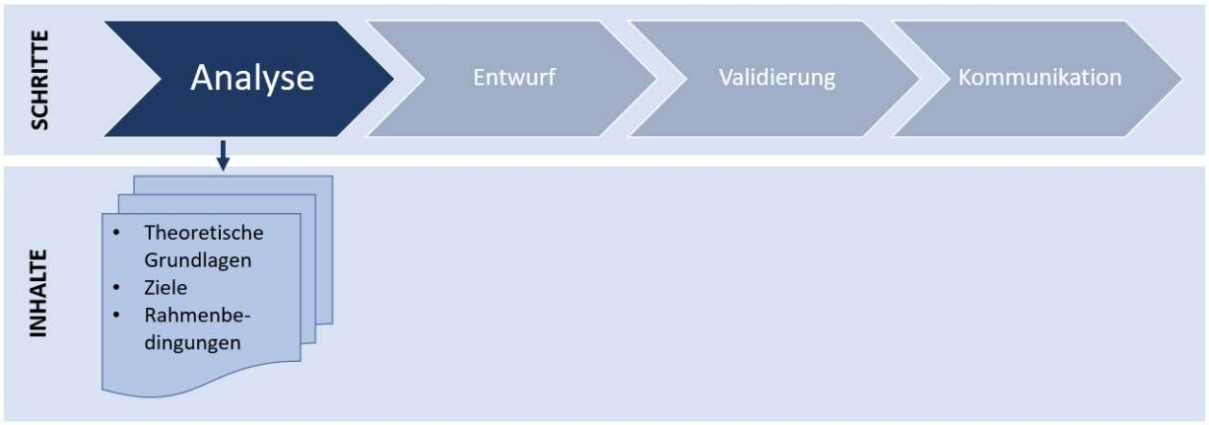



**Abbildung 2: Aktuelle Phase 1 in Österle's Design Science Research[20]**

Kapitel 2.1 befasst sich allgemein mit der Digitalisierung und dem Einsatz von Software in der Automobilindustrie. Neben verschiedenen Digitalisierungsfeldern werden in diesem Kapitel die Rolle von Software-Updates sowie cybersicherheitstechnische Herausforderungen in der Automobilindustrie genauer betrachtet. Kapitel 2.2 beschreibt die Zuliefersituation innerhalb der Automobilindustrie. Dabei liegt der Fokus auf der Qualitätssicherung und der Darstellung der Situation für Softwaretechnologien im Rahmen der Kunden-Lieferanten Schnittstelle. Auf bereits bestehende Standards und Normen zur Informationssicherheit wird in Kapitel 2.3 eingegangen, wobei die neue Regelung Nr. 156 der UNECE zu SUMS im Vordergrund der Betrachtungen steht. Abschließend vermittelt Kapitel 2.4 einen Überblick über den aktuellen Stand der Forschung hinsichtlich Prüfkataloge im Bereich der Informationssicherheit.

[20] Quelle: Eigene Darstellung

## 2.1 Digitalisierung und Software in der Automobilindustrie

Die Sicherung der Zukunftsfähigkeit sowie die Aussicht auf mehr Umsatz und Profit haben dazu geführt, dass das Thema „Digitalisierung“ in den vergangenen Jahren zu einem Schlüsselthema in allen Unternehmen geworden ist.[21] Ganz allgemein werden als Digitalisierung jene technologische Veränderungen bezeichnet, die eine umfassenden Vernetzung aller Bereiche von Wirtschaft und Gesellschaft ermöglichen. Dabei geht die Digitalisierung über den rein technischen Prozess des Transfers von analogen in digitale Daten hinaus und treibt damit Veränderungen sowohl einzelner Prozesse, einzelner Produkte bzw. Leistungen als auch einzelner Geschäftsmodelle voran.[22]

### 2.1.1 Digitalisierungsfelder

Auch für die Automobilhersteller ist es unerlässlich, eine Neuausrichtung der Unternehmensstrategie zu definieren und die Umsetzung einhergehend mit der digitalen Transformation zügig voranzutreiben. Der Wandel der Automobilindustrie umfasst dabei sowohl die Prozesse innerhalb der Unternehmen als auch die technologischen Entwicklungen im Automobil selbst. Bereits heute ist die Informationstechnik im oberen Fahrzeugsegment mit deutlich mehr als 100 Steuergeräten und einem aufwendigen Kabelbaum von über 20 km Länge ein erheblicher Bestandteil des Fahrzeugs. Es ist davon auszugehen, dass die Bedeutung der IT in Zukunft noch weiter ansteigen wird. Fahrzeuge avancieren damit zu „fahrenden Rechenzentren“ oder „IP-Adressen auf Rädern“. Innerhalb der Unternehmen gilt es Geschäftsprozesse auf Basis intelligenter Lösungen automatisch ablaufen zu lassen. Dabei ist das Thema der digitalen Transformation auf Grundlage eines umfassenden Plans mit Nachhaltigkeit anzugehen, und nicht als einmaliges Projekt.[23]

Um diese digitalen Transformationsfelder herum angesiedelt sind jene Technologien, die als „Enabler“ die Umsetzung dieser Wachstumschancen ermöglichen. Im Fokus der Automobilindustrie stehen zum Beispiel IT-Lösungen und Architekturen für Cloud Services, Big Data oder Industrie 4.0.[24] Diese Zusammenhänge sind in Abbildung 3 grafisch dargestellt.

[21] Vgl. Winkelhake (2021), S. 1.
[22] Vgl. Proff (2019), S.32 f.
[23] Vgl. Winkelhake (2019), S. 36f.
[24] Vgl. Winkelhake (2019), S. 37.

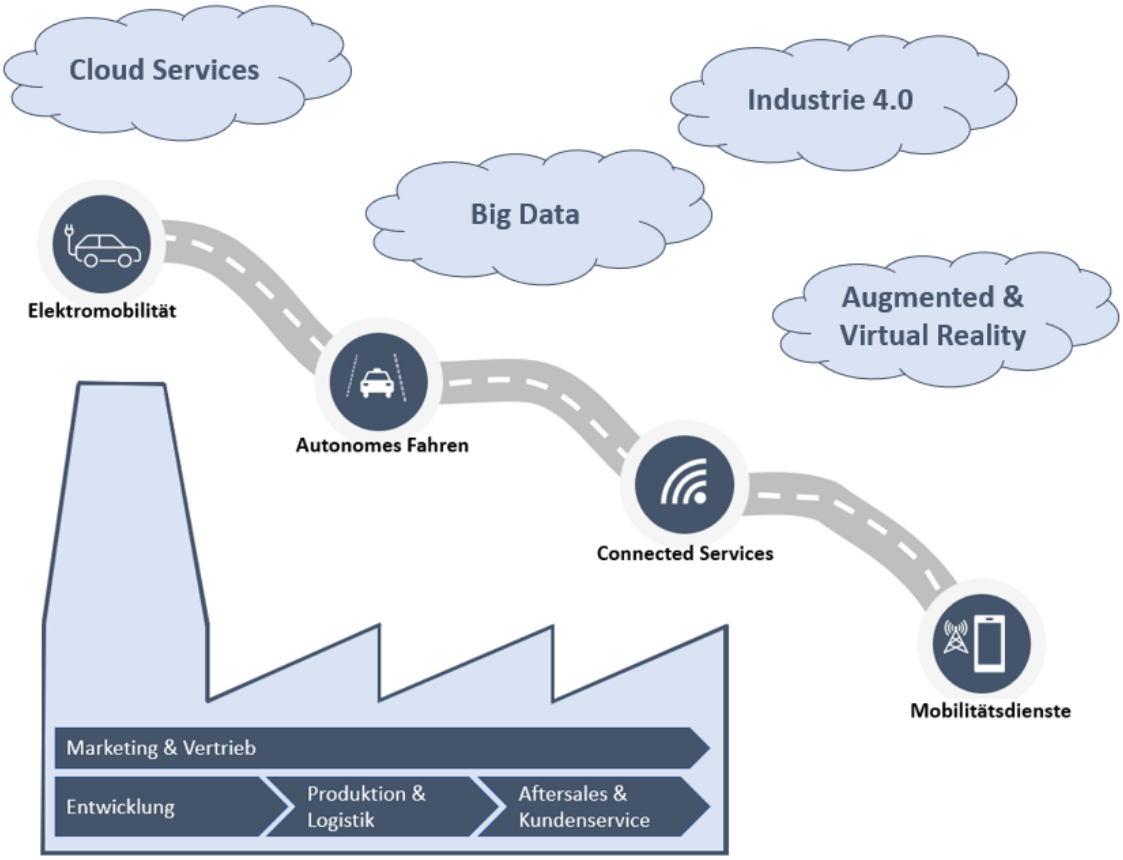



**Abbildung 3: Digitalisierungsfelder sowie „Enabler“[25]**

Basis der Wachstumschancen sind, wie bereits erwähnt, Digitalisierungsthemen sowohl innerhalb der Unternehmen als auch auf das Automobil selbst bezogene Themen.[26] Bei ersteren geht es primär um die umfangreichen Effekte und Potenziale digitaler Technologien und Methoden und deren Einfluss auf verschiedene Geschäftsbereiche eines Unternehmens.[27] Initiativen zur digitalen Transformation setzen nämlich als Querschnittsthema beim Geschäftsmodell eines Unternehmens an und beeinflussen damit fast alle wesentlichen Geschäftsprozesse in sämtlichen Unternehmensbereichen.[28] Die internen Geschäftsprozesse werden durch digitale Methoden wie Vernetzung, mobile Datenerfassung und Analytics schneller, sicherer, kostengünstiger und flexibler. Der Einsatz neuartiger digitaler Technologien in Entwicklung, Produktion, Aftersales und Vertrieb ermöglicht damit einen Wettbewerbsvorteil gegenüber anderen Unternehmen.[29]

[25] Quelle: Eigene Darstellung
[26] Vgl. Winkelhake (2019), S. 36f.
[27] Vgl. Weber (2020), S. 130.
[28] Vgl. Winkelhake (2019), S. 38.
[29] Vgl. Weber (2020), S. 130.

Elektromobilität, verschiedene Mobilitätsservices oder Autonomes Fahren beziehen sich hingegen direkt auf das Automobil. Sie spielen aber ebenso in das Thema Digitalisierung hinein und bedeuten einen weiteren Schritt des Autos hin zum fahrenden IT-System.[30] In jedem Fall ist die digitale Transformation in der Automobilindustrie nicht mehr wegzudenken. Um langfristig am Markt bestehen zu können, ist es deshalb unerlässlich, dass sich die Hersteller intensiv mit diesem Thema auseinandersetzen.

### 2.1.2 Die Rolle von Software-Updates

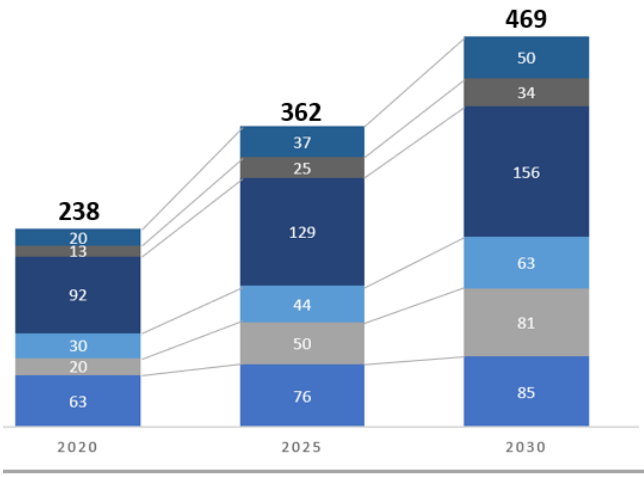
Mit zunehmender Digitalisierung steigt der Softwarebedarf deutlich an. Dabei wird die IT zum Kernelement betrieblicher Abläufe und Produkte und die Bedeutung der Softwareentwicklung in den Unternehmen wächst an.[31]

Definitionsgemäß stellt Software einen „Sammelbegriff für die Gesamtheit ausführbarer Datenverarbeitungsprogramme und die zugehörigen Daten auf der Hardware“ dar. Die Hardware im Gegenzug ist der „Oberbegriff für die mechanische und elektronische Ausrüstung eines datenverarbeitenden Systems“.[32] In der Praxis der Automobilindustrie werden Softwarekomponenten hauptsächlich zur Umsetzung von funktionalen Anforderungen in weiten Bereichen eingesetzt. Dabei handelt es sich um durch die Kunden wahrnehmbare und teilweise explizit als Ausstattung gekaufte Funktionen. Sehr erfolgreich wird Software darüber hinaus zur Kompensation von Schwächen der Mechanik und Elektronik eingesetzt. In diesen Fällen ist die Beseitigung der Ursache eines Problems in der Hardware nur schwer möglich. Die Software kann dann zumindest die Symptome (teilweise) korrigieren und das System damit ausreichend kundentauglich machen. In jedem Fall unterliegen Softwareanforderungen sowohl den funktionalen Anforderungen der Kunden als auch den nichtfunktionalen Anforderungen aus Normen und Gesetzen.[33]

Die wesentlichen Trends der Automobilindustrie – Elektromobilität, Autonomes Fahren, Vernetzte Fahrzeuge und Shared Mobility – basieren allesamt auf den Fortschritten im Bereich der automobilen Software- und Elektroniktechnologien. Folglich gilt dieser Bereich als einer der wachstumsstärksten innerhalb der Automobilindustrie. Abbildung 4 stellt die Entwicklung des automobilen Software- und Elektronikmarktes aufgeteilt nach Komponenten dar.[34]

[30] Vgl. Winkelhake (2021), S. 110ff.
[31] Vgl. Winkelhake (2021), S. 298.
[32] Wolf (2018), S. 42.
[33] Vgl. Wolf (2018), S. 41.
[34] Vgl. Burkacky, Deichmann und Stein (2019), S. 9ff.

**Wachstum des Software- und Elektronikmarktes im Automobilbereich von 2020-2030**




| Komponenten | Wachstumsrate Jahre 2020-2030 |
|---|---|
| **Gesamt** | **+7%** |
| Software | +9% |
| Integrations- und Validierungsservices | +10% |
| Steuergeräte (ECUs & DCUs) | +5% |
| Sensoren | +8% |
| Leistungselektronik (ohne Batteriezellen) | +15% |
| Andere Elektronikkomponenten | +3% |

**Abbildung 4: Entwicklung des Software- und Elektronikmarktes[35]**

Das Wachstum des Software- und Elektronikmarktes von 238 Mrd. US-Dollar im Jahr 2020 auf rund 469 Mrd. US-Dollar im Jahr 2030 entspricht einer jährlichen Wachstumsrate von ca. 7 Prozent. Im Vergleich dazu wächst der gesamte globale Automobilmarkt um „lediglich“ 3 Prozent.

Die oben beschriebene Entwicklung verdeutlicht die Relevanz der Software-Thematik in der Automobilindustrie. Damit einher geht auch die Notwendigkeit einer zunehmenden Pflege dieser Software. Dies geschieht durch Updates, zum Beispiel im Sinne von Bugfixes oder Security Updates bei identifizierten Schwachstellen.[36] Verbindliches Ziel der Automobilhersteller ist dabei die Softwareeffizienz und -aktualität während des gesamten Lebenszyklus der Fahrzeuge zu gewährleisten und zu verwalten. Insbesondere fehlerhafte Software, die sich als nachteilig für die Sicherheit des Fahrzeugs erweisen könnte, muss korrigiert und verbessert werden.[37] Die Freigabe neu entwickelter oder überarbeiteter Software erfolgt in regelmäßigen Abständen, meist alle sechs Monate. Gelegentlich kommt es auch zur Entwicklung von Zwischenfreigaben, dies allerdings nur dann, wenn es um die Behebung schwerwiegender und sicherheitskritischer Fehler geht.[38]

[35] Quelle: Eigene Darstellung in Anlehnung an Burkacky, Deichmann und Stein (2019), S. 12.
[36] Vgl. Herzig und Guderian (2021), S. 2.
[37] Vgl. Halder, Ghosal und Conti (2020), S. 2.
[38] Vgl. Guissouma et al. (2018), S. 299.

### Einteilung von Software-Updates

Generell können Software-Updates nach verschiedenen Gesichtspunkten klassifiziert werden. Die Einteilung nach dem Update-Ziel stellt eine Möglichkeit dar. Wird eine Softwarepflege am Fahrzeug durchgeführt, zum Beispiel als präventive Sicherheitsmaßnahme, zur Steigerung der Performance oder zum Optimieren des Programmcodes, werden Eigenschaften des Fahrzeuges perfektioniert. Ein zweites Update-Ziel kann das Schließen einer entdeckten Security- oder Privacy-Lücke sein. Die Dringlichkeit zur Behebung einer solchen Lücke kann deutlich höher sein als bei einer Softwarepflege und manchmal auch vom Gesetzgeber eingefordert werden. Eine korrektive oder präventive Maßnahme zur Fehlerbehebung kann im Sinne der aktuellen Gesetzgebung als Rückruf ausgelegt werden. Da jeder Rückruf meldepflichtig ist, erweitert sich der Prozess in diesem Fall um die Schnittstelle zu der regulierenden Behörde.

Neben dem Update-Ziel kann eine Klassifizierung nach Funktionsbereichen im Fahrzeug vorgenommen werden. Unterschieden wird demnach zwischen Infotainment-, Karosserie-/Komfort- oder Fahrfunktionen. Updates des Infotainment-Systems sind hauptsächlich Programm- bzw. Applikations-Updates ohne Verbindung zu mechanischen Komponenten. Die Manipulation einer solchen Funktion führt in der Regel zu keiner physischen Gefährdung für die Insassen und die Umwelt und muss folglich nicht unmittelbar abgesichert werden. Karosserie- / Komfortfunktionen sind solche Funktion, die z. B. dem Body-Netzwerk (Türen, Fenster, Klima, etc.) eines Fahrzeugs angehören. Obwohl ein nicht gewünschter Funktionszustand den Fahrer stark von der Fahrzeugführung ablenken kann, besteht meist die Möglichkeit, das Fahrzeug sicher abzustellen. Eine Gefährdung durch Ablenkung durch die Funktionsstörung ist allerdings nicht auszuschließen. Fahrfunktionen der dynamischen Fahrzeugkontrolle adressieren hingegen Update-Funktionen, von denen eine hohe Gefährdung der Fahrzeuginsassen und -umwelt ausgehen kann. Beispielhaft zu erwähnen seien an dieser Stelle Fahrfunktionen, die auf das Gas- oder Bremspedal zugreifen, oder regelnde Fahrassistenzsysteme von (teil-) autonomen Fahrzeugen.

Eine dritte Unterscheidungsmöglichkeit von Software-Updates besteht in der Klassifizierung nach Behördensicht. Für die Updates ergeben sich dabei drei verschiedene Fälle: Software-Updates ohne Typgenehmigungsrelevanz (z.B. Infotainment- und Komfortfunktionen), Software-Updates mit Typgenehmigungs-relevanz (z.B. Sicherheitsupdates) oder Software-Updates mit Typgenehmigungs- und Zulassungsrelevanz (z.B. Leistungssteigerungen).

Die letzte Klassifizierungsmöglichkeit stellt jene nach der Kritikalität des Software-Updates dar. Dabei handelt es sich um eine Kombination der drei vorhergehenden

Klassifizierungen, die eine Einstufung in drei Kategorien der Kritikalität vorsieht (niedrig, mittel, hoch).[39]

### Traditionelle Software-Updates

Unabhängig von Art, Umfang und Kritikalität müssen Software-Updates früher oder später am Fahrzeug durchgeführt werden. Bisher geschah dies in den Werkstätten der Automobilhändler. Zunächst wird der Fahrer per E-Mail über die Verfügbarkeit eines Updates informiert und aufgefordert, das Fahrzeug zur nächsten Werkstatt zu bringen. Inzwischen wird die neue Software zur Fehlerbehebung vom OEM an die Werkstätte verschickt. Sobald Fahrzeug und Software dort eintreffen, wird das Update über die On-Board-Diagnose (OBD)-Schnittstelle auf das Ziel-Steuergerät aufgespielt. Die Dauer für das Aufspielen des Updates liegt, je nach Steuergerät, bei ca. 15 bis 90 Minuten. Je nach Sicherheitskritikalität des Updates muss der Techniker das aktualisierte Steuergerät auch testen, z.B. durch eine Diagnose über die OBD-Schnittstelle oder einen Funktionstest. In jedem Fall erfordert der beschrieben Update-Prozess sowohl vom Fahrzeughalter als auch vom Techniker einen hohen Zeit- und Arbeitsaufwand, der hohe Kosten und einige Unannehmlichkeiten für den Kunden mit sich bringt.[40] In Abbildung 5 ist der traditionelle Software-Update Prozess grafisch dargestellt.

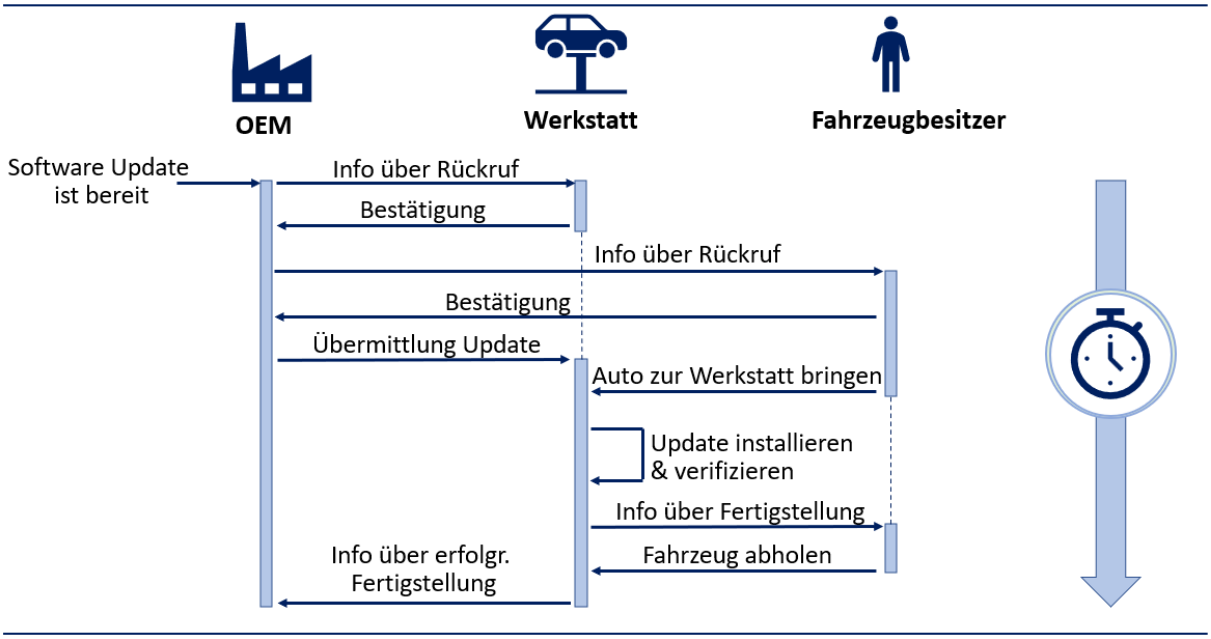



Abbildung 5: Traditionelles Software-Update[41]

[39] Vgl. Römer, Kreyenberg und Großmann (2018), S. 39ff.
[40] Vgl. Guissouma et al. (2018), S. 299.
[41] Quelle: Eigene Darstellung in Anlehnung an Halder, Ghosal und Conti (2020), S. 4.

Da die Fahrzeuge zunehmend elektronik- und softwareabhängig sind, hat die Zahl der Rückrufe wegen Elektronik- und Softwarefehlern exponentiell zugenommen. Verschiedenen Untersuchungen zufolge sind in den Jahren 2015 bis 2020 mehr als 13 Millionen Fahrzeugrückrufe auf fehlerhafte Software zurückzuführen. Ein Großteil dieser Rückrufe hätte durch sogenannte Over-The-Air Updates vermieden werden können. Nicht zuletzt deswegen ist davon auszugehen, dass die Möglichkeit, Updates ohne Werkstattaufenthalt durchzuführen, eines der wichtigsten Merkmale künftiger vernetzter Fahrzeuge darstellen wird.[42]

### Over-The-Air Updates

Drahtlose Over-The-Air-Updates ermöglichen es aus der Ferne die Softwarefunktionalität eines Fahrzeugs anzupassen oder Fehler in der Software der elektronischen Steuergeräte zu beheben. Solche Aktualisierungen können sowohl für den OEM als auch für den Fahrzeugbesitzer sehr vorteilhaft sein, da sie es überflüssig machen, das Fahrzeug zu einem Service-Center zu bringen.[43] Viel mehr basiert der OTA-Update Prozess auf einer Client-Server Architektur, die dem OEM die Verteilung von Aktualisierungen an die Clients, also die Verarbeitungseinheiten der jeweiligen Fahrzeuge, ermöglicht. Der Client verbindet sich mit dem Server über einen drahtlosen Zugangspunkt, lädt die Software-Update-Dateien herunter und verteilt sie über interne Systeme an die entsprechenden Steuergeräte.[44] Dieser Prozess ist in der nachfolgenden Abbildung 6 dargestellt.

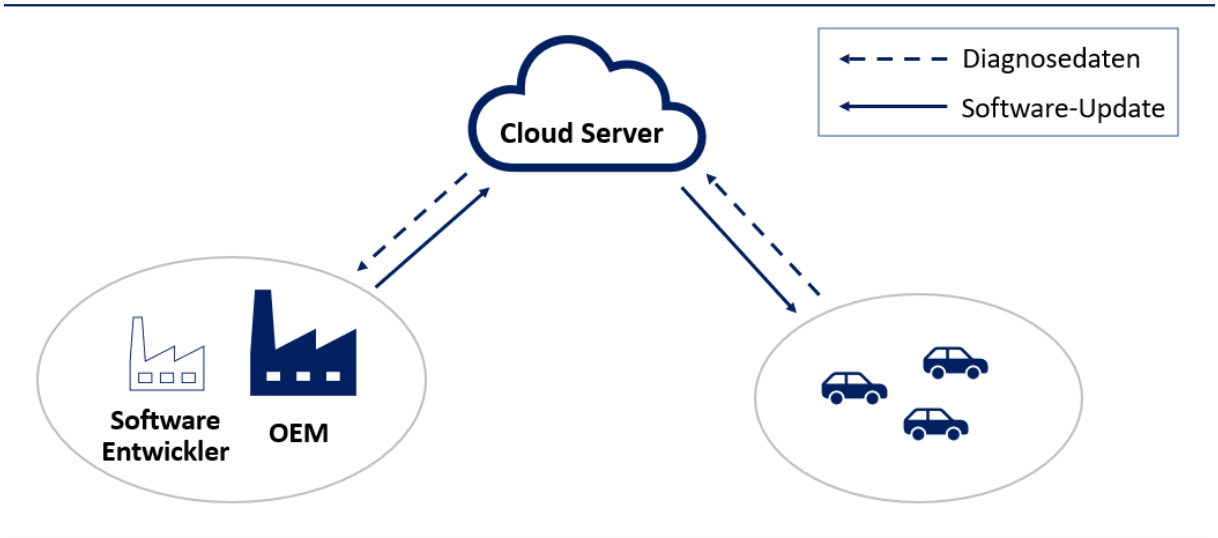



Abbildung 6: Over-The-Air Software-Updates[45]

[42] Vgl. Halder, Ghosal und Conti (2020), S. 2.
[43] Vgl. Steger et al. (2018), S. 138.
[44] Vgl. Guissouma et al. (2018), S. 299.
[45] Quelle: Eigene Darstellung in Anlehnung an Halder, Ghosal und Conti (2020), S. 4.

Die ersten Fahrzeuge mit der Fähigkeit zur Aktualisierung von Updates „Over-The-Air“ sind bereits auf dem Markt. Hauptanwendungsfall sind derzeit sicherheitsunkritische Systeme, wie zum Beispiel verschiedene Infotainment-Anwendungen und die Aktualisierung von Navigationskarten. Als einer der ersten Autokonzerne bietet Tesla bereits Updates für Funktionen des Autopiloten, und damit sicherheitsrelevanteren Funktionen, an.[46]

Danach streben viele OEMs, denn es ist offensichtlich, dass OTA-Updates enorme Vorteile gegenüber dem klassischen Software-Update Prozess bieten. Der Eindeutigste ist die Kosteneinsparung für den OEM. So tragen OTA-Updates maßgeblich dazu bei, Gewährleistungszahlungen und Rückrufaktionen bei potenziell Millionen von Fahrzeugen zu reduzieren. Prognosen zufolge werden die Einsparungen für die Automobilhersteller bereits im Jahr 2022 rund 35 Mrd. US-Dollar betragen, ausgehend von ca. 2,7 Mrd. US-Dollar im Jahr 2015. Sehr deutlich ist auch der Beitrag von OTA-Updates zur Erhöhung der Kundenzufriedenheit. Durch sie ersparen sich Fahrzeugnutzer die Unannehmlichkeit, ihr Auto zu einem Händler zu bringen, und sie erhalten die neuesten Sicherheitsupdates häufig ohne sich der Änderung überhaupt bewusst zu sein. Weiters können sicherheitskritische Systeme mittels OTA-Technologie sofort aktualisiert werden, sobald ein Problem festgestellt wird. Daneben existieren noch weitere Vorteile, wie z.B. eine Erhöhung der Umsatzmöglichkeiten für Automobilhersteller im After Sales Bereich. Diesen zahlreichen Vorteilen gegenüber stehen allerdings auch gewisse Risiken und Herausforderungen, die mit der Umsetzung von OTA-Updates verbunden sind.[47] Auf diese und allgemeine cybersicherheitstechnische Bedrohungen in der Automobilindustrie wird im folgenden Kapitel eingegangen.

### 2.1.3 Cybersicherheitstechnische Herausforderungen

Die Ausführungen in Kapitel 2.1.1 haben uns gezeigt, dass die digitale Transformation in Automobilunternehmen und Fahrzeugen in allen Bereichen mehr oder weniger weit fortgeschritten ist. Mit der fortschreitenden Vernetzung der Fahrzeuge wird auch das gesamte Steuerungssystem in den Fahrzeugen immer komplexer. Die Zunahme der Funktionen, der Konnektivität und der Komplexität führt zu einer großen Anzahl von Dateninteraktionen, sowohl innerhalb des Fahrzeugs als auch mit seiner Umgebung. Damit einhergehend entstehen eine Vielzahl an Ansatzpunkten für unberechtigte Zugriffe Dritter auf die Fahrzeugsteuerung. Die dynamischen und vielfältigen Angriffe, denen intelligente und vernetzte Fahrzeuge ausgesetzt sind, können zu Problemen führen. Sie betreffen die Fahrzeugsicherheit, die Privatsphäre von Personen und in

[46] Vgl. Guissouma et al. (2018), S. 299.
[47] Vgl. Halder, Ghosal und Conti (2020), S. 2ff.

äußerst weitreichenden Fällen sogar die nationale Sicherheit.[48] Die konkreten Bedrohungen, die sich aus Cyberangriffen in der Automobilindustrie ergeben, sind äußerst vielfältig. Eine Liste von Schwachstellen bzw. Angriffsmethoden bezogen auf verschiedene Bedrohungen ist im Anhang der 2021 verabschiedeten Regelung R155 zu CSMS der UNECE enthalten. Einige wesentliche Kerninhalte sind in der folgenden Tabelle 1 zusammengefasst.

| **Bedrohungsart** | **Beschreibung** |
|---|---|
| *Back-End-Server* | • Können zum Angriff auf ein Fahrzeug oder zum Extrahieren von Daten genutzt werden.<br>• Back-End-Serverdienste können zudem unterbrochen und der Fahrzeugbetrieb dadurch beeinträchtigt werden, wenn z.B. Fahrzeuge auf die Bereitstellung gewisser Dienste angewiesen sind. |
| *Kommunikationskanäle* | • Können für die unerlaubte Manipulation, Löschung oder sonstige Änderung von Fahrzeugcode/-daten genutzt werden.<br>• Ermöglichen den Empfang nicht vertrauenswürdiger/ unzuverlässiger Nachrichten.<br>• Informationen können leicht offengelegt werden, beispielsweise durch Abhören der Kommunikation.<br>• In Kommunikationsmedien eingebettete Viren oder schädliche Inhalte können Fahrzeugsysteme infizieren. |
| *Externe Vernetzungen und Verbindungen* | • Eine Manipulation von vernetzten Fahrzeugfunktionen, z.B. drahtlosen Kommunikationssystemen, kann einen Cyberangriff ermöglichen.<br>• Software von Drittanbietern, z.B. Unterhaltungs-anwendungen, können zum Angriff auf Fahrzeugsysteme genutzt werden.<br>• Mit externen Schnittstellen, z.B. USB- oder OBD-Anschlüsse, verbundene Geräte können zum Angriff auf Fahrzeugsysteme genutzt werden. |
| *Fahrzeugdate und -Code* | • Durch Cyberangriffe können Fahrzeugdaten extrahiert, manipuliert und gelöscht werden.<br>• Es kann zur Einspeisung von Schadsoftware und zur Überschreibung vorhandener Software kommen. |

[48] Vgl. Wang et al. (2021), S. 253.

| | |
|---|---|
| | • Durch unbefugten Zugriff können Systeme oder Vorgänge gestört und Fahrzeugparameter manipuliert werden. |

Tabelle 1: Cybersicherheitstechnische Bedrohungen[49]

Weitere Bedrohungen für Fahrzeuge bestehen bezüglich ihrer Software-Aktualisierungsverfahren und im Besonderen für OTA-Updates. Angesichts des Fokus der vorliegenden Arbeit auf Software-Update Management Systeme erfolgt eine gesonderte Betrachtung dieser Herausforderung und Bedrohungsart im nachfolgenden Absatz.

**Bedrohungen bezüglich Software (OTA-)Updates**

Aus cybersicherheitstechnischer Sicht sind Risiken bezüglich traditioneller Software-Updates zwar vorhanden, in ihrem Ausmaß sind sie allerdings überschaubar. Die wesentlichste Bedrohungsart ist die Manipulation der neu aufzuspielenden Software vor dem Aktualisierungsprozess. Dazu gehört sowohl die Fälschung des Programms als auch das Aufspielen einer Malware durch das Update. Daneben kann es auch zu einer sogenannten „Denial-of-Service-Attacke“ gegen den Aktualisierungsserver kommen. Darunter versteht man die Attacke auf ein Netzwerk, um zu verhindern, dass wichtige Softwareaktualisierungen und/oder die Freigabe kundenspezifischer Funktionen durchgeführt werden können.[50] Da aber die Aktualisierung im Rahmen einer Inspektion in einer Kfz-Werkstatt durchgeführt wird, kann auf das Fahrzeugnetz über eine physische Diagnoseschnittstelle zugegriffen werden. Dabei besteht eine zuverlässige und geschützte Verbindung zwischen dem Fahrzeugnetz und dem OEM-Netz über die Kfz-Werkstatt. Geschulte Werkstattmitarbeiter können darüber hinaus sicherstellen, dass Störungen während der Aktualisierung vermieden und die Korrektheit der Anwendung anschließend getestet wird.[51] Folglich ist das Risiko einer cybersicherheitstechnischen Bedrohung in diesem Fall meist überschaubar.

Im Unterschied dazu unterliegen OTA-Updates sehr wohl einer wesentlichen Gefährdung durch Cyberattacken. Neue Schnittstellen sowie die komplexen, technischen Abläufe erhöhen die Wahrscheinlichkeit, dass Sicherheitslücken von Angreifern mit verschiedenen Motivationen ausgenutzt werden. Die Öffnung des Fahrzeuges über die Luftschnittstelle birgt das Risiko, dass Angreifer über Schwachstellen in der Verteilinfrastruktur auf das Fahrzeug bzw. das Software-Update zugreifen können. Bei fehlender Absicherung und entsprechendem Knowhow der Angreifer könnten Daten und Software mitgelesen oder manipuliert werden.

[49] Quelle: Eigene Darstellung in Anlehnung an UNECE R155:2021-03, Anhang 3, S. 19ff.
[50] Vgl. UNECE R155:2021-03, Anhang 3, S. 21.
[51] Vgl. Placho et al. (2020), S. 3.

Kompromittierte Software erlaubt außerdem den Zugriff auf verschiedene Funktionen des Fahrzeugs. Infolgedessen drohen Störungen der Fahrzeugfunktionalität und damit einhergehend Konsequenzen für die Fahrsicherheit. Auch sind Attacken möglich, die Fahrzeugfunktionen vollständig blockieren, wie zum Beispiel eine Deaktivierung der Lenkung oder der Bremsen.[52]

Zusammenfassend stehen die Automobilhersteller jedenfalls vor der großen Herausforderung, den Schritt vom reinen Hardware- zum Software-Hersteller zu vollziehen. Die vielen Datenschnittstellen und der große Softwareanteil erhöhen dabei die Angriffsfläche für sicherheitsrelevante Cyber-Attacken.[53] Automobilhersteller müssen nun dementsprechend dafür sorgen, dass die Fahrzeugsicherheit nicht durch mangelnde Datensicherheit beeinträchtigt wird und dass das Fahrzeug vor Manipulation geschützt ist.[54] Zusätzlich angeregt wurde diese Diskussion Anfang 2021 als eine Arbeitsgruppe der Vereinten Nationen die ersten verbindlichen Regularien zum Thema Cybersecurity Management System (CSMS) und Software Update Management System (SUMS) verabschiedet hat. Diese und andere bereits bestehenden Regelungen der Informationssicherheit in der Automobilindustrie werden in Kapitel 2.3 im Detail beleuchtet. Zuvor widmet sich das anschließende Kapitel noch der Zuliefersituation in der Automobilindustrie, da eine Vielzahl der Software- und Elektronikkomponenten von Lieferanten bezogen werden.

## 2.2 Zuliefersituation in der Automobilindustrie

Die Automobilindustrie ist gekennzeichnet durch eine ausgeprägte Arbeitsteiligkeit zwischen den OEMs einerseits und ihren Zulieferern andererseits. Sie zielt auf eine Konzentration der OEMs auf ihre Kernkompetenzen und entsprechend auf Weitergabe von Nicht-Kernkompetenzfunktionen an die Zulieferer.[55] Kennzeichnend für diese Arbeitsteiligkeit im Automobilbereich ist eine Gliederung in verschiedene Schichten innerhalb der Lieferkette, den sogenannten Tiers, die zusammengesetzt die Zulieferpyramide bilden. Abbildung 7 gibt einen Überblick über eine typische Automobil-Lieferkette.[56]

[52] Vgl. Römer, Kreyenberg und Großmann (2018), S. 46 & 51.
[53] Vgl. Dassow, Herzig und Guderian (2021), S. 2f.
[54] Vgl. Steurich, Klimke und Pedersen (2017).
[55] Vgl. Gehr (1984), S. 1.
[56] Vgl. Placho et al. (2020), S. 2.

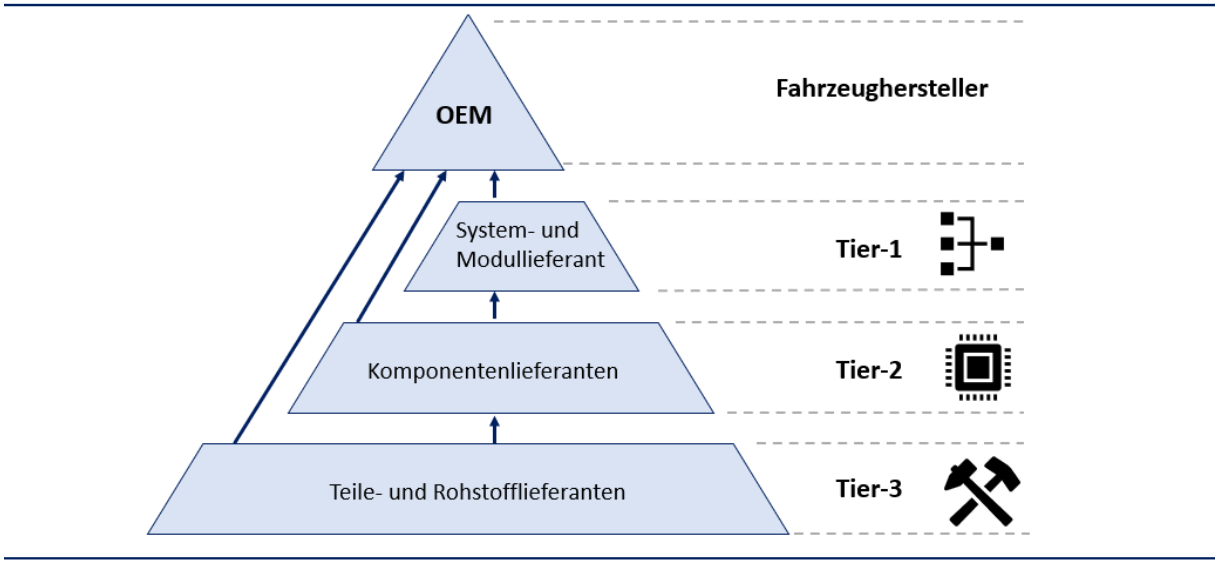



**Abbildung 7: Automobile Zulieferpyramide**[57]

Der OEM ist für das Gesamtfahrzeug verantwortlich und bildet die wichtige Schnittstelle zu den Kunden. Das Fahrzeug wird vom OEM entwickelt und zusammengebaut, die dazu notwendigen Systeme und Module bezieht er von den sogenannten Tier-1-Lieferanten. Dabei handelt es sich um jene Lieferanten, die meist automobilspezifisch agieren und dazu in der Lage sind, eine ganze Fahrzeugfunktionalität, zum Beispiel ein Bremssystem, zu entwickeln. Tier 2 sind Komponentenlieferanten auf Hardware- oder Softwareebene. Sie sind Experten in einem bestimmten Bereich und unterstützen oft auch Kunden außerhalb des Automobilbereichs. An unterster Ebene stehen die Tier-3 Lieferanten, die u.a. für den Abbau und die Aufbereitung der Rohmaterialen zuständig sind.[58]

## 2.2.1 Qualitätssicherung und IATF 16949

Angesichts des großen Wettbewerbsdrucks, der in der Automobilbranche herrscht, nimmt das Outsourcing, d.h. die Auslagerung von Aufgaben an externe Lieferanten, weiter zu. Es gilt allgemein als kluge Lösung, um einerseits die Gemeinkosten zu reduzieren und andererseits die Leistung voranzutreiben. Diese Entwicklung führt allerdings zur Entstehung hochkomplexer vernetzter Zuliefersysteme, die wiederum kontinuierliche und strenge Qualitätskontrollen bei Zukaufprodukten erfordern.[59] Meist wird die Qualitätssicherung für Lieferanten im Zuge von Lieferantenaudits durchgeführt. Sie dienen dazu das Qualitätsmanagementsystem eines Lieferanten durch eine neutrale Prüfung zu analysieren und zu bewerten. Das nach erfolgreicher

[57] Quelle: Eigene Darstellung in Anlehnung an https://www.wikiwand.com/de/Zulieferpyramide (Gelesen am 19.11.2021).
[58] Vgl. Placho et al. (2020), S. 2.
[59] Vgl. Biegaj (2018), S. 3.

Prüfung ausgestellte Zertifikat dient dann als Nachweis über die Zuverlässigkeit des Lieferanten.[60]

Die wesentlichste Zertifizierung für ein Qualitätsmanagementsystem in der Automobilindustrie ist die im Oktober 2016 veröffentlichte Norm IATF 16949. Sie wurde entwickelt, um der Forderung nach einem international gültigen Dokument mit weltweit harmonisierten Qualitätsmanagementsystem (QMS)-Anforderungen nachzukommen. Dabei legt die Norm IATF 16949 die Anforderungen an die Qualitätsmanagementsysteme von Organisationen in der Lieferkette der Automobilbranche fest und hilft damit, Probleme entlang der Lieferkette zu vermeiden. Ziel der Norm ist die Entwicklung eines QMS, das unter anderem für kontinuierliche Verbesserung sorgt sowie eine Reduzierung von Abweichungen und Verschwendung in der Lieferkette fördert. Insgesamt umfasst IATF 16949 10 Kapitel, wobei folgende in Abbildung 8 dargestellten Aspekte zu den Hauptinhalten der Norm gehören:[61]


**Abbildung 8: Hauptthemen der IATF 16949[62]**

In jedem Fall gilt IATF 16949 mittlerweile für viele Unternehmen in der Automobilindustrie als Grundvoraussetzung für die Zusammenarbeit mit einem Lieferanten. So fordert zum Beispiel das *Knorr-Bremse Quality Management Program for Procurement (QMPP)* ein wirksames Qualitätsmanagementsystem nach IATF 16949 als Grundlage, um als Lieferant ausgewählt zu werden.[63] Selbiges liest sich in den Qualitätssicherheitsbestimmungen für Kaufteile der *Brose Fahrzeugteile SE & Co.*

[60] Vgl. TÜV Rheinland Cert GmbH (2021), S. 1.
[61] Vgl. Biegaj (2018), S. 4ff.
[62] Quelle: Eigene Darstellung in Anlehnung an Biegaj (2018), S. 6.
[63] Vgl. Knorr-Bremse System für Nutzfahrzeuge GmbH (2018), S. 22f.

*KG*, die von ihren Lieferanten ebenfalls ein funktionierendes Qualitätsmanagementsystem gemäß IATF 16949 einfordert. In den Bestimmungen ist zudem der Umgang mit funktionaler Sicherheit bei Software und Komponenten mit integrierter Software geregelt.[64] In Anbetracht des zunehmenden Softwareanteils an der Fahrzeug-Wertschöpfung und der Tatsache, dass ein großer Teil davon fremdbezogen ist, stellt diese Integration einen wichtigen Aspekt dar.[65] Im folgende Kapitel wird die Situation für Softwaretechnologien innerhalb dieser Schnittstelle zwischen Fahrzeugherstellern und Lieferanten näher betrachtet.

### 2.2.2 Situation für Softwaretechnologien

Im Bereich der elektrischen und elektronischen Systeme und Software-Komponenten beziehen die Fahrzeughersteller bis zu 100 Prozent der Umfänge von externen Zulieferfirmen. Diese Entwicklung war bisher geprägt durch eine starke Arbeitsteilung. Die Anforderungen an die Funktionalität eines elektronischen Systems wurden in der Regel durch den Automobilhersteller festgelegt werden, während die eigentliche Entwicklung und damit die Realisierung der Funktionen durch die entsprechenden Zulieferer erfolgte.[66] Die in Kapitel 2.1 beschriebenen Treiber der digitalen Transformation innerhalb der Automobilindustrie führen allerdings dazu, dass sich die Beziehung zwischen den OEMs und ihren (Software-)Lieferanten verändert. Die stetig wachsenden Anforderungen seitens der Fahrzeughersteller an die neuen Technologien brechen die „Machtdynamik“ der traditionellen Beziehungen zwischen OEM und Zulieferer auf. So sind mittlerweile weder der OEM noch die traditionellen Zulieferer dazu in der Lage, die technologischen Anforderungen an neue Systeme vollständig zu definieren. Infolgedessen wird die gemeinschaftliche Entwicklung von OEMs und Zulieferern in Zukunft nicht nur weit verbreitet, sondern voraussichtlich auch notwendig werden. Gleichzeitig besitzt mittlerweile kaum ein einzelner Zulieferer die Fähigkeit, ein System zu liefern, das alle geforderten Technologien durchgängig und wettbewerbsfähig abdeckt. Vielmehr schafft diese Entwicklung Chancen für neue Anbieter, die dazu im Stande sind, den Markt mit neuartigen Kooperationsmodellen zu beliefern.[67]

Angesichts dieser Entwicklung sollte der Einkaufsbereich eine neue Perspektive einnehmen, etwa bei der Lieferantenauswahl für Software. Dabei muss er sich die Frage stellen, ob der jeweilige Zulieferer überhaupt dazu fähig ist, regulatorisch konform zu arbeiten. Da die Verantwortung für zugekaufte Software beim OEM liegt, sind spezifische Maßnahmen und Nachweise zu vereinbaren und festzulegen, um die

[64] Vgl. Brose Fahrzeugteile SE & Co. KG (2017), S. 7f.
[65] Vgl. Herzig und Guderian (2021), S. 3.
[66] Vgl. Kutritz (2004), S. 32.
[67] Vgl. Burkacky, Deichmann und Stein (2019), S. 8 & 30.

Compliance des Zulieferers zu gewährleisten. Auch in Hinblick auf eine Update-Verpflichtung während des gesamten Fahrzeug-Lebenszyklus ist eine wesentlich engere prozessuale Verzahnung zwischen OEMs und ihren Zulieferern erforderlich. Diese Entwicklungen stellen die Fahrzeughersteller jedenfalls vor große Herausforderungen und müssen, zum Beispiel in Lieferantenverträgen, entsprechend berücksichtigt werden.[68]

## 2.3 Normen, Standards und Regelungen zur Informationssicherheit

Die Darstellungen in Kapitel 2.1 haben gezeigt, dass mit der fortschreitenden Digitalisierung und der Entwicklung der Informationstechnologie in der Automobilindustrie das IT-Risiko kontinuierlich zunimmt. Dementsprechend groß ist das Streben vieler Automobilhersteller danach, ihre Daten und Informationen in angemessenem Ausmaß zu schützen.[69] Um die Risiken und Gefährdungen, die sich aus Lücken in der Informationssicherheit ergeben, auf ein akzeptables Niveau zu reduzieren, sollten adäquate Kontrollen gewählt werden. Im Fokus steht dabei der Schutz von Daten hinsichtlich der Anforderungen an die drei Grundwerte der Informationssicherheit: Vertraulichkeit, Verfügbarkeit und Integrität.[70] Sie werden wie folgt definiert:

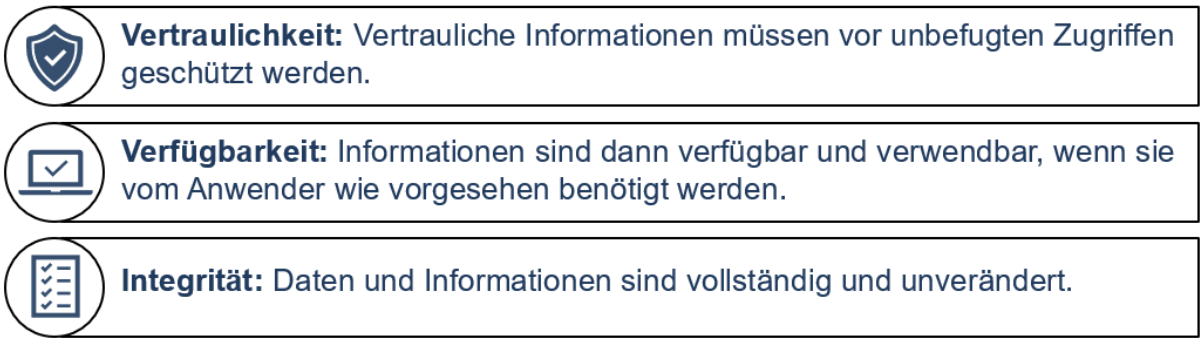



**Abbildung 9: Drei Grundziele der Informationssicherheit[71]**

Bei der Auswahl adäquater Sicherheitskontrollen kann auf eine Vielzahl gängiger Normen und Standards zurückgegriffen werden. Wesentlicher Unterschied zwischen diesen beiden Begriffen ist, dass lediglich offiziell ernannte Normungsorganisationen

[68] Vgl. Herzig und Guderian (2021), S. 3 & 5.
[69] Vgl. Królikowski und Ubowska (2021), S. 4259f.
[70] Vgl. Bundesamt für Sicherheit in der Informationstechnik – BSI (2017), S. 85.
[71] Quelle: Eigene Darstellung auf Basis von Bundesamt für Sicherheit in der Informationstechnik – BSI (2017), S. 87, 93 & 94.

ihre Standards auch „Norm“ nennen dürfen.[72] Die wichtigsten Standards und Normen mit Bezug zur Informationssicherheit sind in Tabelle 2 dargestellt:

| Typ | Titel | Herausgeber |
|---|---|---|
| Norm | ISO/IEC 27001 IT-Sicherheitsverfahren-Informationssicherheits-Managementsysteme-Anforderungen | International Standards Organization |
| Norm | ISO 9001 Qualitätsmanagementsysteme-Anforderungen | International Standards Organization |
| Norm | ISO/IEC 20000 Informationstechnik-Service Management | International Standards Organization |
| Norm | ISO 22301 - Sicherheit und Resilienz-Business Continuity Management System-Anforderungen | International Standards Organization |
| Standard | ISO 27001 Zertifizierung auf Basis von IT-Grundschutz | Bundesamt für Sicherheit in der Informationstechnik (BSI) |
| Standard | StarAudit | EuroCloud® Europe a.s.b.l |
| Standard | Trusted Information Security Assessment Exchange (TISAX) | ENX Association |
| Standard | CSA Security Trust, Assurance and Risk (STAR) | Cloud Security Alliance (CSA) |

Tabelle 2: Standards und Normen zur Informationssicherheit[73]

Ziel dieses Kapitels ist es einen Überblick über verschiedene Regelwerke der Informationssicherheit in der Automobilindustrie zu verschaffen. International weit verbreitet sind die Norm ISO 27001 sowie der vom VDA entwickelte und speziell auf die Automobilindustrie zugeschnittene TISAX Standard. Angesichts ihrer Relevanz werden sie in Kapitel 2.3.1 näher betrachtet. Im Unterschied zu ISO 27001 und TISAX bilden die Anfang 2021 von der UNECE verabschiedeten Regelungen R155 und R156 zu CSMS und SUMS eine gesetzlich verpflichtende Grundlage für die Zulassung neuer Fahrzeuge. Ihre genaue Betrachtung erfolgt in Kapitel 2.3.2 und stellt die Basis für die nachfolgende Entwicklung des Prüfkatalogs dar.

## 2.3.1 ISO 27001 und TISAX

Bei der ISO 27001 handelt es sich um die erste internationale Norm zum Informationssicherheitsmanagement, die auch eine Zertifizierung ermöglicht. Diesem Aspekt verdankt die ISO 27001 ihre besondere Popularität in der Wirtschaft.[74] Der vom VDA entwickelte TISAX Standard spielt angesichts des Fokus dieser Arbeit auf die Automobilindustrie eine ebenso wichtige Rolle. Gemeinsam bilden diese beiden

[72] Vgl. Naybzadeh (2021), S. 10.
[73] Quelle: Eigene Darstellung auf Basis von Naybzadeh (2021), S. 13ff.
[74] Vgl. Sowa (2017), S. 9.

Normen und Standards häufig die Basis zur weiteren Zertifizierung nach UNECE R155 und R156.

### ISO 27001

ISO 27001 ist eine internationale Norm, die Managementsysteme für die Informationssicherheit regelt. Sie wurde erstmals am 14. Oktober 2005 veröffentlicht und basiert auf der britischen Norm BS 7799-2 (Information Security Management System).[75] ISO 27001 ist dabei Teil der sehr umfangreichen ISO 27000 Normenreihe. Diese wird ständig weiter ausgebaut und besteht neben der Hauptnorm 27001 aus den unterstützenden Normen 27002 bis 27008 (exkl. 27006). Sie vertiefen bestimmte Aspekte der Hauptnorm, während die Basisnorm ISO 27000 das gesammelte Begriffskompendium enthält.[76] Dieser Zusammenhang ist in Abbildung 10 dargestellt.

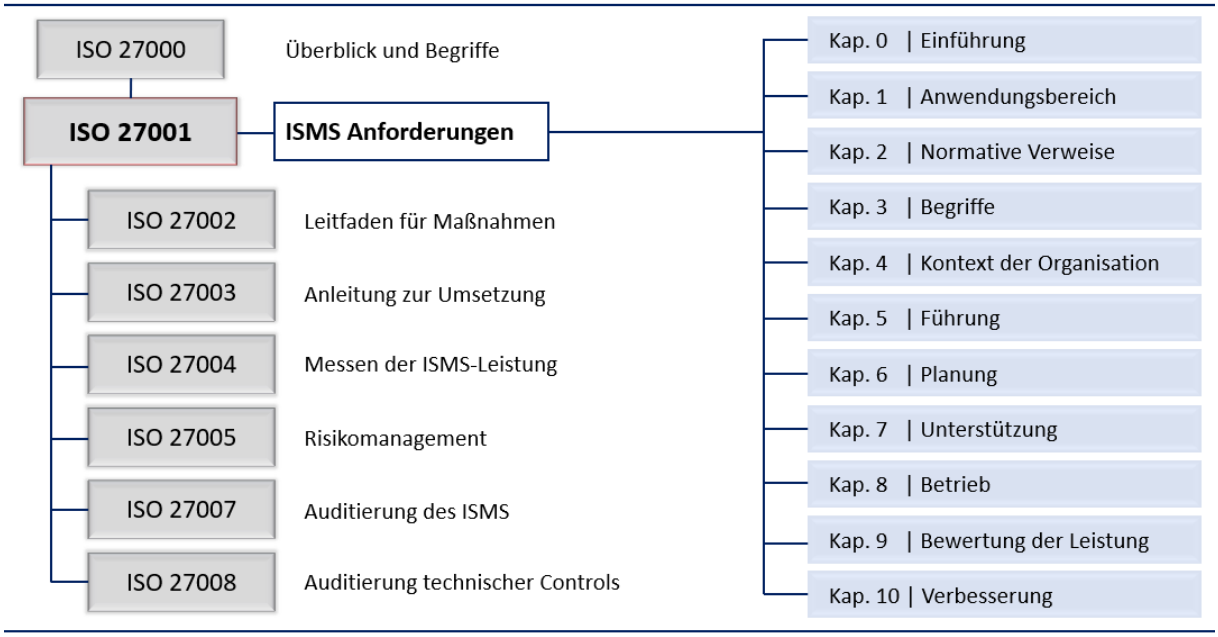



**Abbildung 10: Normenreihe ISO / IEC 27000 und Inhaltsverzeichnis[77]**

Die Hauptnorm selbst beginnt mit einer allgemeinen Einleitung in das Themengebiet in Kapitel 0, worin die Notwendigkeit und das Ziel von Informationssicherheits-managementsystemen betont wird. Nach der Beschreibung des Anwendungsbereiches der Norm in Kapitel 1 wird in Kapitel 2 und 3 auf die Basisnorm verwiesen. Kapitel 4 bis 10 stellen den Hauptteil der Norm dar und definieren die Anforderungen an ein System zum Management der Informationssicherheit, kurz:

[75] Vgl. Królikowski und Ubowska (2021), S. 4262.
[76] Vgl. Kersten et al. (2020), S. 3.
[77] Quelle: Eigene Darstellung in Anlehnung an Kersten et al. (2020), S. 3.

ISMS = Informations-Sicherheits-Managementsystem. Deren Inhalte werden im Folgenden gekürzt dargestellt:

*Kapitel 4: Kontext der Organisation:*

Die Organisation muss jene Themen bestimmen, die eine Auswirkung auf das Informationssicherheitsmanagementsystem haben. Dazu muss sie die Erfordernisse und Erwartungen aller involvierten Parteien verstehen, den Anwendungsbereichs des Informationssicherheitsmanagementsystems festlegen sowie das gesamte System aufbauen und fortlaufend verbessern.[78]

*Kapitel 5: Führung*

Hier wird unter anderem festgelegt, dass die oberste Leitung eines Unternehmens für die Verankerung der Informationssicherheitsziele, das Bereitstellen der notwendigen Ressourcen sowie die Förderung der fortlaufenden Verbesserung verantwortlich ist. Auch muss sie eine angemessene Informationssicherheitspolitik festlegen und sicherstellen, dass die Verantwortlichkeiten und Befugnisse für Rollen mit Bezug zur Informationssicherheit zugewiesen und bekannt gemacht werden.[79]

*Kapitel 6: Planung*

Dieses Kapitel behandelt hauptsächlich Maßnahmen zum Umgang mit Chancen und Risiken für die Informationssicherheit. Dabei muss einerseits innerhalb der Informationssicherheitsrisikobeurteilung festgelegt werden, wie Sicherheitsrisiken identifiziert, analysiert und bewertet werden. Andererseits muss im Zuge der Informationssicherheitsrisikobehandlung ein Plan mit erforderlichen Maßnahmen zum Entgegenwirken von Risiken definiert werden.[80]

*Kapitel 7: Unterstützung*

Kapitel 7 der ISO 27001 ist recht umfangreich und behandelt unterstützende Elemente und Ressourcen für das ISMS. Dazu zählt zum Beispiel die Bestimmung von Kompetenzen, das Schaffen von Bewusstsein, die Bereitstellung erforderlicher Ressourcen, die Bestimmung interner und externer Kommunikation sowie die Dokumentation von Information.[81]

*Kapitel 8: Betrieb*

ISO 27001 sieht vor, dass die Organisation jene Prozesse plant, verwirklicht und steuert, die zur Erfüllung der Informationssicherheitsanforderungen notwendig sind.

[78] ISO/IEC 27001:2017-02, Kap. 4.
[79] ISO/IEC 27001:2017-02, Kap. 5.
[80] ISO/IEC 27001:2017-02, Kap. 6.
[81] ISO/IEC 27001:2017-02, Kap. 7.

Das beinhaltet etwa die Durchführung von Informationssicherheitsrisikobeurteilungen in bestimmten Abständen oder die Umsetzung des Plans zur Informationssicherheits-risikobehandlung.[82]

*Kapitel 9: Bewertung der Leistung*

In diesem Kapitel geht es um die Bewertung der Informationssicherheitsleistung und der Wirksamkeit des Informationssicherheitsmanagementsystems durch die Organisation. Ein geeignetes Instrument hierzu wären zum Beispiel interne Audits, die die Organisation in geplanten Abständen durchführt. In jedem Fall muss die Organisation dokumentierte Information als Nachweis der Ergebnisse der Bewertung aufbewahren.[83]

*Kapitel 10: Verbesserung*

Wie bereits mehrfach erwähnt, stellt die Sicherstellung der kontinuierlichen Verbesserung einen wichtigen Aspekt innerhalb von ISO 27001 dar. Ebenso muss die Organisation entsprechend reagieren, sobald eine Nichtkonformität auftritt.[84]

Im Anhang der Norm, dem Annex A, befinden sich zudem vorgeschlagene Maßnahmen und Maßnahmenziele, die im Rahmen des Risikomanagements berücksichtigt werden müssen.[85] Abgesehen davon ist die Norm ISO 27001 aber recht allgemein gehalten. Das hat den Grund, dass es sich bei ihr um kein direkt umsetzbares Arbeitsprogramm handelt. Auch sind die Methoden für die Umsetzung nicht festgeschrieben. Dafür ist die Norm auf Organisationen jeder Art und Größe sowie länderübergreifend anwendbar. Die wesentlichen Aufgaben des ISMS zusammengefasst sind dabei die Formulierung von (Sicherheits-)Zielen, die Bestimmung der Assets, die Risikobeurteilung, die Risikobehandlung sowie die kontinuierliche Verbesserung.[86]

**TISAX**

Bis 2017 stellte ISO 27001 auch in der Automobilindustrie das häufigste Instrument zur Verringerung von IT-Risiken dar. Mit Trusted Information Security Assessment Exchange (TISAX) wurde in diesem Jahr jedoch eine neue Lösung eingeführt, die sich spezifisch an die Unternehmen der Automobilindustrie richtet und fortan einen neuen Standard zur Sicherstellung der Informationssicherheit innerhalb des Automotive Sektors bildete.[87] Konkret handelt es sich bei TISAX um einen vom Verband der

[82] ISO/IEC 27001:2017-02, Kap. 8.
[83] ISO/IEC 27001:2017-02, Kap. 9.
[84] ISO/IEC 27001:2017-02, Kap. 10.
[85] Vgl. Naybzadeh (2021), S. 13f.
[86] Vgl. Kersten et al. (2020), S. 4ff.
[87] Vgl. Królikowski und Ubowska (2021), S. 4260.

deutschen Automobilindustrie (VDA) ins Leben gerufenen Prüf- und Austauschmechanismus, der die gemeinsame Anerkennung von Prüfergebnissen zwischen den teilnehmenden Unternehmen ermöglichen soll. Als Grundlage für die Prüfungen gilt der Katalog zum Information Security Assessment des VDA (VDA ISA), welcher verschiedene Stufen der Informationssicherheit festlegt.[88]

Ab 2018 muss jedes Unternehmen, das für Kunden aus der deutschen Automobilindustrie arbeitet, ein TISAX-Zertifikat besitzen. Aufgrund der Tatsache, dass die (Zuliefer-)Unternehmen der Automobilindustrie häufig international ausgerichtet sind, wurde TISAX zunächst auf europäische Unternehmen ausgedehnt, entwickelt sich aber mittlerweile sogar zu einem weltweiten Standard. Dem VDA zufolge haben sich bis Ende 2020 über 2.800 Unternehmen mit 5.100 Standorten für TISAX angemeldet und es wurden über 2.600 Prüfungen durchgeführt. TISAX-Teilnehmer können dabei alle Unternehmen mit Bezug zur Automobilbranche sein, die Informationssicherheit nachweisen wollen (siehe Abbildung 11).[89]

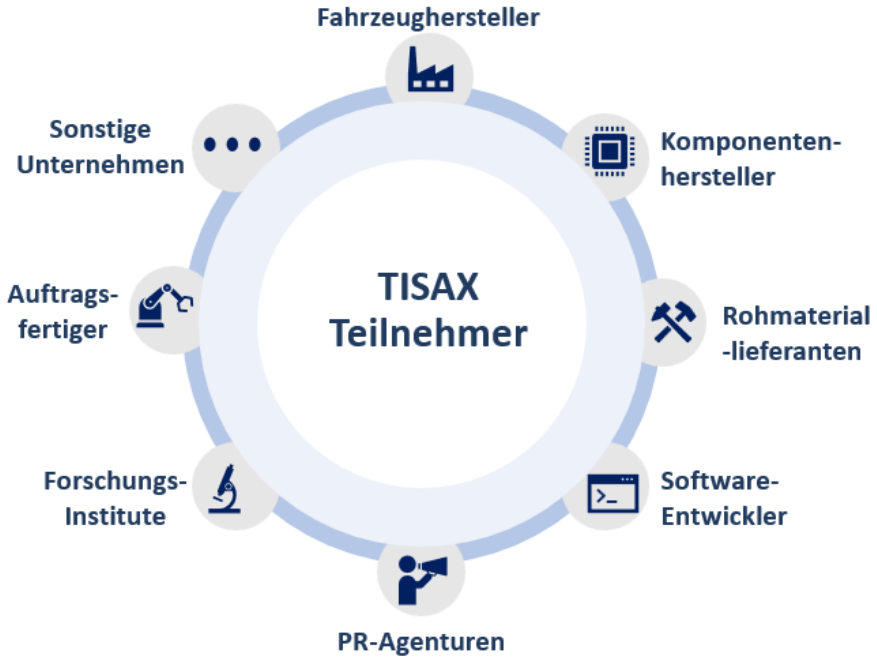



Abbildung 11: TISAX teilnehmende Unternehmen[90]

Der TISAX-Prozess beginnt in der Regel damit, dass ein Unternehmen von einem Partner aufgefordert wird, ein definiertes Niveau der Informationssicherheit nachzuweisen. Um dieser Aufforderung nachzukommen, muss ein 3-stufiger TISAX-

[88] Vgl. Naybzadeh (2021), S. 29f.
[89] Vgl. Królikowski und Ubowska (2021), S. 4260f.
[90] Quelle: Eigene Darstellung in Anlehnung an Królikowski und Ubowska (2021), S. 4261.

Prozess durchlaufen werden. An erster Stelle steht die **Registrierung**, innerhalb der der Umfang der Prüfung, festgelegt wird. Anschließend bestreitet das teilnehmende Unternehmen die **Prüfung**, die von einem TISAX-Prüfdienstleister durchgeführt wird. Der dritte und letzte Schritt besteht darin, das **Prüfergebnis** mit dem Partner zu teilen.[91] Aufwand und Tiefe der Prüfung orientieren sich dabei anhand der Anzahl angestrebter Prüfziele. Derer gibt es insgesamt acht Stück und sie können als Maßstab für das angestrebte Informationssicherheitsmanagementsystem betrachtet werden. In der nachstehenden Tabelle sind die acht TISAX-Prüfziele dargestellt.

| Nr. | ISA-Kriterienkatalog | TISAX-Prüfziel |
|---|---|---|
| 1 | Informationssicherheit | Informationen mit hohem Schutzbedarf |
| 2 | Informationssicherheit | Informationen mit sehr hohem Schutzbedarf |
| 3 | Prototypenschutz | Schutz von Prototypen-Bauteilen und -Komponenten |
| 4 | Prototypenschutz | Schutz von Prototypenfahrzeugen |
| 5 | Prototypenschutz | Umgang mit Erprobungsfahrzeugen |
| 6 | Prototypenschutz | Schutz von Prototypen während Veranstaltungen und Film- und Fotoshootings |
| 7 | Datenschutz | Gemäß Artikel 28 der Datenschutz-Grundverordnung (DSGVO) |
| 8 | Datenschutz | Datenschutz bei besonderen Kategorien personenbezogener Daten gemäß Artikel 28 mit besonderen Kategorien personenbezogener Daten wie in Artikel 9 der Datenschutz-Grundverordnung (DSGVO) angegeben. |

Tabelle 3: TISAX-Prüfziele[92]

Zusätzlich zu ISO 27001 stellt TISAX in jedem Fall eine weitere Möglichkeit zur Standardisierung, Qualitätssicherung und Anerkennung von Audits dar. Dank des Standards können Unternehmen in der Automobilindustrie ihren Vertragspartnern zeigen, dass das Niveau der Informationssicherheit in ihrer Organisation ausreichend ist und den Erwartungen eines an einer Zusammenarbeit interessierten Vertragspartners entspricht.[93]

### 2.3.2 UNECE Regelungen R155 und R156

Während ISO 27001 und TISAX Informationssicherheit gesamtheitlich betrachten, waren konkrete Fragestellungen zum Thema Cybersicherheit im Automobilsektor bis vor kurzem unreguliert. Das änderte sich jedoch im Juni 2020 als eine Arbeitsgruppe der Vereinten Nationen die UNECE-Regelungen R155 und R156 verabschiedete.[94] UNECE R155 fordert von den OEMs einen Nachweis über ein funktionierendes

[91] Vgl. ENX Association (2021), S. 10f.
[92] Quelle: Eigene Darstellung in Anlehnung an ENX Association (2021), S. 31.
[93] Vgl. Królikowski und Ubowska (2021), S. 4266.
[94] Vgl. Burkacky et al. (2020), S. 7.

Cybersecurity Management System (CSMS) für den gesamten Fahrzeug-Lebenszyklus. UNECE R156 schreibt vor, dass ein normgerechtes Software-Update Management System (SUMS) aufgebaut und betrieben werden muss.[95] In Kraft getreten sind die Regelungen bereits im Januar 2021. Ab Juli 2022 sind die Vorgaben innerhalb der Europäischen Union verpflichtend für alle neuen Fahrzeugtypen, ab Juli 2024 dann für sämtliche neu produzierten und neu zugelassenen Fahrzeuge. Diese verpflichtende Eigenschaft der beiden Regelungen stellt einen der wesentlichsten Unterschiede gegenüber ISO 27001 und TISAX dar. Sofern die OEMs Fahrzeuge in den Mitgliedsstaaten der UNECE absetzen wollen, führt künftig kein Weg an einer SUMS und CSMS Zertifizierung vorbei. Die beiden Regelungen sind dabei das Ergebnis der Arbeit des Weltforums für die Harmonisierung von Fahrzeugvorschriften des Inland Transport Comittee (ITC). Als Arbeitsgruppe WP.29 ist sie Teil der Wirtschaftskommission der Vereinten Nationen für Europa (UNECE), bzw. der Untergruppe GRVA für automatisierte Fahrzeuge. In Abbildung 8 sind diese Zusammenhänge inklusive Einordnung der neuen Regelung zu CSMS und SUMS dargestellt.

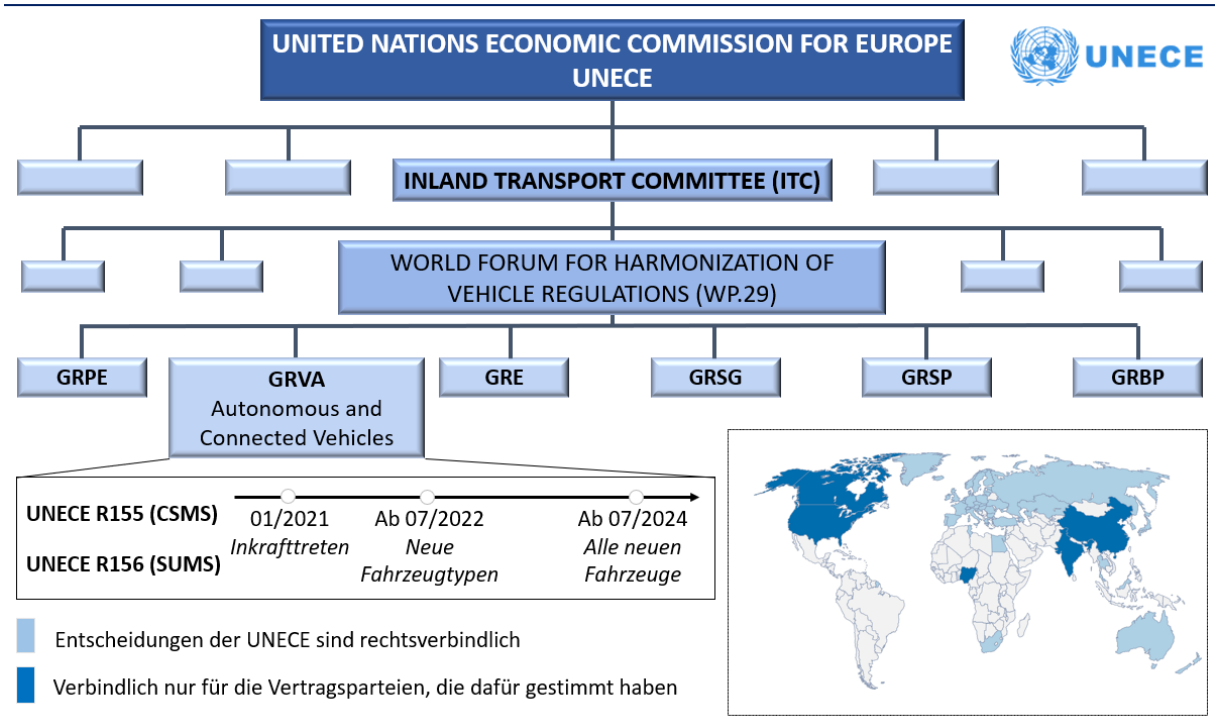



**Abbildung 12: UNECE Organisation und Mitgliedsstaaten[96]**

Sobald die Richtlinien von den Mitgliedsstaaten der UNECE in nationale Gesetze überführt worden sind, müssen die OEMs für die Typgenehmigung von ihren

[95] Vgl. Herzig und Guderian (2021), S. 1f.
[96] Quelle: Eigene Darstellung auf Basis von: https://unece.org/wp29-introduction (Gelesen am: 21.10.2021)

Fahrzeugen spezielle Verfahren zur Sicherstellung der Cybersicherheit und Software-Update Fähigkeit nachweisen.[97] Wie in Abbildung 13 ersichtlich, sieht der Genehmigungsprozess vor, dass der Fahrzeughersteller oder ein bevollmächtigter Vertreter einen Antrag auf Typgenehmigung bei der Genehmigungsbehörde einreichen. Diese oder ein von ihr benannter technische Dienst führt anschließend eine Prüfung der Cybersicherheits- und Software-Update-Managementsysteme durch, wobei die notwendigen Dokumentationen und Informationen vom OEM bereitzustellen sind. Ist die Prüfung erfolgreich, erteilt die Genehmigungsbehörde die Fahrzeugzulassung.[98]

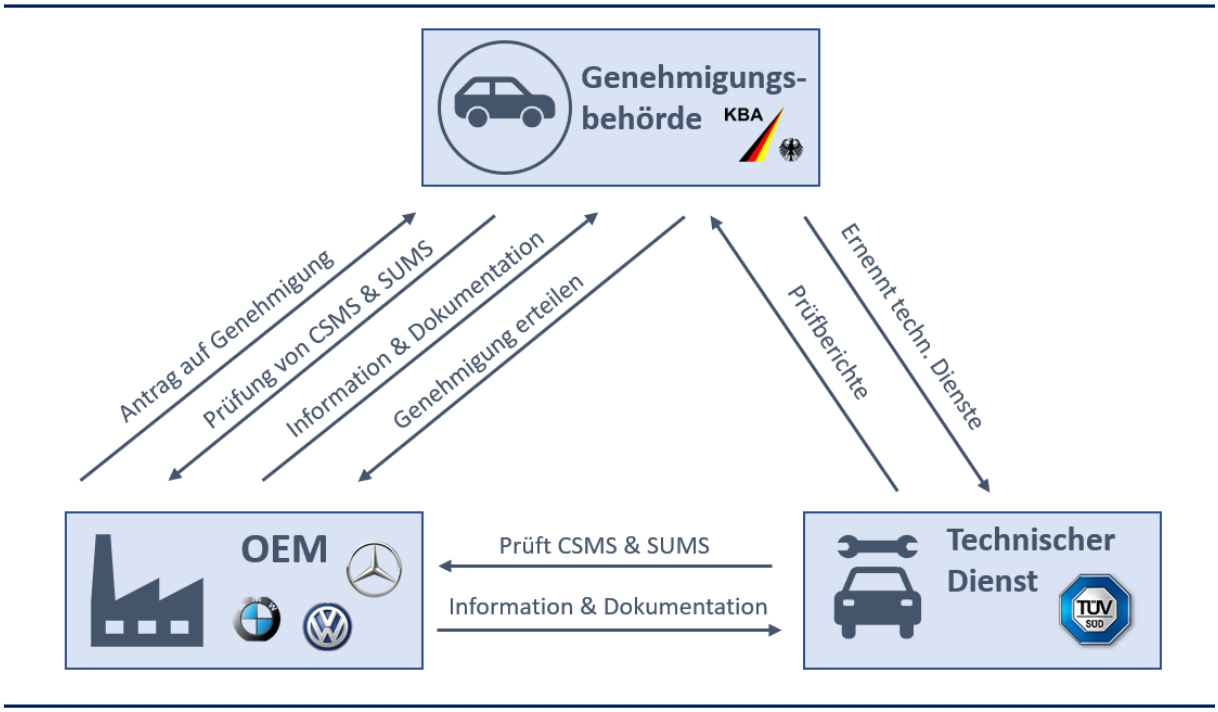



**Abbildung 13: SUMS & CSMS Genehmigungsprozess[99]**

Oben beschriebene Prozesse und Informationen beziehen sich gleichermaßen auf UNECE R155 und R156. Angesichts des Ziels dieser Arbeit – der Entwicklung eines Prüfkatalogs im Bereich Software-Update Management – wird im Folgenden näher auf die Inhalte der UNECE Regelung R156 (SUMS) eingegangen.

### Grundlegendes zu UNECE R156 (SUMS)

Die Beschäftigung mit der Regelung seitens der OEMs ist jedenfalls längst überfällig. Fehler beim Update Management können auch nachträglich zum Verlust der Zulassung führen und die Situation wird aktuell durch den Umstand verschärft, dass

[97] Vgl. Burkacky et al. (2020), S. 8.
[98] Vgl. UNECE R156:2021-03, Kap. 3 & Kap. 5.
[99] Eigene Darstellung

der Zeitplan für R156 kurzfristig vorgezogen wurde und nun analog zu dem für UNECE R155 gilt.[100] Insgesamt besteht die Regelung der UNECE zu SUMS aus 12 Kapiteln. Außerdem enthält UNECE R156 einen Anhang, der sich aus vier weiteren Kapiteln zusammensetzt. Im Folgenden werden die inhaltlichen Anforderungen der UNECE R156 kurz erläutert und es wird aufgezeigt, was es bei deren Umsetzung zu berücksichtigen gilt.

*Kapitel 1: Anwendungsbereich*

Kapitel 1 definiert den Anwendungsbereich für die UNECE Regelung. Folglich handelt es sich dabei um Fahrzeuge der nachfolgenden Fahrzeugklassen:

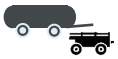
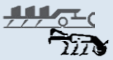
| Klasse | Beschreibung | |
|---|---|---|
| M | Kraftwagen zur Personenbeförderung mit mindestens vier Rädern |  |
| N | Kraftfahrzeuge zur Güterbeförderung mit mindestens vier Rädern |  |
| O | Anhänger verschiedener Klassen |  |
| R | Land- oder Forstwirtschaftliche Anhänger |  |
| S | Gezogene auswechselbare Geräte für den Einsatz in der Land- und Forstwirtschaft |  |
| T | Land- oder Forstwirtschaftliche Zugmaschinen auf Rädern |  |

**Tabelle 4: Fahrzeugklassen mit Verpflichtung zu einem SUMS[101]**

*Kapitel 2: Begriffsbestimmungen*

Kapitel 2 enthält eine Sammlung und Kurzbeschreibung aller relevante Begriffe, die in der Regelung zur Anwendung gelangen. Dazu zählen unter anderem „RX-Software-Identifikationsnummer“, „Softwareaktualisierungsmanagementsystem“ oder „Sicherer Zustand“. Auf die genaue Bedeutung der Begriffe wird im Rahmen dieses Kapitels nicht näher eingegangen. Sofern relevant und notwendig erfolgt eine Begriffserläuterung im Rahmen der Entwicklung des Prüfkatalogs in Kapitel 5.[102]

*Kapitel 3: Antrag auf Genehmigung*

Kapitel 3 regelt den Prozess zur Beantragung auf Genehmigung eines Fahrzeugtyps im Rahmen der UNECE R156. Dieser gleicht weitestgehend dem Beantragungsprozess, der auch im Zuge von UNECE R155 zur Anwendung kommt,

[100] Vgl. Herzig und Guderian (2021), S. 3.
[101] Quelle: Eigene Darstellung in Anlehnung an UNECE R156:2021-03, Kap. 1.
[102] Vgl. UNECE R156:2021-03, Kap. 2.

und wurde in seinen Grundzügen bereits in Kapitel 3.2 erläutert. Ergänzend hierzu beschreibt Kapitel 3 das Vorgehen für den Fall, dass an Beschreibungen nachweislich geistige Eigentumsrechte bestehen oder spezifisches Know-How preisgegeben wird. In solchen Fällen müssen lediglich jene Informationen übermittelt werden, die zur Überprüfung der Regelung ausreichend sind.[103]

Im Zuge dieses Absatzes wird zudem explizit darauf hingewiesen, dass dieses Vorgehen gleichermaßen für den Umgang mit geistigen Eigentumsrechten oder spezifischem Know-How von Lieferanten anzuwenden ist. Obwohl dies in der Regelung ansonsten nicht gefordert wird, impliziert es indirekt die Notwendigkeit der Umsetzung und Sicherstellung von gewissen SUMS Anforderungen auch bei Lieferanten. So sind die Fahrzeughersteller die juristische Einheit, die den Antrag auf Genehmigung stellen, gleichzeitig müssen sich aber auch ihre vorgelagerten Partner in der Supply Chain auf die Erfordernisse des SUMS vorbereiten.[104]

*Kapitel 4: Kennzeichnung*

Kapitel 4 legt fest, dass an jedem Fahrzeug sichtbar und an gut zugänglicher Stelle ein entsprechendes Genehmigungszeichen anzubringen ist, welches dem im Anhang befindlichen Muster entspricht. Dabei muss das Genehmigungszeichen auf dem vom Hersteller angebrachten Typenschild des Fahrzeugs oder in dessen Nähe angebracht werden.[105]

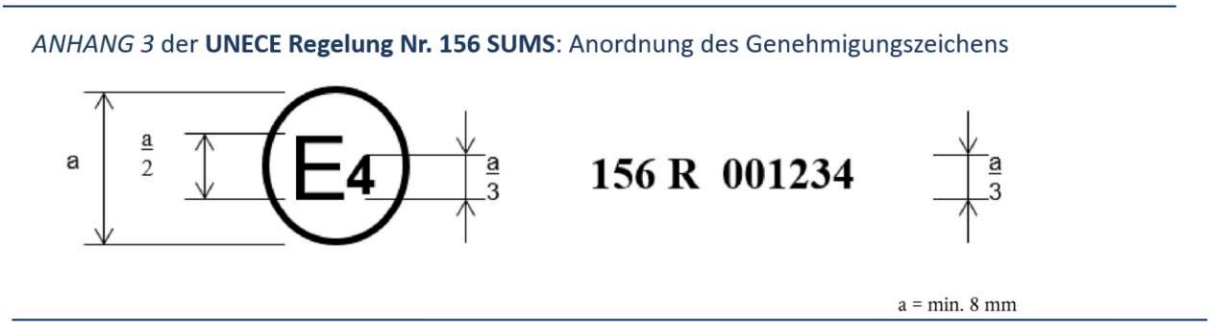



**Abbildung 14: Kennzeichnung der Typgenehmigung[106]**

Das in Abbildung 14 dargestellte Muster für die Anordnung eines Genehmigungskennzeichens besagt, dass der betreffende Typ des Straßenfahrzeugs in den Niederlanden (E4) nach der Regelung Nr. 156 unter der Genehmigungsnummer 001234 genehmigt worden ist. Aus den ersten beiden Ziffern der

[103] Vgl. UNECE R156:2021-03, Kap. 3.
[104] Vgl. Herzig und Guderian (2021), S. 3.
[105] Vgl. UNECE R156:2021-03, Kap. 4.
[106] Quelle: UNECE R156:2021-03, Anhang 3.

Genehmigungsnummer geht hervor, dass die Genehmigung nach den Vorschriften dieser Regelung in ihrer ursprünglichen Fassung (00) erteilt wurde.[107]

*Kapitel 5: Genehmigung*

In Kapitel 5 ist der vorgeschriebene Genehmigungsprozess abgebildet. Er sieht vor, dass eine Typgenehmigung nur dann erteilt werden darf, wenn sichergestellt wurde, dass der Hersteller entsprechende Verfahren zur Softwareaktualisierung ordnungsgemäß implementiert hat. Auch dieser Prozess ist weitestgehend deckungsgleich mit jenem nach UNECE R155 und wurde in Kapitel 3.2 bereits im Detail erläutert.[108]

*Kapitel 6: Konformitätsbescheinigung für das Softwareaktualisierungs-managementsystem*

Kapitel 6 der UNECE R156 legt fest, dass eine Genehmigungsbehörde die Bewertung des Herstellers durchführt und eine Konformitätsbescheinigung für das Softwareaktualisierungsmanagementsystem ausstellt. Sofern sie nicht widerrufen wird, bleibt diese Bescheinigung höchstens drei Jahre ab dem Datum der Ausstellung gültig. Die Behörde kann zudem jederzeit überprüfen, ob die Anforderungen weiterhin erfüllt sind. Kommt es seitens des Herstellers zu einer Änderung, die einen Einfluss auf das Softwareaktualisierungsmanagementsystem hat, ist die Genehmigungsbehörde darüber zu unterrichten. Sie entscheidet anschließend, ob neue Prüfungen erforderlich sind.[109]

*Kapitel 7: Allgemeine Vorschriften*

Kapitel 7 stellt das umfangreichste Kapitel der UNECE Regelung zu SUMS dar. Es verlangt eine Vielzahl an (dokumentierten) Verfahren und Prozessen zur Erfüllung sämtlicher Anforderungen an das Softwareaktualisierungsmanagementsystem. Die wesentlichsten Anforderungen umfassen folgende Aspekte:[110]

- Speicherung und Schutz von für das SUMS relevanten Informationen und Dokumentationen
- Sicherstellung der Zugänglichkeit zu Informationen und Dokumentationen
- Eindeutige Identifizierbarkeit von Software(-Aktualisierungen) mittels einer Software-Identifikationsnummer (inkl. Möglichkeit der Aktualisierung und leichte Ablesbarkeit der Identifikationsnummer)

[107] Vgl. UNECE R156:2021-03, Anhang 3.
[108] Vgl. UNECE R156:2021-03, Kap. 5.
[109] Vgl. UNECE R156:2021-03, Kap. 6.
[110] Vgl. UNECE R156:2021-03, Kap. 7.

- Möglichkeit der Identifikation von Zielfahrzeugen mittels Software-Identifikationsnummer
- Definition von Abhängigkeiten verschiedener Systeme
- Schutz vor Manipulation von Softwareaktualisierungen
- Gewährleistung der Fahrzeugsicherheit

*Kapitel 8: Änderung des Fahrzeugtyps und Erweiterung der Typgenehmigung*

Dieses Kapitel regelt das Vorgehen für den Fall von Änderungen am Fahrzeugtyp. Diese müssen der Genehmigungsbehörde mitgeteilt werden, die dann entweder zum Schluss kommt, dass die vorgenommenen Änderungen weiterhin den Vorschriften der vorherigen Typgenehmigung entsprechen oder dass ein neuer Prüfbericht erforderlich ist.[111]

*Kapitel 9: Übereinstimmung der Produktion*

Kapitel 9 verweist auf das Verfahren zur Kontrolle der Übereinstimmung der Produktion aus einer anderen UNECE Norm (E/ECE/TRANS/505/Rev.3). Dort ist geregelt, dass jedes hergestellte Fahrzeug auch tatsächlich mit dem genehmigten Fahrzeugtyp übereinstimmen muss.[112] Innerhalb von SUMS wird zusätzlich auf die ordnungsgemäße Protokollierung und Überprüfung durch den technischen Dienst hingewiesen.[113]

*Kapitel 10: Maßnahmen bei Abweichungen der Produktion*

Aufbauend darauf regelt Kapitel 10 das Vorgehen für die Nicht-Einhaltung der Übereinstimmung der Produktion. In diesem Fall kann die für einen Fahrzeugtyp erteilte Genehmigung zurückgenommen werden, wobei alle Vertragsparteien darüber zu unterrichten sind.[114]

*Kapitel 11: Endgültige Einstellung der Produktion*

Wird die Produktion eines nach dieser Regelung genehmigten Fahrzeugtyps eingestellt, müssen die Genehmigungsbehörde und in weiterer Folge sämtliche weitere Vertragsparteien darüber unterrichtet werden.[115]

*Kapitel 12: Namen und Anschriften der Typgenehmigungsbehörde und der technischen Dienste, die die Prüfung für die Genehmigung durchführen*

[111] Vgl. UNECE R156:2021-03, Kap. 8.
[112] Vgl. UNECE/TRANS/505/Rev.3, Schedule 1.
[113] Vgl. UNECE R156:2021-03, Kap. 9.
[114] Vgl. UNECE R156:2021-03, Kap. 10.
[115] Vgl. UNECE R156:2021-03, Kap. 11.

Kapitel 12 regelt die Kommunikation und das Vorgehen zwischen an der Regelung beteiligten Genehmigungsbehörden und technischen Diensten. Sie richtet sich in erster Linie nicht an die OEMs.[116]

Im Anschluss an Kapitel 1 bis 12 befinden sich zudem vier Anhänge. Neben einem Beschreibungsbogen handelt es sich dabei um ein Mitteilungsblatt, dem Muster für ein Genehmigungszeichen sowie einem Muster der Konformitätsbescheinigung für das Softwareaktualisierungsmanagementsystem.[117] Ziel des OEM muss es jedenfalls sein, ein SUMS aufzubauen, das eine Qualitätskontrolle, eine zuverlässige Ausführung der Updates und eine ausreichende Cybersicherheit gewährleistet. 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). Bei der Umsetzungsplanung für ein SUMS lohnt sich folglich eine umfassende Betrachtung entlang der gesamten Zeitachse.[118]

Gleichzeitig macht sich zudem die vertiefende Berücksichtigung aller Interaktionen in der Lieferkette bezahlt. Wie bereits erwähnt sieht die Regelung zumindest indirekt vor, dass auch Lieferanten zur Umsetzung von Verfahren zur Risikoeindämmung in Bezug auf Software-Updates verpflichtet werden. Als Vertragspartner in Richtung Fahrzeugkäufer obliegt es dem OEM sicherzustellen, dass der jeweilige Zulieferer dazu in der Lage ist, regulatorisch konform zu arbeiten.[119] Zum derzeitigen Zeitpunkt unklar ist jedoch die konkrete Bedeutung der Regelung für die Beziehung zwischen OEM und Lieferant. Wenngleich offensichtlich ist, dass spezifische Vereinbarungen zu treffen sind, bietet sie keine expliziten Anweisungen für den Umgang mit Zulieferunternehmen in Hinblick auf Software-Updates.

**Zusammenhang mit UNECE R155 (CSMS)**

Ungeachtet der Tatsache, dass UNECE R155 und R156 zwei unterschiedliche Regelungen darstellen, geht die Umsetzung der beiden Regelungen in jedem Fall miteinander einher. So kann beispielsweise ohne SUMS kein zuverlässiges Level bei der Cyber Security von Fahrzeugen erzielt werden.[120] Ebenso sind die Zeitpläne für die Umsetzung der beiden Regularien identisch. Inhaltlich gibt es deutliche Überschneidungen in Bezug auf den Beantragungs- und Genehmigungsprozess, auf die Kennzeichnung sowie auf das Vorgehen zur Sicherstellung der Übereinstimmung der Produktion. Das CSMS Thema ist also eng mit dem Komplex Software Update Management (SUMS) verbunden.

[116] Vgl. UNECE R156:2021-03, Kap. 12.
[117] Vgl. UNECE R156:2021-03, Anhang.
[118] Vgl. Herzig und Guderian (2021), S. 5 & 2.
[119] Vgl. Burkacky et al. (2020), S. 10.
[120] Vgl. Herzig und Guderian (2021), S. 4.

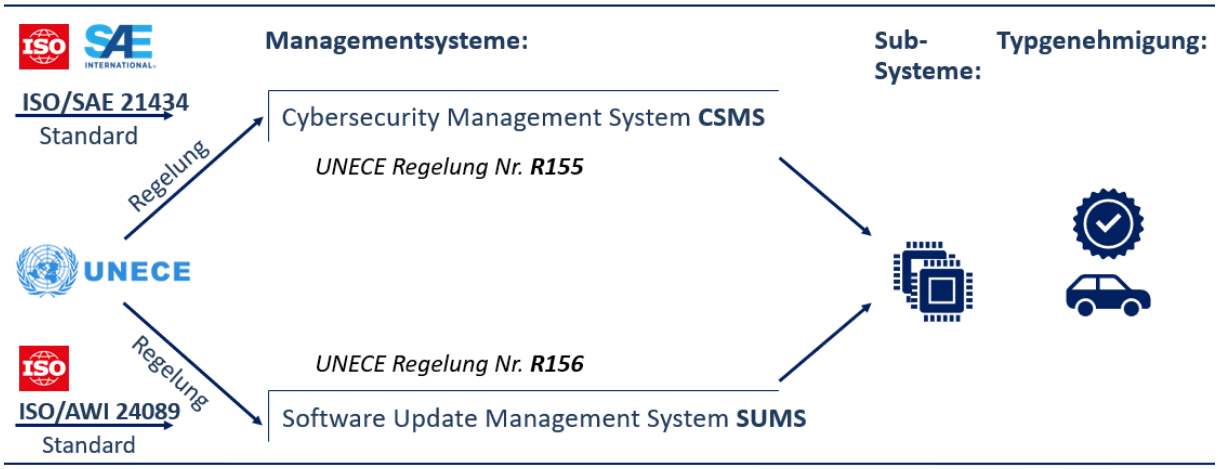



**Abbildung 15: Zusammenhang zwischen SUMS und CSMS**[121]

In Abbildung 15 ist das Zusammenspiel zwischen den beiden Regelungen ersichtlich. An erster Stelle steht auf der linken Seite die UNECE, die zwei Regularien mit ähnlichen Forderungen verabschiedet hat. Der obere Strang beschreibt die regulatorischen Anforderungen an ein Cybersicherheitsmanagementsystem die sich aus der UNECE R156 ergeben. Der untere Strang bezieht sich auf R156, also auf das Software-Update Managementsystem. Passend zur jeweiligen Regelung gibt es zwei von der ISO entwickelte Standards, wobei die Veröffentlichung der ISO 24089 als SUMS Standard noch ausständig ist. Beide Stränge kommen zusammen, wenn Komponenten oder der gesamte Fahrzeugtyp von der zuständigen Behörde möglichst vor dem Start der Produktion abgenommen werden sollen. Im Einklang mit einem ganzen Stapel von Zertifikaten wird dieses Verfahren für die OEMs in Zukunft erforderlich sein.[122]

Im Kern beinhaltet UNECE R155 die Vorschrift ein normgerechtes und zertifiziertes Cyber Security Management System (CSMS) einzuführen. Die Dimensionen eines CSMS sind dabei noch etwas weitreichender als jene bei SUMS. Beim Aufbau eines CSMS kommt es daher wesentlich auf eine kooperative, ganzheitliche Perspektive an, von der Entwicklung eines Fahrzeugs über die Produktion inklusive Lieferkette bis hin zur Überwachung der Fahrzeugflotte im Feld. Gleichzeitig steht das Thema Risikobewertung und Risikobehandlung deutlich stärker im Fokus von UNECE R155. Neue Arten der Lieferanteneinbindung betreffen prinzipiell SUMS und CSMS gleichermaßen, werden aber im Zuge von CSMS noch intensiver und eingehender betrachtet. Angesichts des hohen Zukaufanteils im Bereich der Softwaretechnologien stellt die Einhaltung dieser Anforderungen entlang der kompletten Lieferkette eine

[121] Quelle: Eigene Darstellung in Anlehnung an Liedtke (2020), S. 5.
[122] Vgl. Liedtke (2020), S. 6.

komplexe Aufgabe dar und wird in den Anforderungen der UNECE R155 explizit gefordert.[123]

In jedem Fall bedeuten die neuen Regelungen der UNECE eine Herausforderung für die Automobilhersteller. Einerseits steht ihre verpflichtende Umsetzung unmittelbar bevor. Andererseits zeigt z.B. die derzeit (November 2021) noch ausbleibende Veröffentlichung der Norm ISO 24089, dass längst nicht alle Details festgezurrt sind, insbesondere wenn es um Anforderungen an ein SUMS (UNECE R156) geht. Infolgedessen ist es notwendig einen Blick auch auf andere Arbeiten zu werfen, die in Zusammenhang mit SUMS und CSMS stehen.

### 2.3.3 Weitere Arbeiten in Verbindung mit SUMS und CSMS

Weltweit arbeiten verschiedene Forschungsinstitute und internationale bzw. nationale Gremien an unterschiedlichen Teilaspekten der Thematik. Das Betrachtungsspektrum reicht dabei von Berichten über die Übersetzung einzelner Prozessbausteine in Programmiersprachen bis hin zu ganzen Software-Frameworks oder übergeordneten organisatorischen Fragestellungen. Im Allgemeinen zielen aber alle Arbeiten auf eine mögliche Standardisierung im Umfeld von Cyber-Security und Software-Updates.[124] Abbildung 11 gibt einen Überblick über die wesentlichsten Arbeiten.

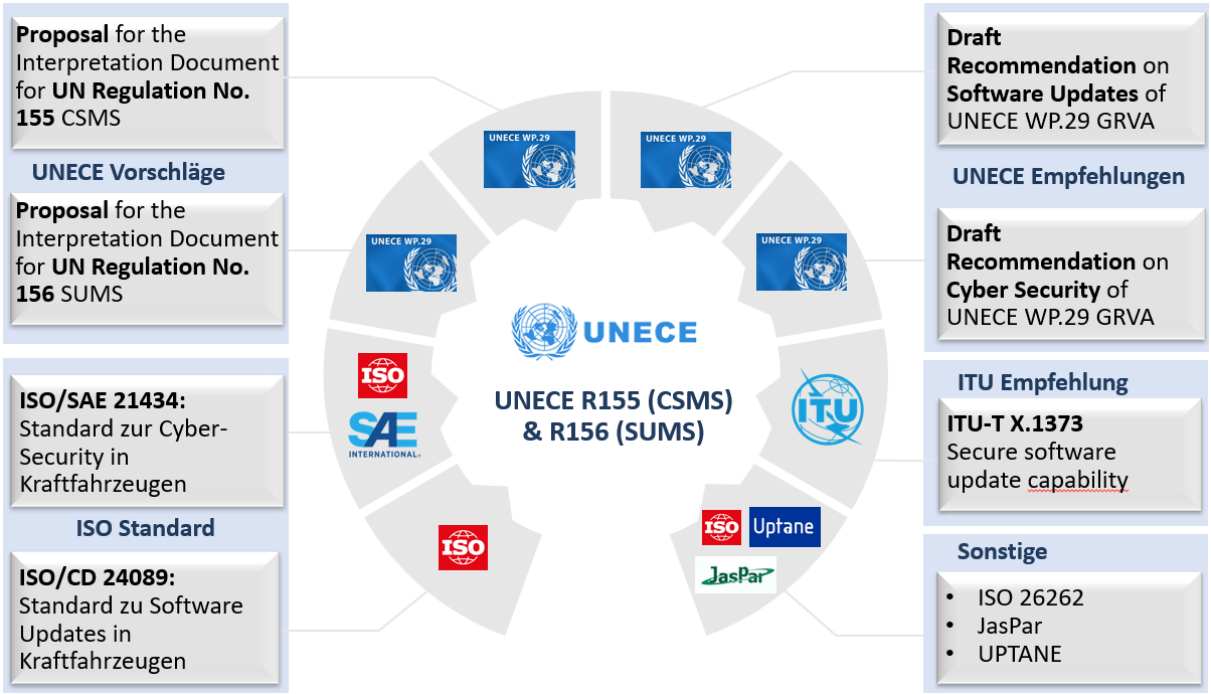



Abbildung 16: Arbeiten in Zusammenhang mit UNECE R155 & R156[125]

[123] Vgl. Dassow, Herzig und Guderian (2021), S. 2ff.
[124] Vgl. Harde und Großmann (2018), S. 10f.
[125] Quelle: Eigene Darstellung.

### ISO/SAE 21434 und ISO/CD 24089

Der von der ISO-Organisation in Zusammenarbeit mit SAE International entwickelte Standard ISO/SAE 21434 vermittelt einen guten Anhaltspunkt, wie man ein Cybersicherheits Managementsystem aufsetzt. Er befasst sich dabei aus der Cyber-Security Perspektive mit der Entwicklung elektrischer und elektronischer Systeme in Straßenfahrzeugen und zielt darauf ab, verschiedenen Angriffsmethoden Stand zu halten. Dazu enthält das Dokument Begriffe, Ziele, Anforderungen und Richtlinien in Bezug auf Cybersicherheitstechnik als Grundlage für ein gemeinsames Verständnis in der gesamten Lieferkette. Dies ermöglicht den OEMs Cybersicherheitsrichtlinien und -prozesse zu definieren sowie das Management von Cybersicherheitsrisiken und einer Cybersicherheitskultur zu fördern.[126] In einem eigenen Kapitel beschäftigt sich ISO/SAE 21434 zudem mit Anforderungen, Interaktionen, Abhängigkeiten und Verantwortlichkeiten für verteilte Cybersicherheitsaktivitäten zwischen OEMs und Lieferanten. Diese sehen zum Beispiel vor, dass die Fähigkeit eines Lieferanten zur Entwicklung und gegebenenfalls zur Durchführung von Tätigkeiten nach der Entwicklung in Übereinstimmung mit der Regelung der UNECE zu bewerten ist.[127]

Ein bisschen komplizierter ist es, wie bereits erwähnt, mit dem Software-Update Managementsystem. Mit der ISO 24089 wird es zwar auch einen Standard geben, dieser befindet sich allerdings erst in Ausarbeitung. Gemäß ISO ist die Veröffentlichung dabei nicht vor dem vierten Quartal des Jahres 2022, und damit nach Inkrafttreten der zugehörigen UNECE Regelung, vorgesehen. Geplant ist, analog zur ISO/SAE 21434, einen Standard zu schaffen mit der Beschreibung jener technischen Anforderungen, die in der UNECE Regelung Nr. 156 enthalten sind.[128]

### Proposal for Interpretation Document on Cyber Security and Software Updates

Gleichzeitig mit Verabschiedung und Inkrafttreten der verbindlichen Regularien wurden von der Arbeitsgruppe 29 der UNECE auch zwei sogenannten „Proposal Documents“ zu CSMS und SUMS veröffentlicht. Dabei handelt es sich um Dokumente mit verschiedenen Informationen darüber, was zum Nachweis der Anforderung aus UNECE R155 und R156 verwendet werden kann. Zielgruppe der Proposal Documents sind einerseits die Fahrzeughersteller, die Systeme zur Prüfung einreichen, und andererseits die technischen Dienste bzw. Genehmigungsbehörden, die diese Systeme bewerten. Dabei sollen die Dokumente dazu beitragen, die Prüfungen zwischen verschiedenen Technischen Diensten und Genehmigungsbehörden zu harmonisieren. Es gilt allerdings zu beachten, dass es sich bei den Dokumenten

[126] Vgl. ISO/SAE 21434:2021-08, S. iv.
[127] Vgl. ISO/SAE 21434:2021-08, Kap. 7.
[128] Vgl. Pilz (5.10.2021).

lediglich um Leitfäden handelt, die Informationen darüber enthalten, welches Vorgehen für die technischen Dienste bzw. Genehmigungsbehörden akzeptabel sein könnte.

Bezugnehmend auf das Proposal Document für UNECE R156 liegt der Fokus auf den Inhalten aus Kapitel 7. Folglich trägt das Dokument dazu bei, diese Anforderungen genauer aufzuklären und schlägt Ansätze vor, die zur Erfüllung der Anforderung beitragen können.[129]

**Draft Recommendation on Cyber Security and Software Update**

Seitens der UNECE existieren zudem zwei bereits im Vorfeld der UN-Regelungen Nr. 155 und 156 veröffentlichte Empfehlungen zum Umgang mit Cybersicherheit und Software-Updates. Sie beinhalten im Wesentlichen jene Aspekte, die auch Teil der später veröffentlichten Regelungen selbst sind. Die Empfehlung zum Umgang mit Software-Updates inkludiert aber etwa auch ein Flussdiagramm, das den Prozess zur Ermöglichung von Software-Updates nach bereits erteilter Typgenehmigung darstellt.[130] Ebenso interessant ist ein Passus in Kapitel 4.3.2. der Empfehlung. Demzufolge „müssen der Fahrzeughersteller **(und gegebenenfalls seine Lieferanten)** gegenüber der Genehmigungsbehörde nachweisen, dass sie über gewisse geeignete Verfahren verfügen.“[131] Diese Inkludierung der Lieferanten bekräftigt einmal mehr die Wichtigkeit der Einhaltung von SUMS Anforderungen auch bei Zulieferern.

**ITU-T X.1373**

ITU-T X.1373 wurde 2017 von der International Telecommunication Union veröffentlicht und stellt eine weitere Empfehlung für sichere Software-Update Verfahren dar. Sie beschreibt die Interaktion zwischen Software-Update-Server und Fahrzeugen sowie die notwendigen Absicherungsmaßnahmen zur Durchführung sicherer Updates. Dazu gehört ein grundlegendes Modell des Software-Update-Prozesses, eine Bedrohungs- und Risikoanalyse, Sicherheitsanforderungen sowie die Spezifikation der abstrakten Datenformate für die Update-Kommunikation.[132]

**Sonstige Standards und Empfehlungen**

Daneben existieren weitere Standards und Empfehlungen, die einen mehr oder weniger großen Einfluss auf die Umsetzung eines Software-Update oder Cybersicherheits-Managementsystems haben. Dazu zählen zum Beispiel ISO 26262

[129] Vgl. UNECE/TRANS/WP.29/2021/60, S. 2.
[130] Vgl. Informal document GRVA-01-18, S. 7.
[131] Vgl. Informal document GRVA-01-18, Kap. 4.3.2.
[132] Vgl. Römer, Kreyenberg und Großmann (2018), S. 11.

oder die Organisation „Japan Automotive Software Plattform and Architecture“ (JasPar).[133]

## 2.4 Prüfkataloge zur Informationssicherheit

Kapitel 2.3 hat gezeigt, dass die alleinige Betrachtung der neuen UNECE Regelung zu SUMS nur bedingt bei der Umsetzung der Anforderungen auf operativer Ebene hilft. Mit verschiedenen Standards, Normen und Empfehlungen stehen allerdings einige Dokumente zur Verfügung, welche zur Erfüllung von Anforderungen an ein Software-Update Managementsystem beitragen. Unabhängig von der Art der zu erzielenden Zertifizierung ist es wünschenswert, dass man darüber hinaus über einen Prüfkatalog verfügt, der geeignet ist, die Vollständigkeit, Angemessenheit und Wirksamkeit der angestrebten Lösung zu überprüfen und zu dokumentieren.[134] Solche Prüfkataloge sehen die Ausarbeitung eindeutiger und objektiv zu bewertender Prüfkriterien vor. Damit ermöglichen sie in weiterer Folge die Vorbereitung und Durchführung von kosteneffizienten Zertifizierungen gemäß verschiedenen gesetzlichen Vorgaben.[135] Angesichts der zunehmenden Relevanz von Informationssicherheit für Unternehmen wurden in den vergangenen Jahren einige Prüfkataloge mit Bezug zur Informationssicherheit entwickelt. Mithilfe einer systematischen Literaturanalyse wird in diesem Kapitel der gegenwärtige Stand der Forschung zu Prüfkatalogen der Informationssicherheit eruiert. Die drei für diese Arbeit wesentlichsten Ergebnisse werden im Anschluss dargestellt. Im Fazit wird ihre Tauglichkeit zur Verwendung für die UNECE Regelung Nr. 156 beurteilt.

### 2.4.1 Stand der Forschung

Die Identifikation von bestehenden Prüfkatalogen zur Informationssicherheit erfolgt, wie erwähnt, auf Basis einer systematischen Literaturanalyse. Bei dieser handelt es sich um ein bewährtes Instrument zur Zusammenfassung einer großen Anzahl an Untersuchungsergebnissen zu einem vordefinierten Untersuchungsobjekt. Sie bildet einen fundamentalen Bestandteil des wissenschaftlichen Arbeitens und zielt darauf ab aus einer Fülle an literarischen Quellen die für das Thema wesentlichen Beiträge zu identifizieren. Die systematische Literaturanalyse ermöglicht dadurch u.a. die Erarbeitung eines neuen Lösungskonzeptes, durch das Inkonsistenzen überbrückt werden können.[136] Die Vorgehensweise der durchgeführten Literaturanalyse ist angelehnt an jene von Fink (2014), wobei sie im Rahmen dieser Arbeit in etwas vereinfachter Form erfolgt (siehe Abb. 17).

[133] Vgl. Römer, Kreyenberg und Großmann (2018), S. 11f.
[134] Vgl. Burgartz (2020), S. 2.
[135] Vgl. Dax et al. (2016), S. 5f.
[136] Vgl. Becker, Ulrich und Stradtmann (2018), S. 75f.


**Abbildung 17: Vorgehensweise bei der systematischen Literaturanalyse[137]**

Die Definition der Untersuchungsfrage kennzeichnet den Beginn der Literaturanalyse. Sie sollte möglichst präzise formuliert sein.[138] Gemäß dem angestrebten Ziel dieser Literaturanalyse kann die Hauptuntersuchungsfrage wie folgt definiert werden:

**1.** *Welche Prüfkataloge existieren zur Erfüllung von informations-sicherheitstechnischen Anforderungen?*

Angesichts des Fokus dieser Arbeit auf Cybersicherheits- und Software-Update-Managementsysteme können zudem zwei Nebenuntersuchungsfragen formuliert werden:

**2.a** *Welche Prüfkataloge existieren zur Erfüllung von cybersicherheits-technischen Anforderungen?*

**2.b** *Welche Prüfkataloge existieren zur Erfüllung von Anforderungen hinsichtlich Softwareaktualisierungen?*

Im nächsten Schritt werden die Datenbanken, welche im Zuge der systematischen Literaturanalyse zur Anwendung kommen, ausgewählt. Insgesamt steht eine Vielzahl solcher Datenbanken zur Verfügung, die in Summe eine breite Abdeckung des Themengebiets sicherstellen.[139] Für die systematische Literaturanalyse der vorliegenden Arbeit wurden die in Tabelle 5 gelisteten Datenbanken verwendet. Wenngleich *Google* keine wissenschaftliche Datenbank darstellt, kommt sie im Zuge dieser Arbeit trotzdem zur Anwendung, da Prüfkataloge häufig in Form von Excel oder Word Dateien zur Verfügung gestellt werden. In solchen Fällen sind die Prüfkataloge meist in keiner wissenschaftlichen Datenbank hinterlegt.

[137] Quelle: Eigene Darstellung in Anlehnung an Fink (2014), S. 4.
[138] Vgl. Fink (2014), S. 3.
[139] Vgl. Becker, Ulrich und Stradtmann (2018), S. 78.

| Suchmaschine | Betreiber | Art der Suchmaschine |
|---|---|---|
| ScienceDirect | Elsevier | Wissenschaftliche Online-Datenbank |
| CatalogPlus | TU Wien | Wissenschaftliche Online-Datenbank |
| Google | Google LLC | Online-Suchmaschine |
| Google Scholar | Google LLC | Wissenschaftliche Online-Suchmaschine |

Tabelle 5: Verwendete Suchmaschinen[140]

Die Entwicklungen im Bereich der Informationssicherheit sind sehr schnelllebig.[141] Insofern werden in der Literaturanalyse lediglich jene Ergebnisse berücksichtigt, die ab dem Jahr 2015 veröffentlicht wurden. Die Suche selbst erfolgt in der Datenbank *ScienceDirect* auf Englisch, während in den anderen Datenbanken in deutscher Sprache gesucht wird. Wie in Tabelle 6 ersichtlich werden außerdem nur die Ergebnisse der Analyse herangezogen, die frei zugänglich sind.

| Filterkriterium | Gesetzter Filter |
|---|---|
| *Zeitraum:* | 2015 bis 2021 |
| *Zugang:* | Freier Zugang |
| *Sprache:* | Deutsch und Englisch |

Tabelle 6: Filterkriterien für die systematische Literaturanalyse[142]

Nach Datenbankfestlegung und Definition der Filterkriterien erfolgt im weiteren Verlauf die Auswahl der Suchbegriffe, nach denen optional im Titel, in Titelstichwörtern oder im Abstract gesucht werden kann. Die Suchbegriffe sollten so gewählt werden, dass, bezugnehmend auf die Untersuchungsfrage, inhaltlich passende Beiträge identifiziert werden können. Sie sollen das zu untersuchende Themengebiet möglichst breit abdecken und fungieren somit als wesentliche Stellhebel, die bei der systematischen Literatursuche zum Einsatz kommen.[143] In einem ersten Schritt werden für die Literaturanalyse relevante Suchblöcke definiert. Sie ergeben sich aus der eingangs beschriebenen Hauptuntersuchungsfrage und den beiden Nebenuntersuchungsfragen. Im Mittelpunkt aller Untersuchungsfragen steht die Identifikation von Prüfkatalogen, die folglich den ersten Suchblock darstellen. Informationssicherheit ist die Grundlage zum Schutz von Informationen jeglicher Art und Herkunft und bildet somit den zweiten Suchblock. Cybersicherheit und Softwareaktualisierungen stellen aufgrund des Fokus dieser Arbeit auf die UNECE Regelungen Nr. 155 und 156 den dritten bzw. vierten Suchblock dar. Für jeden Suchblock können anschließend sowohl

[140] Quelle: Eigene Darstellung.
[141] Vgl. Sowa (2017), S. 12.
[142] Quelle: Eigene Darstellung.
[143] Vgl. Becker, Ulrich und Stradtmann (2018), S. 78f.

deutsche als auch englische synonyme und artverwandte Suchbegriffe abgeleitet werden. Dieses Vorgehen ist in Tabelle 7 abgebildet.

| Block Nr. | Name des Blocks | Synonyme Suchbegriffe des Blocks (de) | Synonyme Suchbegriffe des Blocks (en) |
|---|---|---|---|
| 1 | Prüfkatalog | Prüfkatalog, Checkliste, Leitfaden | Test catalogue, Checklist, Guideline |
| 2 | Informationssicherheit | Informationssicherheit, IT-Sicherheit | Information Security, IT Security |
| 3 | Cybersicherheit | Cybersicherheit | Cybersecurity |
| 4 | Softwareaktualisierung | Softwareaktualisierung, Software-Update | Software-Update |

Tabelle 7: Suchblöcke und synonyme Suchbegriffe[144]

Im nächsten Schritt können die in Tabelle 7 definierten Suchblöcke und in weiterer Folge zusammenhängende Suchbegriffe miteinander kombiniert werden. Dazu kommen sogenannte Boolesche Operatoren zum Einsatz. Die bekanntesten booleschen Operatoren sind „AND“ und „OR“. Während durch die Anwendung des Operators „AND“ die Suchbegriffe miteinander verbunden werden, wird durch den Operator „OR“ festgelegt, dass zumindest eine der beiden Suchbegriffe im Titel vorkommen muss.[145] Die Ergebnisse der Kombination der Suchblöcke und -begriffe sind in Tabelle 8 dargestellt.

| Schwerpunkt | Kombination der Blöcke | Suchbegriffe (de) | Suchbegriffe (en) |
|---|---|---|---|
| Prüfkataloge Informations-sicherheit | Prüfkatalog AND Informationssicherheit | (Prüfkatalog OR Leitfaden OR Checkliste) AND (Informationssicherheit OR IT-Sicherheit) | (Test catalogue OR Checklist OR Guideline) AND (Information Security OR IT-Security) |
| Prüfkataloge Cyber-sicherheit | Prüfkatalog AND Cybersicherheit | (Prüfkatalog OR Checkliste OR Leitfaden) AND (Cybersicherheit) | (Test catalogue OR Checklist OR Guideline) AND (Cybersecurity OR Cyber Security) |
| Prüfkataloge Software-aktualisierung | Prüfkatalog AND Softwareaktualisierung | (Prüfkatalog OR Checkliste OR Leitfaden) AND (Softwareaktualisierung OR Software-Update) | (Test catalogue OR Checklist OR Guideline) AND (Software-Update) |

Tabelle 8: Kombination von Suchblöcken und Suchbegriffen[146]

[144] Quelle: Eigene Darstellung.
[145] Vgl. Becker, Ulrich und Stradtmann (2018), S. 79.
[146] Quelle: Eigene Darstellung.

Mit der Kombination von Suchblöcken und Suchbegriffen sind alle Voraussetzung für die Durchführung der Literaturrecherche in den zuvor ausgewählten Datenbanken geschaffen. Das vorläufige Ergebnis der Analyse ist in Tabelle 9 dargestellt.

| **Schwerpunkt:** | **Anzahl der Resultate:** | | | |
|---|---|---|---|---|
| | *ScienceDirect* | *CatalogPlus* | *Google* | *Google Scholar* |
| Prüfkataloge Informationssicherheit | 2 | 515 | ~ 2.400 | ~ 19.600 |
| Prüfkataloge Cybersicherheit | 7 | 55 | ~ 1.000 | 394 |
| Prüfkataloge Softwareaktualisierung | 0 | 54 | 85 | ~ 6.200 |

**Tabelle 9: Vorläufiges Ergebnis der Literaturanalyse**[147]

Demzufolge konnten mit den festgelegten Suchkriterien insgesamt rund 30.000 Literaturquellen identifiziert werden. Dabei ist anzumerken, dass die Suche in *Google* lediglich mit der Kombination der Suchblöcke durchgeführt wurde. Die Suche mit der Kombination aller Suchbegriffe lieferte über eine Million Ergebnisse und hätte zu einer äußerst zeitaufwendigen Sichtung der Literaturquellen geführt. Die dennoch vermeintlich hohe Anzahl der Resultate überrascht ansonsten nicht, da die primäre Literaturrecherche fast immer zu einer Vielzahl an literarischen Ergebnissen führt. Im nächsten Schritt wird deshalb ein Screening der identifizierten Literaturquellen durchgeführt. Dies dient dazu jene Ergebnisse zu erhalten, die für diese Arbeit relevant sind.[148] Für *Google* und *Google Scholar* beschränkt sich das Screening auf die ersten 100 Ergebnisse, da die relevantesten Literaturquellen auf diesen Seiten zu finden sind.[149]

| **Schwerpunkt:** | **Anzahl der Resultate nach Screening:** | | | |
|---|---|---|---|---|
| | *ScienceDirect* | *CatalogPlus* | *Google* | *Google Scholar* |
| Prüfkataloge Informationssicherheit | 0 | 3 | 5 | 7 |
| Prüfkataloge Cybersicherheit | 0 | 0 | 1 | 2 |
| Prüfkataloge Softwareaktualisierung | 0 | 0 | 0 | 1 |

**Tabelle 10: Ergebnis der Literaturanalyse nach Screening**[150]

[147] Quelle: Eigene Darstellung.
[148] Vgl. Fink (2014), S. 5.
[149] Vgl. Diesch, Pfaff und Krcmar (2020), S. 3.
[150] Quelle: Eigene Darstellung.

Im Zuge der vorliegenden Arbeit erfolgt das Screening primär auf Basis der Titel und Titelstichwörter sowie ggf. des Abstracts. Übrig geblieben sind in Summe 19 Resultate, die in Tabelle 10 abgebildet sind. Wie in der Tabelle ersichtlich wurden die meisten Resultate in *Google* und *Google Scholar* gefunden. Nach nochmaliger genauer Betrachtung der Literaturquellen wurden schließlich drei Resultate als für diese Arbeit wesentlich identifiziert. Dabei handelt es sich um einen Informationssicherheits-Prüfkatalog des VDA, einen Prüfkatalog nach ISO/IEC 27001 des TÜV Rheinland sowie einen Leitfaden zur Durchführung von Cybersicherheits-Checks der ISACA Deutschland. Sie werden nachfolgend genauer betrachtet.

**VDA Information Security Assessment Katalog**

Der VDA Information Security Assessment Katalog ist das Ergebnis des Arbeitskreises „Informationssicherheit“, der 2003 vom Verband der Automobilindustrie (VDA) etabliert wurde. Hier arbeiten verschiedene Experten zusammen, um gemeinsame Standards und angemessene Schutzmaßnahmen zu erarbeiten. Der VDA ISA Katalog basiert auf der Norm ISO/IEC 27001 und hat sich als Branchenstandard innerhalb der Automobilindustrie für Informationssicherheits-Assessments etabliert. Er dient unter anderem als Grundlage zur Bestimmung des Zustandes der Informationssicherheit in der Organisation (z. B. Unternehmen) und für Audits durch interne Fachabteilungen (z. B. Revision, Informationssicherheit). Daneben werden jegliche TISAX-Assessments durch die Prüfdienstleister auf Grundlage des VDA ISA Katalogs durchgeführt.

Seitens des VDA wird der Katalog kostenlos in Form einer Excel-Datei zur Verfügung gestellt und besteht aus mehreren Tabellenblättern. In einem allgemeinen Grundmodul sind die wesentlichen Anforderungen (im ISA Katalog als „Controls“ bezeichnet) an ein Informationssicherheitsmanagementsystem (ISMS) abgebildet. Die Controls selbst sind als Frage formuliert. Das Ziel des jeweiligen Controls und die Anforderungen zur Erreichung des Ziels sind in den entsprechend benannten Spalten hinterlegt. Die Zusatzmodule „Prototypenschutz“ und „Datenschutz“ ergänzen den Katalog branchenspezifisch. Während der Reiter „Datenschutz“ die Eignung im Sinne der Europäischen Datenschutz-Grundverordnung feststellt, umfasst der Prototypenschutz als „schutzbedürftig“ klassifizierte Fahrzeuge, Komponenten und Bauteile, welche noch nicht der Öffentlichkeit vorgestellt wurden. Neben diesen Tabellen mit den eigentlichen Anforderungen enthält der ISA Prüfkatalog weitere Informationen wie Umsetzungsbeispiele, die Definition eines Reifegradmodells und beispielhafte Key-Performance-Indicators (KPIs). Ende 2020 wurde der VDA ISA Katalog grundlegend überarbeitet und sowohl strukturell als auch inhaltlich optimiert.[151]

[151] Vgl. VDA ISA Katalog (2020).

### TÜV Rheinland Prüfkatalog nach ISO/IEC 27001

Ein weiterer wesentlicher Prüfkatalog für Informationssicherheit ist jener von *Burgartz* (2020) der TÜV Rheinland Group. Er ist entweder als E-Book oder als Teil des Handbuchs „Informations Security Assessment“ erhältlich und orientiert sich ebenfalls an der Norm ISO/IEC 27001. Dabei umfasst der Katalog die Forderungen dieser Norm aus den Kapiteln 4 bis 10 sowie die Maßnahmenziele (control objectives) und Maßnahmen (controls) aus Anhang A der Norm. Die Bereitstellung erfolgt in Form einer 60-seitigen Word-Datei inklusive einer Anleitung zur richtigen Anwendung. Der Prüfkatalog enthält zudem ein Muster für Feststellungsberichte, mit dem die Ergebnisse der Prüfung dokumentiert werden können. Dadurch kann der Katalog sowohl bei kontinuierlichen Überprüfungen während der Aufbau- und Betriebsphase als auch zur Vorbereitung auf eine geplante Zertifizierung des Systems verwendet werden.

Der Aufbau des Prüfkatalogs nach ISO 27001 ist formularmäßig und gliedert sich nach den verschiedenen Prüfpunkten, bzw. -gegenständen. Zu jedem Prüfpunkt/-gegenstand sind ein oder mehrere Forderungen angeführt. Sie beinhalten u.a. die Angabe ob und wie die festgelegten Verfahren, Richtlinien usw. in der betrieblichen Praxis umgesetzt und angewendet werden. Im Feststellungsbericht können anschließend nähere Angaben zur Bewertung und zu den vereinbarten Korrektur- oder Verbesserungsmaßnahmen festgehalten werden.[152]

### ISACA Leitfaden Cybersicherheits-Check

Beim Leitfaden Cybersicherheits-Check handelt es sich um das Ergebnis der Kooperation vom ISACA Germany Chapter e.V. Ressort Facharbeit und Arbeitskreise (Fachgruppe Informationssicherheit) und verschiedenen Experten des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Er wurde erstmals im April 2014 veröffentlicht und seither laufend aktualisiert. Der Leitfaden Cyber-Sicherheits-Check ermöglicht es, den Status der Cyber-Sicherheit auf Basis einer Cyber-Sicherheits-Risikoeinschätzung zu bestimmen. Im Unterschied zu den meisten anderen Prüfmechanismen richtet er sich verstärkt an kleinere und mittelständische Unternehmen. Die fachliche Grundlage des Cyber-Sicherheits-Checks bilden die im Rahmen der Allianz für Cyber-Sicherheit definierten „Basismaßnahmen der Cyber-Sicherheit“ in Kapitel 7. Sie beinhalten Maßnahmenziele, die bei der Durchführung eines Cyber-Sicherheits-Checks verbindlich zu beurteilen sind. Im Vergleich zu anderen Methoden stellt der Cyber-Sicherheits-Check damit eine äußerst kostengünstige, etablierte und tief in Technik und Prozesse Einblick nehmende Methodik dar. Die regelmäßige Durchführung eines Cyber-Sicherheits-Checks

[152] Vgl. Prüfkatalog nach ISO/IEC 27001 (2020).

ermöglicht auch kleineren Unternehmen ohne ein formales Informationssicherheitsmanagementsystem den Reifegrad ihrer Cybersicherheit regelmäßig zu beurteilen.[153]

### 2.4.2 Fazit zum aktuellen Forschungsstand

Sofern Unternehmen danach streben, den Zustand ihrer Informationssicherheit zu bestimmten, stellen alle drei identifizierten Prüfkataloge eine gute Möglichkeit dar. Der *ISACA Leitfaden Cybersicherheits-Check* überzeugt durch seinen übersichtlichen Aufbau und einfache Handhabung. Steht bei einem Unternehmen eine ISO 27001 Zertifizierung bevor, bietet der *Prüfkatalog nach ISO/IEC 27001* von *Burgartz* (2020) eine optimale Vorbereitung. Der *VDA ISA Katalog* wiederum bildet die Grundlage für jegliche TISAX Zertifizierungen in der Automobilbranche. Zudem präsentiert er sich nach seiner Überarbeitung in einem noch übersichtlicheren Tabellenformat und verringert dadurch den Aufwand für die Unternehmen und Prüfer weiter.

Wenngleich die Prüfkataloge damit einen guten Anhaltspunkt bieten, geht keiner von ihnen spezifisch auf die Anforderungen der neuen UNECE Regelung zu SUMS ein. Als einziger der drei Prüfmechanismen behandelt der *ISACA Leitfaden Cybersicherheits-Check* das Thema der Softwareaktualisierung innerhalb eines Maßnahmenziels. Allerdings entspricht das nicht ansatzweise dem, was innerhalb von UNECE R156 gefordert wird. Der mangelnde Bezug der Prüfkataloge zu Softwareaktualisierungen lässt sich auch in den Ergebnissen der systematischen Literaturanalyse in Tabelle 10 erkennen. So reduzierte sich die Anzahl der Suchergebnisse für den kombinierten Suchblock „Prüfkataloge Softwareaktualisierungen“ nach dem Screening auf lediglich eine Literaturquelle. Nach genauer Sichtung des Resultats wurde auch dieses als nicht relevant eingestuft und in weiterer Folge nicht mehr betrachtet.

Als Grund für dieses Ergebnis der Literaturanalyse kann angenommen werden, dass die Regelung Nr. 156 der UNECE erst Anfang des Jahres 2021 veröffentlicht wurde und somit in der wissenschaftlichen Literatur noch wenig behandelt wurde. Dennoch erfolgt die verpflichtende Umsetzung von UNECE R156 bereits im Juli 2022, weshalb die Automobilhersteller mit der Verwirklichung der Regulierungsanforderungen beginnen müssen.

[153] Vgl. Bartsch und Frey (2018), S. 463ff.

# 3 Forschungsbedarf, Ziel und Abgrenzung der Arbeit

Die konkreten Anforderungen innerhalb der neuen Regelung Nr. 156 der UNECE zu SUMS sind sehr allgemein gehalten. Ihre alleinige Betrachtung bietet keine detaillierte Anleitung für die betriebliche Umsetzung innerhalb des Unternehmens. Die in Kapitel 2.4 durchgeführte systematische Literaturanalyse offenbart zudem, dass bis dato kein Prüfkatalog existiert, der spezifisch auf die Anforderungen der UNECE Regelung Nr. 156 eingeht. Angesichts dessen ergibt sich ein Forschungsbedarf, auf den im folgenden Kapitel 3.1 näher eingegangen wird. Weiters wird in Kapitel 3.2 das genaue Ziel der Arbeit sowie die Vorgehensweise erläutert. In Kapitel 3.3 erfolgt eine Abgrenzung der Arbeit zu anderen Themengebieten.

## 3.1 Forschungsbedarf & Forschungsfrage

Die Herausforderungen für die Automobilhersteller im Bereich der Software-Technologien und Entwicklungen sind, wie bereits erwähnt, sehr weitreichend. Zur perspektivischen Sicherstellung der einzelnen Produkte und in weiterer Folge der Fahrzeuge werden Prüfungen als Teil vorgeschriebener Zulassungs- und Aufsichtsverfahren von unabhängigen Zertifizierungsstellen durchgeführt. Mit R156 SUMS wurde von der UNECE eine neue Regelung verabschiedet, die demnächst ein Software Update Management System für alle Fahrzeuge vorschreibt. Damit soll das Risiko cybersicherheitskritischer Bedrohungen auf ein akzeptables Niveau gesenkt werden.

Wenngleich die Regelung der UNECE einen ersten organisatorischen Rahmen für die sichere Durchführung von Software-Updates festlegt, bleibt sie mit ihren konkreten Ausführungen vage. So sind die Anforderungen größtenteils nicht als eindeutige Kriterien formuliert und bieten keine detaillierte Anleitung für die betrieblichen Vorgänge innerhalb von Unternehmen. Zumal auch die Ausgestaltung der entsprechenden Norm ISO 24089 noch ausständig ist, hinterlässt die Regelung bei den Automobilherstellern einen (ungewollten) Ermessungsspielraum darüber, was zur Erfüllung der Anforderung notwendig ist. Die weitere Literaturrecherche hat ergeben, dass immerhin einige Dokumente, Standards und Normen mit Bezug zur UN-Regelung Nr. 156 bestehen. Dennoch bieten auch sie keinen strukturierten und praxistauglichen Leitfaden zur erfolgreichen Vorbereitung auf eine SUMS-Zertifizierung. Ein solcher wäre jedoch für die an einem SUMS-Zertifizierungsprozess Beteiligten wünschenswert - zum Beispiel in Form eines Prüfkatalogs. Die in Kapitel 2.4 durchgeführte systematische Literaturanalyse hat allerdings ergeben, dass ein solcher für Anforderungen an ein Software-Update Managementsystem ebenfalls noch nicht

existiert. Ausgehend von diesen Herausforderungen ergibt sich der Bedarf nach einem Prüfkatalog, der eine fundierte und strukturierte Vorbereitung auch für eine Zertifizierung nach UNECE R156 (SUMS) ermöglicht. Auf Basis dessen kann für die vorliegende Arbeit folgende Forschungsfrage formuliert werden:

*Welche konkreten operativen Anforderungen an Automobilhersteller ergeben sich durch die Regelung Nr. 156 der UNECE und wie können diese entsprechend gruppiert und in einem Prüfkatalog integriert werden?*

Neben diesen grundsätzlich bestehenden Umständen stellt die Tatsache, dass Softwaresysteme häufig von unterschiedlichen Lieferanten entwickelt und zugekauft werden, eine weitere Herausforderung dar. Gemäß den Inhalten der UNECE Regelung ist zwar der OEM die zu prüfende Vertragspartei im Zuge eines SUMS Zertifizierungsprozesses. Ungeachtet dessen muss er darlegen können, dass die SUMS-Compliance auch bei den Zulieferunternehmen eingehalten wird. Ein genaues Vorgehen dafür liefert die UNECE Regelung allerdings nicht. Dadurch ergibt sich ein weiterer Subforschungsbedarf, der wie folgt formuliert werden kann:

*Welche Bedeutung hat die UNECE Regelung R156 für die Kunden-Lieferanten Schnittstelle?*

## 3.2 Ziel der Arbeit und Vorgehensweise

Gemäß dem identifizierten Forschungsbedarf ist das Ziel der vorliegenden Arbeit die Entwicklung eines Prüfkatalogs mit den operationalisierten Anforderungen aus der UNECE Regelung Nr. 156. Dieser soll Unternehmen bei der Konzeption, Implementierung und Aufrechterhaltung eines Software-Update Management Systems unterstützen. Er stellt zudem eine Grundlage zur Vorbereitung auf ein Zertifizierungsaudit nach SUMS dar. Durch die Anwendung von KPIs und einer Prozessfähigkeitsmessung soll er außerdem die Feststellung des Erfüllungsgrads der SUMS Anforderungen beim Aufbau und in der Betriebsphase ermöglichen. Daneben stellt die Beantwortung der Subforschungsfrage ein weiteres Ziel der Arbeit dar. Im Zuge dieser sollen Ansätze diskutiert werden, die die Fähigkeit des Lieferanten zur Durchführung von Aktivitäten in Übereinstimmung mit SUMS sicherstellen.

Das Vorgehen zum Erstellen des Prüfkatalogs richtet sich nach dem in Abbildung 18 dargestellten Prozess. In einem ersten Schritt wird eine Analyse hinsichtlich der Anforderungen an die Eigenschaften des Prüfkatalogs durchgeführt. Unter Berücksichtigung dieser erfolgt anschließend die Erstellung eines Grobkonzepts bzw. einer Struktur für den Prüfkatalog. Es folgt in Kapitel 4.2 mit der „Befüllung“ des Grobkonzepts die tatsächliche Entwicklung des Prüfkatalogs. Abschließend wird der Prüfkatalog in Kapitel 5 einer Validierung unterzogen. Sie dient der Sicherstellung der

Praxistauglichkeit des Prüfkatalogs und erfolgt auf Basis der sogenannten System Usability Scale (SUS) Methode. Keinen direkten Beitrag zur Erstellung des Prüfkatalogs leistet die Beantwortung der Subforschungsfrage. Sie dient der ergänzenden Betrachtung der Bedeutung der Regelung für den Umgang mit Lieferanten und wird maßgeblich mithilfe eines Experteninterviews aufgeklärt.


Abbildung 18: Vorgehensweise für die Erstellung des Prüfkatalogs[154]

## 3.3 Abgrenzung der Arbeit

Hervorzuheben sei an dieser Stelle, dass sich der Prüfkatalog explizit auf die Anforderungen der UNECE Regelung Nr. 156 zu SUMS bezieht. Wenngleich die Regelung inhaltlich eng mit jener zu CSMS verknüpft ist, verfolgt dieser Prüfkatalog lediglich das Ziel der Erfüllung aller Anforderungen an ein Software-Update Managementsystem. Auch strebt der Prüfkatalog nicht nach der Erfüllung von allgemeinen informationssicherheitstechnischen Anforderungen. Für dieses Vorhaben sei z.B. auf die drei innerhalb der Literaturanalyse identifizierten Prüfkataloge in Kapitel 2.3.1 verwiesen.

Daneben gilt es zu erwähnen, dass der Prüfkatalog vornehmlich für Zwecke der Audit Vorbereitung gedacht ist. Er soll die Unternehmen primär in der Aufbauphase für ein Software Update Management System unterstützen. Mithilfe von KPIs kann in weiterer Folge auch die Einhaltung der Maßnahmen in der Betriebsphase überprüft werden. Die Durchführung des eigentlichen SUMS Audits obliegt jedoch der ausgewählten Prüfstelle/Zertifizierungsstelle. Sofern die Möglichkeit gegeben ist, ist es empfehlenswert, deren Prüfkatalog im Vorfeld der Zertifizierung einzusehen.

[154] Quelle: Eigene Darstellung.

# 4 Konzeption und Entwicklung

Nachdem im vorangegangenen Kapitel das Ziel definiert wurde, folgt nun mit der Konzeption und Entwicklung des Prüfkatalogs der Kern der Arbeit. Damit einhergehend beginnt Phase 2 des vierstufigen Erkenntnisprozesses von Österle's Design Science Research Methode – Konstruktion und Entwicklung des Artefakts.

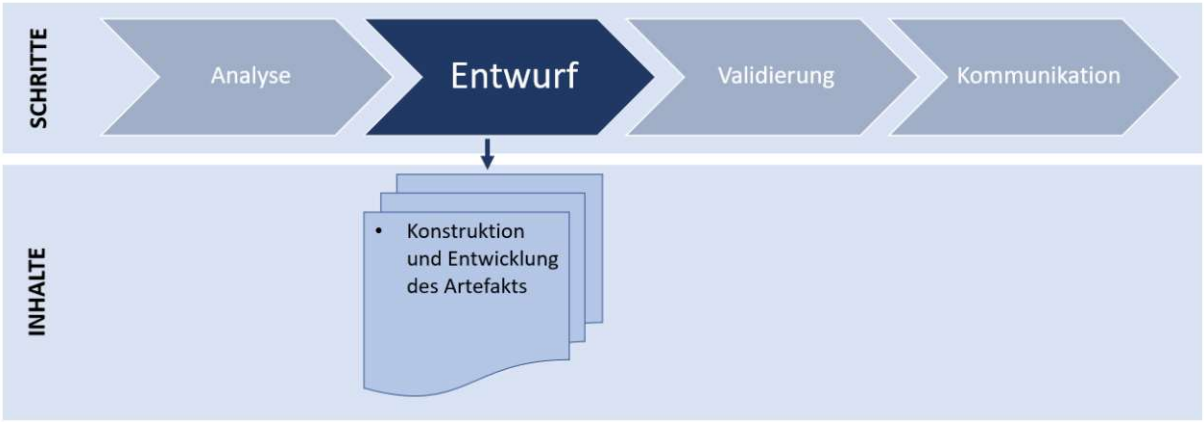



**Abbildung 19: Aktuelle Phase 2 in Österle's Design Science Research[155]**

Im Fokus dieses Kapitels steht folglich das Entwerfen des Prüfkatalogs. Dazu werden in einem ersten Schritt jene Anforderungen und Eigenschaften definiert, denen der Prüfkatalog entsprechen soll. In Kapitel 4.1 wird zudem die Struktur des Katalogs erstellt. Es folgt in Kapitel 4.2 die tatsächliche Entwicklung des Prüfkatalogs durch „Befüllen" der zuvor erstellten Struktur. Das fertige Ergebnis wird abschließend in Kapitel 4.3 dargestellt.

## 4.1 Konzeption des Prüfkatalogs

In der Phase der Konzeption wird versucht zuvor definierte Nutzungsanforderungen in einen ersten Prototyp einer Anwendung zu überführen. Wichtig in dieser Phase ist es abstrakt zu bleiben und sich nicht in inhaltlichen Details zu verlieren. Der Fokus liegt viel mehr auf dem grundlegenden Aufbau der Anwendung und deren einzelnen Seiten. Am Ende der Phase steht eine erste individuelle Repräsentation der Anwendung, die auf den Anforderungen der Nutzer basiert.[156]

### Nutzungsanforderungen an den Prüfkatalog

Für den im Zuge dieser Arbeit zu entwickelnden Prüfkatalog bedeutet das die Erstellung eines grundlegenden Aufbaus für den Prüfkatalog auf Basis von verschiedenen Nutzungsanforderungen. Diese Nutzungsanforderungen setzen sich

[155] Quelle: Eigene Darstellung
[156] Vgl. https://www.user-experience-methods.com/conception/ (Gelesen am: 16.12.2021)

einerseits zusammen aus den Anforderungen an den Prüfkatalog, die im Rahmen des Ziels der Arbeit beschrieben wurden, und andererseits aus charakteristischen Eigenschaften, die einen guten Prüfkatalog auszeichnen.

Erstere inhaltliche Anforderungen haben sich aus dem Forschungsbedarf ergeben. Sie zielen darauf ab, die Anforderungen der Regelung Nr. 156 der UNECE zu SUMS zu operationalisieren und entsprechend gruppiert im Prüfkatalog zu integrieren. Dabei soll der Katalog:

- Unternehmen bei der Konzeption, Implementierung und Aufrechterhaltung eines Software-Update Management Systems unterstützen,
- eine Grundlage zur Vorbereitung auf ein Zertifizierungsaudit nach SUMS darstellen,
- sowie die Feststellung des Erfüllungsgrads der SUMS Anforderungen beim Aufbau und in der Betriebsphase ermöglichen.

Die charakteristischen Eigenschaften fassen wiederum jene Anforderungen zusammen, die darauf abzielen, den Prüfkatalog intuitiv und effizient nutzen zu können. Sie stellen dementsprechend kein inhaltliches Ziel des Prüfkatalogs dar. Sie müssen aber während der Entwicklung des Katalogs dennoch stets berücksichtigt werden, um am Ende eine qualitativ hochwertige Anwendung zu erhalten. Die anzustrebenden charakteristischen Eigenschaften dieses Prüfkatalogs sind angelehnt an jene Eigenschaften, die drei ausgewählte Autoren an ihre jeweiligen Artefakte gestellt haben. Konkret handelt sich dabei um Burgartz (2020) und ihrem Prüfkatalog zur ISO 27001, um die Eigenschaften an einen Anforderungskatalog von Boles (1998) und um die Anforderungen an ein Bewertungsmodell für die Softwareentwicklung von Pirklbauer (2014). Folgende charakteristische Eigenschaften soll der im Zuge dieser Arbeit zu entwickelnde Prüfkatalog erfüllen:

| **Eigenschaften des Prüfkatalogs** | **Beschreibung der Eigenschaft** |
|---|---|
| Richtigkeit & Vollständigkeit | Die Gesamtheit aller Anforderungen ist vollständig und korrekt im Prüfkatalog berücksichtigt. |
| Wirksamkeit & Zweck | Der Prüfkatalog hilft beim Überprüfen der Anforderungen an das Software Update Management System. |
| Benutzerfreundlichkeit | Die notwendigen Anforderungen sind im Prüfkatalog logisch und strukturiert dargestellt. |
| Konsistenz | Der Katalog enthält keine Widersprüche. |
| Allgemeine Einsetzbarkeit | Die Anforderungen im Prüfkatalog sind allgemein gültig formuliert und in der Automobilindustrie einsetzbar. |
| Einmaligkeit | Keine Anforderung im Prüfkatalog ist mehrfach aufgelistet. |
| Ergebnis & Verifizierbarkeit | Die Anforderungen im Prüfkatalog sind eindeutig überprüfbar und der Erfüllungsgrad wird grafisch dargestellt. |

| | |
|---|---|
| Nachvollziehbarkeit | Der Ursprung jeder Anforderung im Prüfkatalog ist nachvollziehbar dargestellt. |
| Praxistauglichkeit | Die Anforderungen des Prüfkatalogs sind praxisnah formuliert und für den Anwender interpretierbar. |
| Risikoberücksichtigung | Mögliche inhaltliche Risiken und Bedrohungsszenarien sind im Prüfkatalog berücksichtigt. |

Tabelle 11: Charakteristische Eigenschaften des Prüfkatalogs[157]

Die Formulierung und Definition von charakteristischen Eigenschaften des Prüfkatalogs ist insofern auch wichtig, als dass sie im späteren Verlauf der Arbeit die Basis zur Validierung des Prüfkatalogs bilden. Mithilfe der System Usability Scale (SUS) Methode wird dann die Tauglichkeit des neuen Prüfkatalogs überprüft. Sie umfasst 10 Fragen nach der Likert-Skala, dessen Grundlage eben jene 10 charakteristische Eigenschaften aus Tabelle 11 bilden.[158]

### Aufbau und Struktur des Prüfkatalogs

Basis zur inhaltlichen Befüllung des Prüfkatalogs sind die in Kapitel 2.3 beschrieben Standards, Regelungen und Empfehlungen zu Softwareaktualisierungen und Informationssicherheit. Im Mittelpunkt steht folgerichtig die Regelung Nr. 156 der UNECE zu SUMS. Daneben stellt z.B. das Proposal Document der UNECE zur SUMS Regelung oder der bereits veröffentlichte ISO 21434 Standard zu Cybersicherheits Managementsystemen einen zentralen Aspekt bei der Entwicklung des Prüfkatalogs dar. Zuvor muss aber der grundlegende Aufbau und die Struktur des Prüfkatalogs geschaffen werden. Dazu werden die im Rahmen der systematischen Literaturanalyse identifizierten bereits bestehenden Prüfkataloge betrachtet. Im Zuge der Literaturanalyse hat sich gezeigt, dass keiner der Kataloge spezifisch auf die Anforderungen der neuen UNECE Regelung zu SUMS eingeht. Dennoch bieten sie einen guten Anhaltspunkt für die Konstruktion einer Struktur für den zu entwickelnden Prüfkatalog. In dieser Hinsicht überzeugt vor allem der vom VDA entwickelte Information Security Assessment (ISA) Prüfkatalog. Zum einen hat er sich bereits als Branchenstandard innerhalb der Automobilindustrie für Informationssicherheits-Assessments etabliert. Sein Format ist dadurch unter Informationssicherheitsverantwortlichen in der Automobilindustrie bereits bekannt und anerkannt. Zum anderen bieten sich Aufbau und Struktur des VDA ISA auch für die Integration von Anforderungen an ein SUMS in einem Prüfkatalog an. Die Verwendung eines Reifegradmodells inklusive Ergebnisdarstellung, die Formulierung der Anforderungen als einzelne Controls sowie die Anführung von Beispiel KPIs ermöglichen einen einfachen und effizienten Umgang mit dem Katalog. Dasselbe Ziel – den Aufwand für Unternehmen möglichst gering zu halten – steht auch im Mittelpunkt

[157] Quelle: Eigene Darstellung.
[158] Vgl. Brooke (1996), S. 207ff.

bei der Entwicklung des vorliegenden Prüfkatalogs. Insofern orientiert sich der zu entwickelnde Prüfkatalog am Aufbau und der Struktur des VDA ISA Katalogs.

Die Umsetzung des Prüfkatalogs erfolgt mithilfe des Tabellenkalkulationsprogramms *Microsoft Excel*. Gegenüber anderen Programmformaten, wie etwa *Microsoft Word*, weist *Microsoft Excel* für die Entwicklung des Prüfkatalogs einige wesentliche Vorteile auf. Dazu zählen u.a. die Möglichkeit der:

- Verwendung von mehreren Tabellenblättern für eine bessere Übersichtlichkeit
- Filterung von verschiedenen Datensätzen
- Eintragung von Reifegradwerten mittels Dropdown Funktion
- Auswertung und Ergebnisdarstellung mithilfe von Zellenbezügen und Formelanwendungen

In Anlehnung an die Struktur des VDA ISA Katalogs sowie auf Basis der zu Beginn des Kapitels erörterten Nutzungsanforderungen wurde der in Abbildung 20 dargestellte Aufbau für den Prüfkatalog in *Microsoft Excel* entwickelt. Der Katalog besteht folglich aus insgesamt 9 Tabellenblättern, wobei Tabellenblatt 0 lediglich der Einleitung dient und einen Überblick über die folgenden Tabellenblätter gibt.

Die farbliche Kennzeichnung weist auf die unterschiedliche Funktion der einzelnen Tabellenblätter hin. Tabellenblätter 0 bis 2 haben eine informierende Funktion, wie etwa die Beschreibung der Erfüllungsgradmessung in Tabellenblatt 2. In Tabellenblatt 3 sind die einzelnen Anforderungen aus der UNECE Regelung in ihrer ursprünglichen Reihung aufgelistet, inklusive Verweis auf die jeweilige Kontrollfrage im entwickelten Prüfkatalog. Damit lässt sich auf die Schnelle feststellen, welche Kontrollfrage des Prüfkatalogs zu welcher Anforderung der UNECE Regelung gehört. Tabellenblätter 4 bis 6 bilden den Kern des Prüfkatalogs. Sie beinhalten die konkreten vom OEM zu erfüllenden Anforderungen für eine erfolgreiche Zertifizierung nach UNECE R156. Tabellenblatt 4 und 5 beziehen sich auf die Anforderung an ein SUMS bzw. an Produktionsprozesse. Tabellenblatt 6 weicht in seinem Aufbau ein wenig von den anderen beiden Tabellenblättern ab und bezieht sich auf die notwendigen Prozessschritte, die im Rahmen der Beantragung einer SUMS Zertifizierung zu befolgen sind. Erklärtes Ziel des Prüfkatalogs ist zudem die Feststellung des Erfüllungsgrads der SUMS Anforderungen sowohl beim Aufbau als auch in der Betriebsphase zu ermöglichen. Dazu beinhaltet Tabellenblatt 7 die Auswertung und grafische Darstellung der Ergebnisse der Erfüllungsgradmessung. Zur kontinuierlichen Überwachung der Einhaltung der SUMS Anforderungen in der Betriebsphase befinden sich in Tabellenblatt 8 schließlich eine Reihe von Beispiel KPIs.

Mit dieser Struktur ist die Grundlage zur weiteren Entwicklung des Prüfkatalogs geschaffen. In einem nächsten Schritt erfolgt daher die Befüllung der Tabellenblättern

mit den Inhalten der UNECE Regelung sowie den weiteren Standards und Empfehlungen.

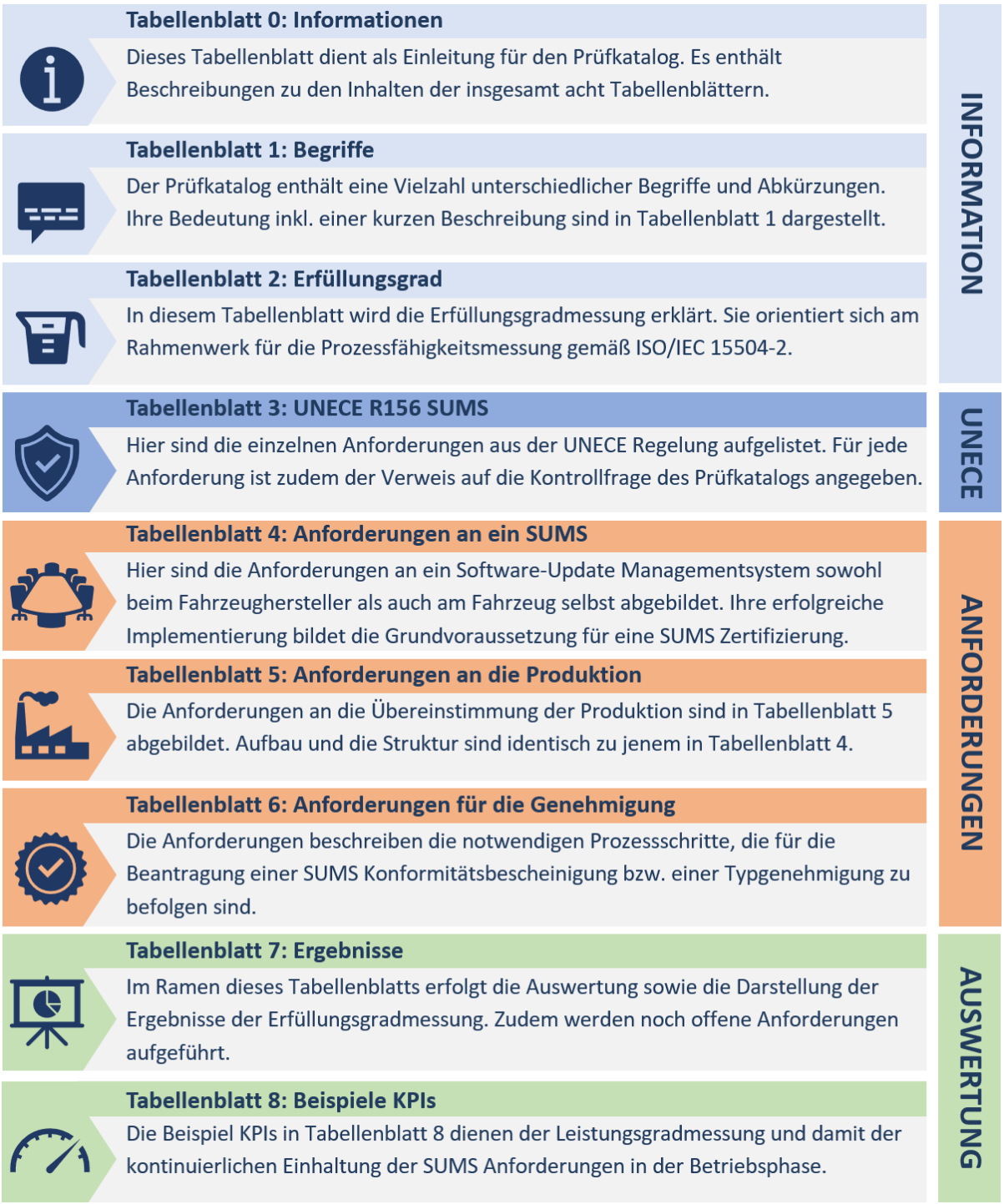



Abbildung 20: Konzeption und Aufbau des Prüfkatalogs[159]

[159] Quelle: Eigene Darstellung.

## 4.2 Entwicklung des Prüfkatalogs

Dieses Kapitel widmet sich der Entwicklung des Prüfkatalogs. Basis dafür ist die zuvor erstellte grundlegende Struktur des Prüfkatalogs. Die einzelnen Tabellenblätter werden nun mit verschiedenen Informationen, Beschreibungen, Anforderungen, etc. befüllt. Die Gliederung dieses Kapitels erfolgt entsprechend der farblichen Unterteilung der Tabellenblätter des Prüfkatalogs. Folglich widmet sich Kapitel 4.2.1 den informierenden Tabellenblättern 0, 1 und 2. Die in Tabellenblatt 3 übernommenen Anforderungen der UNECE Regelung werden in Kapitel 4.2.2 dargestellt. Kapitel 4.2.3 beschreibt im Detail die Entwicklung der Tabellenblätter 4 bis 6 mit den konkreten operationalisierten Anforderungen der Regelung. Die auswertenden Tabellenblätter 7 und 8 werden schließlich in Kapitel 4.2.3 behandelt.

### 4.2.1 Informationen, Begriffe und Erfüllungsgrad

Bei den im Rahmen dieses Kapitels betrachteten Tabellenblättern handelt es sich um eine Hinführung zu den darauffolgenden Tabellenblättern mit den konkreten Anforderungen der UNECE Regelung. Sie stellen für den Anwender des Prüfkatalogs die Grundlage zum Verständnis der nachfolgenden Inhalte dar. Dementsprechend muss er sich vorab mit ihnen auseinandersetzen, um im Anschluss die jeweiligen Funktionen des Prüfkatalogs gezielt nutzen zu können.


**Tabellenblatt 0 – Informationen**

*Informationen* stellt das erste Tabellenblatt des Prüfkatalogs dar. Es enthält einleitende Worte zur UNECE Regelung Nr. 156 sowie zu den Funktionen des Prüfkatalogs. Im weiteren Verlauf sind zudem die einzelne Tabellenblätter des Prüfkatalogs genauer beschrieben. Auf Basis der *Microsoft Excel* Funktion „Daten – Gliederung – Gruppieren“ lassen sich die Informationen zu den einzelnen Tabellenblättern aufklappen. Dem Anwender des Prüfkatalogs wird empfohlen, mit diesem Tabellenblatt zu starten. Er erhält dadurch einen ersten Überblick über das, was ihn auf den restlichen Tabellenblättern erwartet.

**Tabellenblatt 1 – Begriffe**

Die Regelung Nr. 156 der UNECE zu SUMS und damit auch der vorliegende Prüfkatalog enthalten eine Vielzahl unterschiedlicher Abkürzungen. Für die erfolgreiche Konzeption, Implementierung und Aufrechterhaltung eines Software-Update Management Systems ist es essenziell, dass alle verwendeten Abkürzungen bekannt sind. Darüber hinaus müssen die Begriffe erklärt werden, damit der Prüfkatalog intuitiv genutzt werden kann. Im Tabellenblatt *Begriffe* werden deshalb

sämtliche im Prüfkatalog enthaltende Abkürzungen aufgelistet. Nach der Bedeutung der Abkürzung in der zweiten Spalte befindet sich in der dritten Spalte eine Erklärung der Abkürzung.

Im Anschluss an das Abkürzungsverzeichnis werden zudem weitere spezifische Begriffe erklärt, die im Prüfkatalog enthalten sind. Deren Verständnis ist für die Anwendung des Prüfkatalogs ebenso wichtig und wird in Form eines zweispaltigen Begriffsglossars dargestellt. Abbildung 21 repräsentiert den Aufbau dieses Tabellenblatts.

***Beispiel Abkürzungsverzeichnis:***

| Abkürzung: | Bedeutung: | Erklärung: |
|---|---|---|
| OTA | Over-The-Air | Ein OTA-Update bezeichnet jede Art der drahtlosen Übertragung von Daten anstelle der Verwendung eines Kabels oder einer anderen ortsgebundenen Verbindung. |

***Beispiel Begriffsglossar:***

| Abkürzung: | Erklärung: |
|---|---|
| Sicherer Zustand | Sicherer Zustand bezeichnet einen Betriebsmodus ohne unverhältnismäßiges Risiko bei Ausfall eines Merkmals oder einer Funktionskomponente. |

**Abbildung 21: Abkürzungsverzeichnis und Begriffsglossar im Prüfkatalog[160]**

### Tabellenblatt 2 – Erfüllungsgrad

Die Erfüllungsgradmessung wurde im Kapitel 3.1 als eine der drei wesentlichen inhaltlichen Anforderungen an den Prüfkatalog identifiziert. Sie stellt dementsprechend einen sehr wichtigen Teil des Katalogs dar. Durch sie kann der OEM den aktuellen Zustand seines Software-Update Managementsystems bestimmen. Darauf aufbauend kann er entscheiden, welche weiteren Handlung an welcher Stelle im Unternehmen zu treffen sind. Die Erfüllungsgradmessung ist auch einer der wesentlichen Gründe für die Auswahl von *Microsoft Excel* als Tool zur Entwicklung des Prüfkatalogs. Zum einen kann der Anwender dadurch den Erfüllungsgrad per Dropdown Funktion auswählen, was die Eingabe von ungültigen Werten vermeidet. Zum anderen ermöglicht *Microsoft Excel* im weiteren Verlauf eine effiziente Auswertung der Erfüllungsgradmessung, inklusive grafischer Darstellung. In jedem Fall kann sich der im Kontext dieser Arbeit zu entwickelnde Prüfkatalog durch diese Funktion von anderen Leitfäden und Anforderungskatalogen der Informationssicherheit abheben.

Basis für die Erfüllungsgradmessung ist das Rahmenwerk für die Prozessfähigkeitsmessung gemäß ISO/IEC 15504-2. Dieser Teil der ISO/IEC 15504 legt die Grundlagen für Prozess-Assessments fest. Konkret handelt es sich dabei um

[160] Quelle: Eigene Darstellung.

eine 6-stufige Skala, die die Bewertung der Prozessfähigkeit im Rahmen der jeweiligen Anforderung ermöglicht. Sie reicht von *Unvollständig* am unteren Ende der Skala bis hin zur *Optimierend* am oberen Ende der Skala. Innerhalb dieses Rahmenwerks basiert das Maß der Fähigkeiten auf einer Reihe von Prozessattributen (PA). Jedes Prozessattribut legt einen bestimmten Aspekt der Prozessfähigkeit fest. Der Grad, bis zu dem ein bestimmtes Prozessattribut erreicht wurde, wird anhand einer festgelegten Bewertungsskala beschrieben. In Verbindung mit den vorstehend festgelegten Attributen weisen die Prozessattribute das Erreichen der jeweiligen Stufe nach.[161] In untenstehender Abbildung 22 sind die sechs verschiedenen Prozessfähigkeitsstufen inklusive ihrer Prozessattribute im Detail erläutert.

| | |
|---|---|
| **Stufe 0: Unvollständiger Prozess** | |
| Der Prozess ist nicht umgesetzt oder erreicht seinen Prozesszweck nicht. | |
| **Prozessattribut:** | Nur wenige oder gar keine Nachweise für eine Erreichung des Prozesszwecks. |
| **Stufe 1: Durchgeführter Prozess** | |
| Der umgesetzte Prozess erfüllt seinen Prozesszweck. | |
| **Prozessdurchführung:** | Maß für den Grad, bis zu dem der Prozesszweck erreicht ist. |
| **Stufe 2: Gelenkter Prozess** | |
| Der Prozess wird nun auf gelenkte Art und Weise umgesetzt und seine Arbeitsprodukte werden auf angemessene Art und Weise erstellt, gelenkt, aufrechterhalten und gepflegt. | |
| **Durchführungsmanagement:** | Maß für den Grad, bis zu dem die Durchführung des Prozesses gelenkt ist. |
| **Arbeitsproduktmanagement:** | Maß für den Grad, bis zu dem die im betroffenen Prozess erzeugten Arbeitsprodukte auf angemessene Weise gelenkt sind. |
| **Stufe 3: Etablierter Prozess** | |
| Der Prozess wird nun mit Hilfe eines definierten Prozesses umgesetzt, der es ermöglicht, die für ihn festgelegten Prozessresultate zu erzielen. | |
| **Prozessdefinition:** | Maß für den Grad, bis zu dem ein Standardprozess aufrechterhalten und gepflegt ist, um den Einsatz des definierten Prozesses zu unterstützen. |
| **Prozesseinsatz:** | Maß für den Grad, bis zu dem der Standardprozess effektiv als definierter Prozess eingesetzt ist, um die für ihn festgelegten Prozessresultate zu erzielen. |
| **Stufe 4: Vorhersagbarer Prozess** | |
| Der Prozess läuft nun innerhalb definierter Grenzen ab, um die für ihn festgelegten Prozessresultate zu erzielen. | |
| **Prozessmessung:** | Maß für den Grad, bis zu dem Messergebnisse verwendet werden, um sicherzustellen, dass festgelegte Prozessdurchführungsziele erreicht werden. |
| **Prozesskontrolle:** | Maß für den Grad, bis zu dem der Prozess quantitativ gelenkt ist, um zu einem Prozess zu gelangen, der stabil ist, die geforderten Fähigkeiten umfasst und innerhalb festgelegter Grenzwerte vorhersagbar abläuft. |
| **Stufe 5: Optimierender Prozess** | |
| Der Prozess wird stetig verbessert, um den maßgeblichen aktuellen und künftigen Geschäftszielen zu entsprechen | |
| **Prozessinnovation:** | Maß für den Grad, bis zu dem Änderungen am Prozess aus der Analyse allgemeiner Ursachen für Abweichungen und aus innovativen Ansätze heraus abgeleitet werden. |
| **Prozessoptimierung:** | Maß für den Grad, bis zu dem Änderungen an der Definition, Lenkung und Durchführung des Prozesses zur Erfüllung von maßgeblichen Prozessverbesserungszielen beitragen. |

**Abbildung 22: Prozessfähigkeitsmessung gemäß ISO/IEC 15504-2[162]**

[161] Vgl. ISO/IEC 15504-2:2003, S.12 f.
[162] Quelle: Eigene Darstellung auf Basis von ISO/IEC 15504-2.

### 4.2.2 UNECE Regelung Nr. 156

In diesem Kapitel werden die Inhalte des dritten Tabellenblattes des Prüfkatalogs beschrieben. Es enthält die einzelnen Kapitel der UNECE Regelung Nr. 156 zu Software-Update Managementsystemen, wobei die Anforderungen an dieser Stelle in ihrer ursprünglichen Form aus der Regelung übernommen werden.


Wenngleich dieses Tabellenblatt keine wesentlichen inhaltlichen Neuentwicklungen enthält, bietet es dem Anwender dennoch einige Vorteile. Dank der Eingliederung der UNECE Regelung in den Prüfkatalog erspart sich der Anwender die gesonderte Betrachtung des ursprünglichen von der UNECE veröffentlichten PDF-Dokuments zu R156 SUMS. Im Zuge der Arbeit mit dem Prüfkatalog entfällt dadurch das Hin-und-Her Wechseln zwischen den verschiedenen Dokumenten. In einem weiteren Schritt ermöglicht die Filter-Funktion in *Microsoft Excel* die gezielte und schnelle Suche nach einer konkreten Anforderung der UNECE Regelung. Wesentlich für die intuitive Anwendung des Prüfkatalogs ist in diesem Tabellenblatt zudem der Verweis auf die jeweilige Kontrollfrage im Prüfkatalog. Damit lässt sich auf die Schnelle für jede Anforderung der UNECE Regelung das Kapitel der Kontrollfrage mit den operationalen Erläuterungen und Darstellungen herausfinden. Analog zur Filter-Funktion für die Anforderungen aus der UNECE Regelung kann auf gleiche Art und Weise auch nach einer konkreten Kontrollfrage aus dem Prüfkatalog gefiltert werden. Dies ist dann relevant, wenn den Anwender die ursprüngliche Formulierung der Anforderung aus der UNECE Regelung zu einer entsprechenden Kontrollfrage aus dem Prüfkatalog interessiert.

**PRÜFKATALOG UNECE R156 SUMS**

Einheitliche Bestimmungen für die Genehmigung von Kraftfahrzeugen hinsichtlich der Softwareaktualisierung und des Softwareaktualisierungsmanagementsystems gemäß UNECE Regelung Nr. 156 [Stand: 4. März 2021]

| UNECE Kap. | Inhalt | Kapitel im Prüfkatalog |
|---|---|---|
| **4.** | **Kennzeichnung** | |
| 4.1. | An jedem Fahrzeug, das einem nach dieser Regelung genehmigten Fahrzeugtyp entspricht, ist sichtbar und an gut zugänglicher Stelle, die auf dem Mitteilungsblatt anzugeben ist, ein internationales Genehmigungszeichen anzubringen, bestehend aus: | |
| 4.1.1. | einem Kreis, in dem sich der Buchstabe „E“ und die Kennzahl des Landes befinden, das die Genehmigung erteilt hat, | Kap. 6.2 |
| 4.1.2. | der Nummer dieser Regelung, mit dem nachgestellten Buchstaben „R“, einem Bindestrich und der Genehmigungsnummer rechts neben dem Kreis gemäß Nummer 4.1.1. | Kap. 6.2 |
| 4.2. | Entspricht das Fahrzeug einem Fahrzeugtyp, der nach einer oder mehreren anderen Regelungen zum Übereinkommen in dem Land genehmigt wurde, das die Genehmigung nach dieser Regelung erteilt hat, dann braucht das Zeichen nach Nummer 4.1.1 nicht wiederholt zu werden; in diesem Fall sind die Regelungs- und Genehmigungsnummern und die zusätzlichen Zeichen aller Regelungen, aufgrund deren die Genehmigung in dem Land erteilt wurde, das die Genehmigung nach dieser Regelung erteilt hat, untereinander rechts neben dem Zeichen nach Nummer 4.1.1 anzuordnen. | Kap. 6.3 |

Abbildung 23: UNECE Regelung Nr. 156 im Prüfkatalog[163]

[163] Quelle: Prüfkatalog UNECE R156 SUMS, Tabellenblatt 3.

Exemplarisch ist in Abbildung 23 ein Ausschnitt aus diesem Tabellenblatt des Prüfkatalogs dargestellt. Zu erkennen sind dabei ein Teil der Anforderungen aus Kapitel 4 der UNECE Regelung – Kennzeichnung. In der rechten Spalte ist zudem der Verweis auf die jeweilige Kontrollfrage im Prüfkatalog abgebildet.

Im Zuge dieses Tabellenblatts gilt es lediglich zu beachten, dass die Regelung von der UNECE ggf. überarbeitet werden könnte. Dazu steht am Beginn des Tabellenblatts das Datum des aktuellen Standes der Anforderungen im Prüfkatalog. Im Zuge der Vorbereitung auf eine Zertifizierung nach SUMS muss folglich überprüft werden, ob dieser Stand dem aktuellen auf der UNECE Webseite zugänglichen Veröffentlichungsdokument entspricht. Ist dies nicht der Fall, müssen die seitens der UNECE vorgenommenen Änderungen entsprechend beurteilt und in den Prüfkatalog übernommen werden.

### 4.2.3 Anforderungen der UNECE R156

Die im Zuge dieses Kapitels entwickelten Tabellenblätter 4 bis 6 bilden den Kern des Prüfkatalogs. Wie bereits erwähnt beinhalten sie die konkreten vom OEM zu erfüllenden Anforderungen für eine erfolgreiche Zertifizierung nach UNECE R156. Während Tabellenblätter 4 und 5 einen identischen Aufbau aufweisen, weicht die Struktur von Tabellenblatt 6 geringfügig von den beiden vorhergehenden Tabellenblättern ab. In beiden Fällen erfolgt die Entwicklung der Tabellenblätter jedenfalls in zwei Stufen. Zuallererst wird die vertikale Entwicklung betrachtet, d.h. die inhaltliche Gliederung des Tabellenblatts mit einer logischen Gruppierung und Strukturierung der UNECE Anforderungen in verschiedenen Zeilen. In einem zweiten Schritt werden die einzelnen Spalten des Tabellenblatts definiert, die der logischen und intuitiven Bearbeitung des Prüfkatalogs dienen. In den folgenden Absätzen ist die Entwicklung der jeweiligen Tabellenblätter beschrieben.


**Tabellenblatt 4: Anforderungen – SUMS**

In Tabellenblatt 4 des Prüfkatalogs sind die konkreten Anforderungen an ein Software-Update Managementsystem sowohl beim Fahrzeughersteller als auch am Fahrzeug selbst abgebildet. Sie entstammen Kapitel 7 der UNECE Regelung und ihre erfolgreiche Implementierung bildet die Grundvoraussetzung für die Ausstellung einer SUMS Konformitätsbescheinigung.

*Vertikale Entwicklung:*

Wie oben erwähnt, erfolgt in einem ersten Schritt mit der inhaltlichen Gestaltung die vertikale Entwicklung des Tabellenblatts, beginnend mit der Gruppierung und

Strukturierung der UNECE Anforderungen. Diese sieht die Unterteilung des Tabellenblatts in zwei Kapitel vor. Ersteres bezieht sich auf die Anforderungen der UNECE an das Software-Update Managementsystem beim Fahrzeughersteller. Das zweite Kapitel enthält die Auflistung der (technischen) Spezifikationen und Anforderungen direkt am Fahrzeug gemäß UNECE R156. Beide Kapitel unterteilen sich weiters in mehrere Unterkapitel. Sofern angebracht, werden mehrere Anforderungen der UNECE Regelung in einer Kontrollfrage zusammengeführt. Umgekehrt erfolgt in manchen Fällen im Sinne einer besseren Verständlichkeit auch die Aufteilung einer Anforderung der UNECE Regelung auf mehrere Kontrollfragen. In Abbildung 24 ist der vertikale Aufbau von Tabellenblatt 4 – Anforderungen an ein SUMS – grafisch dargestellt.

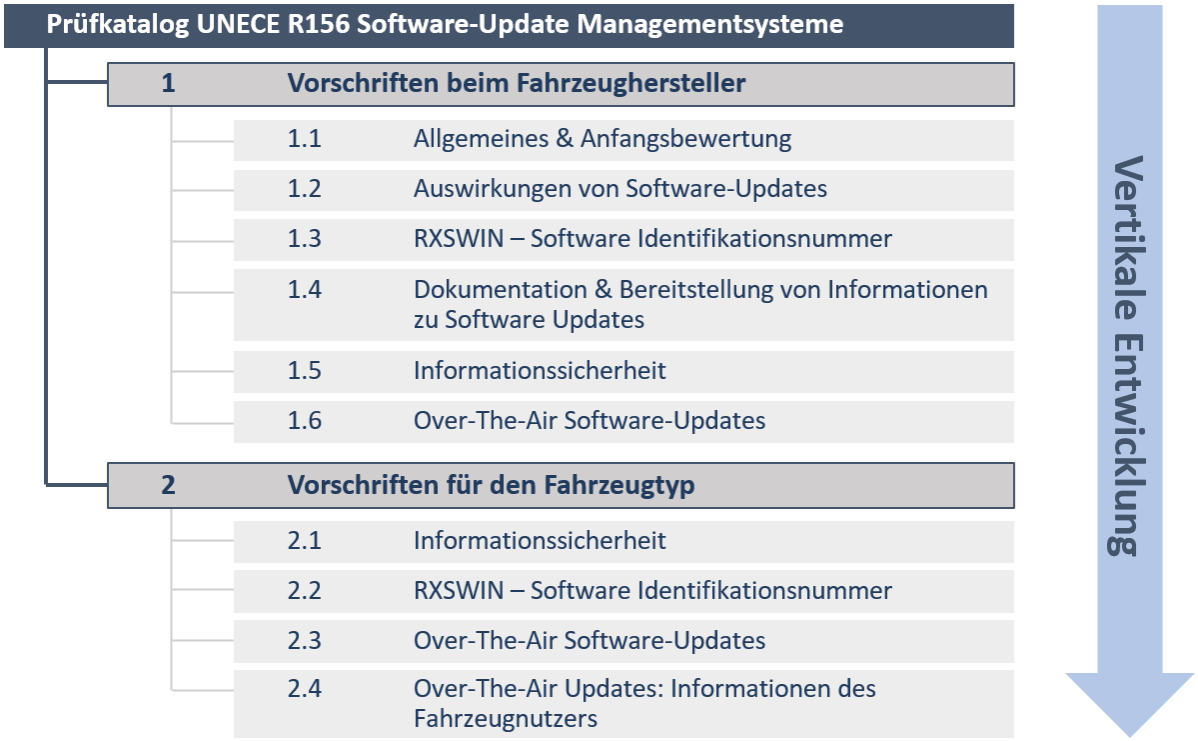



**Abbildung 24: Vertikale Entwicklung von Tabellenblatt 4 des Prüfkatalogs[164]**

Beginnend mit *Kapitel 1.1* des Prüfkatalogs werden zunächst einige allgemeine Anforderungen der UNECE Regelung geclustert und abgebildet. Sie betreffen z.B. die Dokumentation von jeglichen Informationen zum Software-Update Managementsystem.

*Kapitel 1.2* bestimmt den Umgang mit sämtlichen Auswirkungen von Software-Updates sowie Interaktionen zwischen verschiedenen Software-Systemen. Da die einzelnen in einem Fahrzeug verbauten Software-Systeme stark miteinander vernetzt sind kommt diesem Kapitel eine besondere Bedeutung zu. Die Aktualisierung der

[164] Quelle: Eigene Darstellung.

Software eines Systems kann nämlich zu einem veränderten Verhalten eines anderen Systems führen. Es ist deshalb wichtig, dass die Fahrzeughersteller über die Abhängigkeiten zwischen dem zu aktualisierenden System und anderen Systemen Bescheid wissen.

Wesentlicher Bestandteil der UNECE Regelung Nr. 156 zu SUMS ist zudem die sogenannte Software-Identifikationsnummer RXSWIN. Bei ihr handelt es sich um eine spezielle fahrzeugindividuelle alphanumerische Kennzeichnung für typgenehmigungsrelevante Software-Systeme. Im Rahmen des Release Management ermöglicht sie die Nachverfolgbarkeit darüber, welche Softwareversion derzeit im Fahrzeug verbaut ist.[165] Die Anforderungen hinsichtlich der RXSWIN auf Seiten des Fahrzeugherstellers sind in *Kapitel 1.3* des Prüfkatalogs definiert und sehen u.a. vor, dass die Fahrzeughersteller jederzeit auf die Software-Identifikationsnummer zugreifen können.

Die Dokumentation und Bereitstellung von Informationen zu Software-Updates stellen im Rahmen von SUMS eine weitere wesentliche Rolle dar. Dazu zählen u.a. Informationen zu den Bedingungen, unter denen ein Software-Update ausgeführt werden darf. Diese und weitere derartige Vorgaben befinden sich in *Kapitel 1.4* des Prüfkatalogs.

Die Anforderungen an den informationssicherheitstechnischen Schutz von Software-Updates auf der Fahrzeugherstellerseite sind in *Kapitel 1.5* geregelt. Sie sollen sicherstellen, dass Software-Updates sowohl vor Beginn des Aktualisierungsprozesses als auch während ihrer Übermittlung an das Fahrzeug ausreichend geschützt sind. In *Kapitel 1.6* werden schließlich spezifische Anforderungen an Over-The-Air Updates angeführt.

Die Inhalte von Kapitel 2 im Prüfkatalog entstammen ebenso dem Kapitel 7 der UNECE Regelung zu SUMS und befinden sich deshalb auch in Tabellenblatt 4. Im Unterschied zu den Anforderungen in Kapitel 1 sind sie aber eher technischer Natur und beziehen sich direkt auf den Fahrzeugtyp. *Kapitel 2.1* zur Informationssicherheit schließt an *Kapitel 1.5* des Prüfkatalogs an. Hier wird vorgeschrieben, dass eine Fahrzeugfunktion die Authentizität und Integrität des erhaltenen Updates überprüft, wodurch nur gültige Updates heruntergeladen und ausgeführt werden. Zusammen mit den im Abschnitt 1.5 beschriebenen Anforderungen soll dies gewährleisten, dass das gesamte System für Software-Updates, von der Erstellung über die Auslieferung bis zur Ausführung, sicher ist.

Anforderungen hinsichtlich der RXSWIN bestehen zudem nicht nur auf der Fahrzeugherstellerseite, sondern auch für den jeweiligen Fahrzeugtyp. Diese sind in

[165] Vgl. UNECE Document No. TFCS-ahSWTAN-04 (02.08.2017), Kap. 2.Y.1.

*Kapitel 2.2* operationalisiert dargestellt und fordern u.a. eine Beschreibung darüber, inwieweit die Änderung eines typgenehmigungspflichtigen Software-Systems zu einer Aktualisierung der RXSWIN am Fahrzeug führt.

*Kapitel 2.3* befasst sich wiederum mit spezifischen Anforderungen an Over-The-Air Updates, diesmal aber eben direkt am Fahrzeug. So muss z.B. bei Fehlschlagen eines OTA-Updates entweder die Vorversion des Systems wiederhergestellt oder alternativ das Fahrzeug in einen sicheren Zustand versetzt werden. Sehr wesentlich bei OTA-Updates ist zudem die Informationsübermittlung und Einbindung des Fahrzeugnutzers, weshalb diese Anforderungen in einem eigenen *Kapitel 2.4* angeführt werden.

Inhaltliche Basis für die Ausformulierung der einzelnen Anforderungen in diesem Tabellenblatt ist für beide Kapitel allen voran das Proposal Document der UNECE zur Regelung Nr. 156. Mit seinen Ansätzen zur Erfüllung der Regelung trägt es maßgeblich zur Operationalisierung der Anforderungen bei. Sofern eine Überschneidung gegeben ist, wurden für einige Anforderung außerdem Inhalte aus dem ISO 21434 Standard zu CSMS sowie aus dem Proposal Document zu CSMS entnommen.

*Horizontale Entwicklung*

Nach der inhaltlichen Gestaltung und Strukturierung folgt nun die horizontale Entwicklung des Tabellenblatts gemäß Spalten. Diese sieht die Unterteilung des Tabellenblatts in zwei Hälften vor.

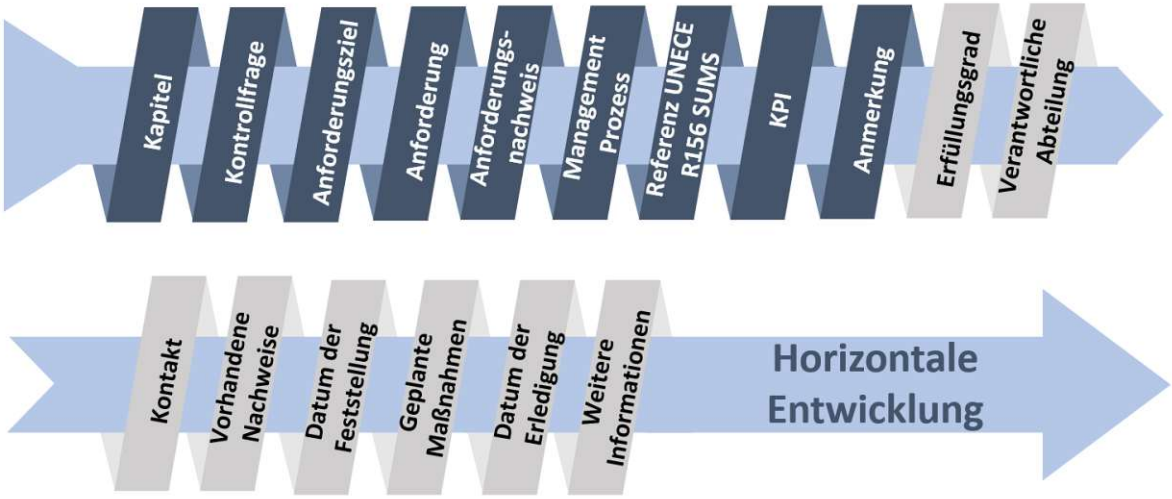



**Abbildung 25: Horizontale Entwicklung des Tabellenblatts 4 des Prüfkatalogs[166]**

In Abbildung 25 ist dieser horizontale Aufbau des Tabellenblattes dargestellt. Links befinden sich jene Spalten, die sämtliche Informationen zu den einzelnen operativen Anforderungen beinhalten (blau hinterlegt). Auf der rechten Seite befinden sich die Spalten, die vom Anwender des Prüfkatalogs im Laufe der Implementierung bzw.

[166] Quelle: Eigene Darstellung.

während der Aufrechterhaltung eines Software-Update Managementsystems zu befüllen sind (grau hinterlegt). Eine Beschreibung der einzelnen Spalten befindet sich in untenstehender Tabelle 12.

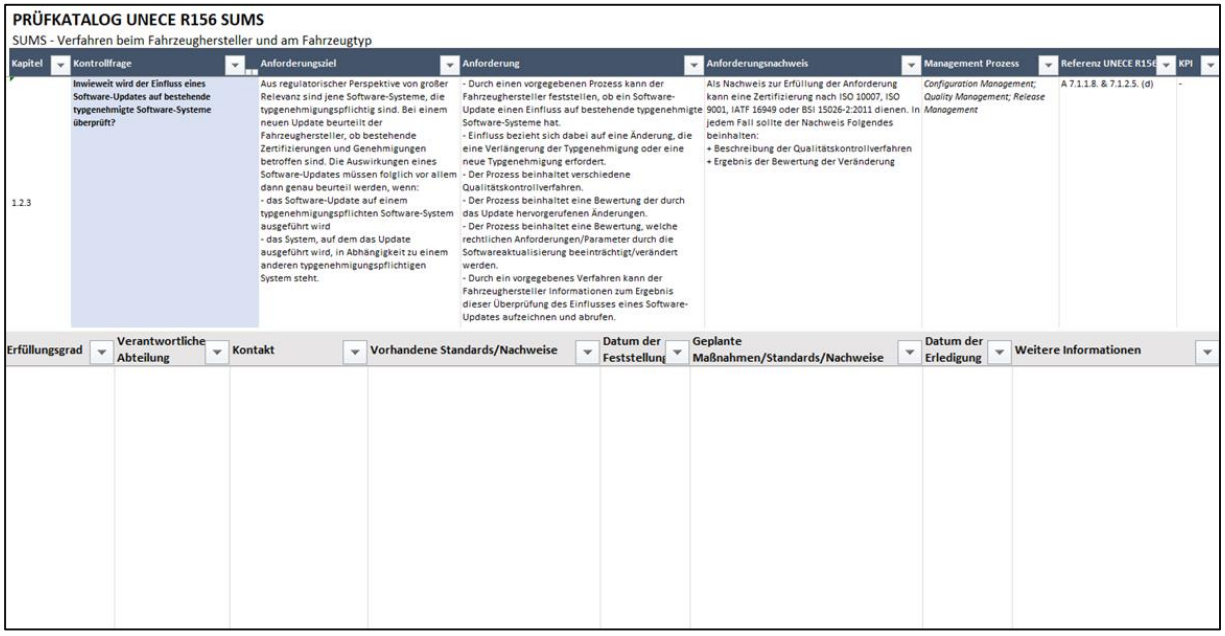
| Operative Anforderungen an ein SUMS | |
|---|---|
| **Spalte** | **Beschreibung der jeweiligen Spalte** |
| Kapitelnummer | Kapitelnummer der jeweiligen Anforderung im Prüfkatalog. |
| Kontrollfrage | Kontrollfrage der jeweiligen Anforderung im Prüfkatalog. |
| Anforderungsziel | Hier ist das Ziel der jeweiligen Anforderung in Fließtextform beschrieben. Die Erklärung enthält zudem Hintergrund-informationen, um die Relevanz der Anforderung hervorzuheben. |
| Anforderung | Auf Basis verschiedener Standards, Regelungen und Empfehlungen in Zusammenhang mit SUMS sind in dieser Spalte die konkreten Anforderungen aus der Regelung auf operative Ebene abgeleitet. |
| Anforderungsnachweis | Auf Basis derselben Standards, Regelungen und Empfehlungen sind an dieser Stelle Nachweise angeführt, die zur Erfüllung der jeweiligen Anforderung dienen können. Die drei Spalten Anforderungsziel, Anforderung und Anforderungsnachweis stellen den wesentlichsten Teil des Prüfkatalogs dar. |
| Management Prozess | Hier sind jene meist schon bestehenden Management Funktionen angeführt, denen die jeweilige Anforderung zuzuordnen ist. Sofern eine Anforderung möglicherweise bereits erfüllt ist, kann dies hilfreich sein bei der Suche nach dem Anforderungsnachweis. |
| Referenz UNECE R156 | Da die Reihung und Gliederung der Anforderungen im Prüfkatalog von jener in der UNECE Regelung abweicht, ist in dieser Spalte der Verweis zur jeweiligen UNECE Anforderung angeführt. |
| KPI | Für viele Anforderungen sind in Tabellenblatt 8 Beispiel KPIs angeführt, auf die in dieser Spalte verwiesen wird. |
| Anmerkung | Raum für Anmerkungen zur jeweiligen Anforderung. |

| Vom Anwender auszufüllende Spalten | |
|---|---|
| **Spalte** | **Beschreibung der jeweiligen Spalte** |
| Erfüllungsgrad | Während einige Spalten nicht zwingend zu befüllen sind, ist es wesentlich, dass der Erfüllungsgrad für die jeweilige Anforderung eingetragen wird. Andernfalls ist eine Ergebnisdarstellung in Tabellenblatt 7 nicht möglich. Gemäß der Prozessfähigkeits-messung aus Tabellenblatt 2 ist dazu ein Wert zwischen 0 (Unvollständiger Prozess) und 5 (Optimierender Prozess) einzutragen. |
| Verantwortliche Abteilung | An dieser Stelle ist die für die jeweilige Anforderung verantwortliche Abteilung einzutragen. |
| Kontakt | Sofern bekannt, können an dieser Stelle Kontaktdaten eingetragen werden. |
| Vorhandene Standards/ Nachweise | Bereits bestehende Standards, die als Nachweis zur (teilweisen) Erfüllung der Anforderungen dienen, können in dieser Spalte eingetragen werden. |

| | |
|---|---|
| Datum der Feststellung | In dieser Spalte ist das Datum des aktuellen Bearbeitungsstandes der jeweiligen Kontrollfrage einzutragen. |
| Geplante Maßnahmen/ Standards/ Nachweise | Sofern die Anforderung noch nicht in ausreichendem Maß erfüllt ist, können an dieser Stelle geplante Maßnahmen oder angestrebte Nachweise eingetragen werden. |
| Datum der Erledigung | In dieser Spalte wird jenes Datum eingetragen, ab dem die jeweilige Anforderung als erledigt gilt. |
| Weitere Informationen | Raum für weitere Informationen zur jeweiligen Anforderung. |

Tabelle 12: Beschreibung der Spalten in Tabellenblatt 4[167]

Für alle Spalten besteht zudem die Möglichkeit des Filterns nach einem bestimmten Kriterium. Dazu zählt z.B. das Filtern nach einem bestimmten Management Prozess oder nach einer bestimmten UNECE Anforderungen. Besonders hilfreich ist außerdem das Filtern nach Erfüllungsgraden. Durch Setzen des Filters an dieser Stelle auf „0“ oder „1“ erhält man auf einen Blick alle Anforderungen, bei denen noch großer Handlungsbedarf besteht. Abbildung 26 zeigt einen Auszug aus Tabellenblatt 4 des Prüfkatalogs. Weitere ausführliche Darstellungen werden im Anhang der Arbeit angeführt.



PRÜFKATALOG UNECE R156 SUMS

SUMS - Verfahren beim Fahrzeughersteller und am Fahrzeugtyp

| Kapitel | Kontrollfrage | Anforderungsziel | Anforderung | Anforderungsnachweis | Management Prozess | Referenz UNECE R156 | KPI |
|---|---|---|---|---|---|---|---|
| 1.2.3 | Inwieweit wird der Einfluss eines Software-Updates auf bestehende typgenehmigte Software-Systeme überprüft? | Aus regulatorischer Perspektive von großer Relevanz sind jene Software-Systeme, die typgenehmigungspflichtig sind. Bei einem neuen Update beurteilt der Fahrzeughersteller, ob bestehende Zertifizierungen und Genehmigungen betroffen sind. Die Auswirkungen eines Software-Updates müssen folglich vor allem dann genau beurteil werden, wenn:<br>- das Software-Update auf einem typgenehmigungspflichten Software-System ausgeführt wird<br>- das System, auf dem das Update ausgeführt wird, in Abhängigkeit zu einem anderen typgenehmigungspflichtigen System steht. | - Durch einen vorgegebenen Prozess kann der Fahrzeughersteller feststellen, ob ein Software-Update einen Einfluss auf bestehende typgenehmigte Software-Systeme hat.<br>- Einfluss bezieht sich dabei auf eine Änderung, die eine Verlängerung der Typgenehmigung oder eine neue Typgenehmigung erfordert.<br>- Der Prozess beinhaltet verschiedene Qualitätskontrollverfahren.<br>- Der Prozess beinhaltet eine Bewertung der durch das Update hervorgerufenen Änderungen.<br>- Der Prozess beinhaltet eine Bewertung, welche rechtlichen Anforderungen/Parameter durch die Softwareaktualisierung beeinträchtigt/verändert werden.<br>- Durch ein vorgegebenes Verfahren kann der Fahrzeughersteller Informationen zum Ergebnis dieser Überprüfung des Einflusses eines Software-Updates aufzeichnen und abrufen. | Als Nachweis zur Erfüllung der Anforderung kann eine Zertifizierung nach ISO 10007, ISO 9001, IATF 16949 oder BSI 15026-2:2011 dienen. In jedem Fall sollte der Nachweis Folgendes beinhalten:<br>+ Beschreibung der Qualitätskontrollverfahren<br>+ Ergebnis der Bewertung der Veränderung | *Configuration Management; Quality Management; Release Management* | A 7.1.1.8. & 7.1.2.5. (d) | - |

| Erfüllungsgrad | Verantwortliche Abteilung | Kontakt | Vorhandene Standards/Nachweise | Datum der Feststellung | Geplante Maßnahmen/Standards/Nachweise | Datum der Erledigung | Weitere Informationen |
|---|---|---|---|---|---|---|---|

Abbildung 26: Auszug aus Tabellenblatt 4 des Prüfkatalogs[168]

### Tabellenblatt 5: Anforderungen – Produktion

Die Anforderungen in diesem Tabellenblatt sind deutlich überschaubarer als jene im vorhergehenden Tabellenblatt 4 und beziehen sich auf die Anlage 1 eines anderen

[167] Quelle: Eigene Darstellung.
[168] Quelle: Prüfkatalog UNECE R156 SUMS, Tabellenblatt 4.

Übereinkommens der UNECE für die Harmonisierung von Fahrzeugvorschriften (UNECE/TRANS/505/Rev.3). Dort sind Verfahren zur Kontrolle der Konformität der Produktion beschrieben, die von den Fahrzeugherstellern einzuhalten sind. Im Rahmen der UNECE Regelung Nr. 156 zu SUMS wird dieses Thema in Kapiteln 9 und 11 behandelt.

*Vertikale Entwicklung*

Für den vorliegenden Prüfkatalog genügt die Eingliederung dieser Inhalte in einem Kapitel. Gemäß Abbildung 27 teilt sich dieses wiederum in zwei Unterkapitel 3.1 und 3.2 auf.


**Abbildung 27: Vertikale Entwicklung von Tabellenblatt 5 des Prüfkatalogs[169]**

Die Erteilung einer Typgenehmigung erfolgt zu Beginn eines Fahrzeuglebenszyklus. Die Konformität der Produktion (CoP) legt jedoch fest, dass die Produkte der Fahrzeughersteller während der gesamten Produktionslaufzeit die in den ursprünglichen Typgenehmigungsunterlagen festgelegten Spezifikationen und Leistungen erfüllen müssen.[170] *Kapitel 3.1* des Prüfkatalogs regelt die Kontrolle der Einhaltung dieser Verfahren, inklusive Dokumentation der Kontrollergebnisse.

Werden bei einer Kontrolle Abweichungen festgestellt, muss der Fahrzeughersteller zudem sicherstellen, dass Maßnahmen umgesetzt werden, um die Konformität der betroffenen Produktion wiederherzustellen. Dieses und das Vorgehen bei endgültiger Einstellung der Produktion sind in *Kapitel 3.2* beschrieben.

*Horizontale Entwicklung*

Auf die horizontale Entwicklung von Tabellenblatt 5 wird zu diesem Zeitpunkt nicht eingegangen. Sie entspricht demselben Aufbau mit den identischen Spalten wie in

[169] Quelle: Eigene Darstellung.
[170] UNECE/TRANS/505/Rev.3, Anlage 1.

Tabellenblatt 4 und wurde bereits im vorhergehenden Absatz im Detail beschrieben. Auch wird auf die Abbildung eines Auszugs aus Tabellenblatt 5 verzichtet. An dieser Stelle sei ein weiteres Mal auf den Anhang der vorliegenden Arbeit verwiesen, in dem sich ein Großteil des Prüfkatalogs befindet.

**Tabellenblatt 6: Anforderungen – Genehmigung**

Der Fokus liegt nun auf der Entwicklung von Tabellenblatt 6, das sich, wie eingangs erwähnt, in seinem Aufbau ein wenig von den beiden vorhergehenden Tabellenblättern unterscheidet. Die Anforderungen aus Kapiteln 1 bis 3 des Prüfkatalogs verlangen die Umsetzung konkreter Verfahren und Prozesse im Rahmen von SUMS. Im Gegensatz dazu beziehen sich die Inhalte in Tabellenblatt 6 (Kapitel 4,5 und 6 des Prüfkatalogs) auf die notwendigen Prozessschritte, die im Rahmen der Beantragung einer SUMS Konformitätsbescheinigung bzw. einer Typgenehmigung einmalig zu befolgen sind.

*Vertikale Entwicklung*

Für die vertikale Entwicklung, also die inhaltliche Strukturierung dieses Tabellenblattes, bietet sich die Aufteilung in drei Kapitel gemäß Abbildung 28 an.

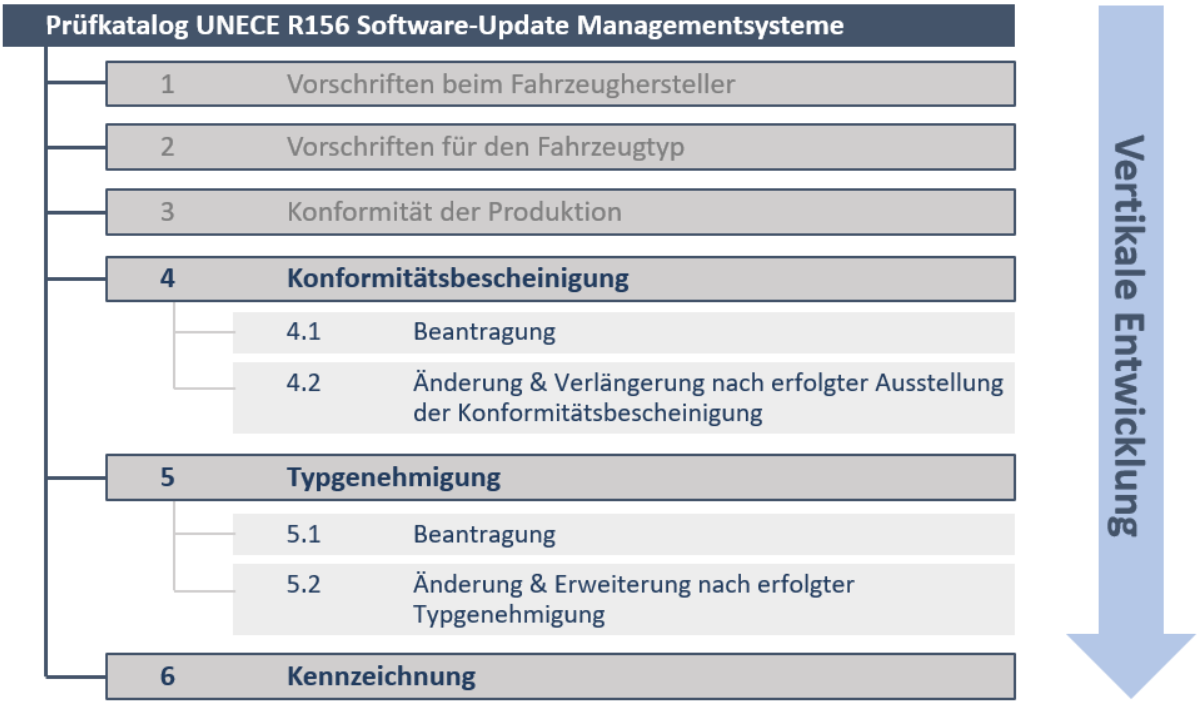



**Abbildung 28: Vertikale Entwicklung von Tabellenblatt 6 des Prüfkatalogs**[171]

Im Rahmen von *Kapitel 4.1* des Prüfkatalogs werden die einzelnen Vorgehensschritte zur Erlangung der SUMS Konformitätsbescheinigung beschrieben. Sie entstammen dem Kapitel 6 der UNECE Regelung und führen z.B. notwendige Unterlagen an, die dem Antrag auf Ausstellung der Konformitätsbescheinigung beizufügen sind. Im

[171] Quelle: Eigene Darstellung.

*Kapitel 4.2* wird zudem das Vorgehen bei Änderungen (z.B. neues Software Update) oder vor Ablauf der Gültigkeitsdauer der Konformitätsbescheinigung beschrieben.

Der Erhalt der Konformitätsbescheinigung stellt jedenfalls eine Grundvoraussetzung für den Antrag auf Genehmigung für einen Fahrzeugtyp hinsichtlich der Verfahren für Softwareaktualisierungen dar. Die im Zuge dieser Beantragung durchzuführenden Verfahrensschritte sind in *Kapitel 5.1* angeführt. Darin ist u.a. festgelegt, dass dem technischen Dienst ein Fahrzeug des zu genehmigenden Fahrzeugtyps zur Verfügung gestellt werden muss. Analog zu *Kapitel 4.2* ist in *Kapitel 5.2* das Vorgehen bei Änderung und Erweiterung nach erfolgter Typgenehmigung beschrieben. Innerhalb der UNECE Regelung werden diese Anforderungen zum Antrag auf Typgenehmigung in den Kapiteln 3 und 5 und damit vor der Konformitätsbescheinigung angeführt. Da aber die Konformitätsbescheinigung Voraussetzung für die Beantragung auf Typgenehmigung ist, wurde dieses Kapitel im Prüfkatalog vorgezogen.

*Kapitel 6* stellt das finale Kapitel im Prüfkatalog dar, welches sich mit Anforderungen an die Fahrzeughersteller beschäftigt. An jedem Fahrzeug, das einem nach dieser Regelung genehmigten Fahrzeugtyp entspricht, ist ein Genehmigungszeichen gemäß dem Muster in Anhang 3 der UN-Regelung Nr. 156 anzubringen. *Kapitel 6* definiert dann u.a. Anbringungsort und Form der Kennzeichnung.

*Vertikale Entwicklung*

Wenngleich sich der Aufbau von Tabellenblatt 6 von den beiden vorherigen Tabellenblättern unterscheidet, weisen sie dennoch einige Gemeinsamkeiten auf. So folgt auch Tabellenblatt 6 einer Unterteilung in zwei Hälften mit Informationen zu den Anforderungen auf der linken Seite und einem Bereich zur Befüllung vom Anwender auf der rechten Seite. Ebenso sind die ersten zwei Spalten *Kapitel* und *Kontrollfrage* identisch zu jenen in Tabellenblättern 4 und 5. Wie sich in Abbildung 29 erkennen lässt, ist der Aufbau der Spalten in Tabellenblatt 6 insgesamt jedoch etwas kompakter.

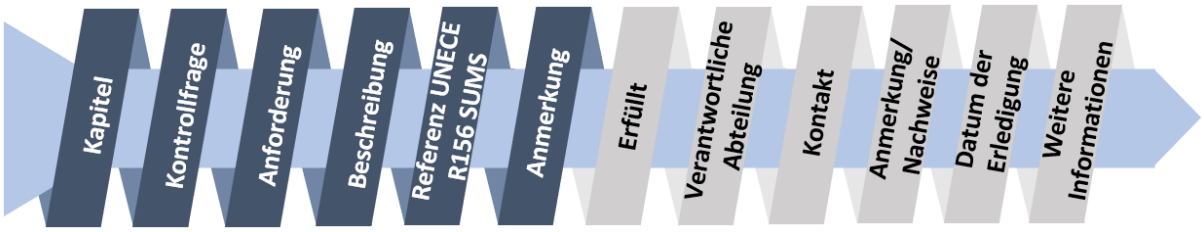
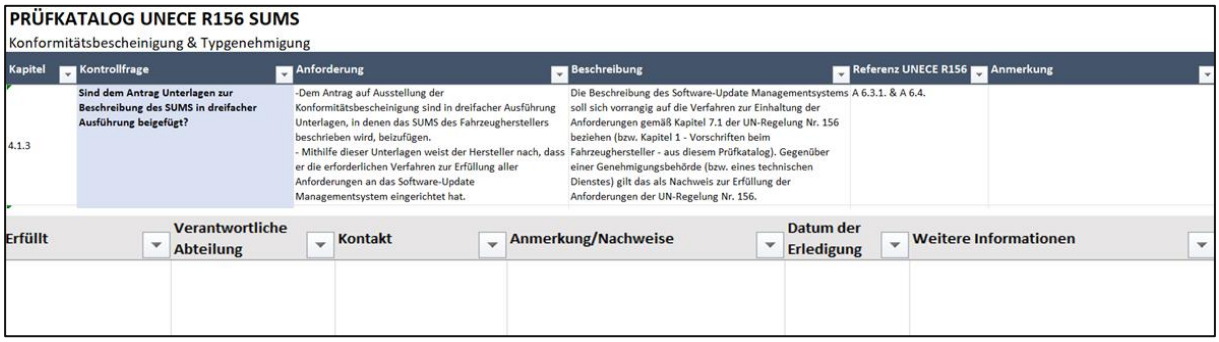



**Abbildung 29: Horizontale Entwicklung von Tabellenblatt 6 des Prüfkatalogs**[172]

Wie bereits erwähnt, liegt die Ursache für diesen unterschiedlichen horizontalen Aufbau in der Tatsache, dass die Anforderungen in Tabellenblatt 6 lediglich einmalig im Zuge des Beantragungs- und Genehmigungsprozesses zu befolgen sind. Damit

[172] Quelle: Eigene Darstellung.

einher geht auch, dass kein explizierter Anforderungsnachweis, z.B. in Form eines anerkannten Qualitätsstandards, zu erbringen ist. Ebenso wenig lassen sich die Anforderungen einer bestimmten Managementdisziplin zuordnen. Für die Erfüllungsgradmessung ergibt sich ebenfalls ein entscheidender Unterscheid. Zwar muss der Anwender wie schon zuvor die Spalte bearbeiten, allerdings ist an dieser Stelle kein Wert zwischen „0“ und „5“ einzutragen, sondern lediglich ob die Anforderung erfüllt ist („Ja“) oder nicht („Nein“). Infolgedessen lassen sich für diese Anforderungen auch keine KPIs definieren, weshalb diese Spalte komplett entfällt. Abbildung 30 zeigt einen Auszug aus Tabellenblatt 6 des Prüfkatalogs, bei dem die genannten Unterschiede zu erkennen sind.



PRÜFKATALOG UNECE R156 SUMS

Konformitätsbescheinigung & Typgenehmigung

| Kapitel | Kontrollfrage | Anforderung | Beschreibung | Referenz UNECE R156 | Anmerkung |
|---|---|---|---|---|---|
| 4.1.3 | **Sind dem Antrag Unterlagen zur Beschreibung des SUMS in dreifacher Ausführung beigefügt?** | -Dem Antrag auf Ausstellung der Konformitätsbescheinigung sind in dreifacher Ausführung Unterlagen, in denen das SUMS des Fahrzeugherstellers beschrieben wird, beizufügen.<br>- Mithilfe dieser Unterlagen weist der Hersteller nach, dass er die erforderlichen Verfahren zur Erfüllung aller Anforderungen an das Software-Update Managementsystem eingerichtet hat. | Die Beschreibung des Software-Update Managementsystems soll sich vorrangig auf die Verfahren zur Einhaltung der Anforderungen gemäß Kapitel 7.1 der UN-Regelung Nr. 156 beziehen (bzw. Kapitel 1 - Vorschriften beim Fahrzeughersteller - aus diesem Prüfkatalog). Gegenüber einer Genehmigungsbehörde (bzw. eines technischen Dienstes) gilt das als Nachweis zur Erfüllung der Anforderungen der UN-Regelung Nr. 156. | A 6.3.1. & A 6.4. | |

| Erfüllt | Verantwortliche Abteilung | Kontakt | Anmerkung/Nachweise | Datum der Erledigung | Weitere Informationen |
|---|---|---|---|---|---|
| | | | | | |

**Abbildung 30: Auszug aus Tabellenblatt 6 des Prüfkatalogs[173]**

## 4.2.4 Ergebnisse und Key Performance Indicators

Nachdem die konkreten Anforderungen, die sich aus der UNECE Richtlinie für OEMs ergeben, abgeleitet und in Audit-gerechter Form dargestellt wurden, beschäftigt sich dieses Kapitel mit Ergebnissen und Key Performance Indicators. Der Grundstein für das Tabellenblatt 7 – Ergebnisse – wurde bereits in den Tabellenblätter zuvor mit der Eintragung des Erfüllungsgrades gelegt. Während die Ergebnisse der Erfüllungsgradmessung in Tabellenblatt 7 vorrangig in der Aufbauphase für ein SUMS zum Einsatz kommen, dienen die Beispiel KPIs in Tabellenblatt 8 der kontinuierlichen Einhaltung der SUMS Anforderungen in der Betriebsphase. Auf die Entwicklung beider Tabellenblätter wird nun im Detail eingegangen.


### Tabellenblatt 7 – Ergebnisse

Die Feststellung des SUMS Erfüllungsgrades in der Aufbauphase stellt einen Schwerpunkt des vorliegenden Prüfkatalogs dar. Wie bereits erwähnt, muss dazu in der Zeile der jeweiligen Kontrollfrage im Prüfkatalog der Erfüllungsgrad eingetragen

[173] Quelle: Prüfkatalog UNECE R156 SUMS, Tabellenblatt 6.

werden. Auf Basis der vom Anwender eingetragenen Erfüllungsgrade erfolgt in einem ersten Schritt die grafische Auswertung mit den ungekürzten Originalwerten in Form eines Netzdiagramms. Ein solches eignet sich besonders gut zur grafischen Darstellung von Bewertungen für zuvor festgelegte Kriterien.

Für jedes Kapitel des Prüfkatalogs gibt es eine Achse und für alle Achsen gilt die gleiche Orientierung. Die besten Werte, d.h. im vorliegenden Fall der Wert „5“ für den optimierenden Prozess, liegen einheitlich am äußeren Rand des Netzes. Die Auswertung der Ergebnisse erfolgt dabei sowohl je Kapitel als auch je Unterkapitel. Für letztere Variante werden die Werte direkt aus der Erfüllungsgradspalte übernommen, wohingegen bei der Auswertung je Kapitel die Mittelwerte aus jedem Unterkapitel herangezogen werden. In strichliertem Grün dargestellt ist zudem der zu erreichende Zielreifegrad für die Kontrollfragen. Er ist individuell vom OEM zu bestimmen, liegt in der Regel aber durchgängig bei „3“ (etablierter Prozess). Das Streben nach einem Zielreifegrad von „5“ (Optimierender Prozess) ist nicht nur äußerst aufwendig, sondern geht auch über die Notwendigkeit für eine Zertifizierung nach UNECE R156 hinaus. Eine weitere Besonderheit ergibt sich für die Auswertung der Erfüllungsgrade der Kontrollfragen 4 bis 6 des Prüfkatalogs. Wie in Kapitel 4.2.3 dieser Arbeit beschrieben, wird bei deren Erfüllungsgrad kein Zahlenwert zwischen 0 und 5 eingetragen, sondern lediglich angegeben, ob die Anforderungen erfüllt ist („Ja“) oder nicht („Nein“). Um ihr Ergebnis dennoch in die grafische Gesamtauswertung einfließen lassen zu können, wird einem „Ja“ der vom OEM definierte Zielreifegrad zugeordnet. Einem „Nein“ wird der Wert „0“ vergeben. Sofern für alle Kontrollfragen ein Wert eingetragen wurde, erhält man folgende in Abbildung 31 dargestellte beispielhafte Auswertung.


**Abbildung 31: Auswertung der Erfüllungsgradmessung je Kapitel und Unterkapitel**[174]

Die oben abgebildete Darstellungsform der Erfüllungsgradmessung weist jedoch einen Nachteil auf. Für die erfolgreiche Zertifizierung nach SUMS gilt, dass bei allen

[174] Quelle: Prüfkatalog UNECE R156 SUMS, Tabellenblatt 7.

Kontrollfragen zumindest der Zielreifegrad erreicht werden muss. Sofern ein OEM bei gewissen Kontrollfragen einen sehr hohen Erfüllungsgrad aufweist, kann es vorkommen, dass andere nicht erfüllte Kontrollfragen dadurch in der Gesamtauswertung überkompensiert werden und nicht aufscheinen. In den zwei weiteren grafischen Auswertungen in Tabellenblatt 7 ist deshalb das Gesamtergebnis mit gekürzten Werten dargestellt. Bei der Berechnung des Gesamtergebnisses werden in diesem Fall jene Erfüllungsgrade, die den Zielreifegrad übererfüllen, auf den Zielreifegradwert gekürzt. Erst im Anschluss daran wird der Durchschnittswert pro (Unter-)Kapitel ermittelt. Dies stellt sicher, dass die Anforderungen themenübergreifend erfüllt werden und kein Ausgleich von über- und untererfüllten Controls stattfindet. Das Ergebnis dieser Auswertung – ebenfalls im Netzdiagrammformat und mit denselben fiktiven Erfüllungsgradwerten – befindet sich in Abbildung 32.

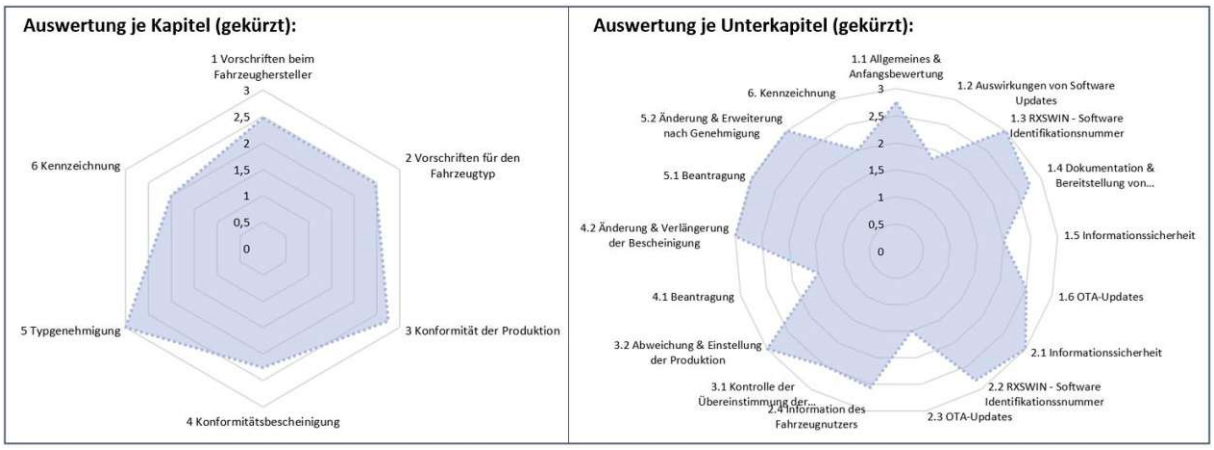



**Abbildung 32: Auswertung der Erfüllungsgradmessung mit gekürzten Werten[175]**

Beim Vergleich der beiden Abbildungen 31 und 32 ist bei der linken Auswertung je Kapitel der eben erwähnte Nachteil der Auswertung mit Originalwerten gut zu erkennen. Während in Abbildung 31 das Kapitel 3 des Prüfkatalogs – Konformität der Produktion – auf den ersten Blick den Zielreifegrad sogar zu übertreffen scheint, offenbart die Auswertung in Abbildung 32 Gegenteiliges. Wenngleich mehrere Anforderungen des Kapitels einen hohen Erfüllungsgrad aufweisen, erreichen einige von ihnen den Zielreifegrad offenbar nicht. Dementsprechend ist bei der Gesamtauswertung mit gekürzten Werten der Zielreifegrad des Kapitels auch noch nicht erreicht.

Welche konkreten Kontrollfragen die Anforderungen nicht erfüllen lässt sich dann u.a. in der anschließenden Detailauswertung der Erfüllungsgradmessung erkennen. Dort ist für jede Kontrollfrage des Prüfkatalogs sowohl das Originalergebnis als auch der gekürzte Wert der Erfüllungsgradmessung angegeben. Ebenso befindet sich dort das

[175] Quelle: Prüfkatalog UNECE R156 SUMS, Tabellenblatt 7.

Feld, in dem der Anwender des Prüfkatalogs den individuell zu definierenden Zielreifegrad einzutragen hat. Für die einzelnen Kontrollfragen der Kapitel 4 bis 6 scheint auf, ob die Anforderung erfüllt ist oder nicht. Zudem wird für die (Unter-)Kapitel angezeigt, wie viele der Anforderungen bereits erfüllt sind. Dazu ist im Hintergrund des *Microsoft Excel* Tabellenblattes die entsprechende Formel hinterlegt. Ein Ausschnitt aus dieser Detailauswertung befindet sich in Abbildung 33.

**Prüfkatalog UNECE R156 SUMS**

Auswertung & Ergebnis der Erfüllungsgradmessung

**Detailauswertung - Anforderungen SUMS & Produktion**

**Angestrebter Zielreifegrad:** 3

| Kapitel: | Kontrollfrage: | Ergebnis: | Ergebnis gekürzt: |
|---|---|---|---|
| **3** | **Konformität der Produktion** | **3,50** | **2,75** |
| **3.1** | **Verfahren zur Kontrolle der Übereinstimmung der Produktion** | **3,50** | **2,50** |
| 3.1.1 | Inwieweit wird kontrolliert, ob jedes hergestellte Fahrzeug dem ursprünglich genehmigten Typ entspricht? | 5,00 | 3,00 |
| 3.1.2 | Inwieweit werden die Ergebnisse der Kontrolle der Konformität dokumentiert und aufbewahrt? | 2,00 | 2,00 |
| **3.2** | **Vorgehen bei Abweichung und Einstellung der Produktion** | **3,50** | **3,00** |
| 3.2.1 | Inwieweit ist das Vorgehen bei Abweichungen der Produktion definiert? | 3,00 | 3,00 |
| 3.2.2 | Inwieweit ist das Vorgehen bei Einstellung der Produktion definiert? | 4,00 | 3,00 |

**Detailauswertung - Anforderungen Genehmigung**

| Kapitel: | Kontrollfrage: | Erfüllt: |
|---|---|---|
| **6** | **Kennzeichnung** | **2 von 3** |
| 6.1 | Ist das Genehmigungskennzeichen an der richtigen Stelle angebracht? | Nein |
| 6.2 | Ist das Genehmigungskennzeichen in der richtigen Form angebracht? | Ja |
| 6.3 | Das zu genehmigende Fahrzeug entspricht einem Fahrzeugtyp, der im betroffenen Land bereits nach einer oder mehreren anderen Regelungen genehmigt wurde. Ist das Verhalten des Fahrzeugherstellers für diese Situation korrekt? | Ja |

**Abbildung 33: Detailauswertung der Erfüllungsgradmessung**[176]

Abschließend werden in Tabellenblatt 7 in einer eigenen Auflistung noch offene Anforderungen angeführt, d.h. jene Kontrollfragen, die den Zielreifegrad nicht erreicht haben. Gleichermaßen gelten Kontrollfragen der Kapitel 4 bis 6 als noch offen, bei denen in der Spalte *Erfüllt* „Nein“ eingetragen wurde. Im Hintergrund dieser Darstellung arbeitet eine Filter-Funktion. Mittels einer „IF-Bedingung“ wird für jede Anforderung überprüft, ob der Zielreifegrad erreicht ist. Ist dies der Fall, wird in einer Hilfsspalte „Ausblenden“ eingetragen, andernfalls „Anzeigen“. Die Filter-Funktion sorgt

[176] Quelle: Prüfkatalog UNECE R156 SUMS, Tabellenblatt 7.

anschließend dafür, dass am Ende lediglich jene Zeilen mit dem Wert „Anzeigen“ aufscheinen.

**Tabellenblatt 8 – Key Performance Indicators**

Tabellenblatt 8 stellt das letzte Tabellenblatt des Prüfkatalogs dar und listet eine Reihe von Beispiel-KPIs. Im Unterschied zur Erfüllungsgradmessung in Tabellenblatt 7 dienen die Beispiel KPIs in Tabellenblatt 8 der kontinuierlichen Einhaltung der SUMS Anforderungen in der Betriebsphase.

Generell handelt es sich bei KPIs um aussagekräftige Kennzahlen, wobei der Begriff ursprünglich aus dem Controlling kommt. Die Zuordnung eines KPIs zu einem spezifischen Attribut eines Prozesses charakterisiert dessen Effizienz und Leistungsfähigkeit. Er macht ihn somit vergleichbar mit ähnlichen Prozessen in anderen Unternehmen oder anderen Zeiträumen. Im Rahmen der Informationstechnologie stellen die Verfügbarkeit eines Dienstleistungsservices oder die Anzahl von gelösten Incidents übliche KPIs dar.[177]

Für die Entwicklung von Tabellenblatt 8 des vorliegenden Prüfkatalogs folgt, dass in einem ersten Schritt jene Kontrollfragen bzw. Anforderungen identifiziert werden, für die eine Definition von KPIs möglich ist und sinnvoll erscheint. Dabei handelt es sich durchwegs um Kontrollfragen aus den Kapiteln 1 bis 3 des Prüfkatalogs. Die Anforderungen aus Kapiteln 4 bis 6 betreffen, wie bereits ausführlich beschrieben, einmalig durchzuführende Prozessschritte. Eine laufende Überwachung ist bei ihnen nicht vorgesehen und erfordert dementsprechend auch keine Definition von KPIs. Für die Anforderungen aus Kapiteln 1 bis 3 gilt, dass insbesondere für jene Kontrollfragen KPIs definiert werden, die gut mess- und bewertbar sind. Diese Kontrollfragen werden schließlich in horizontaler Ebene (d.h. jede Spalte gleich eine Kontrollfrage) im Tabellenblatt 8 aufgetragen.

In der vertikalen Ebene werden für jeden KPI insgesamt 11 Eigenschaften zur Charakterisierung des KPIs festgelegt. Sie sind in Tabelle 13 gelistet und beschrieben.

| Eigenschaften KPI | Beschreibung der Eigenschaft |
|---|---|
| Kapitel im Prüfkatalog | An dieser Stelle ist das Kapitel im Prüfkatalog inklusive der entsprechenden Kontrollfrage angegeben. |
| Bereich | Sofern möglich und sinnvoll werden für jede angeführte Kontrollfrage zwei KPIs definiert. Dabei handelt es sich zum einen um den KPI „Abdeckung“, der den Abdeckungsgrad der jeweiligen Anforderungsmaßnahme misst. Der zweite KPI „Effektivität“ misst, inwiefern die umgesetzten Maßnahmen wirksam sind zur Erfüllung der Anforderung. |
| ID | Jedem KPI wird eine ID-Nummer zugeordnet. Auf diese wird im jeweiligen Kapitel des Prüfkatalogs verwiesen. |

[177] Vgl. Köhler und Köhler (2007), S. 35f.

| | |
|---|---|
| Bezeichnung | Jeder KPI erhält eine individuelle Bezeichnung. |
| Beschreibung | In dieser Spalte befindet sich eine Beschreibung des jeweiligen KPIs, inklusive etwaiger Hintergrundinformationen zum KPI. |
| Ziel | Hinter der Anforderung eines jeden KPIs steht ein konkretes Ziel, das an dieser Stelle dargestellt wird. |
| Messung | Ziel von KPIs ist das mess- und vergleichbar machen einer bestimmten Leistung. Dementsprechend müssen die Leistungskennwerte gemessen werden, z.B. in Form des Quotienten aus Ist-Wert und Soll-Wert. |
| Angestrebter Zielwert | Der angestrebte Zielwert ist jener Wert, den die KPI Messung erreichen soll. Im Optimalfall liegt dieser Wert bei 100% für Relativmessungen und bei 0 für Messungen in absoluten Zahlen von z.B. Incidents. |
| Schwellwerte | In der Praxis werden diese Werte allerdings nur selten erreicht. In der Zeile *Schwellwerte* sind deshalb Abstufungen definiert, die zumindest eine teilweise oder ausreichende Erfüllung der Anforderung kennzeichnen. |
| Durchführungsintervall | Die Messung der KPIs muss in regelmäßigen Abständen erfolgen. Je nach KPI können diese unterschiedlich sein. |
| Bemerkung | In dieser Zeile ist Raum für Anmerkungen zum jeweiligen KPI. |

Tabelle 13: Eigenschaften der KPIs[178]

Der Auszug eines Beispiel-KPIs aus Tabellenblatt 8 ist in Abbildung 34 dargestellt. An dieser Stelle sei generell anzumerken, dass der Inhalt dieses Tabellenblattes als Hilfestellung für Unternehmen dient, eigene passende KPIs zu identifizieren. Zudem müssen insbesondere der angestrebte Zielwert, die Schwellwerte sowie das Durchführungsintervall individuell angepasst werden.

**PRÜFKATALOG UNECE R156 SUMS**

Beispiele zu KPIs

| | | |
|---|---|---|
| **Kapitel im Prüfkatalog** | 1.2.2 Inwieweit wird die Kompatibilität eines Software-Updates mit der bestehenden Konfiguration auf dem Zielfahrzeug überprüft? | |
| **Bereich** | ABDECKUNG | EFFEKTIVITÄT |
| **ID** | **2.1** | **2.2** |
| **Bezeichnung** | **Abdeckungsgrad Kompatibilitätsprüfungen** | **Effektivität von Kompatibilitätsprüfungen** |
| **Beschreibung** | Bevor ein Update installiert wird, muss die Kompatibilität mit den bestehenden Systemen überprüft werden. Dies erfolgt auf Basis einer Kompatibilitätsprüfung. Der KPI misst die durchgehende Anwendung von Kompatibilitätsprüfungen bei Software-Updates. | Ziel der Kompatibilitätsprüfung ist, dass bestehende Systeme auch nach einer Softwareaktualisierung weiterhin problemlos funktionieren. Der KPI misst die Effektivität der Kompatiblitätsprüfungen durch Erfassung aller Vorfälle, die auf Kompatibilitätsprobleme nach einer Aktualisierung zurückzu-führen sind. |
| **Ziel** | Für jedes Software-Update wird im Vorfeld eine Kompatibilitätsprüfung durchgeführt. | Es treten keine Kompatibilitätsprobleme mit bestehenden Software-Systemen auf. |
| **Messung** | KPI Quotient = Anzahl der durchgeführten Kompatibilitätsprüfungen / Anzahl aller durchgeführten SW-Updates | KPI = Anzahl aller Software-Updates, bei denen Kompatibilitätsprobleme mit der bestehenden Software aufgetreten sind |
| **Angestrebter Zielwert** | 100% | 0 |
| **Schwellwerte** | individuell zu bestimmen (z. B. Grün: > 90%, Gelb: 70-90%, Rot: < 70%) | individuell zu bestimmen (0-20...gering, 20-50 mittel, 50+ hoch) |
| **Durchführungsintervall** | individuell zu bestimmen (z.B. quartalsweise) | individuell zu bestimmen (z.B. quartalsweise) |
| **Bemerkung** | | |

Abbildung 34: Beispiel KPI aus Tabellenblatt 8 des Prüfkatalogs[179]

[178] Quelle: Eigene Darstellung.
[179] Quelle: Prüfkatalog UNECE R156 SUMS, Tabellenblatt 8.

## 4.3 Resultat

Am Ende der Konzeption und Entwicklung steht der fertige Prüfkatalog. Strukturelle Basis der Anwendung ist der unter Informationssicherheitsverantwortlichen weit verbreitete ISA Katalog des VDA. Die Anlehnung an diesen Katalog erleichtert folglich den Umgang mit dem entwickelten Prüfkatalog zu SUMS.

Inhaltlich vereint der Prüfkatalog sämtliche bestehende Standards, Normen und Empfehlungsdokumente mit Bezug zur Regelung Nr. 156 zu SUMS. Die zweckmäßige Gruppierung und Integration aller Informationen ermöglicht einen intuitiven Umgang mit dem Prüfkatalog. Insbesondere die Erweiterung der Anforderungen aus der Regelung um das konkrete Anforderungsziel und operativen Anforderungsnachweisen bietet dem Anwender eine Hilfestellung bei der Umsetzung seiner Verfahren für Softwareaktualisierungen.

Auf Basis dieser Ausarbeitung eindeutiger und objektiv zu bewertender Anforderungskriterien stellt der Prüfkatalog einen ganzheitlichen Ansatz zur Konzeption, Implementierung und Aufrechterhaltung eines Software-Update Management Systems dar. Er bietet damit eine Grundlage zur kosteneffizienten Vorbereitung auf ein Zertifizierungsaudit nach SUMS.

Angesichts der verbreiteten Verwendung von *Microsoft Excel* in sämtlichen Unternehmen entfällt beim Prüfkatalog die Notwendigkeit zur Installation einer eigenen Applikation. Darüber hinaus ermöglicht die Umsetzung in *Microsoft Excel* u.a. das Filtern nach bestimmten Kapiteln und Kontrollfragen, die Auswahl von Erfüllungsgraden per Dropdown Menü oder die grafische Darstellung der Erfüllungsgradmessung am Ende des Prüfkatalogs.

Mithilfe des Prüfkatalogs erhalten die Anwender einen Überblick über den derzeitigen Ist-Zustand im eigenen Unternehmen hinsichtlich der Verfahren zu Softwareaktualisierungen. Auf Basis dessen können Schritt für Schritt Maßnahmen umgesetzt werden, um das gemäß der UNECE Regelung geforderte Niveau zu erreichen. Ist dieses Niveau erreicht, kann mithilfe der KPIs die fortlaufende Einhaltung der Anforderungen überwacht werden.

# 5 Validierung

Im Rahmen dieses Kapitels erfolgt die Validierung des entwickelten Prüfkatalogs. Sie stellt damit den Beginn der dritten Phase des vierstufigen Erkenntnisprozesses entsprechend der Design Science Research Methode von Österle dar – Bewertung und Prüfung des Artefakts.

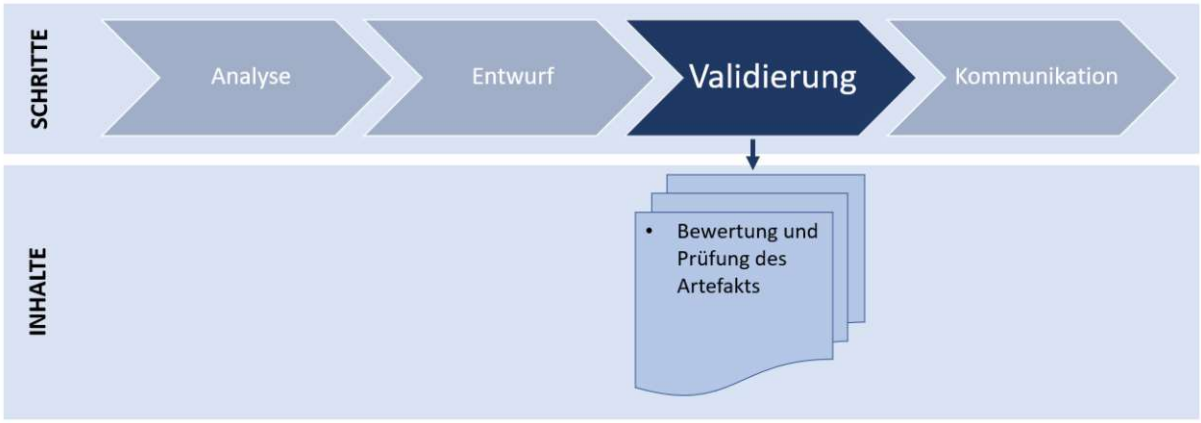



**Abbildung 35: Aktuelle Phase 3 in Österle's Design Science Research[180]**

Diese Phase sieht vor, dass die entwickelte Anwendung hinsichtlich ihrer Nützlichkeit sowie der Erfüllung ihrer zuvor definierten Anforderungen überprüft wird. Der Abgleich gegen die Anforderungen hat dabei systematisch zu erfolgen, um zu prüfen, ob die Anwendung die Vorgaben aus der Analyse und dem Entwurf umsetzt. Im Optimalfall wird die erstellte Anwendung im Rahmen der Validierung zudem für den jeweiligen Zweck eingesetzt. Damit kann überprüft werden, ob sie auch wirklich für die Praxis geeignet ist und dort den gewünschten Nutzen bringt. Je nach Rahmenbedingungen und Aufgabenstellungen ist dies allerdings nicht immer möglich.[181]

Für die Validierung des zuvor entwickelten Prüfkatalogs bedeutet das zunächst die Auswahl einer geeigneten Validierungsmethode in Kapitel 5.1. Im Zuge dessen offenbart sich die 1986 von John Brooke entwickelte sogenannten System Usability Scale (SUS) Methode als angebracht zur Validierung des vorliegenden Prüfkatalogs. Durch Befragung mehrerer Experten erfolgt die Messung der Usability, also der Tauglichkeit des entwickelten Prüfkatalogs in Kapitel 5.2. In einem letzten Schritt werden in Kapitel 5.3 die Ergebnisse der Validierung zusammengefasst und grafisch dargestellt.

[180] Quelle: Eigene Darstellung.
[181] Vgl. Brenner-Wickner, Kneuper und Schlömer (2020), S. 7.

## 5.1 Auswahl der Validierungsmethode

Die Usability einer Anwendung im Bereich von Informationstechnologien ist entscheidend für ihren Erfolg. Sie stellt ein wesentliches Qualitätsmerkmal des Produktes dar und steht für die Gebrauchstauglichkeit der Anwendung. Im Mittelpunkt der Usability stehen die Benutzer. Sie fordern ein Produkt, das schnell und einfach genutzt werden kann und mit dem sie ihre Ziele erreichen. Die Nützlichkeit einer Anwendung, z.B. eines Prüfkatalogs, hängt folglich davon ab, wie sehr sie dem Benutzer dabei hilft seine Ziele zu erreichen.[182] Der zentrale Aspekt bei der Validierung des vorliegenden Prüfkatalogs ist daher seine Usability.

Zur Messung der Usability stehen unterschiedliche Methoden zur Verfügung. Eine der Gebräuchlichsten stellt die Verwendung von Fragebögen dar. Sie dienen dazu die Meinung von Probanden zur Usability einer Anwendung zu erfahren. Typischerweise sind die Fragen als Multiple-Choice-Fragen formuliert, bei denen die Befragten aus einer Reihe von Alternativen oder Punkten auf einer Bewertungsskala auswählen. Nachfolgend angeführt sind vier aktuelle standardisierte Fragebögen, mit denen die Zufriedenheit der Teilnehmer mit der Usability von Produkten oder Systemen bewertet werden kann:[183]

- Questionnaire for User Interaction Satisfaction (QUIS)
- Software Usability Measurement Inventory (SUMI)
- Post-Study System Usability Questionnaire (PSSUQ)
- System Usability Scale (SUS)

Im Rahmen dieser Arbeit erfolgt die Validierung des Prüfkatalogs mithilfe von System Usability Scale (SUS). Diese quantitative Methode wurde 1986 von John Brooke entwickelt und stellt eine sogenannte „Quick and Dirty“ Methode zur Messung der Usability von Anwendungen dar. Brooke reagiert damit auf die Anforderungen seitens der Industrie nach einer zuverlässigen und kostengünstigen Skala, die für die globale Bewertung der Benutzerfreundlichkeit von Systemen verwendet werden kann. Im Laufe der vergangenen Jahre hat sich SUS deshalb als bewährtes Tool erwiesen, wenn es um die technologieunabhängige Bewertung der Usability geht.

Insgesamt umfasst der im Rahmen von SUS entwickelte Fragebogen von Brooke zehn Fragen auf Basis von Likert-Skalen mit je fünf Antwortoptionen. Dabei enthält der Fragebogen fünf positiv und fünf negativ formulierte Aussagen zur Usability der zu bewertenden Anwendung. Wenngleich diese noch an die individuellen Bedingungen der Bewertung anzupassen sind, schlägt Brooke folgende zehn Aussagen vor:[184]

[182] Vgl. Strutzenberger (2017), S. 10ff.
[183] Vgl. Sauro und Lewis (2016), S. 185f.
[184] Vgl. Brooke (1996), S. 189ff.

1. Ich kann mir sehr gut vorstellen, das System regelmäßig zu nutzen.
2. Ich empfinde das System als unnötig komplex.
3. Ich empfinde das System als einfach zu nutzen.
4. Ich denke, dass ich technischen Support brauchen würde, um das System zu nutzen.
5. Ich finde, dass die verschiedenen Funktionen des Systems gut integriert sind.
6. Ich finde, dass es im System zu viele Inkonsistenzen gibt.
7. Ich kann mir vorstellen, dass die meisten Leute das System schnell zu beherrschen lernen.
8. Ich empfinde die Bedienung als sehr umständlich.
9. Ich habe mich bei der Nutzung des Systems sehr sicher gefühlt.
10. Ich musste eine Menge Dinge lernen, bevor ich mit dem System arbeiten konnte.

Die Antwortmöglichkeiten basieren, wie bereits erwähnt, auf Likert-Skalen und sind in Abbildung 36 dargestellt. Sie reichen von der Note 0 (Stimme gar nicht zu) bis hin zur Note 4 (Stimme voll zu).

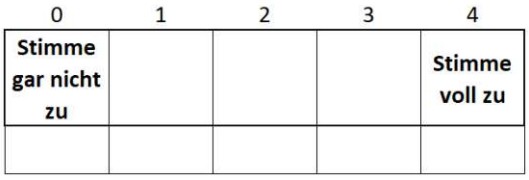



**Abbildung 36: SUS Likert-Skala mit 5 Antwortmöglichkeiten[185]**

Die Beantwortung der Fragen erfolgt in der Regel nachdem der Befragte Gelegenheit hatte, das zu bewertende System zu benutzen. Sofern ein Befragter das Gefühl hat, dass er eine bestimmte Aussage nicht beantworten kann, sollte er den Mittelpunkt der Skala markieren. Um den SUS-Score zu generieren, werden zunächst die Punkte der einzelnen Aussagen addiert. Der Score-Beitrag jeder Aussage reicht – analog zur Skalenposition – von 0 bis 4. Aussagen 1, 3, 5, 7 und 9 sind positiv formuliert, ihr Score-Beitrag entspricht folglich der Skalenposition. Aussagen 2, 4, 6, 8 und 10 hingegen sind negativ formuliert. Ihr Score-Beitrag ergibt sich durch 4 minus der Skalenposition. Die gewonnenen Zahlen werden addiert – die Summe liegt zwischen 0 und 40 – und anschließend mit 2,5 multipliziert. Der Gesamt-Score hat dadurch eine Ausprägung zwischen 0 (schlechteste vorstellbare Anwendung) und 100 (beste vorstellbare Anwendung).[186] Nach der Befragung mehrerer Probanden wird im

[185] Quelle: Eigene Darstellung auf Basis von Brooke (1996), S. 192.
[186] Quelle: https://blog.seibert-media.net/blog/2011/04/11/usablility-analysen-system-usability-scale-sus/ (Gelesen am: 07.01.2022)

Anschluss ein durchschnittlicher SUS-Score ermittelt, welcher als Prozentwert gemäß Abbildung 37 interpretiert werden kann.

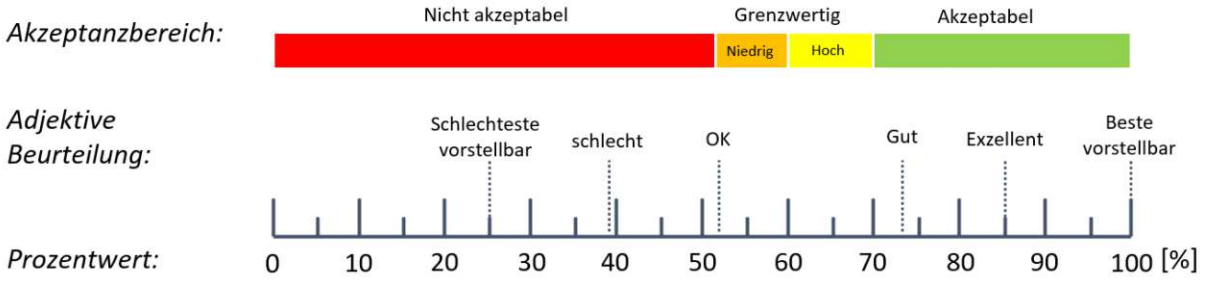



Abbildung 37: Interpretation des SUS-Scores[187]

## 5.2 Anwendung für den Prüfkatalog

Für die Anwendung der SUS-Methode zur Validierung des im Zuge dieser Arbeit entwickelten Prüfkatalogs müssen die Aussagen des Fragebogens angepasst werden. Im Fokus der Validierung steht, wie zu Beginn des Kapitels erwähnt, die Überprüfung der Nützlichkeit des Prüfkatalogs sowie der eingangs an ihn gestellten Anforderungen. Folglich müssen die Aussagen im Rahmen des SUS-Fragebogens so umformuliert werden, dass sie diese Aspekte der Validierung abdecken.

| NR: | EIGENSCHAFTEN PRÜFKATALOG: | SUS AUSSAGE FRAGEBOGEN: |
|---|---|---|
| 1 | Richtigkeit & Vollständigkeit | Ich denke, dass die Anforderungen vollständig und korrekt im Prüfkatalog berücksichtigt sind. |
| 2 | Wirksamkeit & Zweck | Ich empfinde den Prüfkatalog als nicht hilfreich beim Überpüfen der Anforderungen an das SUMS. |
| 3 | Benutzerfreundlichkeit | Ich finde, dass die Anforderungen logisch und strukturiert dargestellt sind. |
| 4 | Konsistenz | Ich finde, dass die Anforderungen widersprüchlich sind. |
| 5 | Allgemeine Einsetzbarkeit | Ich finde, dass die Anforderungen allgemein gültig formuliert und in der Automobilindustrie einsetzbar sind. |
| 6 | Einmaligkeit | Ich denke, dass die Anforderungen mehrfach aufgelistet sind. |
| 7 | Ergebnis & Verifizierbarkeit | Ich finde, dass die Anforderungen eindeutig überprüfbar sind und der Erfüllungsgrad ersichtlich ist. |
| 8 | Nachvollziehbarkeit | Ich finde, dass die Anforderungen nicht nachvollziehbar dargestellt sind. |
| 9 | Praxistauglichkeit | Ich empfinde die Anforderungen als praxisnah formuliert und interpretierbar. |
| 10 | Risikoberücksichtigung | Ich denke, dass mögliche inhaltliche Risiken und Bedrohungsszenarien nicht berücksichtigt sind. |

Abbildung 38: Für die Validierung des Prüfkatalogs adaptierte SUS-Aussagen[188]

[187] Quelle: Eigene Darstellung auf Basis von Bangor, Kortum und Miller (2009).
[188] Quelle: Eigene Darstellung.

Als Basis zur Formulierung der SUS-Aussagen können die in Kapitel 4.1 definierten charakteristischen Eigenschaften, die der Prüfkatalog erfüllen soll, herangezogen werden. Dadurch ergeben sich die in Abbildung 38 dargestellten Aussagen für den SUS-Fragebogen zur Validierung des Prüfkatalogs. Gemäß den Beschreibungen in Kapitel 5.1 sind diese von den Probanden mit einem Zustimmungswert zwischen 0 („Stimme gar nicht zu“) und 4 („Stimme voll zu“) zu bewerten.

Die Probanden zur Validierung des Prüfkatalogs sind Mitarbeiter der österreichischen Unternehmensberatung *EFS Consulting GmbH*. Dabei handelt es sich um eine Automotive-Beratung mit Sitz in Wien, die sich in den vergangenen Jahren zusehends auf eine Vielzahl an IT-Themen spezialisiert hat. Die befragten Mitarbeiter sind durchwegs Experten auf dem Gebiet der Informationssicherheit. Sie werden in der folgenden Tabelle 14 vorgestellt.

| Proband | Personenbeschreibung |
|---|---|
| Dr. Wolfgang Walter | Dr. Wolfgang Walter ist Engagement Manager bei der österreichischen Unternehmensberatung *EFS Consulting GmbH.* Im Rahmen seiner Tätigkeit hat er sich auf die Themenfelder IT Security, Informationssicherheit und Zertifizierungen sowie auf Cloud Service Management spezialisiert. |
| Michael Bereczuk | Michael Bereczuk ist Projektleiter bei der österreichischen Unternehmensberatung *EFS Consulting GmbH*. Er ist Experte in den Gebieten IT-Service Management, Change Management und Prozessoptimierung. Im Zuge seiner Tätigkeit bei *EFS* hat er bereits an SUMS und CSMS Zertifizierungen mitgewirkt. |

Tabelle 14: Probanden zur Validierung des Prüfkatalogs[189]

Zur Validierung des Prüfkatalogs erfolgt in einem ersten Schritt die Vorstellung des Katalogs im Rahmen einer Präsentation. Anschließend wird der Prüfkatalog den Probanden zum selbstständigen Ausprobieren überlassen. In einem letzten Schritt erfolgt die Bewertung der SUS-Aussagen durch die Experten von *EFS*. Die Ergebnisse dieser Bewertung sind im folgenden Kapitel 5.3 dargestellt.

## 5.3 Ergebnis der Validierung

Die Auswertung des ersten SUS-Fragebogens zur Validierung des entwickelten Prüfkatalogs zeigt einen Wert von 36 Punkten. Der sich dadurch ergebende Prozentwert von 90 Prozent attestiert dem Prüfkatalog somit bereits eine hohe Usability. Die Analyse der zweiten Auswertung offenbart einen Wert von 38 Punkten, respektive 95 Prozent. Im Durchschnitt erreicht der Prüfkatalog damit einen SUS Score von 92,5 Prozent und liegt folglich im besten Akzeptanzbereich „Akzeptabel“. Im

[189] Quelle: Eigene Darstellung.

Rahmen der Adjektiven Beurteilung liegt der Prüfkatalog mit diesem Ergebnis zwischen „Exzellent“ und „Beste vorstellbar“. Unterstrichen wird die Plausibilität des Ergebnisses der Validierung durch die wesentliche Übereinstimmung der beiden Bewertungen.

**Ergebnis der Validierung**

| *SUS AUSSAGE FRAGEBOGEN:* | 0 Stimme gar nicht zu | 1 | 2 | 3 | 4 Stimme voll zu |
|---|---|---|---|---|---|
| Ich denke, dass die Anforderungen vollständig und korrekt im Prüfkatalog berücksichtigt sind. | | | | | X X |
| Ich empfinde den Prüfkatalog als nicht hilfreich beim Überpüfen der Anforderungen an das SUMS. | X X | | | | |
| Ich finde, dass die Anforderungen logisch und strukturiert dargestellt sind. | | | | | X X |
| Ich finde, dass die Anforderungen widersprüchlich sind. | X | X | | | |
| Ich finde, dass die Anforderungen allgemein gültig formuliert und in der Automobilindustrie einsetzbar sind. | | | | X | X |
| Ich denke, dass die Anforderungen mehrfach aufgelistet sind. | X X | | | | |
| Ich finde, dass die Anforderungen eindeutig überprüfbar sind und der Erfüllungsgrad ersichtlich ist. | | | | X | X |
| Ich finde, dass die Anforderungen nicht nachvollziehbar dargestellt sind. | X X | | | | |
| Ich empfinde die Anforderungen als praxisnah formuliert und interpretierbar. | | | | | X X |
| Ich denke, dass mögliche inhaltliche Risiken und Bedrohungsszenarien nicht berücksichtigt sind. | | X | X | | |

**X – Dr. Wolfgang Walter** | **X – Michael Bereczuk**

| **Ø Punktesumme:** | **37** | **Ø Erreichter SUS-Score:** | **92,5 %** |
|---|---|---|---|

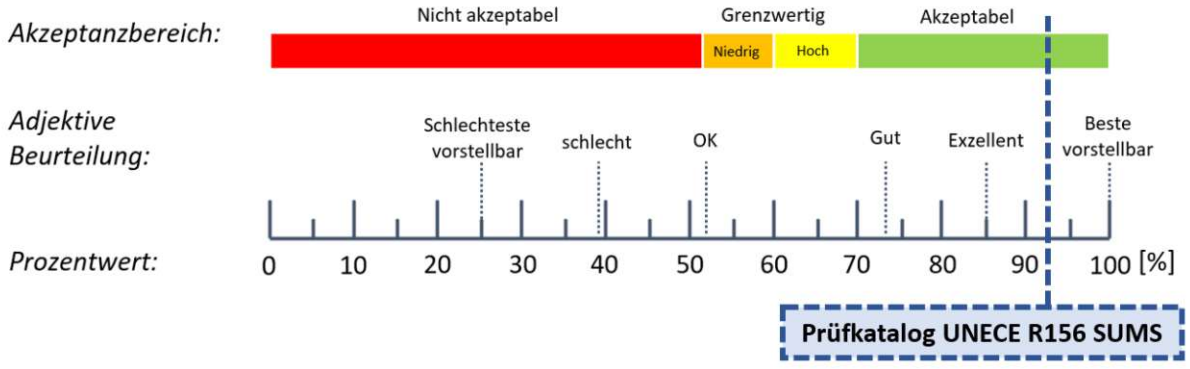



**Abbildung 39: Ergebnis der Validierung des Prüfkatalogs mittels SUS-Fragebogen**[190]

[190] Quelle: Eigene Darstellung.

Seitens der Probanden besonders positiv beurteilt wird die logische Struktur und der Aufbau der Anforderungen im Prüfkatalog. Im Unterschied zur UNECE Regelung selbst erfolgt im Prüfkatalog die Reihung der Anforderungen in chronologischer Weise. Damit lassen sich Schritt für Schritt die im Rahmen eines SUMS erforderlichen Verfahren implementieren, die Konformitätsbescheinigung beantragen und im Anschluss die fahrzeugspezifische Typgenehmigung erlangen. Darüber hinaus positiv hervorgehoben wird die praxisnahe Formulierung und nachvollziehbare Darstellung der Anforderungen im Prüfkatalog. Die Erweiterung der Anforderungen aus der Regelung um das konkrete Anforderungsziel und operativen Anforderungsnachweisen erleichtert demnach maßgeblich die Umsetzung sämtlicher Verfahren für sichere Softwareaktualisierungen.

Abstriche bei der Gebrauchstauglichkeit des Prüfkatalogs offenbaren sich bei seiner Berücksichtigung von inhaltlichen Risiken und möglichen Bedrohungsszenarien. Sie sind nur bedingt Bestandteil des Prüfkatalogs, werden allerdings in der Regelung der UNECE ebenso wenig berücksichtigt. Daneben zeigen sich nur kleine Kritikpunkte, wenn es etwa um die universelle Einsetzbarkeit in der Automobilindustrie oder die eindeutige Überprüfbarkeit der Anforderungen geht. Insgesamt attestierten beide Probanden dem Prüfkatalog eine hohe Gebrauchstauglichkeit, indem er eine wesentliche Unterstützung zur Vorbereitung auf eine Zertifizierung gemäß UNECE Regelung Nr. 156 darstellt.

# 6 SUMS und die Kunden-Lieferanten Schnittstelle

Mit der Entwicklung und Validierung des Prüfkatalogs inklusive der operationalisierten Anforderungen an ein SUMS ist der primäre identifizierte Forschungsbedarf dieser Arbeit gedeckt. Daneben wurde in Kapitel 3 eine Subforschungsfrage formuliert, dessen Beantwortung im Rahmen dieses Kapitels erfolgt. Der Ursprung dieser Subforschungsfrage liegt in der Tatsache, dass, wie in Kapitel 2.2.2 ausführlich beschrieben, ein Großteil der Softwaresysteme von unterschiedlichen Lieferanten entwickelt und zugekauft werden. Wenngleich der OEM die zu prüfende Vertragspartei im Zuge eines SUMS Zertifizierungsprozesses ist, hat die Regelung der UNECE damit auch eine unmittelbare Auswirkung auf das Verhältnis des OEMs zu seinen Lieferanten. In Kapitel 6.1 wird deshalb die allgemeine Bedeutung der Regelung für den OEM und seine Zulieferer beleuchtet. In einem zweiten Schritt wird in Kapitel 6.2 auf Ansätze zur Sicherstellung der SUMS Compliance auch bei Zulieferunternehmen eingegangen.

Basis zur Beantwortung der Subforschungsfrage stellen bereits bestehende Standards und Empfehlungen zu diesem Fachgebiet dar. Ergänzend dazu wird ein leitfadengestütztes Experteninterview durchgeführt, welches maßgeblich zur Aufklärung der Subforschungsfrage beiträgt. Bei dieser Art der Befragung handelt es sich um eine verbreitete, ausdifferenzierte und methodologisch vergleichsweise gut ausgearbeitete Methode zur Datenerzeugung. Der Leitfaden stellt dabei eine vorab vereinbarte und systematisch angewandte Vorgabe zur Gestaltung des Interviewablaufs dar. Das Experteninterview selbst definiert sich über die spezielle Auswahl und den Status der Befragten.[191] In einem ersten Schritt werden die Fragen für das leitfadengestützte Experteninterview formuliert und sortiert. Nach Auswahl des Experten erfolgt die Durchführung des Interviews, inklusive Datenerfassung. Abschließend werden die Inhalte des Interviews ausgewertet und in die Arbeit integriert.[192]

Insgesamt werden für die leitfadengestützte Durchführung des Experteninterviews sechs Fragen formuliert. Gemäß der Gliederung von Kapitel 6 unterteilen diese sich in einen allgemeinen Teil mit Fragen zur Bedeutung der Regelung für den OEM und den Lieferanten sowie in einen zweiten spezifischeren Teil, der Fragen zur Sicherstellung der SUMS Compliance beim Zulieferer umfasst.

[191] Vgl. Baur und Blasius (2019), S. 669f.
[192] Vgl. https://www.bachelorprint.at/forschung/leitfadeninterview/#1588687179476-90528804-5cd9 (Gelesen am: 11.01.2022)

*Allgemeine Fragen zur Bedeutung der Regelung für den OEM und den Zulieferer:*

- Welche Relevanz hat die Regelung für die Kunden-Lieferanten Schnittstelle und inwieweit sind auch die Lieferanten dazu verpflichtet, die Vorgaben aus der Regelung einzuhalten?
- Inwieweit bestimmt der OEM die Prozesse und das Vorgehen beim Lieferanten?
- Wie intensiv wird die Einhaltung der Vorgaben aus der Regelung bei Lieferanten im Zuge von SUMS Zertifizierungsaudits überprüft?

*Fragen zur Sicherstellung der SUMS Compliance beim Zulieferer:*

- Was sind die wichtigsten und gebräuchlichsten Ansätze zur Sicherstellung der SUMS Compliance beim Zulieferer?
- Welche Standards können als Nachweis der SUMS Compliance eines Lieferanten dienen?
- Wie erfolgt die Überprüfung der Einhaltung von vertraglichen Vereinbarungen beim Lieferanten in der Praxis (durch den OEM)?

Der im Rahmen des Interviews befragte Experte arbeitet als Projektleiter bei einer österreichischen Unternehmensberatung. Als Experte auf dem Gebiet der Informationssicherheit setzt er sich u.a. intensiv mit dem Thema Supplier Risk Management auseinander. Seine Antworten fließen in die nachfolgenden Ausführungen zur Bedeutung der Regelung für die Kunden-Lieferanten Schnittstelle sowie in die Ansätze zur Sicherstellung der SUMS Compliance ein.

## 6.1 Bedeutung der Regelung für den OEM und den Zulieferer

Abbildung 39 zeigt die typische Beziehung eines OEMs zu seinen Lieferanten im Bereich der Software-Technologien.


**Abbildung 40: Typische Lieferkette im Bereich der Softwaretechnologien[193]**

Zu erkennen ist das fertige Software-System (z.B. Steuergerät), das der OEM von seinem Tier-1 Lieferanten direkt bezieht. Dieser wiederum kauft einzelne Module und

[193] Quelle: Eigene Darstellung.

Komponenten des Software-Systems (z.B. Mikrocontroller) bei weiteren Tier-2 Lieferanten (aus Sicht des OEMs) zu. Im Zuge der SUMS Zertifizierung geprüft wird das Softwareaktualisierungsmanagementsystem des Fahrzeugherstellers sowie das fertige Fahrzeug im Rahmen der Typgenehmigung. Nichtsdestotrotz geht mit dieser Verzahnung von OEM und Lieferant auch eine Einhaltung (zumindest) gewisser Vorgaben bei den Lieferanten einher. Darauf hingewiesen wird indirekt in Kapitel 3.4 der UNECE Regelung Nr. 156 zu SUMS:

*„Falls an den Beschreibungen…Eigentumsrechte bestehen oder…Know-How des Herstellers* ***oder seiner Zulieferer*** *preisgegeben wird, übermitteln der Hersteller* ***oder sein Zulieferer*** *Informationen…“*

Das bereits im Vorfeld der Regelung Nr. 156 veröffentlichte Draft Recommendation Paper der UNECE legt in Kapitel 4.3.2 fest:

*„Der Fahrzeughersteller* ***(und gegebenenfalls seine Zulieferer)*** *müssen… nachweisen, dass sie über folgende Verfahren verfügen: …“*

Noch deutlicher wird das Thema im Rahmen der Regelung Nr. 155 der UNECE zu Cybersicherheitsmanagementsystemen aufgegriffen. Im zugehörigen ISO Standard 21434 widmet sich z.B. das gesamte Kapitel 7 dem cybersicherheitstechnischen Umgang mit Lieferanten. In der Regelung selbst wird u.a. in Absatz 7.2.2.5 festgehalten:

*„Der Fahrzeughersteller muss…darlegen, wie sein CSMS mit bestehenden… Abhängigkeiten* ***mit Zulieferern****…umgeht.“*

Wenngleich es sich dabei um eine andere Regelung der UNECE handelt, kann davon ausgegangen werden, dass solche Inhalte in ähnlichem Umfang auch für die Regelung Nr. 156 zu SUMS gelten. So erkennen etwa Herzig und Guderian (2021) erhebliche Auswirkungen auf das Management der Lieferkette durch SUMS. Die OEMs müssen sich die Frage stellen, ob der jeweilige Zulieferer überhaupt in der Lage ist, regulatorisch konform zu arbeiten. Da die Verantwortung für zugekaufte Software beim OEM liegt, muss die SUMS-Compliance der Zulieferer gründlich kontrolliert werden.[194] In ähnlicher Form sehen auch Stimm und Minzlaff (2021) eine Überprüfung der Lieferanten, in dem sie dazu verpflichtet sind, Informationen über ihre eigenen SUMS relevanten Prozesse zur Verfügung zu stellen. Sie erkennen außerdem eine generelle Delegation von Aufgaben und Verantwortlichkeiten an Lieferanten. Diese betreffen z.B. die Verfolgbarkeit und Identifikation von Änderungen der Software-Version oder das Management von fehlgeschlagenen Updates.[195]

[194] Vgl. Herzig und Guderian (2021), S. 3.
[195] Vgl. Stimm und Minzlaff (10. Juni 2021), Folie 16.

Weitestgehend bestätigt werden diese Ausführungen vom befragten Experten. Auch er sieht in der Regelung eine Auswirkung auf die Schnittstelle zwischen dem OEM und seinen Lieferanten. Ihm zufolge ist es allerdings schwierig, diese Auswirkungen pauschal zu beurteilen. Viel mehr hängen sie davon ab, um welche Art von Lieferanten es sich handelt. Er unterscheidet dabei in erster Linie zwischen Teilelieferanten und Lieferanten im IT-Bereich:

**Teilelieferanten:**

Teilelieferanten versorgen die Fahrzeughersteller mit Bauteilen, die für die Fertigstellung des Fahrzeugs notwendig sind. In der einfachsten Form beliefern sie den OEM mit „Rohteilen“ ohne Software (z.B. Steuergerät ohne Software). Diese wird erst anschließend vom OEM selbst aufgespielt, womit lediglich die internen Regelungen zu SUMS eingehalten werden müssen. Einen Schritt weiter gehen jene Lieferanten, die Bauteile mit bereits aufgespielter Software an den OEM liefern (z.B. fertig bestückte Steuergeräte). In diesem Fall ist die Tauglichkeit des Lieferanten in Hinblick auf seine SUMS Prozesse sehr wohl zu berücksichtigen. In der letzten Stufe kommen insbesondere im Nutzfahrzeugbereich sogenannten Aufbauhersteller als Lieferanten ganzer Nutzfahrzeugaufbauten ins Geschehen. Im Falle von Einrechnungsgeschäften wird dem Kunden nur eine einzelne Rechnung seitens des OEMs gestellt. Folglich ist der OEM dafür verantwortlich, dass die Anforderungen an ein SUMS beim Aufbaulieferanten eingehalten werden. Handelt es sich hingegen um ein Zweirechnungsgeschäft gibt der Kunde sowohl beim OEM als auch beim Aufbauhersteller eine Leistung in Auftrag. In diesem Fall ist jede Partei selbständig für die Einhaltung sämtlicher informationssicherheitstechnischer Anforderungen verantwortlich.

**Lieferanten im IT-Bereich:**

Bei Lieferanten, die für den OEM z.B. als Entwicklungs- oder Support-Dienstleister im IT-Umfeld agieren, gestaltet sich die Situation abermals anders. Handelt es sich um Anbieter von Software, die frei am Markt verfügbar ist, sind die Möglichkeiten für den OEM auf die Prozesse des Lieferanten Einfluss zu nehmen oder sie einzusehen stark begrenzt. Infolgedessen sollten sie nur für den Bezug von nicht sicherheitsrelevanter Fahrzeugsoftware in Frage kommen. Die zweite Variante bilden jene Software-Anbieter, die vom OEM explizit für die Erstellung einer konkreten Leistung beauftragt werden. In diesem Fall können die Vorgaben, die hinsichtlich sicherer Softwareaktualisierungen an den Lieferanten bestehen, im Rahmen der vertraglichen Leistungsvereinbarung festgehalten werden. Die letzte Variante stellen jene Software-Dienstleister dar, die mangels eigener Kapazitäten beim OEM zur Unterstützung direkt ins Unternehmen dazu geholt werden. An dieser Stelle müssen die Dienstleister dazu

verpflichtet werden, die internen Vorgaben des OEMs zu übernehmen. Vonseiten des OEMs ist ihre Einhaltung zu überprüfen.

Wesentlich im Rahmen der SUMS Zertifizierung ist grundsätzlich die genaue Dokumentation der vom OEM angewandten Prozesse, wenn es um die Überprüfung von SUMS Standards bei Lieferanten geht. Dass ein Lieferant bei einer SUMS Zertifizierung vorstellig wird, ist gemäß dem befragten Experten in der Praxis nicht üblich. Umso wichtiger ist es daher, dass der OEM dem Auditor darlegen kann, wie er die Einhaltung der SUMS Anforderungen bei den jeweiligen Lieferanten überprüft. Eine Möglichkeit stellt in dieser Hinsicht z.B. die Vorlage von Prozessdokumentationen und Arbeitsanweisungen dar.

## 6.2 Ansätze zur Sicherstellung der SUMS Compliance beim Zulieferer

Infolge der in Kapitel 6.1 identifizierten Bedeutung der UNECE Regelung für die Kunden-Lieferanten Schnittstelle müssen sich die OEMs in jedem Fall Gedanken darüber machen, wie sie die SUMS Compliance bei ihren Zulieferern sicherstellen können. Seitens des befragten Experten wird dabei zuallererst auf die Überprüfung von bereits bestehenden Informationssicherheitszertifizierungen verwiesen. Sofern relevante Nachweise vorhanden sind, stellen sie die leichteste Form der Sicherstellung der SUMS Compliance bei Lieferanten dar. In erster Linie von Bedeutung sind die beiden allgemeinen Standards zur Informationssicherheit ISO 27001 und TISAX. Sie bilden, wie bereits erwähnt, häufig die Grundlage für die Zusammenarbeit mit den meisten OEMs.

Daneben kann eine beim Lieferanten vorhandene ISO 21434 Zertifizierung einen guten Nachweis für die Einhaltung der SUMS Anforderungen darstellen. Im Rahmen von Kapitel 7 des Standards wird z.B. auf die Wichtigkeit der Fähigkeitsüberprüfung eines Lieferanten und seiner cybersicherheitstechnischen Prozesse bereits in der Auswahlphase hingewiesen. Demnach soll ein Lieferant schon im Vorfeld einer Auftragsvergabe Dokumente zur Verfügung stellen, die seine Fähigkeiten im Bereich der Cybersicherheit nachweisen. Außerdem sieht der Standard eine klare Aufgabenverteilung zwischen OEM und Lieferant vor. In einer Vereinbarung ist dahingehend z.B. festzuhalten, welche der beiden Vertragsparteien für die Durchführung von cybersicherheitstechnischen Validierungstests zuständig ist.[196] Diese und weitere im Rahmen des Standards vorgegebene Vorgehensweisen können in entsprechend angepasster Form ebenso für die UNECE Regelung Nr. 156 zu SUMS übernommen werden.

[196] Vgl. ISO/SAE 21434:2021-08, Kap. 7.

Als Teil der ISO 27000 Reihe enthält zudem die ISO 27002 in Kapitel 15 sämtliche Vorschläge zum sicheren Umgang mit Lieferanten im Kontext der Informationssicherheit. Im Wesentlichen betreffen diese die Anforderungen an die Informationssicherheit, die mit dem Zugriff des Lieferanten auf jegliche Assets des OEMs verbunden sind.[197] Des Weiteren enthalten ISO 27036-1 bis 4 im Speziellen detaillierte Anleitungen zur Durchführung von Überprüfungen in Zusammenhang mit Lieferantenbeziehungen.[198]

Gehen die Anforderungen an die Lieferanten über ein gewisses Maß hinaus, reicht der alleinige Nachweis von Standards und Normen mit Bezug zur Informationssicherheit allerdings nicht mehr aus. In diesen Fällen müssen gemäß dem befragten Experten weitere individuelle Richtlinien mit dem Lieferanten vertraglich vereinbart werden. Dieses Vorgehen ist dann relevant, wenn es sich z.B. um Bauteile mit sicherheitsrelevantem Einfluss auf das Fahrzeugverhalten handelt.

Während eine ISO 27001 oder TISAX Zertifizierung eines Lieferanten durch einen externen Auditor durchgeführt wird, muss die Einhaltung von solchen individuellen vertraglichen Vereinbarungen durch den OEM selbst kontrolliert werden. Ein solches Recht zur eigenständigen Durchführung von stichprobenartigen Kontrollen ist in der Regel in den allgemeinen Einkaufsbestimmungen eines Fahrzeugherstellers festgehalten. Demnach kann der OEM zu jeder Zeit unangekündigt Einsichtnahme in die Prozesse beim Lieferanten nehmen, um sich von der Einhaltung der vereinbarten Richtlinien bezgl. SUMS zu überzeugen.

Zusammenfassend lässt sich festhalten, dass:

- für jeden Lieferanten beurteilt werden muss, bis zu welchem Grad die Einhaltung von Anforderungen der UNECE Regelung zu SUMS relevant ist,
- nach Möglichkeit die Einhaltung der SUMS Anforderungen über den Nachweis von bestehenden Informationssicherheitszertifikaten erfolgen soll,
- bei sicherheitskritischen Bauteilen darüberhinausgehenden individuelle Richtlinien mit dem Lieferanten vertraglich zu vereinbaren sind,
- der OEM die im Rahmen einer SUMS Zertifizierung zu prüfende Partei ist. Demzufolge muss er dem Auditor darlegen, wie die Einhaltung der SUMS Compliance bei Lieferanten sichergestellt wird.

[197] Vgl. ISO/IEC 27002:2017-02, Kap. 15.
[198] Vgl. ISO/IEC 27036-1:2021.

# 7 Resümee

Dieses Kapitel bildet das Resümee der vorliegenden Diplomarbeit. Dazu werden in Kapitel 7.1 die Inhalte der Arbeit zusammengefasst. Es erfolgt außerdem eine Diskussion der Ergebnisse, dessen Kernelement der entwickelte Prüfkatalog darstellt. In Kapitel 7.2 wird ein Ausblick auf mögliche zukünftige Entwicklungen mit Bezug zu SUMS und Informationssicherheit gegeben. Dabei wird auch auf künftige noch offene Forschungsfelder eingegangen.

## 7.1 Zusammenfassung und Ergebnisse

Weitestgehend bekannt ist, dass die Digitalisierung in den vergangenen Jahren zu einem Schlüsselthema in sämtlichen Unternehmen der Automobilbranche avanciert ist. Infolgedessen steigt auch der Bedarf nach Softwaretechnologien und damit einhergehende die Notwendigkeit nach der Pflege dieser Software durch Updates. Während bei traditionellen Softwareaktualisierungen das Update im Rahmen von Werkstattaufenthalten aufgespielt wird, ermöglichen drahtlose Over-The-Air-Updates die Anpassung der Softwarefunktionalität eines Fahrzeugs aus der Ferne. Dadurch lassen sich einerseits Kosten sparen und andererseits die Kundenzufriedenheit erhöhen. Gleichzeitig erhöhen OTA-Updates die Angriffsfläche für sicherheitsrelevante Cyber-Attacken zusätzlich. Um die Risiken, die sich aus Lücken in der Informationssicherheit ergeben, gering zu halten, fordern die Gesetzesgeber die Umsetzung adäquater Sicherheitskontrollen. International bereits weit verbreitet sind ISO 27001 und TISAX. Daneben bildet die Anfang 2021 von der UNECE verabschiedete Regelung Nr. 156 zu Software-Update Managementsystemen erstmals eine gesetzlich verpflichtende Grundlage zur Implementierung einer zentralen Kontrolleinheit für Software-Updates.

Die alleinige Betrachtung der neuen UNECE Regelung zu SUMS stellt die Automobilhersteller jedoch vor Schwierigkeiten bei der Umsetzung der Anforderungen auf operativer Ebene. Es besteht der Wunsch nach einem Prüfkatalog, mit dem die Vollständigkeit, Angemessenheit und Wirksamkeit der angestrebten Lösung überprüft werden kann. Ein solcher existierte bis dato noch nicht und wurde deshalb im Rahmen dieser Diplomarbeit entwickelt.

Basis zur Entwicklung des Prüfkatalogs sind einerseits bereits bestehende Normen, Standards und Empfehlungen mit Bezug zu Software-Updates und Informationssicherheit. Im Mittelpunkt steht dabei die Regelung selbst sowie ein Proposal Document der UNECE, welches Ansätze zur Erfüllung der Regelung enthält. Daneben bilden andere bereits bestehende Leitfäden und Prüfkataloge die Basis zur Erstellung der grundlegenden Struktur des SUMS Prüfkatalogs. In dieser Hinsicht orientiert sich der zu entwickelnde Prüfkatalog insbesondere am Aufbau und der

Struktur des Information Security Assessment (ISA) Katalogs vom VDA. Dieser hat sich bereits als Branchenstandard innerhalb der Automobilindustrie für Informationssicherheits-Assessments etabliert und weist daher ein dementsprechend bekanntes Format auf.

**Ergebnisse:**

Am Ende der Entwicklung steht ein Prüfkatalog, der Unternehmen der Automobilindustrie bei der Konzeption, Implementierung und Aufrechterhaltung eines Software-Update Management Systems unterstützt. Im Rahmen von drei einleitenden Tabellenblätter wird der Anwender des Prüfkatalogs zu den wesentlichen Inhalten hingeführt. Dazu zählt u.a. die Erklärung sämtlicher im Prüfkatalog enthaltener Abkürzungen und Begriffe sowie eine Beschreibung der zur Anwendung gelangenden Erfüllungsgradmessung. Es folgt eine Auflistung der einzelnen Kapitel der UNECE Regelung Nr. 156 zu SUMS in ihrer ursprünglichen Form, inklusive Verweis auf die jeweilige Kontrollfrage im Prüfkatalog. Mithilfe der integrierten Filter-Funktion lässt sich dadurch auf die Schnelle für jede Anforderung der UNECE Regelung das Kapitel der Kontrollfrage mit den jeweiligen Erläuterungen und Darstellungen herausfinden.

Die daran anschließenden operationalisierten Anforderungen der UNECE Regelung bilden den Kern des entwickelten Prüfkatalogs. Die zweckmäßige Gruppierung und Integration aller Informationen ermöglicht einen intuitiven Umgang mit dem Prüfkatalog. Wesentlich ist zudem die Erweiterung der Anforderungen aus der Regelung um das konkrete Anforderungsziel und operativen Anforderungsnachweisen. Sie bieten dem Anwender eine Hilfestellung bei der Umsetzung seiner Verfahren für Softwareaktualisierungen und damit eine Grundlage zur kosteneffizienten Vorbereitung auf ein Zertifizierungsaudit nach SUMS. Am Ende jeder Anforderung ist vom Anwender ein entsprechender Erfüllungsgradwert einzutragen. Er muss zwischen 0 (Unvollständiger Prozess) und 5 (Optimierender Prozess) liegen und bildet die Basis zur anschließenden Ergebnisauswertung.

Eben jene Ergebnisauswertung ermöglicht nach Durchgang durch die Anforderungen im Prüfkatalog die Feststellung des derzeitigen Ist-Zustandes im Unternehmen. Mithilfe einer grafischen Auswertung lässt sich erkennen, in welchen Unternehmensbereichen derzeit noch Aufholungsbedarf besteht und wo die Anforderungen bereits erfüllt werden. Auf Basis dessen können im Anschluss gezielt Maßnahmen umgesetzt und die notwendigen Prozesse implementiert werden. Neben der Erfüllungsgradmessung für die Aufbauphase dienen Beispiel-KPIs der Überwachung der SUMS-Anforderungen in der Betriebsphase. An dieser Stelle gilt es allerdings zu erwähnen, dass die Beispiel-KPIs lediglich als Hilfestellung für die Unternehmen dienen, eigene passende KPIs zu definieren.

Die im Anschluss durchgeführte Validierung bestätigt die Effektivität des Prüfkatalogs, wenn es um die Konzeption, Implementierung und Aufrechterhaltung eines Software-Update Managementsystems geht. Sie erfolgte auf Basis der sogenannten SUS-Methode und ergab einen SUS-Score von 92,5 Prozent. Gemäß der angewendeten Interpretation für den Prozentwert liegt der entwickelte Prüfkatalog damit im besten Akzeptanzbereich „Akzeptabel“ und erreicht eine adjektive Beurteilung, die zwischen „Exzellent“ und „Beste vorstellbar“ liegt.

Als identifizierter Subforschungsbedarf wurde im Rahmen der Arbeit zudem die Bedeutung der UNECE Regelung Nr. 156 für die Kunden-Lieferanten Schnittstelle analysiert. Mithilfe eines Experteninterviews ergab diese Analyse eine hohe Auswirkung der Regelung auf die (vertragliche) Beziehung zwischen dem OEM und seinen Lieferanten. Je nach Art der Lieferantenbeziehung muss bereits zu Beginn des Fahrzeuglebenszyklus darauf geachtet werden, dass die Fähigkeit des Lieferanten zur Einhaltung der SUMS Anforderungen gegeben ist. Im Optimalfall verfügt der Lieferant über anerkannte Standards, die seine Fähigkeit zum sicheren Umgang mit Software-Updates sowie generell seine Informationssicherheit nachweisen. Im Rahmen von vertraglichen Vereinbarungen sind zudem ggf. zusätzliche Anforderungen an den Lieferanten seitens des OEMs festzuhalten.

## 7.2 Ausblick

Die Verabschiedung der Regelung Nr. 156 der UNECE stellt einen weiteren wichtigen Schritt in Richtung der Absicherung von Softwareaktualisierungen gegen Cyberangriffe dar. Durch ihre verpflichtende Umsetzung für alle neu produzierten Fahrzeuge spätestens Mitte des Jahres 2024 ist es für die Automobilhersteller höchste Zeit, mit der Implementierung eines Software-Update Managementsystems zu beginnen. Der im Zuge dieser Arbeit entwickelte Prüfkatalog unterstützt die Unternehmen sowohl bei der Konzeption als auch bei der Aufrechterhaltung eines SUMS.

Als nächster wesentlicher Meilenstein gilt die Veröffentlichung des noch ausstehenden ISO Standards 24089. Eine Nachfrage bei der entsprechende ISO Organisation hat ergeben, dass eine Publikation des SUMS Standards Ende des Jahres 2022 anvisiert wird. Die Veröffentlichung einer ersten sogenannten Draft Version soll bereits etwas früher erfolgen. Die Erweiterung des entwickelten Prüfkatalogs um den entsprechenden Standard stellt jedenfalls eine Forschungslücke in Zusammenhang mit SUMS dar und bietet sich für zukünftigen Forschungsarbeiten an. Ein weiterer Forschungsbedarf kann zudem in einer vertieften Abstimmung mit offiziellen Genehmigungsbehörden gefunden werden. Die Einbringung ihrer Meinungen könnte die Qualität des Prüfkatalogs weiter erhöhen.

# 8 Literaturverzeichnis

Arbeitskreis Informationssicherheit (2020): Information Security Assessment; Prüfkatalog; Berlin: Verband der Automobilindustrie.

Bangor, Aaron; Kortum, Phil; Miller, James (2009): Determining What Individual SUS Scores Mean: Adding an Adjective Rating Scale; in: J. Usability Stud.; 4 (2009); S. 114–123.

Bartsch, Michael; Frey, Stefanie (2018): Cybersecurity Best Practices; Wiesbaden: Springer Fachmedien Wiesbaden.

Baur, Nina; Blasius, Jörg (2019): Handbuch Methoden der empirischen Sozialforschung; Wiesbaden: Springer Fachmedien Wiesbaden.

Becker, Wolfgang; Ulrich, Patrick; Stradtmann, Meike (2018): Geschäftsmodellinnovationen als Wettbewerbsvorteil mittelständischer Unternehmen; Wiesbaden: Springer Fachmedien Wiesbaden.

Biegaj, Adam (2018): IATF 16949 – Qualitätsmanagement in der Automobilindustrie; München: TÜV Süd.

Brenner-Wickner, Marian; Kneuper, Ralf; Schlömer, Inga (2020): Leitfaden für die Nutzung von Design Science Research in Abschlussarbeiten; Erfurt: IUBH Internationale Hochschule.

Brooke, John (1996): SUS: A 'Quick and Dirty' Usability Scale; in: Usability Evaluation In Industry: CRC Press; S. 189–194.

Brose Fahrzeugteile SE & Co. KG (2017): Qualitätssicherungsbestimmungen Kaufteile; Coburg.

Bundesamt für Sicherheit in der Informationstechnik – BSI (2017): Leitfaden zur Basis-Absicherung nach IT-Grundschutz – In drei Schritten zur Informationssicherheit; Bonn: Bundesamt für Sicherheit in der Informationstechnik – BSI.

Burgartz, Dieter (2020): Prüfkatalog nach ISO/IEC 27001; 1. Aufl.; Köln: TÜV Media GmbH, TÜV Rheinland Group.

Burkacky, Ondrej et al. (2020): Cybersecurity in automotive – Mastering the challenge; München: McKinsey & Company.

Burkacky, Ondrej; Deichmann, Johannes; Stein, Jan Paul (2019): Automotive software and electronics 2030 – Mapping the sector's future landscape; München: McKinsey & Company.

Dassow, Ingo; Herzig, Andreas; Guderian, Anke (2021): Cyber Security Management – Neue Dimensionen automobiler Sicherheit; München: Deloitte.

Dax, Julian et al. (2016): Sichere Informationsinfrastrukturen für kleine und mittlere Energieversorger; in: Teilkonferenz IT-Sicherheit für Kritische Infrastrukturen.

Diesch, Rainer; Pfaff, Matthias; Krcmar, Helmut (2020): A comprehensive model of information security factors for decision-makers; in: Computers & Security.

Endres, Cornelia: Leitfadeninterview für die Bachelorarbeit – Beispiele & Ablauf; URL: https://www.bachelorprint.at/forschung/leitfadeninterview/#1588687179476-90528804-5cd9 (abgerufen am: 11.01.2022).

ENX Association (2021): TISAX Teilnehmerhandbuch; Frankfurt am Main.

Fink, Arlene (2014): Conducting research literature reviews – From the internet to paper; Fourth edition; Thousand Oaks California: SAGE.

Gehr, Frank (1984): Logistik in der Automobilindustrie; Dordrecht: Springer.

Guissouma, Houssem et al. (2018): An Empirical Study on the Current and Future Challenges of Automotive Software Release and Configuration Management; in: 44th Euromicro Conference on Software Engineering and Advanced Applications (SEAA): IEEE; S. 298–305.

Halder, Subir; Ghosal, Amrita; Conti, Mauro (2020): Secure over-the-air software updates in connected vehicles: A survey; in: Computer Networks (2020).

Harde, Gunnar; Großmann, Jürgen (2018): Automotive Cybersecurity Incident Response – Pocket Guide; Berlin: AQI Automotive Quality Institute GmbH.

Herzig, Andreas; Guderian, Anke (2021): Das Fahrzeug als mobiles Endgerät: Herausforderung „Software Update Management“; Stuttgart: Deloitte.

Informal document GRVA-01-18: Draft Recommendation on Software Updates of the Task Force on Cyber Security and Over-the-air issues; Genf: UNECE.

ISO/IEC 15504-2:2003: Informationstechnik — Prozessbewertung – Teil 2: Durchführung eines Assessments.

ISO/IEC 27001:2017-02: Informationstechnik-Sicherheitsverfahren-Informationssicherheitsmanagementsysteme-Anforderungen.

ISO/IEC 27002:2017-02: Informationstechnik — Sicherheitsverfahren — Leitfaden für Informationssicherheitsmaßnahmen.

ISO/IEC 27036-1:2021: Cybersecurity - Supplier relationships – Overview and concepts.

ISO/SAE 21434:2021-08: Road vehicles — Cybersecurity engineering.

Kersten, Heinrich et al. (2020): IT-Sicherheitsmanagement nach der neuen ISO 27001; Wiesbaden: Springer Fachmedien Wiesbaden.

Knorr-Bremse System für Nutzfahrzeuge GmbH (2018): Quality Management Program for Procurement; München.

Köhler, Peter Thomas (2007): ITIL – Das IT-Servicemanagement Framework; 2., überarb. Aufl.; Berlin, Heidelberg: Springer.

Królikowski, Tomasz; Ubowska, Agnieszka (2021): TISAX - optimization of IT risk management in the automotive industry; in: Procedia Computer Science; 192 (2021); S. 4259–4268.

Kutritz, Thomas (2004): Umfassendes Qualitätsmanagement für den Bereich Elektronik im Versuchsbau der Automobilindustrie; Dissertation; Berlin: Technische Universität.

Liedtke, Thomas (2020): So erfüllen Sie die UNECE-Regulierungen zu Automotive Cybersecurity; Kornwestheim: Kuugler Maag CIE GmbH.

Liu, Lei (2019): Automobilhersteller im Wandel zu datengetriebenen Unternehmen; in: ATZextra; 24 (2019); S. 38–41.

MSG Applied Technology Research (2019): User-Experience-Methoden-Katalog, Konzeption; URL: https://www.user-experience-methods.com/conception/ (abgerufen am: 16.12.2021).

Naybzadeh, Milan (2021): Standards und Zertifizierungen für Cloud-Services; 13-21-039; Stralsund: Stralsund Information Management Team (SIMAT).

Österle, Hubert; Otto, Boris (2010): Consortium Research – A Method for Researcher-Practitioner Collaboration in Design-Oriented IS Research; in: Business & Information Systems Engineering; 2 (2010); 5; S. 283–293.

Pilz, Tobias (5.10.2021): UN Regulation No. 156 & SUMS; Webinar; Cyres Consulting.

Placho, Teresa et al. (2020): Management of automotive software updates; in: Microprocessors and Microsystems; 78 (2020).

Proff, Heike (2019): Mobilität in Zeiten der Veränderung; Wiesbaden: Springer Fachmedien Wiesbaden.

Raumer, Matthias (2011): Quantitative Usablility-Analysen mit der System Usability Scale (SUS); URL: https://blog.seibert-media.net/blog/2011/04/11/usablility-analysen-system-usability-scale-sus/ (abgerufen am: 07.01.2022).

Römer, Jonas; Kreyenberg, Danny; Großmann, Jürgen (2018): Over-The-Air Updates – Eine Prozess- und Risikoanalyse mittels Simulation; Berlin: AQI Automotive Quality Institute GmbH.

Sauro, Jeff; Lewis, James R. (2016): Standardized usability questionnaires; in: Quantifying the User Experience: Elsevier; S. 185–248.

Sowa, Aleksandra (2017): Management der Informationssicherheit; Wiesbaden: Springer Fachmedien Wiesbaden.

Steger, Marco et al. (2018): Secure Wireless Automotive Software Updates Using Blockchains: A Proof of Concept; in: Advanced Microsystems for Automotive Applications; Cham: Springer International Publishing; (Lecture Notes in Mobility); S. 137–149.

Steurich, Bjoern; Klimke, Martin; Pedersen, Indes (2017): Automotive ECUs: Architecture considerations to implement secure software updates over the air; URL: https://www.embeddedcomputing.com/application/automotive/automotive-ecus-architecture-considerations-to-implement-secure-software-updates-over-the-air (abgerufen am: 01.10.2021).

Stimm, Thomas; Minzlaff, Moritz (10. Juni 2021): Die Auswirkungen von SUMS auf OEMs und Zulieferer; Webinar; Escrypt.

Strutzenberger, Johanna (2017): Usability Evaluierung von komplexen Systemen zur Informationsanalyse im Bereich der Applikationsüberwachung; Masterarbeit; Wien: FH Technikum.

TÜV Rheinland Cert GmbH (2021): Fragen und Antworten zum Lieferantenaudit; Köln.

UNECE Document No. TFCS-ahSWTAN-04: Integration of Regulation X Software Identification Number (RXSWIN) in existing and new UN Regulations (02.08.2017).

UNECE R155:2021-03: Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system; Genf.

UNECE R156:2021-03: Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system; Genf.

UNECE/TRANS/505/Rev.3: Agreement Concerning the Adoption of Harmonized Technical United Nations Regulations for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for

Reciprocal Recognition of Approvals Granted on the Basis of these United Nations Regulations; Genf.

UNECE/TRANS/WP.29/2021/60: Proposals for Interpretation Documents for UN Regulation No. 156 on software update and software update management system; Genf.

UNECE: WP.29 – Introduction; URL: https://unece.org/wp29-introduction (abgerufen am: 21.10.2021).

Wang, Yunpeng et al. (2021): A Systematic Risk Assessment Framework of Automotive Cybersecurity; in: Automotive Innovation; 4 (2021); 3; S. 253–261.

Weber, Julian (2020): Bewegende Zeiten; Wiesbaden: Springer Fachmedien Wiesbaden.

Wikiwand: Zulieferpyramide; URL: https://www.wikiwand.com/de/Zulieferpyramide (Gelesen am: 19.11.2021).

Wind River Systems, Inc. (2017): Implementing Over-the-Air Software Updates for Automotive Applications – A Look at the Opportunities and Challenges; Alameda.

Winkelhake, Uwe (2019): Herausforderungen bei der digitalen Transformation der Automobilindustrie; in: ATZ - Automobiltechnische Zeitschrift; 121 (2019); 7-8; S. 36–43.

Winkelhake, Uwe (2021): Die digitale Transformation der Automobilindustrie; Berlin, Heidelberg: Springer Berlin Heidelberg.

Wolf, Fabian (2018): Fahrzeuginformatik; Wiesbaden: Springer Fachmedien Wiesbaden.

# 9 Abbildungsverzeichnis

# 10 Tabellenverzeichnis

# 11 Abkürzungsverzeichnis

| | |
|---|---|
| € | Euro |
| BSI | Bundesamt für Sicherheit in der Informationstechnik |
| bzw. | beziehungsweise |
| ca. | circa |
| CoP | Conformity of Production |
| CSMS | Cybersecurity Management System |
| d.h. | das heißt |
| DCU | Digital Control Unit |
| ECU | Electronic Control Unit |
| etc. | et cetera |
| f. | folgend |
| ff. | folgende |
| ggf. | gegebenenfalls |
| IATF | International Automotive Task Force |
| IEC | International Electrotechnical Commission |
| ISA | Information Security Assessment |
| ISACA | Information Systems Audit and Control Association |
| ISMS | Information Security Management System |
| ISO | International Organization for Standardization |
| IT | Informationstechnik |
| ITC | Inland Transport Committee |
| ITU | Internation Telecommunication Union |
| KBA | Kraftfahrtbundesamt |
| Kfz. | Kraftfahrzeug |
| KPI | Key Performance Indicator |
| max. | maximal |
| min. | minimal |
| Mrd. | Milliarde |
| Nr. | Nummer |
| OBD | On-Board-Diagnose |
| OEM | Original Equipment Manufacturer |
| OTA | Over-The-Air |
| PA | Prozessattribut |
| QMS | Qualitätsmanagementsystem |
| RXSWIN | Regelung [Nr] Software-Identifikationsnummer |
| S. | Seite |

| | |
|---|---|
| SAE | Society of Automotive Engineers |
| SoP | Start of Production |
| SUMS | Software-Update Management System |
| SUS | System Usability Scale |
| TISAX | Trusted Information Security Assessment Exchange |
| u.a | Unter anderem |
| UNECE | United Nations Economic Commission for Europe |
| USB | Universal Serial Bus |
| VDA | Verband der deutschen Automobilindustrie |
| z.B. | zum Beispiel |

# Anhang

## UNECE R156 SUMS Prüfkatalog – Tabellenblatt 0:

### PRÜFKATALOG UNECE R156 SUMS

Willkommen

Mit R156 SUMS wurde von der UNECE eine neue Regelung verabschiedet, die ein Software Update Management System für alle Fahrzeuge vorschreibt. Sie gilt verpflichtend für alle neu entwickelten Fahrzeuge ab Juni 2022 und für alle neuen Fahrzeuge ab Juni 2024. Zusammen mit Regelung Nr. 155 CSMS soll sie das Risiko cybersicherheitskritischer Bedrohungen auf ein akzeptables Niveau senken.

Der vorliegende Prüfkatalog dient als Unterstützung für Unternehmen bei der Konzeption, Implementierung und Aufrechterhaltung eines Software-Update Management System. Er stellt zudem eine Grundlage zur Vorbereitung auf ein Zertifizierungsaudit nach SUMS dar.

Insgesamt setzt sich der Prüfkatalog aus 8 Tabellenblättern zusammen. Sie sind im folgenden Absatz beschrieben:

| **Tabellenblatt 1: Begriffe** |
|---|
| Die Regelung Nr. 156 der UNECE zu SUMS und damit auch der vorliegende Prüfkatalog enthalten eine Vielzahl unterschiedlicher Abkürzungen. Ihre Bedeutung inkl. einer kurzen Beschreibung sind in Tabellenblatt 1 dargestellt. Darüberhinaus werden verschiedene spezfische Begriffe beschrieben, deren Verständnis wesentlich ist für die Anwendung des Prüfkatalogs. |

| **Tabellenblatt 2: Erfüllungsgrad** |
|---|
| Zur Messung des Erfüllungsgrades der einzelnen UNECE Anforderungen in der Aufbauphase bedient sich der vorliegende Prüfkatalog dem Rahmenwerk für die Prozessfähigkeitsmessung gemäß ISO/IEC 15504-2. Dabei handelt es sich um eine 6-stufige Skala, die die Bewertung der Prozessfähigkeit im Rahmen der jeweiligen Anforderung ermöglicht. Sie reicht von Unvollständig am unteren Ende der Skala bis hin zur Optimierend am oberen Ende der Skala. Innerhalb dieses Rahmenwerks basiert das Maß der Fähigkeiten auf einer Reihe von Prozessattributen (PA). Jedes Prozessattribut legt einen bestimmten Aspekt der Prozessfähigkeit fest. Der Grad, bis zu dem ein bestimmtes Prozessattribut erreicht wurde, wird anhand einer festgelegten Bewertungsskala beschrieben. In Verbindung mit den vorstehend festgelegten Attributen weisen die Prozessattribute das Erreichen der jeweiligen Stufe nach. |

| **Tabellenblatt 3: UNECE R156 SUMS** |
|---|
| In diesem Tabellenblatt sind die einzelnen Anforderungen aus der UNECE Regelung in ihrer ursprünglichen Reihung aufgelistet. Abgesehen von Kapitel 1,2 und 5 der Regelung ist für jede Anforderung der Verweis auf die Kontrollfrage des vorliegenden Prüfkatalogs angegeben. Damit lässt sich auf die Schnelle feststellen, welche Kontrollfrage des Prüfkatalogs zu welcher Anforderung der UNECE Regelung gehört. Bei Kapiteln 1, 2, und 5 der Regelung handelt es sich um Beschreibungen, bzw. Anforderungen an die jeweilige Genehmigungsbehörde, die folglich nicht im Prüfkatalog mit Anforderungen an die Automobilhersteller angeführt werden. |

| **Tabellenblatt 4: Anforderungen - SUMS** |
|---|
| Hier sind die wesentlichen Anforderungen an ein Software-Update Managementsystem sowohl beim Fahrzeughersteller als auch am Fahrzeug selbst abgebildet. Sie entstammen Kapitel 7 der UNECE Regelung und ihre erfolgreiche Implementierung bildet die Grundvoraussetzung für die Ausstellung einer SUMS Konformitätsbescheinigung. Das Tabellenblatt ist folgendermaßen aufgebaut:<br><br>*Kapitel und Kontrollfrage:*<br>Der vorliegende Prüfkatalog weist eine zur UNECE Regelung abweichende Gliederung und Reihung der Anforderungen auf. Zum Teil sind die Anforderungen aus der Regelung außerdem aufgespaltet oder zusammengefasst. Zu jeder Anforderung ist eine Kontrollfrage formuliert. |

*Anforderungsziel:*
In dieser Spalte ist das Ziel der jeweiligen Anforderung in Fließtextform beschrieben. Die Erklärung enthält zudem Hintergrundinformationen, um die Relevanz der Anforderung hervorzuheben.

*Anforderung:*
Auf Basis verschiedener Standards, Regelungen und Empfehlungen in Zusammenhang mit SUMS sind in dieser Spalte die konkreten Anforderungen aus der Regelung auf operative Ebene abgeleitet.

*Anforderungsnachweis:*
Auf Basis derselben Standards, Regelungen und Empfehlungen sind an dieser Stelle Nachweise angeführt, die zur Erfüllung der jeweiligen Anforderung dienen können. Die drei Spalten Anforderungsziel, Anforderung und Anforderungsnachweis stellen den wesentlichsten Teil des Prüfkatalogs dar.

*Management Prozess, Referenz UNECE R156 und KPI:*
Die meisten Anforderung sind einer meist schon bestehenden Management Funktion zuzuordnen. Da die Reihung und Gliederung der Anforderungen im Prüfkatalog von jener in der UNECE Regelung abweicht, ist an dieser Stelle der Verweis zur jeweiligen UNECE Anforderung dargestellt. Für viele Anforderungen sind in Tabellenblatt 8 zudem Beispiel KPIs angeführt, auf die in der nachstehenden Spalte verwiesen wird.

*Weitere Spalten:*
Die nachfolgende Spalten sind im Zuge der Audit Vorbereitung vom Fahrzeughersteller zu befüllen. Während einige Spalten nicht zwingend zu befüllen sind, ist es wesentlich, dass der Erfüllungsgrad für die jeweilige Anforderung eingetragen wird. Andernfalls ist eine Ergebnisdarstellung in Tabellenblatt 7 nicht möglich. Gemäß der Prozessfähigkeitsmessung aus Tabellenblatt 2 ist dazu ein Wert zwischen 0 (Unvollständiger Prozess) und 5 (Optimierender Prozess) einzutragen.

**Tabellenblatt 5: Anforderungen - Produktion**

Die Anforderungen an die Übereinstimmung der Produktion sind in Tabellenblatt 5 abgebildet. Basis dieser Anforderungen sind einerseits Kapitel 9 und 11 der UNECE Regelung zu SUMS sowie die Anlage 1 zum Übereinkommen von 1958 (E/ECE/TRANS/505/Rev.3). Der Aufbau und die Struktur des Tabellenblattes sind identisch zu jenem in Tabellenblatt 4, weshalb an diesem Punkt nicht noch einmal darauf eingegangen wird.

**Tabellenblatt 6: Anforderungen - Genehmigung**

Die Anforderungen aus Kapitel 1 bis 3 des Prüfkatalogs verlangen die Umsetzung konkreter Verfahren und Prozesse im Rahmen von SUMS. Im Gegensatz dazu beziehen sich die Inhalte in Tabellenblatt 6 (Kapitel 4,5 und 6 des Prüfkatalogs) auf die notwendigen Prozessschritte, die im Rahmen der Beantragung einer SUMS Konformitätsbescheinigung bzw. einer Typgenehmigung zu befolgen sind. Aufbau und Struktur unterscheiden sich dabei leicht zu den beiden vorherstehenden Tabellenblättern. Anstelle eines Anforderungsziels steht an dieser Stelle eine Beschreibung der jeweiligen Anforderung. Zweiter wesentlicher Unterscheid ist zudem, dass beim Erfüllungsgrad kein Wert zwischen 0 und 5 eingetragen wird. Stattdessen wird die Kontrollfrage in diesem Tabellenblatt mit *Ja* (Prozess erfüllt) oder *Nein* (Prozess nicht erfüllt) beantwortet.

**Tabellenblatt 7: Ergebnisse**

Ein Schwerpunkt des vorliegenden Prüfkatalogs ist die Feststellung des SUMS Erfüllungsgrades in der Aufbauphase. Wie bereits erwähnt, muss dazu in der Zeile der jeweiligen Anforderung der Erfüllungsgrad eingetragen werden. Die Auswertung und das Ergebnis der Erfüllungsgradmessung sind schließlich in Tabellenblatt 7 abgebildet.
Die ersten zwei Abbildungen stellen die Auswertung je Kapitel bzw. je Unterkapitel mit den originalen Ergebniswerten dar. In Grün ist zudem der angestrebten Zielreifegrad abgebildet. In Abbildung 3 und 4 ist dann das Gesamtergebnis mit den gekürzten Werten dargestellt. Bei der Berechnung des Gesamtergebnisses werden in diesem Fall jene Erfüllungsgrade, die den Zeilreifegrad übererfüllen, gekürzt und anschließend der Durchschnitt ermittelt. Dies stellt sicher, dass die Anforderungen themenübergreifend erfüllt werden und kein Ausgleich von über- oder untererfüllten Anforderungen stattfindet.
Am Ende des Tabellenblattes werden zudem noch offene Anforderungen (also jene Anforderungen, die den Zielreifegrad noch nicht erfüllen) gelistet.

**Tabellenblatt 8: Beispiel KPIs**

Während die Erfüllungsgradmessung in Tabellenblatt 7 vorrangig in der Aufbauphase für ein SUMS zum Einsatz kommt, dienen die Beispiel KPIs in Tabellenblatt 8 der kontinuierlichen Einhaltung der SUMS Anforderungen in der Betriebsphase. An dieser Stelle sei anzumerken, dass es sich lediglich um Beispiel KPIs handelt, die ggf. für den Gebrauch im eigenen Unternehmen angepasst werden müssen. Auch sind KPIs nur für jene Anforderungen definiert, bei denen die Messung des Prozessergebnisses sinnvoll erscheint.

## UNECE R156 SUMS Prüfkatalog – Tabellenblatt 1:

### PRÜFKATALOG UNECE R156 SUMS

Abkürzungsverzeichnis & Begriffsglossar

| Abkürzung: | Bedeutung: | Erklärung: |
|---|---|---|
| UNECE | United Nations Economic Commission for Europe | Die UNECE (deutsch: Wirtschaftskommission für Europa) wurde 1947 gegründet. Ihr Hauptziel ist die Förderung der gesamteuropäischen wirtschaftlichen Integration. Der UNECE gehören 56 Mitgliedsstaaten in Europa, Nordamerika und Asien an. Alle interessierten Mitgliedstaaten der Vereinten Nationen können sich jedoch an der Arbeit der UNECE beteiligen. |
| SUMS | Software-Update Management System | SUMS (deutsch: Softwareaktualisierungsmanagementsystem) bezeichnet einen systematischen Ansatz zur Festlegung organisatorischer Verfahren und Vorgänge, um den Anforderungen an die Bereitstellung von Softwareaktualisierungen zu entsprechen. |
| RXSWIN | RX-Software-Identifikationsnummer | Die RXSWIN bezeichnet eine vom Fahrzeughersteller festgelegte spezielle Identifikationsnummer, die Informationen über die für die Typgenehmigung relevante Software enthält und zu einem für die Typgenehmigung nach Regelung Nr. X maßgeblichen Merkmal (Funktion) des Fahrzeugs gehört. |
| OTA | Over-The-Air | Ein OTA-Update bezeichnet jede Art der drahtlosen Übertragung von Daten anstelle der Verwendung eines Kabels oder einer anderen ortsgebundenen Verbindung. |
| OBD | On-Board-Diagnose | OBD ist ein Diagnosesystem in Fahrzeugen. Das System überwacht das Auto und kann dem Fahrer oder der Werkstatt Fehlermeldungen und Daten übermitteln. |
| ISO | International Organization for Standardization | Die ISO (deutsch: Internationale Organisation für Normung) ist eine internationale Vereinigung von Normungsorganisationen mit Sitz in Genf und erarbeitet internationale Normen in allen Bereichen mit Ausnahme der Elektrik und der Elektronik. |
| IEC | International Electrotechnial Commission | Die IEC (deutsch: Internationale Elektrotechnische Kommission) ist eine internationale Normungsorganisation für Normen im Bereich der Elektrotechnik und Elektronik mit Sitz in Genf. |
| SAE | Society of Automotive Engineers | Die SAE International (deutsch: Verband der Automobilingenieure) ist ein weltweiter Verband von mehr als 128.000 Ingenieuren und technischen Experten in der Luft- und Raumfahrt-, Automobil- und Nutzfahrzeugindustrie, der sich dem Fortschritt der Mobilitätstechnologie widmet. |
| ISMS | Information Security Management System | Ein ISMS (deutsch: Informationssicherheits Managementsystem) definiert Regeln und Methoden, um die Informationssicherheit in einem Unternehmen oder in einer Organisation zu gewährleisten. |
| CSMS | Cybersecurity Management System | CSMS (deutsch: Cybersicherheitsmanagementsystem) bezeichnet einen systematischen, risikobasierten Ansatz zur Festlegung von organisatorischen Abläufen, Zuständigkeiten und Governance beim Umgang mit Risiken im Zusammenhang mit Cyberbedrohungen für Fahrzeuge und beim Schutz von Fahrzeugen vor Cyberangriffen. |
| MFT | Managed File Transfer | MFT ist eine Technologie, die die sichere Übertragung von Daten auf effiziente und zuverlässige Weise ermöglicht. |
| ITIL | IT Infrastructure Library | ITIL wurde in den vergangenen Jahren zu einem weltweiten Standard für das IT-Service-Management. Es stellt eine Sammlung von Best Practices bzw. Good Practices dar, die eine mögliche Umsetzung eines IT-Service-Managements beschreiben |
| IATF | International Automotive Task Force | Die IATF ist eine Gruppe von Automobilherstellern und ihren jeweiligen nationalen Verbänden der Automobilindustrie, die gegründet wurde, um den Automobilkunden weltweit Produkte mit verbesserter Qualität anzubieten. |
| SPICE | Software Process Improvement and Capability Determination | Automotive SPICE ist eine domänenspezifische Variante des internationalen Standards ISO/IEC 15504 (SPICE). Ziel ist die Bewertung der Leistungsfähigkeit der Entwicklungsprozesse von Steuergerätelieferanten in der Automobilindustrie. |
| BSI | Bundesamt für Sicherheit in der Informationstechnik | Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die Cyber-Sicherheitsbehörde des Bundes und Gestalter einer sicheren Digitalisierung in Deutschland. |
| VIN | Vehicle Identification Number | Die VIN (deutsch: Fahrzeug-Identifizierungsnummer) entspricht der vormaligen Fahrgestellnummer und ermöglicht die eindeutige Identifikation eines Fahrzeuges. |
| KPI | Key Performance Indicator | KPIs (deutsch: Leistungskennzahl) sind Leistungskennzahlen, an denen der Erfolg einer unternehmerischen Aktivität oder auch der Erfüllungsgrad eines bestimmten Ziels gemessen werden kann. |
| COP | Conformity of Production | CoP-Verfahren sind vom Inhaber einer Typgenehmigung verpflichtend durchzuführen. Sie stellen sicher, dass jedes hergestellte Fahrzeug, System und Bauteil sowie jede hergestellte selbstständige technische Einheit dem genehmigten Typ entspricht. |
| KBA | Kraftfahrt-Bundesamt | Das KBA ist die verantwortliche Bundesbehörde für den Straßenverkehr in Deutschland. Es übernimmt u.a. für Kraftfahrzeuge die Typgenehmigung und die Typprüfung von Fahrzeugen und Fahrzeugteilen. |
| OEM | Original Equipment Manufacturer | Der Begriff „OEM" (deutsch: Erstausrüster) wird in der Automobilindustrie synonym mit einem Fahrzeughersteller verwendet. |

| Begriff: | Erklärung: |
|---|---|
| Fahrzeugtyp | Fahrzeugtyp bezeichnet Fahrzeuge, die sich zumindest in folgender Hinsicht nicht voneinander unterscheiden:<br>a) vom Hersteller angegebene Bezeichnung des Fahrzeugtyps,<br>b) wesentliche Merkmale der Konzeption des Fahrzeugtyps in Bezug auf die Verfahren zur Softwareaktualisierung. |
| Softwareaktualisierung | Softwareaktualisierung bezeichnet das Upgrade einer Software auf eine neue Version; dies schließt eine Änderung der Konfigurationsparameter ein. |
| Durchführung | Durchführung bezeichnet das Verfahren zur Installation und Aktivierung einer Aktualisierung, die heruntergeladen wurde. |
| Fahrzeugnutzer | Fahrzeugnutzer bezeichnet eine Person, die das Fahrzeug bedient oder fährt, einen Fahrzeugbesitzer, einen bevollmächtigten Vertreter oder Mitarbeiter eines Flottenmanagers, einen bevollmächtigten Vertreter oder Mitarbeiter des Fahrzeugherstellers oder einen befugten Techniker. |
| Sicherer Zustand | Sicherer Zustand bezeichnet einen Betriebsmodus ohne unverhältnismäßiges Risiko bei Ausfall eines Merkmals oder einer Funktionskomponente. |
| System | System bezeichnet einen Satz von Bauteilen und/oder Subsystemen, die eine oder mehrere Funktionen erfüllen. |
| Validierungsdaten für die Integrität | Validierungsdaten für die Integrität bezeichnet eine Darstellung digitaler Daten, mit der Vergleiche zur Erkennung von Fehlern oder Änderungen der Daten angestellt werden können. Hierzu können Prüfsummen und Hashwerte gehören. |
| Cybersicherheit | Cybersicherheit bezeichnet den Zustand, in dem Straßenfahrzeuge und deren Funktionen vor Cyberbedrohungen für elektrische oder elektronische Bauteile geschützt sind. |
| Bedrohung | Bedrohung bezeichnet eine potenzielle Ursache eines unerwünschten Vorfalls, der zur Schädigung eines Systems, einer Organisation oder einer Person führen kann. |
| Schwachstelle | „Schwachstelle" bezeichnet die Schwäche eines Elements oder einer Risikominderungsmaßnahme, die durch eine oder mehrere Bedrohungen ausgenutzt werden kann. |
| Informationssicherheit | Ziel von Informationssicherheit ist es, sich vor Gefahren und Bedrohungen zu schützen und einen möglichen wirtschaftlichen Schaden zu vermeiden oder mindestens zu minimieren. Im Fokus steht die Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit von Daten. |
| Risiko | „Risiko" bezeichnet die Möglichkeit, dass durch eine bestimmte Bedrohung Schwachstellen eines Fahrzeugs ausgenutzt werden und dadurch einer Organisation oder einer Person Schaden zugefügt wird. |
| Configuration Management | Configuration Management (deutsch: Konfigurationsmanagement) ist ein technischer Prozess, der die korrekte Zuordnung von Configuration Items (deutsch: Konfigurationselemente) eines Unternehmens ebenso sicherstellt wie deren Beziehung in einer Betriebsumgebung. |
| Release Management | Releasemanagement (deutsch: Freigabemanagement) bezieht sich auf den Prozess des Planens, Entwerfens, Terminierens, Testens, Bereitstellens und Kontrollierens von Software-Releases. |

| | |
|---|---|
| Quality Management | Quality Management (deutsch: Qualitätsmanagement) bezeichnet die Überwachung aller Aktivitäten und Aufgaben, die durchgeführt werden müssen, um ein gewünschtes Qualitätsniveau zu erreichen. |
| Information Management | Information Management (deutsch: Informationsmanagement) konzentriert sich auf den zielgerichteten und wirtschaftlichen Umgang mit den Informationen innerhalb eines Unternehmens. Es sorgt dementsprechend für eine adäquate Informationsbereitstellung. |
| Infrastructure and Platform Management | Aufgabe des Infrastructure and Platform Management (deutsch: Infrastruktur- und Plattformmanagement) ist die von einer Organisation genutzte Infrastruktur und Plattformen zu koordinieren und zu überwachen. |
| Supplier Management | Supplier Management (deutsch: Lieferantenmanagement) ist der Prozess, der sicherstellt, dass ein Unternehmen einen maximalen Gegenwert erhält für das Geld, das es an seine Lieferanten zahlt. |
| Safety Management | Safety Management (deutsch: Sicherheitsmanagement) ist die Vorsorge von Sicherheit für Personen und Sachwerten in einer professionellen Form. |
| Availability Management | Availability Management (deutsch: Verfügbarkeitsmanagement) sorgt für das Definieren, Analysieren, Planen, Messen und Verbessern aller Faktoren, die für die Verfügbarkeit von IT-Services wesentlich sind. |
| Incident Management | Incident Management (deutsch: Störungsmanagement) umfasst typischerweise den gesamten organisatorischen und technischen Prozess der Reaktion auf erkannte oder vermutete Sicherheitsvorfälle. Das primäre Ziel besteht darin, einen IT Service für den Anwender so schnell wie möglich wieder herzustellen. |
| Business Continuity Management | Business Continuity Management (deutsch: Betriebliches Kontinuitätsmanagement) ist ein Managementprozess mit dem Ziel, gravierende Risiken für eine Organisation frühzeitig zu erkennen und Maßnahmen dagegenzusetzen. |
| Authentizität | Mit Authentizität ist gewährleistet, dass nur autorisierte Person (Identiätsnachweis) Zugang haben, Informationen echt und glaubwürdig sind (Quellenangabe) oder es sich um manipulationsfreie, unversehrte IT Systeme und IT Anwendungen handelt. |
| Integrität | Die Integrität stellt sicher, dass Daten vollständig und unverändert sind. Ihr unbemerktes Verändern wird damit verhindert. |
| Validierung | Das Ziel der (Software-)Validierung ist der Nachweis, dass eine Software fehlerfrei arbeitet. (siehe auch ISO 13485) |
| Verifizierung | Die Verifizierung überprüft, ob eine Software richtig entwickelt wurde und ihrer Spezifikation entspricht. |
| Charge | Charge bezeichnet eine bestimmte Menge gleichartiger Güter, die in einem zusammenhängenden Prozess gemeinsam verarbeitet werden. |
| Konformität | Die Konformität bescheinigt die Übereinstimmung (z.B. eines Produktes) mit den genannten Spezifikationen. |

## UNECE R156 SUMS Prüfkatalog – Tabellenblatt 2:

**PRÜFKATALOG UNECE R156 SUMS**

Rahmenwerk für die Erfüllungsgradmessung gemäß ISO/IEC 15504-2

| Erfüllungsgrad: | Stufe 0 | Stufe 1 | Stufe 2 |
|---|---|---|---|
| **Bezeichnung:** | **Unvollständiger Prozess** | **Durchgeführter Prozess** | **Gelenkter Prozess** |
| **Beschreibung:** | Der Prozess ist nicht umgesetzt oder erreicht seinen Prozesszweck nicht. | Der umgesetzte Prozess erfüllt seinen Prozesszweck. | Der Prozess wird nun auf gelenkte (d. h. auf geplante, überwachte und angepasste) Art und Weise umgesetzt und seine Arbeitsprodukte werden auf angemessene Art und Weise erstellt, gelenkt, aufrechterhalten und gepflegt. |
| **Prozessattribut 1:** | Bei dieser Stufe gibt es nur wenige oder gar keine Nachweise für eine systematische Erreichung des Prozesszwecks. | Das Attribut **Prozessdurchführung** ist ein Maß für den Grad, bis zu dem der Prozesszweck erreicht ist. Wird dieses Attribut in vollem Umfang erreicht, so gilt, dass:<br>+ der Prozess die für ihn festgelegten Resultate erzielt. | Das Attribut **Durchführungs-Management** ist ein Maß für den Grad, bis zu dem die Durchführung des Prozesses gelenkt ist. Wird dieses Attribut in vollem Umfang erreicht, so gilt, dass:<br>+ die Ziele für die Durchführung des Prozesses angegeben sind;<br>+ die Durchführung des Prozesses geplant ist und überwacht wird;<br>+ die Durchführung des Prozesses angepasst wird, um die Pläne zu erfüllen;<br>+ die Verantwortlichkeiten und Befugnisse für die Durchführung des Prozesses festgelegt, zugewiesen und mitgeteilt sind;<br>+ die zur Durchführung des Prozesses erforderlichen Ressourcen und Informationen ermittelt, zur Verfügung gestellt, zugewiesen und genutzt sind;<br>+ die Schnittstellen zwischen den beteiligten Parteien sind geregelt, um sowohl die Effektivität der Kommunikation als auch die Eindeutigkeit der Verantwortungszuweisung sicherzustellen. |
| **Prozessattribut 2:** | - | - | Das Attribut **Arbeitsproduktmanagement** ist ein Maß für den Grad, bis zu dem die im betreffenden Prozess erzeugten Arbeitsprodukte auf angemessene Weise gelenkt sind. Wird dieses Attribut in vollem Umfang erreicht, so gilt, dass:<br>+ die Anforderungen an die Arbeitsprodukte des Prozesses festgelegt sind;<br>+ die Anforderungen an die Dokumentation und Kontrolle der Arbeitsprodukte festgelegt sind;<br>+ die Arbeitsprodukte auf angemessene Art und Weise identifiziert, dokumentiert und gelenkt sind;<br>+ die Arbeitsprodukte den geplanten Regelungen entsprechend überprüft und, falls zur Erfüllung der Anforderungen erforderlich, angepasst sind. |

| Stufe 3 | Stufe 4 | Stufe 5 |
|---|---|---|
| **Etablierter Prozess** | **Vorhersagbarer Prozess** | **Optimierender Prozess** |
| Der Prozess wird nun mit Hilfe eines definierten Prozesses umgesetzt, der es ermöglicht, die für ihn festgelegten Prozessresultate zu erzielen. | Der Prozess läuft nun innerhalb definierter Grenzen ab, um die für ihn festgelegten Prozessresultate zu erzielen. | Der Prozess wird stetig verbessert, um den maßgeblichen aktuellen und künftigen Geschäftszielen zu entsprechen. |
| Das Attribut **Prozessdefinition** ist ein Maß für den Grad, bis zu dem ein Standardprozess aufrechterhalten und gepflegt ist, um den Einsatz des definierten Prozesses zu unterstützen. Wird dieses Attribut in vollem Umfang erreicht, so gilt, dass:<br>+ ein Standardprozess einschließlich entsprechender Tailoring-Richtlinien definiert ist, der die grundlegenden Elemente beschreibt, die in einen definierten Prozess aufgenommen werden müssen;<br>+ die Abfolge des Standardprozesses und seine Wechselwirkung mit anderen Prozessen festgelegt sind;<br>+ die zur Durchführung eines Prozesses erforderlichen Kompetenzen und Rollen als Teil des Standardprozesses ermittelt sind;<br>+ die zur Durchführung eines Prozesses erforderliche Infrastruktur und die entsprechende Arbeitsumgebung als Teil des Standardprozesses ermittelt sind;<br>+ geeignete Methoden zur Überwachung der Effektivität und Eignung des Prozesses festgelegt sind. | Das Attribut **Prozessmessung** ist ein Maß für den Grad, bis zu dem Messergebnisse verwendet werden, um sicherzustellen, dass festgelegte Prozessdurchführungsziele erreicht werden. Wird dieses Attribut in vollem Umfang erreicht, so gilt, dass:<br>+ der Bedarf an Prozessinformation zur Unterstützung der maßgeblichen festgelegten Geschäftsziele festgestellt ist;<br>+ die Ziele in Bezug auf die Prozessmessung vom Bedarf an Prozessinformationen abgeleitet sind;<br>+ die quantitativen Prozessdurchführungsziele zur Unterstützung der maßgeblichen Geschäftsziele festgelegt sind;<br>+ die Messgrößen und die Zeitabstände zwischen den Messungen im Einklang mit den Zielen in Bezug auf die Prozessmessung und den quantitativen Pozessdurchführungszielen ermittelt und festgelegt sind;<br>+ die Messergebnisse erfasst, analysiert und in einem Bericht angegeben sind, um den Grad, bis zu dem die quantitativen Prozessdurchführungsziele erreicht wurden, zu überwachen;<br>+ die Messergebnisse zur Beschreibung der Prozessdurchführung genutzt sind. | Das Attribut **Prozessinnovation** ist ein Maß für den Grad, bis zu dem Änderungen am Prozess aus der Analyse allgemeiner Ursachen für Abweichungen und aus der Untersuchung innovativer Ansätze abgeleitet werden. Wird dieses Attribut in vollem Umfang erreicht, so gilt, dass:<br>+ Prozessverbesserungsziele für den Prozess festgelegt sind, die zur Unterstützung der maßgeblichen Geschäftsziele beitragen;<br>+ die entsprechenden Daten analysiert sind, um allgemeine Ursachen für Abweichungen in der Prozessdurchführung zu ermitteln;<br>+ die entsprechenden Daten analysiert sind, um Möglichkeiten für Best Practice und Innovation zu erkennen;<br>+ Verbesserungsmöglichkeiten, die sich aus neuen Techniken und Prozesskonzepten ergeben, erkannt sind.<br>+ eine Strategie zur Umsetzung eingeführt ist, die dazu dient, die Prozessverbesserungsziele zu erreichen. |
| Das Attribut **Prozesseinsatz** ist ein Maß für den Grad, bis zu dem der Standardprozess effektiv als definierter Prozess eingesetzt ist, um die für ihn festgelegten Prozessresultate zu erzielen. Wird dieses Attribut in vollem Umfang erreicht, so gilt, dass:<br>+ ein definierter Prozess eingesetzt wird, der auf einem angemessen ausgewählten und/oder angepassten Standardprozess basiert;<br>+ die zur Durchführung des definierten Prozesses erforderlichen Rollen, Verantwortlichkeiten und Befugnisse zugewiesen und mitgeteilt sind;<br>+ das an der Durchführung des definierten Prozesses beteiligte Personal aufgrund entsprechener Ausbildung, Schulung und Erfahrung über die erforderliche Kompetenz verfügt;<br>+ die zur Durchführung des definierten Prozesses erforderlichen Ressourcen und Informationen zur Verfügung gestellt, zugewiesen und genutzt sind;<br>+ die zur Durchführung des definierten Prozesses erforderliche Infrastruktur und die entsprechende Arbeitsumgebung zur Verfügung gestellt, verwaltet, aufrechterhalten und gepflegt sind;<br>+ geeignete Daten gesammelt und analysiert sind, die als Basis für das Verständnis des Verhaltens des Prozesses und zum Nachweis seiner Eignung und Effektivität sowie zur Evaluierung, an welchen Stellen eine kontinuierliche Verbesserung des Prozesses vorgenommen werden kann, dienen. | Das Attribut **Prozesskontrolle** ist ein Maß für den Grad, bis zu dem der Prozess quantitativ gelenkt ist, um zu einem Prozess zu gelangen, der stabil ist, die geforderten Fähigkeiten umfasst und innerhalb festgelegter Grenzwerte vorhersagbar abläuft. Wird dieses Attribut in vollem Umfang erreicht, so gilt, dass:<br>+ Analyse und Kontrollverfahren werden dort, wo sie einsetzbar sind, festgelegt und angewendet;<br>+ Kontrollgrenzen der Schwankungsbreite der normalen Prozessdurchführung festgelegt sind;<br>+ die entsprechenden Messwerte im Hinblick auf spezielle Abweichungsursachen analysiert sind;<br>+ Korrekturmaßnahmen ergriffen sind, um spezielle Abweichungsursachen zu beseitigen;<br>+ aufgrund der Korrekturmaßnahmen die Kontrollgrenzen (bei Bedarf) neu festgelegt sind. | Das Attribut **Prozessoptimierung** ist ein Maß für den Grad, bis zu dem Änderungen an der Definition, Lenkung und Durchführung des Prozesses zu effektiven Auswirkungen führen, die zur Erfüllung der maßgeblichen Prozessverbesserungsziele beitragen. Wird dieses Attribut in vollem Umfang erreicht, so gilt, dass:<br>+ die Auswirkungen aller vorgeschlagenen Änderungen in Bezug auf die Ziele des definierten Prozesses und des Standardprozesses bewertet sind;<br>+ die Umsetzung aller beschlossenen Änderungen auf eine Weise gelenkt wird, die sicherstellt, dass jede Störung der Prozessdurchführung verstanden und entsprechend darauf reagiert wird;<br>+ die Effektivität der Prozessänderung aufgrund der tatsächlichen Durchführung in Bezug auf die festgelegten Produktanforderungen und Prozessziele evaluiert wird, um festzustellen, ob die Ergebnisse allgemeine oder spezielle Ursachen haben. |

## UNECE R156 SUMS Prüfkatalog – Tabellenblatt 3:

Infolge des großen Umfangs werden nicht alle Inhalte aus Tabellenblatt 3 abgebildet.

### PRÜFKATALOG UNECE R156 SUMS

Einheitliche Bestimmungen für die Genehmigung von Kraftfahrzeugen hinsichtlich der Softwareaktualisierung und des Softwareaktualisierungsmanagementsystems gemäß UNECE Regelung Nr. 156 [Stand: 4. März 2021]

| UNECE Kap. | Inhalt | Kapitel im Prüfkatalog |
|---|---|---|
| **1.** | **Anwendungsbereich** | |
| 1.1. | Diese Regelung gilt für Fahrzeuge der Klassen M, N, O, R, S und T, bei denen Softwareaktualisierungen möglich sind. | - |
| **2.** | **Begriffsbestimmungen** | |
| 2.1. | „Fahrzeugtyp" bezeichnet Fahrzeuge, die sich zumindest in folgender Hinsicht nicht voneinander unterscheiden:<br>a) vom Hersteller angegebene Bezeichnung des Fahrzeugtyps,<br>b) wesentliche Merkmale der Konzeption des Fahrzeugtyps in Bezug auf die Verfahren zur Softwareaktualisierung. | - |
| 2.2. | „RX-Software-Identifikationsnummer" bezeichnet eine vom Fahrzeughersteller festgelegte spezielle Identifikati onsnummer, die Informationen über die für die Typgenehmigung relevante Software des elektronischen Steuersystems enthält und zu einem für die Typgenehmigung nach Regelung Nr. X maßgeblichen Merkmal des Fahrzeugs gehört. | - |
| 2.3. | „Softwareaktualisierung" bezeichnet ein Paket, das für das Upgrade auf eine neue Version verwendet wird; dies schließt eine Änderung der Konfigurationsparameter ein. | - |
| 2.4. | „Durchführung" bezeichnet das Verfahren zur Installation und Aktivierung einer Aktualisierung, die heruntergeladen wurde. | - |
| 2.5. | „Softwareaktualisierungsmanagementsystem" bezeichnet einen systematischen Ansatz zur Festlegung organisatorischer Verfahren und Vorgänge, um den Anforderungen an die Bereitstellung von Softwareaktualisierungen gemäß dieser Regelung zu entsprechen. | - |
| 2.6. | „Fahrzeugnutzer" bezeichnet eine Person, die das Fahrzeug bedient oder fährt, einen Fahrzeugbesitzer, einen bevollmächtigten Vertreter oder Mitarbeiter eines Flottenmanagers, einen bevollmächtigten Vertreter oder Mitarbeiter des Fahrzeugherstellers oder einen befugten Techniker. | - |
| 2.7. | „Fahrzeugnutzer" bezeichnet eine Person, die das Fahrzeug bedient oder fährt, einen Fahrzeugbesitzer, einen bevollmächtigten Vertreter oder Mitarbeiter eines Flottenmanagers, einen bevollmächtigten Vertreter oder Mitarbeiter des Fahrzeugherstellers oder einen befugten Techniker. | - |
| 2.8. | „Software" bezeichnet den Teil eines elektronischen Steuergeräts, der aus digitalen Daten und Befehlen besteht. | - |
| 2.9. | „Drahtloses Update" bezeichnet jede Art der drahtlosen Übertragung von Daten anstelle der Verwendung eines Kabels oder einer anderen ortsgebundenen Verbindung. | - |
| 2.10. | „System" bezeichnet einen Satz von Bauteilen und/oder Subsystemen, die eine oder mehrere Funktionen erfüllen. | - |
| 2.11. | „Validierungsdaten für die Integrität" bezeichnet eine Darstellung digitaler Daten, mit der Vergleiche zur Erkennung von Fehlern oder Änderungen der Daten angestellt werden können. Hierzu können Prüfsummen und Hashwerte gehören. | - |
| **3.** | **Antrag auf Genehmigung** | |
| 3.1. | Der Antrag auf Genehmigung eines Fahrzeugtyps hinsichtlich der Verfahren zur Softwareaktualisierung ist vom Fahrzeughersteller oder seinem ordentlich bevollmächtigten Vertreter einzureichen. | Kap. 5.1.1 & Kap. 5.1.2 |
| 3.2. | Dem Antrag ist in dreifacher Ausfertigung Folgendes beizufügen: | |
| 3.3. | Eine Beschreibung des Fahrzeugtyps hinsichtlich der in Anhang 1 dieser Regelung genannten Merkmale. | Kap. 5.1.3 |
| 3.4. | Falls an den Beschreibungen nachweislich geistige Eigentumsrechte bestehen oder mit ihnen nachweislich spezifisches Know-how des Herstellers oder seiner Zulieferer preisgegeben wird, übermitteln der Hersteller oder seine Zulieferer Informationen, die für die in dieser Regelung genannten Überprüfungen ausreichend sind. Diese Informationen sind vertraulich zu behandeln. | Kap. 5.1.3 |
| 3.5. | Die Konformitätsbescheinigung für das Softwareaktualisierungsmanagementsystem nach Nummer 6 dieser Regelung. | Kap. 5.1.4 |
| 3.6. | Ein Fahrzeug, das dem zu genehmigenden Fahrzeugtyp entspricht, ist dem technischen Dienst, der die Prüfungen für die Genehmigung durchführt, zur Verfügung zu stellen. | Kap. 5.1.5 |
| 3.7. | Die Dokumentation muss zwei Teile umfassen: | |
| | a) Die förmliche Dokumentation für die Genehmigung, einschließlich der in Anhang 1 genannten Unterlagen, die der Genehmigungsbehörde oder dem technischen Dienst zum Zeitpunkt der Einreichung des Antrags auf Typgenehmigung vorzulegen ist. Diese Dokumentation dient der Genehmigungsbehörde oder ihrem technischen Dienst als Grundlage für das Genehmigungsverfahren. Die Genehmigungsbehörde oder ihr technischer Dienst stellen sicher, dass diese Dokumentation mindestens 10 Jahre nach der endgültigen Einstellung der Produktion des Fahrzeugtyps verfügbar bleibt. | - |
| | b) Zusätzliches Material, das für die Anforderungen dieser Regelung von Belang ist, kann vom Hersteller aufbewahrt werden, ist aber zum Zeitpunkt der Typgenehmigung zur Prüfung offenzulegen. Der Hersteller stellt sicher, dass zusätzliches Material, das zum Zeitpunkt der Typgenehmigung zur Prüfung offengelegt worden ist, für einen Zeitraum von mindestens 10 Jahren ab der endgültigen Einstellung der Produktion des Fahrzeugtyps verfügbar ist. | Kap. 5.1.6 |
| **4.** | **Kennzeichnung** | |
| 4.1. | An jedem Fahrzeug, das einem nach dieser Regelung genehmigten Fahrzeugtyp entspricht, ist sichtbar und an gut zugänglicher Stelle, die auf dem Mitteilungsblatt anzugeben ist, ein internationales Genehmigungszeichen anzubringen, bestehend aus: | |
| 4.1.1. | einem Kreis, in dem sich der Buchstabe „E" und die Kennzahl des Landes befinden, das die Genehmigung erteilt hat, | Kap. 6.2 |

## UNECE R156 SUMS Prüfkatalog – Tabellenblatt 4:

### PRÜFKATALOG UNECE R156 SUMS

SUMS - Verfahren beim Fahrzeughersteller und am Fahrzeugtyp

| Kapitel | Kontrollfrage | Anforderungsziel | Anforderung |
|---|---|---|---|
| 1 | **Vorschriften beim Fahrzeughersteller** | Kapitel 7.1 der UN-Regelung Nr. 156 enthält zahlreiche Anforderungen und Vorschriften an ein Software-Update Management System beim Fahrzeughersteller. Die Erfüllung der Anforderungen ist essenziel für die erfolgreiche Ausstellung einer SUMS Konformitätsbescheinigung. | |
| 1.1 | **Allgemeines & Anfangsbewertung** | | |
| 1.1.1 | **Inwieweit werden Informationen zu SUMS dokumentiert, geschützt aufbewahrt und auf Anfrage zur Verfügung gestellt?** | Die Implementierung und Aufrechterhaltung eines SUMS beruht auf einer Vielzahl an unterschiedlichen Verfahren und Prozessen. Um einen Überblick zu bewahren ist es wichtig, dass jegliche Informationen dazu fortlaufend dokumentiert und gespeichert werden. Daneben dienen diese Dokumentation und Information der Genehmigungsbehörde als Untersuchungsgrundlage für eine SUMS Zertifizierung. Auf Anfrage sind sie der Genehmigungsbehörde zu übermitteln. | - Durch ein geeignetes Konzept ist sichergestellt, dass alle relevanten Unterlagen und Informationen zum Software-Update Management gespeichert werden.<br>- Durch geeignete Sicherheitsmaßnahmen ist sichergestellt, dass alle relevanten Unterlagen und Informationen zum Software-Update Management informationstechnische geschützt sind.<br>- Auf Nachfrage einer Genehmigungsbehörde oder eines technischen Dienstes müssen die Informationen/Unterlagen jederzeit verfügbar gemacht werden.<br>- Zur Übermittlung der Unterlagen steht ein geeignetes technisches Tool zur Verfügung. Dieses kann vom Hersteller vorgeschlagen werden, muss aber durch die Genehmigungsbehörde bestätigt werden. |
| 1.1.2 | **Inwieweit existiert ein Verfahren zur Identifkation von Software Versionen?** | Die verschiedenen innerhalb eines Fahrzeug verbauten Systeme beeinflussen sich gegenseitig auf unterschiedliche Art und Weise. Zur Bewertung der gegenseitigen Einflussnahme ist es wichtig, dass die Fahrzeughersteller Kenntnis über die auf einem System installierte (und vormals installierten) Software Versionen haben. Selbiges gilt für Hardwarekomponenten, auf denen Software installiert ist. | - Durch ein geeignetes Konzept kann eindeutig identifiziert werden, welche ursprüngliche und welche aktuelle Software Version auf einem System installiert ist, bzw. war.<br>- Die Identifkation basiert auf einer eindeutigen Software Versionsnummer und muss zumindest vom Fahrzeughersteller durchgeführt werden können.<br>- Es ist bekannt und dokumentiert, wie die verbaute Software als die vom Fahrzeughersteller angegebene Version identifiziert werden kann (Nachweis der Datenintegrität).<br>- Hardwarekomponenten, auf denen Software installiert ist, müssen eindeutig identifiziert werden können. |
| 1.1.3 | **Inwieweit können Zielfahrzeuge für ein Software-Update identifiziert werden?** | Im Laufe des Fahrzeuglebenszyklus können Qualitätsprobleme bei einzelnen Fahrzeugen, bestimmten Teile-Chargen oder gewissen Software-Versionen auftreten. Handelt es sich um Software bezogene Qualitätsthemen können diese Probleme häufig durch eine Softwareaktualisierung beseitigt werden. In diesen Fällen ist es wichtig, dass die OEMs über ein Verfahren verfügen, dass die Identifikation von Zeilfahrzeugen für ein solches Software-Update ermöglicht. | - Es gibt ein Verfahren zur Auflistung der von einer Software-Aktualisierung betroffenen Zielfahrzeuge.<br>- Der Prozess ermöglicht die Identifikation von Zielgruppen einer Aktualisierung (z.B. alles Dieselfahrzeuge eines bestimmten Fahrzeugtyps)<br>- Der Prozess ermöglicht die Identifkation von einzelnen individuell zu aktualisierenden Fahrzeugen, z.B. auf Basis der VIN.<br>- Der Prozess inkludiert Maßnahmen zur Verringerung des Fehlerrisikos bei der Identifizierung von Zielfahrzeugen. |
| 1.1.4 | **Inwieweit existiert ein Verfahren, mit dem Fahrzeugnutzer über das bevorstehende Update informiert werden?** | In einigen Fällen führen Softwareaktualisierungen zu Änderungen bei gewissen Fahrzeugfunktionen. Zum Teil verlangen Softwareaktualisierungen auch ein bestimmtes Verhalten seitens des Fahrzeugnutzers (z.B. keine Inbetriebnahme des Fahrzeugs während des Update-Prozesses). In diesen Situationen ist es wichtig, dass der Fahrzeugnutzer im Vorfeld über ein bevorstehendes Update informiert wird. | - Durch ein vorgegebenes Verfahren kann der Fahrzeugnutzer über ein bevorstehendes Software-Update und die damit einhergehenden Änderungen informiert werden.<br>- Durch das Verfahren erhält der Fahrzeugnutzer Informationen über die Situation, in der er eine oder mehrere Aktionen für das Herunterladen und die Installation des Software-Updates durchführen soll.<br>- Die Auswahl der Mittel zur Informationsübertragung an den Fahrzeugnutzer bleibt dem Fahrzeughersteller überlassen. In jedem Fall muss dem Fahrzeugnutzer der Zugriff auf die Informationen jederzeit ermöglicht werden. |
| 1.2 | **Auswirkungen von Software-Updates** | | |
| 1.2.1 | **Inwieweit können Abhängigkeiten zwischen dem zu aktualisierenden System und anderen Systemen identifiziert werden?** | Die einzelnen in einem Fahrzeug verbauten Software-Systeme sind stark miteinander vernetzt. Die Aktualisierung der Software eines Systems kann zu einem veränderten Verhalten eines anderen Systems führen. Es ist deshalb wichtig, dass die Fahrzeughersteller über die Abhängigkeiten zwischen dem zu aktualisierenden System und anderen Systemen Bescheid wissen. | - Es gibt mindestens einen oder mehrere dokumentierte Prozesse, um zu beurteilen, ob eine Aktualisierung Auswirkungen auf andere Systeme hat.<br>- Durch diese Prozesse ist der Fahrzeughersteller in der Lage, zu erkennen, wie die verschiedenen Systeme zusammenwirken.<br>- Durch diese Prozesse ist der Fahrzeughersteller in der Lage, zu beurteilen, ob eine Aktualisierung das Verhalten eines anderen Systems beeinflussen wird. Dies gilt insbesondere für Systeme, die einen Einfluss auf Sicherheit, Cybersicherheit, Diebstahlschutz, Energieeffizienz und Umweltverhalten haben. |

| Anforderungsnachweis | Management Prozess | Referenz UNECE R156 | KPI | Anmerkung |
|---|---|---|---|---|
| | | | | Quellen: UNECE R156, Proposal Document zu UNECE R156 und UNECE R155, ISO 21434 |
| Als Nachweis zur Erfüllung dieser Anforderung dient:<br>+ Eine ISO 27001 oder ISO 9001 Zertifizierung als Nachweis der informationstechnischen Sicherheit<br>+ Informationen über Zugriffsrechte, Qualitätskontroll- und Managementsysteme, Konfigurationskontrollen, Überwachungssysteme<br>+ Maßnahmen zur Sicherung der Server, auf denen die Informationen gespeichert sind<br>+ Kontaktpersonen beim Automobilhersteller<br>+ Informationen über den Datenzugang auf der Datentransferplattform (z.B. mittels Managed File Transfer (MFT) | *Information Security Management* | A 7.1.1.1. & A 7.1.2.1. | - | |
| Als Nachweis zur Erfüllung der Anforderungen dienen:<br>+ Bestehende Konfigurationskontrollverfahren, sofern ihre Relevanz für die Anforderung dargelegt werden kann<br>+ Weitere eingehaltene Standards, inkl. der Erklärung ihrer Relevanz für diese Anforderung | *Configuration Management* | A 7.1.1.2. | - | |
| Als Nachweis kann die Dokumentation des Verfahrens und ein Auszug aus einer Auflistung dienen. | *Configuration Management* | A 7.1.1.6. | - | VIN - Vehicle Identification Number: ist eine individuelle Fahrzeug-Identifikationsnummer |
| Als Nachweis muss der Fahrzeughersteller der Genehmigungsbehörde Informationen über die verwendeten Kommunikationsmethoden darlegen und deren Effektivität demonstrieren können. | *ITIL (Service Management); Release Management; IT Service Management; Communication Management* | A 7.1.1.11. | 1 | Diese Anforderung betrifft traditionelle Software-Update, die nicht über eine Luftschnittstelle (Over-The-Air) übertragen werden. |
| Als Nachweis der Fähigkeit zur Beurteilung von systemabhängigkeiten können Prozesse der Qualitätskontrolle dienen. Zu den relevanten Qualitätsstandards hierbei zählen ISO 10007, ISO 9001, IATF 16949, SPICE o.ä. In jedem Fall sollten im Nachweis folgende Aspekte berücksichtigt werden:<br>+ Identifikation und Dokumentation der Veränderung<br>+ Identifikation von Schnittstellen und Systemen, die mit dem zu aktualiserenden System in Verbindung stehen<br>+ Bewertung der dadurch hervorgerufenen Veränderung | *Configuration Management; Quality Management; Release Management* | A 7.1.1.5. | - | Unterschied zu 1.2.6: Hier geht es "nur" darum festzustellen, zwischen welchen Systemen Zusammenhänge bestehen, aber weniger darum zu welchen konkreten Änderungen es kommt. |

| | | | |
|---|---|---|---|
| 1.2.2 | **Inwieweit wird die Kompatibilität eines Software-Updates mit der bestehenden Konfiguration auf dem Zielfahrzeug überprüft?** | Bei der Durchführung eines Software Updates muss die Update-Fähigkeit der bestehenden Systeme berücksichtigt werden. Bevor ein Update ausgeführt wird muss sichergestellt sein, dass die bestehende Systeme auch nach dem Update weiterhin problemlos funktionieren. Durch geeignete Tests muss überprüft werden, ob die neue Software in bereits vorhandenen und gestesten Systemen zu Fehlern führt. Für diese Testbarkeit bietet sich z.B. das Konzept eines digitalen Zwillings und die Verwendung von Regressionstests an. | - Durch ein vorgegebenes Verfahren kann die Kompatibilität einer Softwareaktualisierung mit der bestehenden Konfiguration auf dem Zielfahrzeug bestätigt werden, bevor das Update zur Installation freigegeben wird.<br>- Das Verfahren beinhaltet die Durchführung von Regressionstests der Softwareaktualisierung mit der letzten bekannten Konfiguration der Software.<br>- Das Verfahren beinhaltet die Feststellung der Hardware und Software Voraussetzungen für das Software Update. |
| 1.2.3 | **Inwieweit wird der Einfluss eines Software-Updates auf bestehende typgenehmigte Software-Systeme überprüft?** | Aus regulatorischer Perspektive von großer Relevanz sind jene Software-Systeme, die typgenehmigungspflichtig sind. Bei einem neuen Update beurteilt der Fahrzeughersteller, ob bestehende Zertifizierungen und Genehmigungen betroffen sind. Die Auswirkungen eines Software-Updates müssen folglich vor allem dann genau beurteil werden, wenn:<br>- das Software-Update auf einem typgenehmigungspflichten Software-System ausgeführt wird<br>- das System, auf dem das Update ausgeführt wird, in Abhängigkeit zu einem anderen typgenehmigungspflichtigen System steht. | - Durch einen vorgegebenen Prozess kann der Fahrzeughersteller feststellen, ob ein Software-Update einen Einfluss auf bestehende typgenehmigte Software-Systeme hat.<br>- Einfluss bezieht sich dabei auf eine Änderung, die eine Verlängerung der Typgenehmigung oder eine neue Typgenehmigung erfordert.<br>- Der Prozess beinhaltet verschiedene Qualitätskontrollverfahren.<br>- Der Prozess beinhaltet eine Bewertung der durch das Update hervorgerufenen Änderungen.<br>- Der Prozess beinhaltet eine Bewertung, welche rechtlichen Anforderungen/Parameter durch die Softwareaktualisierung beeinträchtigt/verändert werden.<br>- Durch ein vorgegebenes Verfahren kann der Fahrzeughersteller Informationen zum Ergebnis dieser Überprüfung des Einflusses eines Software-Updates aufzeichnen und abrufen. |
| 1.2.4 | **Inwieweit wird der Einfluss eines Software-Updates auf die Genehmigung von bestehenden Software-Systemen überprüft?** | Die Auswirkungen von Software-Updates können nicht nur zu funktionalen Veränderungen bei Software-Systemen führen. Sie können auch das jeweilige Genehmigungsverfahren eines Systems betreffen. Dies ist dann der Fall, wenn die Funktionen eines Systems durch das Update derartig verändert wird, dass auch das Ergebnis des Genehmigungsverfahrens anders ausfallen würde. Dementsprechend wichtig ist es, dass die Fahrzeughersteller den Einfluss eines Software Updates auf die Genehmigung von bestehenden Software-Systemen überprüfen und dokumentieren. | - Durch einen vorgegebenen Prozess kann der Fahrzeughersteller feststellen, ob ein Software-Update einen Einfluss auf die Genehmigung bzw. das Genehmigungsverfahren von bestehenden typgenehmigten Software-Systemen hat.<br>-Dies bezieht sich insbesondere auf das Ergebnis des Genehmigungsverfahren und darauf, ob dieses durch das Update nun anders ausfallen würde als zuvor.<br>- Der Prozess beinhaltet eine Bewertung der durch das Update hervorgerufenen Änderungen.<br>- Der Prozess beinhaltet eine Bewertung, welche rechtlichen Anforderungen/Parameter durch die Softwareaktualisierung beeinträchtigt/verändert werden.<br>- Durch ein vorgegebenes Verfahren kann der Fahrzeughersteller Informationen zum Ergebnis dieser Überprüfung des Einflusses eines Software-Updates auf das Genehmigungsverfahren aufzeichnen und abrufen. |
| 1.2.5 | **Inwieweit wird festgestellt, ob ein Software-Update zusätzliche Funktionen innerhalb eines bestehenden Systems aktiviert oder hinzufügt?** | In gewissen Fällen können durch Software-Updates auch neue Funktionen hinzugefügt, bzw. aktiviert werden. In diesen Fällen muss ebenfalls überprüft werden, inwiefern die ursprünglichen Ergebnisse des Genehmigungsverfahren davon betroffen sind. | - Mithilfe eines vorgegebenen Verfahrens kann der Fahrzeughersteller feststellen, ob durch ein Software-Update Funktionen innerhalb eines bestehenden Software-Systems hinzugefügt oder aktiviert werden, die beim Zeitpunkt der Typgenehmigung nocht nicht vorhanden oder aktiviert waren.<br>- Mithilfe des Verfahrens kann festgestellt werden, ob Einträge und Inhalte in den Zulassungsdokumenten des Fahrzeugs angepasst werden müssen.<br>- Mithilfe des Verfahrens kann festgestellt werden, ob die Ergebnisse des Zulassungsverfahrens nach wie vor valide und gültig sind. |
| 1.2.6 | **Inwieweit wird der Einfluss eines Software-Updates auf andere nicht-genehmigungspflichtige Software-Systeme berücksichtigt?** | Zu Funktionsänderungen, hervorgerufen durch Software-Updates, kann es auch bei nicht typgenehmigungspflichtigen Software-Systemen kommen. Eine genaue Überprüfung des Einflusses ist dann notwendig, wenn diese Software-Systeme eine Auswirkung auf den sicheren Betrieb des Fahrzeugs haben. | - Mithilfe eines vorgegebenen Verfahrens kann der Fahrzeughersteller feststellen, ob ein Software-Update Einfluss auf andere nicht-genehmigungsrelevante Software-System hat.<br>- Die Anforderung bezieht sich auf nicht-genehmigungsrelevante Software-Systeme, die aber dennoch für den sicheren Betrieb des Fahrzeugs notwendig sind.<br>- Das Verfahren beinhalten verschiedene Qualitätskontroll- und Konfigurationsmanagementprozesse.<br>- Das Verfahren beinhaltet eine Bewertung, welche Systeme vom Software-Update betroffen sind.<br>- Das Verfahren ermöglicht die Identifikation von Funktionen, die nach der Zulassung des Fahrzeugs durch das Update hinzugefügt oder geändert wurden. |
| **1.3** | **RXSWIN - Software Identifikationsnummer** | | |

| | | | | |
|---|---|---|---|---|
| Als Nachweis zur Fähigkeit der Kompatibilitätsbestätigung können Prozesse der Qualitätskontrolle dienen. Zu den relevanten Qualitätsstandards hierbei zählen ISO 10007, ISO 9001, IATF 16949, o.ä. In jedem Fall sollte der Nachweis folgendes Aspekte beinhalten:<br>+ Beschreibung der Testmethode zur Kompatibilitätsüberprüfung<br>+ Ergebnis der Regressionstests der Softwareaktualisierungen mit der letzten bekannten Konfiguration der Software<br>+ Beschreibung des Vorgehens zur Feststellung der Hardware und Software Voraussetzungen für das Software Update | *Configuration Management; Quality Management; Release Management* | A 7.1.1.7. | 2 | |
| Als Nachweis zur Erfüllung der Anforderung kann eine Zertifizierung nach ISO 10007, ISO 9001, IATF 16949 oder BSI 15026-2:2011 dienen. In jedem Fall sollte der Nachweis Folgendes beinhalten:<br>+ Beschreibung der Qualitätskontrollverfahren<br>+ Ergebnis der Bewertung der Veränderung | *Configuration Management; Quality Management; Release Management* | A 7.1.1.8. & 7.1.2.5. (d) | - | |
| Als Nachweis zur Erfüllung der Anforderung kann eine Zertifizierung nach ISO 10007, ISO 9001, IATF 16949 oder BSI 15026-2:2011 dienen. In jedem Fall sollte der Nachweis Folgendes berücksichtigen:<br>+ Ergebnis der Bewertung der Veränderung | *Quality Management; Release Management* | A 7.1.1.8. & 7.1.2.5. (e) | - | Nicht auf Software Ebene sondern für Genehmigungsverfahren |
| Als Nachweis kann eine Beschreibung des Verfahrens dienen. | *Configuration Management; Release Management* | A 7.1.1.9 | - | |
| Als Nachweis zur Erfüllung der Anforderung dient:<br>+ Eine ausführliche Beschreibung des vorgegebenen Verfahrens<br>+ Das Ergebnis einer Bewertung, welche Systeme betroffen sind<br>+ Eine Dokumentation der Prozesse | *Configuration Management; Quality Management; Release Management* | A 7.1.1.10. | - | Im Unterschied zu 1.2.1 geht es hier mehr um die Änderungen selbst, die ein Update auslösen kann. |

| | | | |
|---|---|---|---|
| 1.3.1 | **Inwieweit existieren Verfahren zum Zugriff auf und zur Aktualisierung von Informationen innerhalb der Software-Identifikationsnummer?** | Die Software-Identifikationsnummer ist eine spezielle fahrzeugindividuelle alphanumerische Kennzeichnung für typgenehmigungsrelevante Software-Systeme. Im Rahmen des Release Management ermöglicht sie die Nachverfolgbarkeit darüber, welche Softwareversion derzeit im Fahrzeug verbaut ist. U.a. für Aktualisierungszwecke ist es notwendig, dass die Fahrzeughersteller die Identifikationsnummer jederzeit abrufen können. Sie müssen außerdem dazu in der Lage sein, die innerhalb der Identifkationsnummer gespeicherten Informationen nach einem Update zu aktualisieren. | - Durch einen technischen Prozess kann der Fahrzeughersteller zu jeder Zeit auf die Informationen, die innerhalb einer RXSWIN hinterlegt sind, zugreifen. Dazu zählen Informationen über alle Software Versionen, die innerhalb einer bestimmten RXSWIN vorhanden sind, inkl. der Validierungdaten zur Überprüfung ihrer Integrität.<br>- Die Speicherung der Daten und Informationen sollte beim Fahrzeughersteller erfolgen.<br>- Durch einen technischen Prozess kann der Fahrzeughersteller die Daten und Informationen innerhalb einer RXSWIN nach einem Update aktualisieren. |
| 1.3.2 | **Inwieweit wird sichergestellt, dass die installierte Softwareversion mit der innerhalb der RXSWIN hinterlegten Software übereinstimmt?** | Um sicherzustellen, dass die in der RXSWIN gespeicherten Informationen nach einem Update aktualisiert wurden, muss in regelmäßigen Abständen nachgewiesen werden, dass die Software Version mit der innerhalb einer RXSWIN gespeicherten Information auch übereinstimmt. | - Durch einen (technischen) Prozess kann der Fahrzeughersteller überprüfen, ob die Software eines typgenehmigten Systems mit der in der entsprechenden RXSWIN definierten Software übereinstimmt.<br>- Der Prozess muss zumindest in der Lage sein, diese Überprüfung bis auf Komponentenebene zu ermöglichen. |
| **1.4** | **Dokumentation & Bereitstellung von Informationen zu Software-Updates** | | |
| 1.4.1 | **Inwieweit werden die Konfiguration von verschiedenen typgenehmigten Software Systemen dokumentiert?** | Ein umfassendes Vehicle Asset Management stellt einen wesentlichen Bestandteil innerhalb von SUMS dar. Darin wird erfasst, welche Hard- und Software auf einem System, bzw. in einem Fahrzeug verbaut ist. Es wichtig, dass seitens der Fahrzeughersteller jederzeit auf diese Informationen zugegriffen werden kann. | - Durch ein vorgegebenes Verfahren ist sichergestellt, dass die Konfiguration von typgenehmigten Software Systemen vor und nach einem Update aufgezeichnet wird.<br>- Durch das Verfahren werden alle vergangenen Konfigurationen dokumentiert und gespeichert (Bei einer sehr hohen Anzahl vergangener Konfigurationen ist es ausreichend, wenn alle noch relevanten vergangenen Konfigurationen dokumentiert sind)<br>- Die Aufzeichnung ermöglicht dadurch die eindeutige Identifikation der Hardware und Software eines typgenehmigten Systems (einschließlich Softwareversionen) und aller einschlägigen Fahrzeug- oder Systemparameter vor und nach einem Update.<br>- Durch einen technischen Prozess kann diese Dokumentation abgerufen werden. |
| 1.4.2 | **Inwieweit werden Informationen innerhalb verschiedener RXSWINs dokumentiert?** | Sofern Software-Identifikationsnummern zur Anwendung kommen stellen sie die wesentliche Grundlage für die Arbeit im Vehicle Asset Management dar. Im Rahmen eines überprüfbaren Registers müssen jegliche Informationen zu einer RXSWIN abgespeichert und zugänglich sein. Das Register enthält darüber hinaus den Nachweis, dass die verbaute Software auch der entsprechenden im Register eingetragenen Software entspricht. U.a. für Zwecke der Typgenehmigung, zur Prüfung der Übereinstimmung der Produktion oder zur regelmäßigen technischen Überprüfung muss das Register der zuständigen Behörde zur Verfügung gestellt werden. | - Es existiert für jede RXSWIN ein überprüfbares Register mit Informationen zu jeder Software (allen Software Komponenten), die dieser RXSWIN zuzuordnen ist.<br>- Das Register enthält Informationen zu den einzelnen Software Versionen für alle Komponenten vor und nach einem Update.<br>- Das Register enthält das Ergebnis der Authentifizierung der einzelnen Software-Versionen (Integrity Validation Data - zur Sicherstellung dass die verbaute Software auch der entsprechenden im Register eingetragenen Software entspricht)<br>- Mithilfe der Integrity Validation Data kann eine entsprechend geschulte Person sicherstellen, dass die Software nicht manipuliert wurde.<br>- Auf Nachfrage einer Genehmigungsbehörde oder eines technischen Dienstes muss das Register jederzeit verfügbar gemacht werden. Zur Übermittlung steht ein geeignetes technisches Tool zur Verfügung. |
| 1.4.3 | **Inwieweit werden Informationen zu Zielfahrzeugen für Software-Updates dokumentiert?** | Es ist reicht nicht aus, dass die Fahrzeughersteller dazu in der Lage sind, Zielfahrzeuge für ein Software-Update zu identifzieren. Es ist wichtig, dass die Identifkation auch Informationen für jedes Zielfahrzeug enthält. Dies umfasst u.a. Informationen über Kompatiblität der letzten bekannten Software-Konfiguration des Zielfahrzeugs mit dem Software-Update. U.a. für Zwecke der Typgenehmigung, zur Prüfung der Übereinstimmung der Produktion oder zur regelmäßigen technischen Überprüfung muss die Dokumentation der zuständigen Behörde zur Verfügung gestellt werden. | - Durch ein vorgegebenes Verfahren beim Fahrzeughersteller werden alle Zielfahrzeuge für ein Software Update dokumentiert.<br>- Die Dokumentation der Zielfahrzeuge muss auf VIN-Level, d.h. für jedes individuell zugelassenes Fahrzeug, erfolgen.<br>- Die Dokumentation beinhaltet die Bestätigung der Kompatiblität der letzten bekannten Software-Konfiguration des Zielfahrzeugs mit dem Software-Update. Falls technisch gleichwertig kann die Bestätigung der Kompatibilität für eine Gruppe ähnlicher Fahrzeug enthalten sein, und nicht für jedes individuelle Fahrzeug.<br>- Auf Nachfrage einer Genehmigungsbehörde oder eines technischen Dienstes muss die Dokumentation jederzeit verfügbar gemacht werden. Zur Übermittlung steht ein geeignetes technisches Tool zur Verfügung. |
| 1.4.4 | **Inwieweit werden Informationen zum Zweck eines Software-Updates dokumentiert und abgerufen?** | Die angestrebten Ziele von Software Updates sind vielfältig und reichen von der Performance Optimierung bis hin zur Schließung einer entdeckten Sicherheitslücke. In jedem Fall hat jedes Update eine bestimmten Zweck, der entsprechend dokumentiert werden muss. | - Der Fahrzeughersteller hat ein vorgegebenes Verfahren zur Aufzeichnung von Dokumentation über den Zweck eines Software-Update.<br>- Der Fahrzeughersteller hat ein vorgegebenes Verfahren zur Bereitstellung der Dokumentation über den Zweck eines Software-Update. |

| | | | | |
|---|---|---|---|---|
| Als Nachweis zur Erfüllung dieser Anforderung kann der Fahrzeughersteller detailliert beschreiben:<br>+ wie er auf die Informationen innerhalb der RXSWIN zugreifen kann.<br>+ wie er diese Informationen aktualisieren kann. Dazu soll der Fahrzeughersteller auf für diese Anforderung relevante Konfigurationskontrollprozesse verweisen. | *Configuration Management; Access Management* | A 7.1.1.3. | 3 | Die RXSWIN selbst soll sich nur dann ändern, wenn die Änderungen durch ein Update zu einer Verlängerung oder Erneuerung der Typgenehmigung des relevanten Software Systems führen. |
| Als Nachweis dieser Anforderung kann eine IATF 16949 Zertifizierung dienen. In jedem Fall enthält der Nachweis Informationen über die Prozesse und/oder Tools, mit denen überprüft wird, ob die Übereinstimmung gegeben ist. | *Configuration Management; Information Security Management; ITIL (IT Validation and Testing)* | A 7.1.1.4. | 4 | |
| | | | | |
| Als Nachweis zur Erfüllung der Anforderung können verschiedene Konfigurationsmanagementprozesse verwendet werden, die bestimmen, was der Fahrzeughersteller aufzuzeichnen hat. Diese Aufzeichnung umfasst in jedem Fall:<br>+ alle relevanten Fahrzeug- oder Systemparameter des Zielsystems vor und nach dem Update<br>+ Hardware- und Software-Versionsnummern des zu aktualisierenden Systems | *Configuration Management; Configuration Management Database* | A 7.1.2.2. | - | |
| Verschiedene dokumentierte Konfigurations-Managementprozesse können als Fähigkeitsnachweis herangezogen werden. In jedem Fall müssen folgende Aspekte im Rahmen der Prozesse dokumentiert werden:<br>+ Jegliche zu einer RXSWIN gehörige Software<br>+ Software Versionen und Ergebnis der jeweiligen Authentifizierung vor und nach einem Update<br>+ Verwendete Methode zur Software-Authentifizierung<br>+ Jegliche RXSWINs, die von einem Software-Update betroffen sind | *Configuration Management; Configuration Management Database; Information Security Management* | A 7.1.2.3. & A 7.1.1.12. | 5 | |
| Verschiedene dokumentierte Konfigurations-Managementprozesse können als Fähigkeitsnachweis herangezogen werden. In jedem Fall muss ersichtlich sein wie:<br>+ die Informationen zur Identifikation von Zielfahrzeugen für ein Update dokumentiert werden.<br>+ die Informationen zur Kompatibilität der Konfiguration dokumentiert werden. | *Configuration Management; Configuration Management Database; Release Management* | A 7.1.2.4. & A 7.1.1.12. | - | - VIN Level: Vehicle Identification Number, wird jedem zugelassenen KFZ zugeteilt, einzigartig für jedes Fahrzeug (noch genauer nachschauen)<br>- Letzte bekannte Software-Konfiguration bezieht sich darauf, dass der Fahrzeughersteller nicht immer Kenntnis über die aktuelle Software-Konfiguration eines Fahrzeugs haben kann, z.B. im Falle von Modifikationen durch den Fahrzeugeigentümer. |
| Als Nachweis zur Erfüllung der Anforderung muss der Fahrzeughersteller das Verfahren zur Aufzeichnung und Bereitstellung der Dokumentation beschreiben.<br>+ Sofern das Verfahren bereits in Anwendung ist, kann als Nachweis das Ergebnis des Verfahrens (d.h. die daraus resultierende Dokumentation) dienen. | *Release Management* | A 7.1.2.5. (a) | - | - Sofern angemessen, können Informationen zu Software-Updates, die den selben Zweck bedienen, zusammengefasst werden. Das kann z.B. der Fall sein wenn ein Fahrzeug-system regelmäßig mit demselben Typ von Update aktualisiert wird und das zu aktualisierende System nicht typgenehmigt ist. |

| | | | |
|---|---|---|---|
| 1.4.5 | **Inwieweit werden Informationen über Funktionen und Systeme, die von einem Update betroffen sind, dokumentiert und abgerufen?** | Vor Freigabe eines Software-Updates muss der Fahrzeughersteller jegliche Schnittstellen zwischen dem zu aktualisierenden System und anderen Systemen analysieren. Die betroffenen Systeme und Funktionen müssen vom Hersteller beschrieben werden. Dies inkludiert insbesondere die Information darüber, ob das betroffene System typgenehmigungspflichtig ist. | - Der Fahrzeughersteller hat ein vorgegebenes Verfahren zur Aufzeichnung einer Beschreibung über die Ziel-Systeme oder Funktionen, die von einem Software-Update betroffen sind (z.B. Bremssystem, Radio, etc.).<br>- Durch das vorgegebenes Verfahren können Informationen darüber, ob Ziel-Systeme oder Funktionen typgenehmigungspflichtig sind, abgerufen werden. |
| 1.4.6 | **Inwieweit werden Informationen zu den Bedingungen, unter denen ein Update ausgeführt werden darf, dokumentiert und befolgt?** | Je nach Update kann es notwendig sein, dass gewisse Bedingungen zur Ausführung der Aktualisierung gegeben sein müssen. Diese Informationen müssen entsprechend dokumentiert und jederzeit abrufbar sein. Die Erfüllung der Bedingungen garantiert, dass Updates sicher und zuverlässig ausgeführt werden. | - Durch ein vorgegebenes Verfahren werden Informationen über die Bedingungen, unter denen ein Software-Update ausgeführt werden darf, dokumentiert. Bedingungen bezieht sich dabei auf jegliche Kriterien, die zur sicheren Ausführung des Updates notwendig sind.<br>- Durch ein vorgegebenes Verfahren können Informationen über die Bedingungen, unter denen ein Software-Update ausgeführt werden darf, abgerufen werden.<br>- Der Fahrzeughersteller kann nachweisen, dass durch Einhaltung der Bedingungen das Update sicher und zuverlässig ausgeführt wird.<br>- Durch das vorgegebene Verfahren kann nachweislich sichergestellt werden, dass die Bedingungen eingehalten werden. |
| 1.4.7 | **Inwiweit wird das Durchlaufen eines Software-Updates durch ein Verifizierungs- und Validierungsverfahren dokumentiert.** | Bevor ein Software Update freigegeben wird, muss es gewisse Verifizierungs- und Validierungsverfahren durchlaufen. Durch eine entsprechende Dokumentation wird sichergestellt, dass alle Updates diese Verfahren durchlaufen haben. | - Durch ein vorgegebenes Verfahren kann der Fahrzeughersteller sicherstellen, dass alle Software-Updates die Verifizierungs- und Validierungsverfahren durchlaufen haben.<br>- Durch das Verfahren ist sichergestellt, dass das Durchlaufen durch die Verifizierungs- und Validierungsverfahren aufgezeichnet und das Ergebnis dokumentiert wird.<br>- Durch das Verfahren ist es möglich, diese Dokumentation abzurufen. |
| 1.4.8 | **Inwieweit wird festgehalten, ob für das Software-Update eine Genehmigung beantragt wurde?** | Jede Beantragung auf Genehmigung für ein Software Update bei einer Genehmigungsbehörde muss protokolliert werden. Dadurch kann der Fahrzeughersteller jederzeit einsehen, ob für ein Update bereits eine Genehmigung beantragt wurde, und wenn ja, wann der Antrag gestellt wurde. | - Durch ein vorgegebene Verfahren protokolliert der Fahrzeughersteller die Beantragung auf Genehmigung für ein Software Update bei einer Genehmigungsbehörde.<br>- Durch das Verfahren kann der Fahrzeughersteller Informationen darüber, ob für ein Update bereits eine Genehmigung beantragt wurde, abrufen. |
| **1.5** | **Informationssicherheit** | | |
| 1.5.1 | **Inwieweit wird sichergestellt, dass ein Software-Update vor Beginn des Aktualisierungsprozesses ausreichend geschützt ist?** | Angreifer können u.U. durch Ausnutzung einer Schwachstelle Zugriff auf das Update erlangen und Änderungen im Software-Code vornehmen. Wichtig ist daher der informations-sicherheitstechnische Schutz von Software-Updates, bevor sie an das Fahrzeug gesendet werden. Es dürfen nur bekannte und autorisierte Updates an die Zielfahrzeuge gesendet werden. | - Durch einen vorgegebenen (technischen) Prozess kann der Fahrzeughersteller sicherstellen, dass die Integrität und Authentizität eines Software-Updates gegeben ist.<br>- Durch den Prozess wird sichergestellt, dass das Software-Update vor Änderungen oder Eingriffen in den Software-Code, die nicht vom Urheber des Updates genehmigt wurden, geschützt ist (Manipulationsschutz).<br>- Durch den Prozess wird sichergestellt, dass nur bekannte und autorisierte Aktualisierungen an die Zielfahrzeuge gesendet werden.<br>- Der Prozess inkludiert die Überprüfung von Updates, die der Fahrzeughersteller von einem Lieferanten zur Übermittlung an ein Zielfahrzeug erhält.<br>- Der Prozess inkludiert die Entwicklung des Software-Updates. |
| 1.5.2 | **Inwieweit wird sichergestellt, dass die Verfahren zur Bereitstellung von Updates ausreichend geschützt sind?** | Während Bereitstellung von Updates besteht ein besonderes Risiko, dass die Updates durch unberechtigte Dritte mitgelesen oder manipuliert werden. Seitens der Hersteller muss daher der Schutzbedarf für die Bereitstellung von Updates ermittelt und entsprechende Maßnahmen gesetzt werden. | - Durch einen vorgegebenen (technischen) Prozess kann der Fahrzeughersteller sicherstellen, dass die Verfahren zur Bereitstellung von Software-Updates nicht manipuliert werden können.<br>- Durch den Prozess ist sichergestellt, dass keine unautorisierten Updates an das Fahrzeug gesendet werden. |
| 1.5.3 | **Inwieweit wird sichergestellt, dass Software-Updates ausreichend geprüft und gestest werden?** | Nach Ermittlung des Schutzbedarfs müssen Software Updates angemessene Verifzierungs- und Validierungsverfahren durchlaufen. Dadurch wird sichergestellt, dass nur ordnungsgemäß getestete und überprüfte Software-Updates an das Fahrzeug gesendet werden. | - Durch einen vorgegebenen (technischen) Prozess kann der Fahrzeughersteller sicherstellen, dass Software-Update vor Freigabe in ausreichendem Maß überprüft und validiert werden. Ein angemenssenes Ausmaß der Verifizierungs- und Validierungsverfahren ist vom Fahrzeughersteller selbst festzulegen. In jedem Fall müssen die durchgeführten Maßnahmen für die Zwecke der Verifizierung und Validierung ausreichend sein.<br>- Durch den Prozess ist sichergestellt, dass nur ordnungsgemäß getestete und überprüfte Software-Updates an das Fahrzeug gesendet werden. |
| **1.6** | **Over-The-Air Software Updates** | | |

| | | | | |
|---|---|---|---|---|
| Als Nachweis zur Erfüllung der Anforderung muss der Fahrzeughersteller das Verfahren zur Aufzeichnung und Bereitstellung der Dokumentation beschreiben.<br>+ Sofern das Verfahren bereits in Anwendung ist, kann als Nachweis das Ergebnis des Verfahrens (d.h. die daraus resultierende Dokumentation) dienen. | *Release Management* | A 7.1.2.5. (b) & (c) | - | - Sofern angemessen, können Informationen zu Software-Updates, die den selben Zweck bedienen, zusammengefasst werden. Das kann z.B. der Fall sein wenn ein Fahrzeug-system regelmäßig mit demselben Typ von Update aktualisiert wird und das zu aktualisierende System nicht typgenehmigt ist. |
| Als Nachweis dienen die Veröffentlichungshinweise der Software-Updates. Sie müssen zumindest folgende Informationen beinhalten:<br>+ Bedingungen, die einen sicheren Zustand für die Ausführung des Updates definieren<br>+ Maßanhmen, die vom Fahrzeugnutzer vor dem Update zu befolgen sind<br>+ Falls erforderlich: Maßnahmen, die von einer kompetenten Person (z.B. Werkstattmitarbeiter) vor dem Update zu befolgen sind | *Release Management* | A 7.1.2.5. (g) & (h) | 6 | - Sofern angemessen, können Informationen zu Software-Updates, die den selben Zweck bedienen, zusammengefasst werden. Das kann z.B. der Fall sein wenn ein Fahrzeug-system regelmäßig mit demselben Typ von Update aktualisiert wird und das zu aktualisierende System nicht typgenehmigt ist. |
| Als Nachweis zur Erfüllung der Anforderung kann das Ergebnis von Verifizierungs- und Validierungsverfahren dargelegt werden. | *Release Management; Quality Management; Information Security Management; ITIL (IT Validation and Testing)* | A 7.1.2.5. (i) mit Bezug auf A 7.1.3.3 | - | - Diese Anforderung steht in Zusammenhang mit Anforderung 1.5.3. Sie verlangt in Form der Dokumentation die Bestätigung, dass SW-Update die Verifizierungs- und Validierungsverfahren aus 1.5.3 durchlaufen haben.<br><br>- Sofern angemessen, können Informationen zu Software-Updates, die den selben Zweck bedienen, zusammengefasst werden. Das kann z.B. der Fall sein wenn ein Fahrzeug-system regelmäßig mit demselben Typ von Update aktualisiert wird und das zu aktualisierende |
| Als Nachweis zur Erfüllung der Anforderung muss der Fahrzeughersteller das Verfahren zur Protokollierung von Genehmigungsbeantragungen beschreiben.<br>+ Sofern das Verfahren bereits in Anwendung ist, kann als Nachweis das Protokoll mit bereits beantragten Software Updates dienen. | *Release Management* | A 7.1.2.5. (f) | | |
| Folgende Prozesse und Standards können als Nachweis dieser Anforderung dienen:<br>+ ISO/SAE 21434<br>+ CSMS inklusive Erklärung mit Bezug auf den Manipulationsschutz<br>+ Regelungen mit Bezug zu Cybersicherheit<br>+ Beschreibung der angewendeten Methode zur Überprüfung der Integrität von Software-Updates während ihrer Download- und Ausführungsphase<br>+ Nachweis, dass das bezogene Update mit dem an das Fahrzeug gesendeten Update übereinstimmt (Authentizität) | *Information Security Management; Cyber Security Management; ITIL (Validation and Testing); Release Management; Supplier Management* | A 7.1.3.1. | 7 | |
| Folgende Prozesse und Standards können als Nachweis dieser Anforderung dienen:<br>+ CSMS inklusive Erklärung mit Bezug auf den Schutz des Update-Bereitstellungssystems<br>+ Regelungen mit Bezug zu Cybersicherheit<br>+ Beschreibung der angewendeten Sicherheitsverfahren für die Update-Bereitstellung | *Information Security Management; CSMS; Infrastructure & Platform Management; Release Management; Availability Management* | A 7.1.3.2. | - | |
| Als Nachweis zur Erfüllung der Anforderung muss vom Fahrzeughersteller detailliert dargelegt werden, dass die von ihm eingesetzen Verifizierungs- und Validierungsverfahren angemessen sind.<br>+ Verschiedene Prozesse und Standards mit Bezug zu dieser Anforderung können angeführt werden. | *Information Security Management; CSMS; Release Management* | A 7.1.3.3 | 8 | |

| | | | |
|---|---|---|---|
| 1.6.1 | **Inwieweit wird sichergestellt, dass ein OTA-Update die Fahrzeugsicherheit während der Fahrt nicht beeinträchtigt?** | Die Öffnung des Fahrzeuges über die Luftschnittstelle birgt das Risiko, dass Angreifer über Schwachstellen in der Verteilinfrastruktur auf das Software-Update zugreifen können. Demenstprechend dürfen sie nur dann durchgeführt werden, wenn sichergestellt werden kann, dass sie die Fahrzeugsicherheit in keinem Fall beeinträchtigen. | - Durch einen vorgegebenen Prozess kann der Fahrzeughersteller bewerten, ob die Fahrzeugsicherheit durch ein OTA-Update, welches während der Fahrt ausgeführt wird, beeinträchtigt ist. |
| 1.6.2 | **Inwieweit wird sichergestellt, dass OTA-Updates, die ein komplexes Handel erfordern, korrekt ausgeführt werden?** | Manche OTA-Updates erfordern die Anwesenheit einer entsprechend qualifizierten und geschulten Person. Sie dürfen nur dann ausgeführt werden, wenn eine solche geeignete Person verfügbar ist. | *Wenn OTA-Updates bestimmte komplexe Handlungen erfordern:*<br>- Durch einen vorgegebenen Prozess kann der Fahrzeughersteller sicherstellen, dass OTA-Updates, die komplexe Handlungen erfordern, nur dann durchgeführt werden, wenn eine geeignete qualifiziert Person anwesend ist oder die Kontrolle über das Verfahren hat.<br>- Der Prozess stellt sicher, dass der Fahrzeughalter keine technischen oder komplexen Handlungen ergreifen muss, um ein Software-Update einzuleiten oder abzuschließen. |
| **2** | **Vorschriften für den Fahrzeugtyp** | | |
| **2.1** | **Informationssicherheit** | | |
| 2.1.1 | **Inwieweit wird sichergestellt, dass nur gültige Software-Updates installiert werden?** | Nach Erhalt des Updates muss eine Fahrzeugfunktion die Authentizität und Integrität des Updates überprüfen. Dadurch werden nur gültige Updates heruntergeladen und ausgeführt. | - Durch einen auf einem bestimmten Fahrzeugtyp implementierten Mechanismus kann sichergestellt werden, dass nur gültige Software-Updates heruntergeladen und ausgeführt werden.<br>- Der Mechanismus verifiziert die Authentizität und Integrität der Software-Updates, z.B. durch Code-Signing*.<br>- Der Mechanismus stellt sicher, dass Software-Updates seit ihrer Entwicklung nicht verändert wurden.<br>- Zusammen mit den in den Kapitel 1.5.1. und 1.5.2. beschriebenen Prozessen ist gewährleistet, dass das gesamte System für Software-Updates, von der Erstellung über die Auslieferung bis zur Ausführung, sicher ist. |
| **2.2** | **RXSWIN - Software Identifikationsnummer** | | |
| 2.2.1 | **Inwieweit kann eine RXSWIN einem bestimmten Fahrzeug zugeordnet werden?** | Die RXSWIN bildet die Basis für jegliche Aktivitäten im Rahmen des Vehicle Asset Managements. Es ist daher wichtig, dass jedes Fahrzeug über eine einzigartig zuordenbare RXSWIN verfügt. | - Durch einen vorgegebenen Prozess kann sichergestellt werden, dass jede RXSWIN eines Fahrzeug eindeutig identifzierbar ist. |
| 2.2.2 | **Inwieweit verändert sich die RXSWIN bei einer Änderung der Software?** | Jedes Software-Update führt zu einer Änderung einer Funktion innerhalb eines Software-Systems. Sofern es sich um ein typgenehmigungspflichtiges System handelt und die Änderung zu einer Erweiterung oder Erneuerung der Typgenehmigung führt, muss die RXSWIN aktualisiert werden. | *Wenn die Änderung einer für die Typgenehmigung relevanten Software zu einer Erweiterung oder Erneuerung der Typgenehmigung führt:*<br>- Durch einen vorgegebenen Prozess kann sichergestellt werden, dass die RXSWIN aktualisiert wird (sofern die Änderung einer für die Typgenehmigung relevanten Software zu einer Erweiterung oder Erneuerung der Typgenehmigung führt). |
| 2.2.3 | **Inwieweit kann die RXSWIN gelesen werden?** | Die RXSWIN enthält jegliche Informationen über die in einem Fahrzeug verbaute Software. Sofern die RXSWIN am Fahrzeug vorhanden ist, muss sie über eine elektronische Kommunikationsschnittstelle (zumindest über die Standardschnittstelle OBD-Port) in standardisierter Form leicht lesbar sein. | *Wenn die RXSWIN am Fahrzeug vorhanden ist:*<br>- Am Fahrzeug existiert eine elektronische Kommunikationsschnittstelle, über welche die RXSWIN in standardisierter Form leicht lesbar ist. Dazu zählt zumindest die elektronische Standardschnittstelle OBD-Port. |
| 2.2.4 | **Inwieweit kann die RXSWIN gelesen werden?** | Sofern die RXSWIN nicht am Fahrzeug vorhanden ist, muss zumindest die verbaute Softwareversion über eine elektronische Kommunikationsschnittstelle (zumindest über die Standardschnittstelle OBD-Port) in standardisierter Form leicht lesbar sein. | *Wenn die RXSWIN am Fahrzeug nicht vorhanden ist:*<br>- Am Fahrzeug existiert eine elektronische Kommunikationsschnittstelle, über welche die Softwareversionen des Fahrzeugs oder einzelner Motorsteuergeräte in standardisierter Form leicht lesbar sind. Dazu zählt zumindest die elektronische Standardschnittstelle OBD-Port.<br>- Durch ein vorgegebenes Verfahren kann sichergestellt werden, dass die Softwareversionen des Fahrzeugs oder einzelner Motorsteuergeräte in Verbindung mit den betreffenden Typgenehmigungen der Genehmigungsbehörde dargelegt werden.<br>- Durch das Verfahren ist sichergestellt, dass diese Erklärung bei jeder Änderung einer Software-Version aktualisiert wird. |
| 2.2.5 | **Inwieweit sind die RXSWINs und Softwareversionen am Fahrzeug geschützt?** | Der informationssicherheitstechnische Schutz der RXSWIN bzw. der Softwareversionen am Fahrzeug ist eine Grundvoraussetzung für ein erfolgreiches Vehicle Asset Management. Durch sie kann u.a. sichergestellt werden, dass die Informationen innerhalb RXSWINs auch der im Fahrzeug verbauten Software entsprechen. | - Durch einen geeigneten Mechanismus ist sichergestellt, dass die RXSWINs und Softwareversionen am Fahrzeug vor unbefugten Veränderungen geschützt sind.<br>- Der Mechanismus stellt sicher, dass nur authorisierte Personen die RXSWINs und Softwareversionen ändern können.<br>- Der Mechanismus stellt sicher, dass die Veränderungen nur dann vorgenommen werden können, wenn ein Software-Update ausgeführt wurde. |
| **2.3** | **Over-The-Air Software Updates** | | |

| | | | | |
|---|---|---|---|---|
| Als Nachweis zur Erfüllung der Anforderung kann der Fahrzeughersteller:<br>+ diesen Prozess detailliert darzustellen.<br>+ die Kriterien, die zur Bewertung des Einflusses eines OTA-Updates auf die Fahrzeugsicherheit herangezogen werden, darlegen. | *Safety Management; Infrastructure and Platform Management; Release Management* | A 7.1.4.1. | - | - Sofern angemessen, können Informationen zu Software-Updates, die den selben Zweck bedienen, zusammengefasst werden. Das kann z.B. der Fall sein wenn ein Fahrzeug-system regelmäßig mit demselben Typ von Update aktualisiert wird und das zu aktualisierende System nicht typgenehmigt ist. |
| Als Nachweis zur Erfüllung dieser Anforderung ist der Fahrzeughersteller dazu in der Lage, diesen Prozess detailliert darzustellen. | *Safety Management; Release Management* | A 7.1.4.2. | - | - Sofern angemessen, können Informationen zu Software-Updates, die den selben Zweck bedienen, zusammengefasst werden. Das kann z.B. der Fall sein wenn ein Fahrzeug-system regelmäßig mit demselben Typ von Update aktualisiert wird und das zu aktualisierende System nicht typgenehmigt ist. |
| | | | | |
| Zum Nachweis der Erfüllung dieser Anforderung muss der Fahrzeughersteller die verwendeten Mechanismen detailliert beschreiben.<br>+ Sofern vorhanden können die Ergebnisse der Authentifizierungstests als Nachweis verwendet werden.<br>+ Eine Cybersicherheitsrichtline kann angeführt werden. | *Information Security Management; Cyber Security Management; ITIL (Validation and testing); Release Management; Availability Management* | A 7.2.1.1. | 9 | *Code Signing: Beim Code Signing werden ausführbare Dateien und Skripte digital signiert, um den Autor der Software zu bestätigen und zu garantieren, dass der Code seit seiner Signierung nicht verändert oder beschädigt wurde. [Quelle: https://knowledge.broadcom.com/external/article/164958/certificate-validation-errors-cause-soft.html] |
| | | | | |
| Als Nachweis zur Erfüllung der Anforderung kann der Fahrzeughersteller darlegen:<br>+ wie die RXSWIN für einen bestimmten Fahrzeugtyp generiert wird.<br>+ wie die RXSWIN einzigartig individualisiert wird.<br>+ dass für jede RXSWIN eine Eins-Zu-Eins Beziehung mit dem entsprechenden Fahrzeug besteht. | *Configuration Management* | A 7.2.1.2.1. | 10 | |
| Als Nachweis zur Erfüllung der Anforderung kann der Fahrzeughersteller darlegen, nach welchen Prinzip die RXSWIN aktualisiert wird. | *Configuration Management* | A 7.2.1.2.1. | - | |
| Als Nachweis zur Erfüllung der Anforderung kann der Fahrzeughersteller folgende Standards und Regelungen anführen:<br>+ ISO 14229/1<br>+ OBD Port: ISO 14229<br>+ UN-Regelung Nr. 83 | *Configuration Management; Availability Management; Infrastructure and Platform Management* | A 7.2.1.2.2. | - | - ISO 14229 spezfiziert ein Diagnose-Kommunikationsprotokoll im Steuergeräte-Umfeld innerhalb der Automobilelektronik (UDS-Unified Diagnostic Services) |
| Als Nachweis zur Erfüllung der Anforderung kann der Fahrzeughersteller folgende Standards und Regelungen anführen:<br>+ ISO 14229/1<br>+ OBD Port: ISO 14229<br>+ UN-Regelung Nr. 83 | *Configuration Management; Availability Management; Infrastructure and Platform Management* | A 7.2.1.2.2. | - | - ISO 14229 spezfiziert ein Diagnose-Kommunikationsprotokoll im Steuergeräte-Umfeld innerhalb der Automobilelektronik (UDS-Unified Diagnostic Services) |
| Als Nachweis muss der Fahrzeughersteller detalliert beschreiben:<br>+ wo und wie RXSWINs und Softwareversionsnummern gespeichert werden.<br>+ welche Mechanismen zum Schutz der RXSWINs und Softwareversionen eingesetzt werden.<br>+ Zum Zeitpunkt der Typgenehmigung sind die vom Fahrzeughersteller gewählten Mittel vertraulich zur Verfügung zu stellen. | *Information Security Management; Configuration Management; Identity and Access Management; Infrastructure and Platform Management* | A 7.2.1.2.3. | - | |

| | | | |
|---|---|---|---|
| 2.3.1 | **Inwieweit ist die Fahrzeugsicherheit im Falle fehlgeschlagener oder abgebrochener Updates gewährleistet?** | Aufgrund verschiedener Ursachen können Updates manchmal fehlschlagen oder während ihrer Ausführung abgebrochen werden. In solchen Fällen ist es wichtig, dass entweder die Vorversion des Systems wiederhergestellt oder alternativ das Fahrzeug in einen sicheren Zustand versetzt wird. | - Durch einen geeigneten (technischen) Mechanismus kann das Fahrzeug feststellen, ob, im Falle eines fehlgeschlagenen oder abgebrochenen Updates, die Wiederherstellung eines früheren Softwarezustandes möglich und wünschenswert ist.<br>- *Die Wiederherstellung ist möglich und wünschenswert:* Der Mechanismus sorgt dafür, dass das Fahrzeug die Vorversion des Software-Updates wiederherstellt.<br>- *Die Wiederherstellung ist nicht möglich und wünschenswert:* Der Mechanismus sorgt dafür, dass das Fahrzeug in einen sicheren Zustand überführt wird.<br>- Der Fahrzeughersteller muss darlegen, was ein sicherer Zustand sein kann. In jedem Fall muss es sich dabei um einen Betriebszustand ohne relevantem Risiko handeln (Als Referenz kann ISO 26262 herangezogen werden). |
| 2.3.2 | **Inwieweit wird überprüft, ob ausreichend Energie zur Beendigung des Software-Updates vorhandes ist?** | Wie sämtliche andere Fahrzeugfunktionen erfordert auch die Installation eines Software-Updates eine gewisse Energie. Dazu kommt, dass z.B. Elektrofahrzeuge während der Installation von Over-The-Air Updates häufig nicht geladen werden dürfen. Vor Beginn des Updates muss daher überprüft werden, ob ausreichend Energie zur Beendigung des Updates vorhanden ist. | - Durch einen geeigneten (technischen) Mechanismus ist sichergestellt, dass Software Updates nur dann gestartet werden, wenn das Fahrzeug über genügend Energie verfügt, um das Update auch abzuschließen.<br>- Der Mechanismus berücksichtigt die Energie, die nötig ist, um gegebenenfalls eine Vorversion wiederherzustellen oder um das Fahrzeug in einen sicheren Zustand zu versetzen. |
| 2.3.3 | **Inwieweit wird sichergestellt, dass die Ausführung eines Software-Updates die Fahrzeugsicherheit nicht beeinträchtigt?** | Bei gewissen Software-Updates, die sicherheitskritische Funktionsbereiche betreffen, muss darauf geachtet werden, dass sie nur dann ausgeführt werden, wenn sie die Fahrzeugsicherheit nicht beeinträchtigen. Updates, die z.B. Fahrfunktionen der dynamischen Fahrzeugkontrolle addressieren, sollten ggf. nicht während der Fahrt ausgeführt werden. | - Durch geeignete technische Mittel ist sichergestellt, dass Software Updates nur dann gestartet werden, wenn sich das Fahrzeug in einem Zustand befindet, in dem die Aktualisierung sicher durchgeführt werden kann.<br>- Durch die technischen Mittel wird verhindert, dass der Fahrer Funktionen nutzt, die die Sicherheit des Fahrzeugs oder die erfolgreiche Durchführung des Updates beeinträchtigen.<br>- Durch die technischen Mittel wird verhindert, dass das Fahrzeug während der Ausführung eines Updates in Bewegung gesetzt wird, wenn das die Fahrzeugsicherheit beeinträchtigt.<br>- Durch die technischen Mittel wird verhindert, dass die Durchführung eines Updates die Sicherheit des Fahrzeugs beeinträchtigen könnte. |
| 2.3.4 | **Inwieweit werden notwendige Voraussetzungen für die Durchführung des Updates überprüft?** | In Kapitel 1.4.6 wird gefordert, dass Bedingungen zur Ausführung von Software Updates (z.B. in Form von Veröffentlichungshinweise) dokumentiert und abrufbar sein müssen. Dies inkludiert auch technische Voraussetzungen auf der Fahrzeugseite. Bevor ein Update gestartet wird, muss das Fahrzeug überprüfen, ob diese Voraussetzungen auch erfüllt sind (z.B. Fenster müssen geschlossen sein). | - Die notwendigen (technischen) Voraussetzungen, die für die Ausführung des Updates auf einem gewissen Fahrzeugtyp erfüllt sein müssen, sind vom Fahrzeughersteller definiert und dokumentiert.<br>- Durch geeignete technische Mittel ist sichergestellt, dass das Update am Fahrzeug nur dann gestartet wird, wenn diese (technischen) Voraussetzungen gegeben sind. |
| **2.4** | **OTA-Updates: Information des Fahrzeugnutzers** | | |
| 2.4.1 | **Inwieweit wird der Fahrzeugnutzer über den Zweck eines Updates informiert?** | Over-the-Air Updates werden im Hintergrund über den Mobilfunkzugang des Fahrzeugs heruntergeladen und können ohne Werkstattbesuch installiert werden. Das spart Zeit und Kosten. Sie erfordern jedoch umso mehr eine umfassende Informationsübermittlung an den Fahrzeugnutzer. Dies inkludiert z.B. Fahrzeugfunktionen, die für die Dauer der Update-Ausführung nicht verfügbar sind, oder sämtliche Anweisungen zur sicheren Durchführung des Updates durch den Fahrzeugnutzer. | - Es existiert ein (technischer) Prozess, der sicherstellt, dass der Fahrzeugnutzer über ein anstehendes Update noch vor Installationsbeginn informiert wird.<br>- *Vorausgesetzt der Fahrzeugnutzer hat das Recht dazu und will informiert werden:* Durch den Prozess werden dem Fahrzeugnutzer alle Informationen zur Verfügung gestellt, um entscheiden zu können, ob er das Update ausführen will.<br>- *Vorausgesetzt der Fahrzeugnutzer entscheidet sich für eine einmalige Autorisierung für Software-Updates:* Der Fahrzeugnutzer muss nicht über jedes anstehende Update informiert werden. Der Prozess muss aber sicherstellen, dass, bei einem Wechsel des Fahrzeugnutzers oder bei Änderung der Präferenzen eines Fahrzeugnutzer, die Autorisierungsoption zurückgenommen wird. |
| 2.4.2 | **Inwieweit wird der Fahrzeugnutzer über mögliche Änderungen von Fahrzeugfunktionen informiert?** | | |
| 2.4.3 | **Inwieweit wird der Fahrzeugnutzer über die Dauer des Updates informiert?** | | |
| 2.4.4 | **Inwieweit wird der Fahrzeugnutzer über mögliche während der Ausführung nicht zur Verfügung stehende Fahrzeug-funktionen informiert?** | | |
| 2.4.5 | **Inwieweit erhält der Fahrzeugnutzer Anweisungen zur sicheren Durchführung des Updates?** | | Der Fahrzeughersteller ist dazu verpflichtet die Informationen aus den Anforderung 2.4.1 bis 2.4.6 in Form von Veröffentlichungshinweisen zu übermitteln. Dies inkludiert Informationen über:<br>- den Zweck des Updates (z.B. Rückruf-, Sicherheits- oder Schutzzwecke)<br>- jegliche durch das Update hervorgerufene Änderungen der Fahrzeugfunktionen<br>- die voraussichtliche Dauer bis zum Abschluss des Updates<br>- jegliche Fahrzeugfunktionen, die für die Dauer der Update-Ausführung nicht verfügbar sind |
| 2.4.6 | **Inwieweit wird der Fahrzeugnutzer nach Beendigung über den Status des Updates informiert?** | Für die Zeit der Ausführung von Over-the-Air Updates dürfen Fahrzeuge häufig nicht in Betrieb genommen werden. Daher ist es wichtig, dass Fahrzeug nach Beendigung der Installation umgehend informiert werden. Dies inkludiert auch die Information über das mögliche Fehlschlagen der Update Installation. | - Es existiert ein (technischer) Prozess, der sicherstellt, dass der Fahrzeugnutzer nach Beendigung des Updates über den Erfolg (oder das Fehlschlagen) des Updates informiert wird. |

| | | | | |
|---|---|---|---|---|
| Als Nachweis zur Erfüllung der Anforderung muss der Fahrzeughersteller in jedem Fall:<br>+ die Anforderungen an einen sicheren Betriebssustand definieren.<br>+ darlegen, welchen Funktionen zur Erreichung des sicheren Betriebszustandes aktiviert/deaktiviert werden müssen. | *Safety Management; Incident Management* | A 7.2.2.1.1. | 11 | - Die Wiederherstellung eines früheren Software-Zustandes ist dann nicht wünschenswert, wenn dadurch die Leistungsfähigkeit und Funktionalität des Fahrzeugs eingeschränkt würden. |
| Als Nachweis zur Erfüllung der Anforderungen muss der Fahrzeughersteller den Mechanismus detailliert beschreiben. Dies kann in Form einer Präsentation und/oder eines physischen Tests erfolgen. | *Business Continuity Management;* | A 7.2.2.1.2. | 12 | |
| Als Nachweis muss der Fahrzeughersteller detailliert darlegen, wie diese technischen Mittel aussehen. Dies kann in Form einer Präsentation und/oder eines physischen Tests erfolgen. | *Safety Management; Business Continuity Management* | A 7.2.2.1.3. & A 7.2.2.3. | 13 | |
| Als Nachweis muss der Fahrzeughersteller detailliert darlegen, wie diese technischen Mittel aussehen. Dies kann in Form einer Präsentation und/oder eines physischen Tests erfolgen.<br>+ Der Nachweis muss das Dokument mit den definierten notwendigen (technischen) Voraussetzungen beinhalten. | *Release Management; Safety Management; Availability Management* | A 7.2.2.5. | - | |
| | | | | |
| Als Nachweis muss der Fahrzeughersteller detailliert darlegen, wie die Information an den Fahrzeugnutzer übermittelt wird. Dies kann in Form einer Präsentation und/oder eines physischen Tests erfolgen. | *Release Management; Communication Management; Information Management* | A 7.2.2.2. (a) | 14 | Für den Fall von Software-Updates mit ähnlichen Inhalten ist eine Information für die Gruppe dieser Updates ausreichend. |
| | *Release Management; Communication Management; Information Management* | A 7.2.2.2. (b) | | Für den Fall von Software-Updates mit ähnlichen Inhalten ist eine Information für die Gruppe dieser Updates ausreichend. |
| | *Release Management; Communication Management; Availability Management; Information Management* | A 7.2.2.2. (c) | | Für den Fall von Software-Updates mit ähnlichen Inhalten ist eine Information für die Gruppe dieser Updates ausreichend. |
| | *Release Management; Communication Management; Availability Management; Information Management* | A 7.2.2.2. (d) | | Für den Fall von Software-Updates mit ähnlichen Inhalten ist eine Information für die Gruppe dieser Updates ausreichend. |
| | *Release Management; Communication Management; Safety Management; Information Management* | A 7.2.2.2. (e) | | Für den Fall von Software-Updates mit ähnlichen Inhalten ist eine Information für die Gruppe dieser Updates ausreichend. |
| Als Nachweis muss der Fahrzeughersteller detailliert darlegen, wie die Information an den Fahrzeugnutzer übermittelt wird. Dies kann in Form einer Präsentation und/oder eines physischen Tests erfolgen. | *Release Management; Communication Management; Information Management* | A 7.2.2.4. (a) | 15 | |

| | | | |
|---|---|---|---|
| 2.4.7 | **Inwieweit wird der Fahrzeugnutzer nach Beendigung des Updates über vorgenommene Änderungen informiert?** | Die Information an den Fahrzeugnutzer nach Beendigung des Updates inkludiert nicht nur eine Statusmeldung über Erfolg oder Misserfolg der Update Installation. Sie beinhaltet auch eine Auflistung über jegliche Neuerungen, die durch das Update aufgespielt wurden. | - Es existiert ein (technischer) Prozess, der sicherstellt, dass der Fahrzeugnutzer nach Beendigung des Updates über die vorgenommenen Änderungen informiert wird.<br>- Es existiert ein (technischer) Prozess, der sicherstellt, dass der Fahrzeugnutzer nach Beendigung des Updates über alle damit zusammenhängenden Aktualisierungen des Benutzerhandbuchs (sofern relevant) informiert wird. |

| | | | |
|---|---|---|---|
| Als Nachweis muss der Fahrzeughersteller detailliert darlegen, wie die Information an den Fahrzeugnutzer übermittelt wird. Dies kann in Form einer Präsentation und/oder eines physischen Tests erfolgen. | *Release Management;*<br>*Communication Management;*<br>*Information Management* | A 7.2.2.4. (b) | 16 |

## UNECE R156 SUMS Prüfkatalog – Tabellenblatt 5:

### PRÜFKATALOG UNECE R156 SUMS

Konformität der Produktion

| Kapitel | Kontrollfrage | Anforderungsziel | Anforderung |
|---|---|---|---|
| 3 | **Konformität der Produktion** | Die Verfahren zur Kontrolle der Konformität der Produktion sollen sicherstellen, dass jedes Fahrzeug oder jede Komponente so hergestellt und produziert werden, dass sie dem initial genehmigten Typ und den in Anlage 1 zum Übereinkommen von 1958 (E/ECE/TRANS/505/Rev.3) beschriebenen Verfahren entsprechen.<br><br>Die Genehmigungsbehörde, die die Typgenehmigung erteilt hat, kann jederzeit die in jeder Fertigungsanlage angewandten Verfahren zur Kontrolle der Übereinstimmung der Produktion überprüfen. Diese Überprüfungen sind in der Regel einmal alle drei Jahre durchzuführen. Die für einen Fahrzeugtyp nach dieser Regelung erteilte Genehmigung kann zurückgenommen werden, wenn die Vorschriften dieser Regelung nicht eingehalten werden oder Prüffahrzeuge den Vorschriften dieser Regelung nicht entsprechen. Die Genehmigungsbehörde hat dann mit einem Mitteilungsblatt gemäß Anhang 2 der UN-Regelung Nr. 156 alle Vertragsparteien darüber zu unterrichten. | |
| **3.1** | **Verfahren zur Kontrolle der Übereinstimmung der Produktion** | | |
| 3.1.1 | **Inwieweit wird kontrolliert, ob jedes hergestellte Fahrzeug dem urpsprünglich genehmigten Typ entspricht?** | Die Erteilung einer Typgenehmigung erfolgt zu Beginn eines Fahrzeuglebenszyklus.<br>Die Konformität der Produktion (COP) regelt jedoch, dass die Produkte der Fahrzeughersteller während der gesamten Produktionslaufzeit die in den ursprünglichen Typgenehmigungsunterlagen festgelegten Spezifikationen und Leistungen erfüllen müssen. | - Durch vorgegebene Verfahren und Vorkehrungen kann der Fahrzeughersteller wirksam kontrollieren, dass Fahrzeuge und Komponenten so hergestellt werden, dass sie dem ursprünglich genehmigten Typ entsprechen. |
| 3.1.2 | **Inwieweit werden die Ergebnisse der Kontrolle der Konformität dokumentiert und aufbewahrt?** | Die Ergebnisse der Verfahren zur Kontrolle der Konformität der Produktion müssen von den Fahrzeugherstellern sorgfältig dokumentiert. Mit den Ergebnissen der Kontrolle weisen sie nach, dass ihre Produkte die in den ursprünglichen Typgenehmigungsunterlagen festgelegten Spezifikationen und Leistungen nach wie vor erfüllen. | - Durch einen vorgegebenen Prozess ist sichergestellt, dass Ergebnisse der Verfahren zur Kontrolle der Übereinstimmung der Produktion dokumentiert werden.<br>- Durch den Prozess ist sichergestellt, dass Ergebnisse der Verfahren zur Kontrolle der Übereinstimmung der Produktion aufbewahrt werden. Der Zeitraum der Aufbewahrung ist vorab mit der Genehmigungsbehörde oder dem technischen Dienst abzusprechen. Gerechnet vom Zeitpunkt, an dem die Herstellung endgültig eingestellt wird, darf dieser Zeitraum zehn Jahre nicht übersteigen. |
| **3.2** | **Vorgehen bei Abweichung und Einstellung der Produktion** | | |
| 3.2.1 | **Inwieweit ist das Vorgehen bei Abweichungen der Produktion definiert?** | Qualitätsprobleme bestimmter Teile-Chargen, der Ausfall eines Lieferanten oder andere Ereignisse können zu Abweichungen in der Produktion führen. Der Fahrzeughersteller benötigt ein klares Verfahren um solche Abweichungen zu erkennen und entsprechende Maßnahmen zu setzen. | *Wenn eine Kontrolle oder eine Prüfung die Nicht-Konformität einer bestimmten Produktion erkennen lässt:*<br>- Durch ein vorgegebenes Verfahren ist sichergestellt, dass bei einer Abweichung der Produktion weitere Kontrollen zur Überprüfung der Konformität durchgeführt werden.<br>- Durch das Verfahren ist sichergestellt, dass Maßnahmen umgesetzt werden, um die Konformität der betroffenen Produktion wiederherzustellen. |
| 3.2.2 | **Inwieweit ist das Vorgehen bei Einstellung der Produktion definiert?** | Am Ende der Produktionslaufzeit eines Fahrzeugs muss die Genehmigungbehörde über die Einstellung der Produktion unterrichtet werden. | *Wenn die Produktion eines nach dieser Regelung genehmigten Fahrzeugtyps endgültig eingestellt wird:*<br>- Durch ein vorgegebenes Verfahren ist sichergestellt, dass bei der endgültigen Einstellung der Produktion eines nach der UN-Regelung Nr. 156 genehmigten Fahrzeugtyps die Genehmigungsbehörde, die die Genehmigung erteilt hat, darüber unterrichtet wird. |

| Anforderungsnachweis | Management Prozess | Referenz UNECE R156 | KPI | Anmerkung |
|---|---|---|---|---|
| | | | | Die Quellen in diesem Dokument sind einerseits die UNECE Regelung zu SUMS sowie die Anlage 1 zum Übereinkommen von 1958 (E/ECE/TRANS/505/Rev.3). |
| Als Nachweis zur Erfüllung dieser Anforderung kann die Zertifizierung des Fahrzeugherstellers nach der internationalen Norm ISO 9001:2008 dienen. Dabei muss sich der Geltungsbereich der Zertifizierung in jedem Fall auf das (die) zu genehmigende(n) Produkt(e) erstrecken.<br>+ Alternativ kann vom Fahrzeughersteller eine gleichwertige Akkreditierungsnorm zur Erfüllung der Anforderung dargelegt werden. In dem Fall muss der Hersteller Angaben zur Zertifizierung machen. Außerdem verpflichtet sich der Hersteller dazu die Genehmigungsbehörde über jede Änderung der Gültigkeit oder des Geltungsbereichs dieser Zertifizierung zu informieren. | *Quality Management* | E/ECE/TRANS/505/Rev.3 A 1 | 17 | |
| Die Dokumentation der Ergebnisse kann als Nachweis dieser Anforderung dienen. | *Quality Management* | A 9.1.1. | 18 | |
| | | | | |
| Die Dokumentation dieses Verfahrens kann als Nachweis dieser Anforderung dienen. | *Quality Management* | E/ECE/TRANS/505/Rev.3 A 2.3.6. | 19 | |
| Die Dokumentation dieses Verfahrens kann als Nachweis dieser Anforderung dienen. | *Change Management* | A 11.1. | 20 | |

## UNECE R156 SUMS Prüfkatalog – Tabellenblatt 6:

Infolge des großen Umfangs werden nicht alle Inhalte aus Tabellenblatt 6 abgebildet.

**PRÜFKATALOG UNECE R156 SUMS**

Konformitätsbescheinigung & Typgenehmigung

| Kapitel | Kontrollfrage | Anforderung | Beschreibung | Referenz UNECE R156 |
|---|---|---|---|---|
| 4 | **Konformitätsbescheinigung** | Eine von den Vertragsparteien dieser Regelung ernannte Genehmigungsbehörde (oder ein von ihr benannter Technischer Dienst) führt eine **Bewertung des Fahrzeugherstellers** hinsichtlich seines Software-Update Managementsystems durch. Fällt die Bewertung positiv aus, erhält der Fahrzeughersteller eine Konformitätsbescheinigung (Certificate of Compliance), die in weiterer Folge eine Grundvoraussetzung für den Antrag auf Genehmigung für einen Fahrzeugtyp hinsichtlich der Verfahren für Softwareaktualisierungen darstellt.<br><br>- Bei positiver Bewertung wird dem Hersteller die Konformitätsbescheinigung für das Software-Update Managementsystem gemäß Anhang 4 der UN-Regelung R156 ausgestellt. (A 6.5)<br>- Sofern sie nicht widerrufen wird bleibt die Konformitätsbescheinigung höchstens drei Jahre ab dem Datum der Ausstellung der Bescheinigung gültig. (A 6.6)<br>- Die Genehmigungsbehörde, die die Konformitätsbescheinigung erteilt hat, kann jederzeit überprüfen, ob die Anforderungen weiterhin erfüllt sind. Wenn die Anforderungen nicht mehr erfüllt sind, kann die Konformitätsbescheinigung zurückgezogen werden. (A 6.7) | | |
| 4.1 | **Beantragung** | | | |
| 4.1.1 | **Ist der Antrag auf Ausstellung der Konformitätsbescheinigung von der richtigen Vertragspartei eingereicht?** | Der Fahrzeughersteller selbst oder ein von ihm bevollmächtigter Vertreter müssen den Antrag auf Ausstellung einer Konformitätsbescheinigung einreichen. | - | A 6.2 |
| 4.1.2 | **Ist der Antrag auf Ausstellung der Konformitätsbescheinigung bei der richtigen Vertragspartei eingereicht?** | Der Antrag auf Ausstellung der Konformitätsbescheinigung ist bei einer offiziellen Genehmigungsbehörde einzureichen. | In Deutschland ist die offiziell zuständige Behörde das Kraftfahrt-Bundesamt (KBA). Dieses beauftragt einen technischen Dienst mit der Durchführung der Prüfungen für die Konformitätsbescheinigung. | A 6.1 |
| 4.1.3 | **Sind dem Antrag Unterlagen zur Beschreibung des SUMS in dreifacher Ausführung beigefügt?** | -Dem Antrag auf Ausstellung der Konformitätsbescheinigung sind in dreifacher Ausführung Unterlagen, in denen das SUMS des Fahrzeugherstellers beschrieben wird, beizufügen.<br>- Mithilfe dieser Unterlagen weist der Hersteller nach, dass er die erforderlichen Verfahren zur Erfüllung aller Anforderungen an das Software-Update Managementsystem eingerichtet hat. | Die Beschreibung des Software-Update Managementsystems soll sich vorrangig auf die Verfahren zur Einhaltung der Anforderungen gemäß Kapitel 7.1 der UN-Regelung Nr. 156 beziehen (bzw. Kapitel 1 - Vorschriften beim Fahrzeughersteller - aus diesem Prüfkatalog). Gegenüber einer Genehmigungsbehörde (bzw. eines technischen Dienstes) gilt das als Nachweis zur Erfüllung der Anforderungen der UN-Regelung Nr. 156. | A 6.3.1. & A 6.4. |
| 4.1.4 | **Ist dem Antrag die unterschriebene Konformitätserklärung gemäß Anlage 1 Anhang 1 der UN-Regelung Nr. 156 in dreifacher Ausführung beigefügt?** | Dem Antrag auf Ausstellung der Konformitätsbescheinigung ist in dreifacher Ausführung eine unterschriebene Erklärung nach dem Muster gemäß *Anlage 1 Anhang 1* der UN-Regelung Nr. 156 beigefügt. | Bei *Anlage 1 Anhang 1* der UN-Regelung Nr. 156 handelt es sich um ein Muster der Konformitätserklärung für das Software-Update Managementsystem. Darin bescheinigt der Fahrzeughersteller die Einhaltung der Anforderungen gemäß UN-Regelung Nr. 156. | A 6.3.2. |
| 4.2 | **Änderung & Verlängerung nach erfolgter Ausstellung der Konformitätsbescheinigung** | | | |
| 4.2.1 | **Es findet eine Änderung (z.B. neues Software Update) statt, die sich auf die Relevanz der Konformitätsbescheinigung auswirkt: Sind alle notwendigen Schritte eingeleitet?** | Der Hersteller unterrichtet die Genehmigungsbehörde oder den technischen Dienst über jede Änderung, die sich auf die Konformitätsbescheinigung für das Software-aktualisierungsmanagementsystem auswirkt. | Der Fahrzeughersteller beurteilt, ob eine vorgenommene Änderungen einen Einfluss auf die beschriebenen Inhalte und Verfahren der Konformitätsbescheinigung hat. Eine Änderung kann dabei sowohl eine Änderung eines Prozesses innerhalb von SUMS als auch ein neues Software Update bedeuten. Hat die Änderung einen Einfluss auf ein Kriterium der Konformitätsbescheinigung unterrichtet der Hersteller die Genehmigungs oder den technischen Dienst darüber. Diese entscheidet anschließend, ob neue Prüfungen erforderlich sind.<br><br>Je nach Ausgang kann die Genehmigungsbehörde:<br>- die Konformitätsbescheinigung zurückziehen wenn die Anforderungen gemäß UN-Regelung nicht mehr erfüllt sind<br>- die bestehende Bescheinigung verlängern, wenn die Änderungen weiterhin den Vorschriften und Dokumentation des vorherigen Zertifikats entsprechen<br>- eine neue Bescheinigung ausstellen | A 6.8. |
| 4.2.2 | **Vor Ablauf der Gültigkeitsdauer der Konformitätsbescheinigung: Sind alle notwendigen Schritte eingeleitet?** | Der Hersteller muss die Ausstellung einer neuen oder die Verlängerung der vorhandenen Konformitätsbescheinigung für das SUMS beantragen. Die Beantragung muss noch vor Ablauf der Gültigkeitsdauer der vorhandenen Konformitätsbescheinigung erfolgen, um der Genehmigungsbehörde die Gelegenheit zu geben, ihre Bewertung reichtzeitig abzuschließen. | Die Genehmigungsbehörde überprüft, ob das SUMS weiterhin die Vorschriften dieser Regelung erfüllt. Vorbehaltlich einer positiven Bewertung stellt die Genehmigungsbehörde eine neue Konformitätsbescheinigung für das SUMS aus oder verlängert die Gültigkeit der vorhandenen Bescheinigung um weitere drei Jahre.<br><br>Die Genehmigungsbehörde:<br>- stellt eine neue Bescheinigung aus wenn Änderungen des SUMS erfolgt sind und die Neubewertung positiv ausfällt<br>- stellt eine neue Bescheingung aus wenn zwischen Ablauf der Zertifikatsgültigkeit und Beginn des Audits mehr als 90 Tage vergangen sind (Re-Audit gemäß KBA)<br>- verlängert die bestehende Bescheinigung | A 6.9 |
| 5 | **Typgenehmigung** | Ein von der Genehmigungsbehörde benannter technischer Dienst führt eine **Bewertung des Fahrzeugtyps** hinsichtlich der Verfahren zur Softwareaktualisierung durch. Fällt die Bewertung positiv aus, erteilt die Genehmigungsbehörde die Typgenehmigung hinsichtlich der Verfahren zur Softwareaktualisierung. In jedem Fall muss die Genehmigungsbehörde die Vertragsparteien des Übereinkommens von 1958, die diese Regelung anwenden, über die Erteilung, Erweiterung oder Versagung der Genehmigung für einen Fahrzeugtyp unterrichten. Dies erfolgt über ein Mitteilungsblatt, das dem Muster in Anhang 2 der UN-Regelung Nr. 156 entspricht. | | |
| 5.1 | **Beantragung** | | | |
| 5.1.1 | **Ist der Antrag auf Genehmigung eines Fahrzeugtyps von der richtigen Vertragspartei eingereicht?** | Der Fahrzeughersteller selbst oder ein von ihm bevollmächtigter Vertreter müssen den Antrag auf Genehmigung eines Fahrzeugtyps hinsichtlich der Verfahren zur Softwareaktualisierung einreichen. | - | A 3.1 |
| 5.1.2 | **Ist der Antrag auf Ausstellung der Typgenehmigung bei der richtigen Vertragspartei eingereicht?** | Der Antrag auf Genehmigung eines Fahrzeugtyps hinsichtlich der Verfahren zur Softwareaktualisierung ist bei einer offiziellen Genehmigungsbehörde einzureichen. | In Deutschland ist die offiziell zuständige Behörde das Kraftfahrt-Bundesamt (KBA). Dieses führt anschließend selbst oder beauftragt einen technsichen Dienst mit der Durchführung der Prüfungen für die Genehmigung. | A 3.1 |

| | | | | |
|---|---|---|---|---|
| 5.1.3 | **Ist dem Antrag die Beschreibung des Fahrzeugtyps gemäß Anhang 1 der UN-Regelung Nr. 156 in dreifacher Ausführung beigefügt?** | - Dem Antrag auf Genehmigung eines Fahrzeugtyps hinsichtlich der Verfahren zur Softwareaktualisierung ist in dreifacher Ausführung eine Beschreibung des Fahrzeugtyps beizufügen.<br>- Die Beschreibung des Fahrzeugtyps erfolgt gemäß der in Anhang 1 der UN-Regelung Nr. 156 genannten Merkmale.<br>- Mithilfe dieser Beschreibung weist der Hersteller nach, dass er die erforderlichen Anforderungen an den Fahrzeugtyp hinsichtlich Softwareaktualisierungen erfüllt. | Die Beschreibung des Fahrzeugtyps hat sich am Anhang 1 der UN-Regelung Nr. 156 zu orientieren. Dabei geht es vorrangig um die Beschreibung der Verfahren zur Einhaltung der Anforderungen gemäß Kapitel 7.2 der UN-Regelung Nr. 156 beziehen (bzw. Kapitel 2 - Vorschriften für den Fahrzeugtyp - aus diesem Prüfkatalog). In jedem Fall:<br>- sollen die technischen Mittel, die für die Bereitstellung von Software-Updates verwendet werden (z.B. kabelgebunden, über Bluetooth, über Wi-Fi, etc.), dargelegt werden.<br>- soll die Beschreibung ein Inhaltsverzeichnis inkludieren.<br>- müssen Zeichnungen (sofern vorhanden) in einem geeigneten Maßstab mit hinreichenden Einzelheiten im Format A4 angehängt werden.<br>- müssen Fotos (sofern vorhanden) hinreichende Einzelheiten erkennen lassen.<br>- sollen Unterlagen, aus denen hervorgeht, dass der Software-Update Prozess sicher durchgeführt wird, beigefügt werden (z.B. Konformitätsbescheinigung für CSMS)<br><br>Falls an den Beschreibungen nachweislich geistige Eigentumsrechte bestehen oder mit ihnen nachweislich spezifisches Know-how des Herstellers preisgegeben wird, übermittelt der Hersteller Informationen, die für die in dieser Regelung genannten Überprüfungen ausreichend sind. In jedem Fall sind diese Information vertraulich zu behandeln. Selbiges Vorgehen wird für Informationen und spezifisches Know-How von Zulieferern angewandt. (A 3.4) | A 3.3 & A 3.4 |
| 5.1.4 | **Ist dem Antrag die Konformitätsbescheinigung gemäß Kapitel 6 der UN-Regelgung Nr. 156 in dreifacher Ausführung beigefügt?** | - Dem Antrag auf Genehmigung eines Fahrzeugtyps hinsichtlich der Verfahren zur Softwareaktualisierung ist in dreifacher Ausführung die Konformitätsbescheinigung für das SUMS des Fahrzeugherstellers beizufügen. | Bei der Konformitätsbescheinigung handelt es sich um das (positive) Ergebnis der Bewertung der Verfahren aus Kapitel 3 dieses Prüfkatalogs. Die durch die Genehmigungsbehörde ausgestellte Bescheinigung gemäß dem Anhang 4 der UN-Regelung Nr. 156 ist die Grundlage für die Bentragung der Typgenehmigung eines Fahrzeugs. Ohne gültige Konformitätsbescheinigung kann der Fahrzeughersteller keinen Antrag auf Genehmigung eines Fahrzeugtyps stellen.<br><br>Zusammen mit den Informationen gemäß Anhang 1 der UN-Regelung Nr. 156 dient die Konformitätsbescheinigung als Grundlage für das Genehmigungsverfahren. Die Genehmigungsbehörde oder ihr technischer Dienst müssen sicher stellen, dass diese Dokumentation mindestens 10 Jahre nach der endgültigen Einstellung der Produktion des Fahrzeugtyps verfügbar bleibt. | A 3.5 |
| 5.1.5 | **Ist dem technischen Dienst ein Fahrzeug des zu genehmigenden Fahrzeugtyps zur Verfügung gestellt?** | Der Genehmigungsbehörde oder einem benannten technischen Dienst, der die Prüfungen für die Genehmigung durchführt, wird ein Fahrzeug, das dem zu genehmigenden Fahrzeugtyp entspricht, zur Verfügung gestellt. | Die Bereitstellung des Fahrzeugs dient der praktischen Prüfung am Produkt. Aufgabe des technischen Dienstes ist es dabei zu beurteilen, ob die Funktionen betreffend Softwareaktualisierungen am Fahrzeug den Vorgaben der UN-Regelung entsprechen. Zudem wird überprüft, ob der Fahrzeughersteller die von ihm dokumentierten Maßnahmen umgesetzt hat und ob durch sie der geforderte Funktionsumfang erreicht werden kann. | A 3.6 |
| 5.1.6 | **Ist der Umgang mit zusätzlichem Material, das für die Anforderungen der Regelung von Belang ist, korrekt?** | - Zusätzliches Material, das für die Anforderungen der UN-Regelung Nr. 156 von Belang ist, ist vom Hersteller aufzubewahren und zum Zeitpunkt der Typgenehmigung zur Prüfung offenzulegen.<br>- Der Hersteller muss sicherstellen, dass zusätzliches Material, das zum Zeitpunkt der Typgenehmigung zur Prüfung offengelegt worden ist, für einen Zeitraum von mindestens 10 Jahren ab der endgültigen Einstellung der Produktion des Fahrzeugtyps verfügbar ist. | - | A 3.7 |
| **5.2** | **Änderung & Erweiterung nach erfolgter Typgenehmigung** | | | |
| 5.2.1 | **Es findet eine Änderung des Fahrzeugs statt, die sich auf dessen technische Leistung und/oder die nach der UN-Regelung Nr. 156 erforderlichen Unterlagen auswirkt: Sind alle notwendigen Schritte eingeleitet?** | Der Hersteller unterrichtet die Genehmigungsbehörde, die die Genehmigung erteilt hat, über alle Änderung, die sich auf die technische Leistung und/oder die nach der UN-Regelung Nr. 156 erforderlichen Unterlagen auswirken. | Betroffen von dieser Anforderung sind jene Änderungen, die sich auf den Fahrzeugtyp und dessen technisches System zur Bereitstellung von Updates beziehen. Das Vorgehen für Änderungen, die sich auf das Software-Update Management System des Herstellers beziehen, wird in Kapitel 3.2.1 dieses Prüfkatalogs beschrieben.<br><br>In jedem Fall kann die Genehmigungsbehörde entweder:<br>- die Genehmigung bestätigen wenn sie zum Schluss kommt, dass die vorgenommenen Änderungen weiterhin den Vorschriften und der Dokumentation der vorherigen Typgenehmigung entsprechen.<br>- die Genehmigung erweitern wenn sich an der Art der Update Bereitstellung etwas ändert. (z.B. Änderungen beim Auslesen und Schutz der RXSWIN)<br>- die Genehmigung erneuern wenn ein neuer technischer Ansatz zur Update Bereitstellung gewählt wird.<br>- die Genehmigung versagen wenn die Anforderungen gemäß UN-Regelung Nr. 156 nicht mehr erfüllt sind.<br>- beim technischen Dienst einen neuen Prüfbericht anfordern.<br><br>Die Bestätigung, Erweiterung, Erneuerung oder Versagung der Genehmigung ist von der Genehmigungsbehörde unter Angabe der Änderungen mit einem Mitteilungsblatt mitzuteilen, das dem Muster in Anhang 2 der UN-Regelung Nr. 156 entspricht. Bei Erweiterung der Genehmigung muss die Genehmigungsbehörde dieser Erweiterung eine laufende Nummer zuteilen und die anderen Vertragsparteien des Übereinkommens von 1958, die diese Regelung anwenden, darüber unterrichten. | A 8.1.1., A 8.1.2. & A 8.1.3. |
| **6** | **Kennzeichnung** | An jedem Fahrzeug, das einem nach dieser Regelung genehmigten Fahrzeugtyp entspricht, ist ein internationales Genehmigungszeichen gemäß dem Muster in Anhang 3 der UN-Regelung Nr. 156 anzubringen. | | |
| 6.1 | **Ist das Genehmigungskennzeichen an der richtigen Stelle angebracht?** | Das Genehmigungszeichen ist auf dem vom Hersteller angebrachten Typenschild des Fahrzeugs oder in dessen Nähe anzugeben. | - | A 4.4. |

| | | | | |
|---|---|---|---|---|
| 6.2 | **Ist das Genehmigungskennzeichen in der richtigen Form angebracht?** | - Das Genehmigungszeichen muss deutlich lesbar und dauerhaft sein.<br>- Das Genehmigungszeichen besteht aus einem Kreis, in dem sich der Buchstabe „E" und die Kennzahl des Landes befinden, das die Genehmigung erteilt hat.<br>- Das Genehmigungszeichen besteht aus der Nummer dieser Regelung, mit dem nachgestellten Buchstaben „R", einem Bindestrich und der Genehmigungsnummer rechts neben dem Kreis gemäß dem oberen Absatz. | Das internationale Genehmigungszeichen muss dem Muster in Anhang 3 der UN-Regelung Nr. 156 entsprechen. Anhand dieses Kennzeichnungsformats kann abgelesen werden:<br>- in welchem Land die Zulassung erfolgte<br>- um welche Regelung es sich handelt<br>- um welche fortlaufende Genehmigungsnummer es sich handelt<br>- sowie die Fassung der Regelung, nach der die Genhmigung erteilt wurde. | A 4.3., A 4.1.1., A 4.1.2. & A 4.5. |
| 6.3 | **Das zu genehmigende Fahrzeug entspricht einem Fahrzeugtyp, der im betroffenen Land bereits nach einer oder mehreren anderen Regelungen genehmigt wurde. Ist das Verhalten des Fahrzeugherstellers für diese Situation korrekt?** | - Der Kreis, in dem sich der Buchstabe "E" und die Kennzahl des Landes befinden, das die Genehmigung erteilt haben, werden nicht wiederholt.<br>- Die zusätzlichen Regelungs- und Genehmigungsnummern, aufgrund deren die Genehmigung in dem Land erteilt wurde, sind untereinander rechts neben dem Kreis anzuordnen. | | A 4.2. |

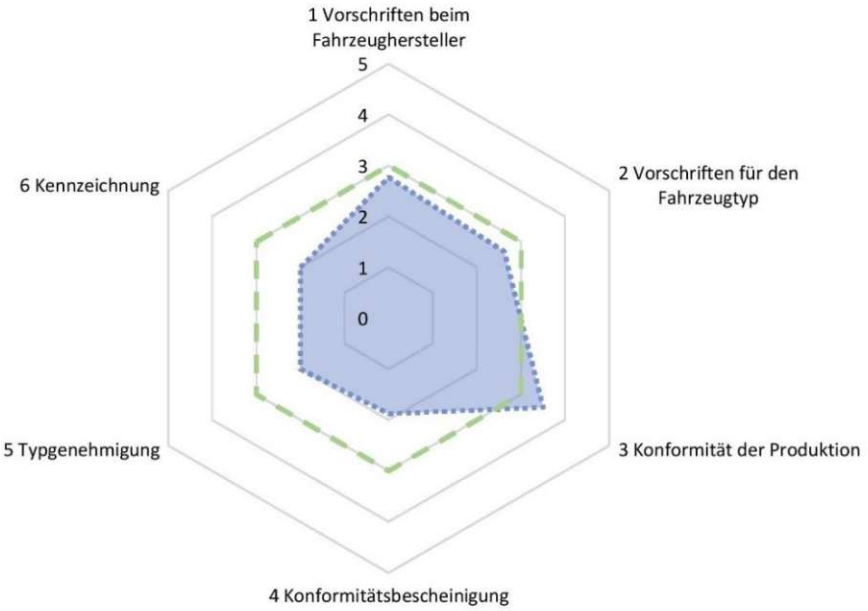
## UNECE R156 SUMS Prüfkatalog – Tabellenblatt 7:

**Prüfkatalog UNECE R156 SUMS**

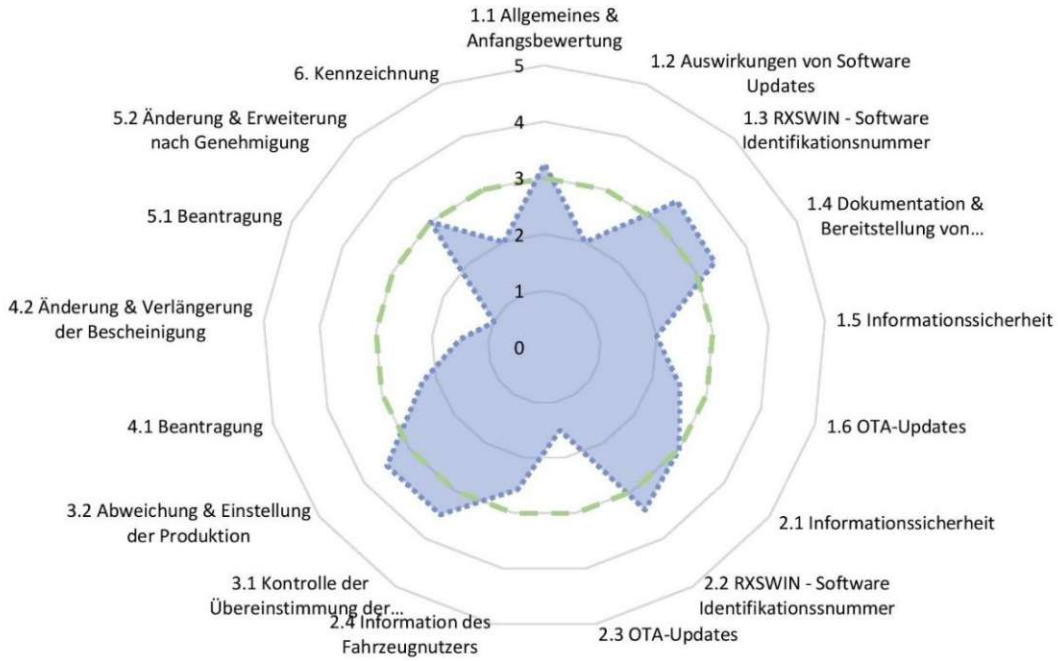
Auswertung & Ergebnis der Erfüllungsgradmessung

**Übersicht**

**Auswertung je Kapitel:**




**Auswertung je Unterkapitel:**

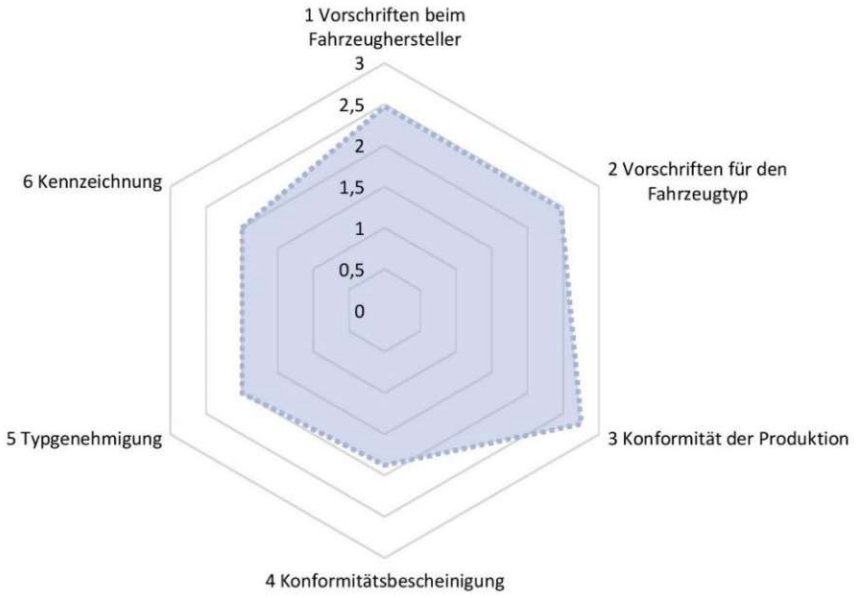


## Prüfkatalog UNECE R156 SUMS

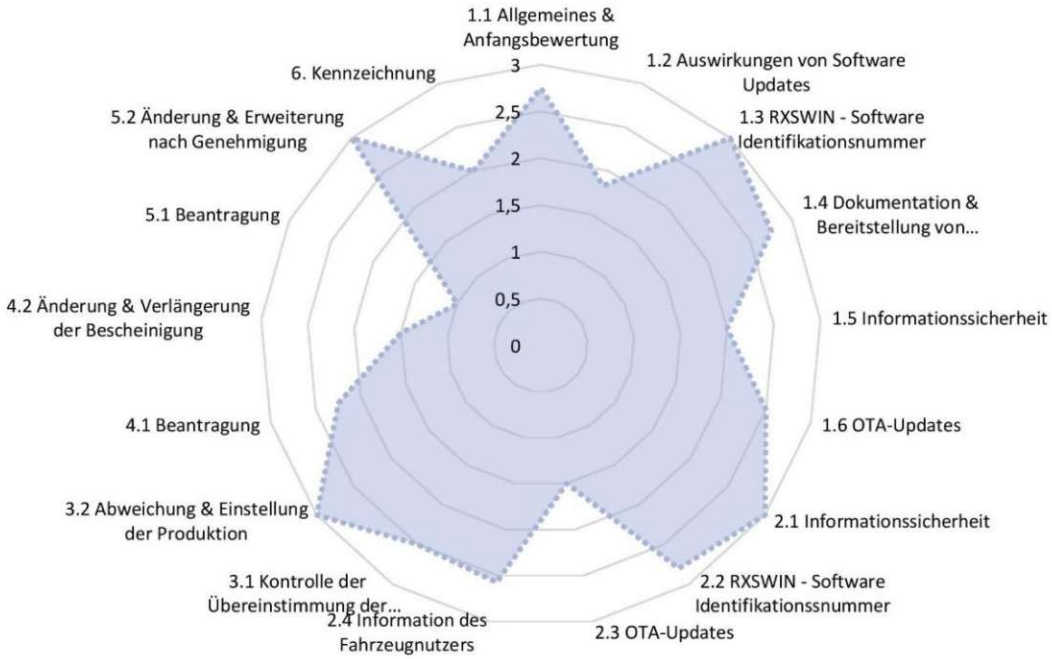
Auswertung & Ergebnis der Erfüllungsgradmessung

**Übersicht**

**Auswertung je Kapitel (gekürzt):**




**Auswertung je Unterkapitel (gekürzt):**



## Prüfkatalog UNECE R156 SUMS

Auswertung & Ergebnis der Erfüllungsgradmessung

**Detailauswertung - Anforderungen SUMS & Produktion**

**Angestrebter Zielreifegrad:** 3

| Kapitel: | Kontrollfrage: | Ergebnis: | Ergebnis gekürzt: |
|---|---|---|---|
| **1** | **Vorschriften beim Fahrzeughersteller** | **2,77** | **2,47** |
| **1.1** | **Allgemeines & Anfangsbewertung** | **3,25** | **2,75** |
| 1.1.1 | Inwieweit werden Informationen zu SUMS dokumentiert, geschützt aufbewahrt und auf Anfrage zur Verfügung gestellt? | 4,00 | 3,00 |
| 1.1.2 | Inwieweit existiert ein Verfahren zur Identifkation von Software Versionen? | 4,00 | 3,00 |
| 1.1.3 | Inwieweit können Zielfahrzeuge für ein Software-Update identifiziert werden? | 2,00 | 2,00 |
| 1.1.4 | Inwieweit existiert ein Verfahren, mit dem Fahrzeugnutzer über das bevorstehende Update informiert werden? | 3,00 | 3,00 |
| **1.2** | **Auswirkungen von Software Updates** | **2,00** | **1,83** |
| 1.2.1 | Inwieweit können Abhängigkeiten zwischen dem zu aktualisierenden System und anderen Systemen identifiziert werden? | 1,00 | 1,00 |
| 1.2.2 | Inwieweit wird die Kompatibilität eines Software-Updates mit der bestehenden Konfiguration auf dem Zielfahrzeug überprüft? | 1,00 | 1,00 |
| 1.2.3 | Inwieweit wird der Einfluss eines Software-Updates auf bestehende typgenehmigte Software-Systeme überprüft? | 1,00 | 1,00 |
| 1.2.4 | Inwieweit wird der Einfluss eines Software-Updates auf die Genehmigung von bestehenden Software-Systemen überprüft? | 2,00 | 2,00 |
| 1.2.5 | Inwieweit wird festgestellt, ob ein Software-Update zusätzliche Funktionen innerhalb eines bestehenden Systems aktiviert oder hinzufügt? | 4,00 | 3,00 |
| 1.2.6 | Inwieweit wird der Einfluss eines Software-Updates auf andere nicht-genehmigungspflichtige Software-Systeme berücksichtigt? | 3,00 | 3,00 |
| **1.3** | **RXSWIN - Software Identifikationsnummer** | **3,50** | **3,00** |
| 1.3.1 | Inwieweit existieren Verfahren zum Zugriff auf und zur Aktualisierung von Informationen innerhalb der Software-Identifikationsnummer? | 3,00 | 3,00 |
| 1.3.2 | Inwieweit wird sichergestellt, dass die installierte Softwareversion mit der innerhalb der RXSWIN hinterlegten Software übereinstimmt? | 4,00 | 3,00 |
| **1.4** | **Dokumentation & Bereitstellung von Informationen zu Software-Updates** | **3,38** | **2,75** |
| 1.4.1 | Inwieweit werden die Konfiguration von verschiedenen typgenehmigten Software Systemen dokumentiert? | 3,00 | 3,00 |
| 1.4.2 | Inwieweit werden Informationen innerhalb verschiedener RXSWINs dokumentiert? | 2,00 | 2,00 |
| 1.4.3 | Inwieweit werden Informationen zu Zielfahrzeugen für Software-Updates dokumentiert? | 4,00 | 3,00 |
| 1.4.4 | Inwieweit werden Informationen zum Zweck eines Software-Updates dokumentiert und abgerufen? | 4,00 | 3,00 |
| 1.4.5 | Inwieweit werden Informationen über Funktionen und Systeme, die von einem Update betroffen sind, dokumentiert und abgerufen? | 3,00 | 3,00 |
| 1.4.6 | Inwieweit werden Informationen zu den Bedingungen, unter denen ein Update ausgeführt werden darf, dokumentiert und befolgt? | 2,00 | 2,00 |
| 1.4.7 | Inwiweit wird das Durchlaufen eines Software-Updates durch ein Verifizierungs- und Validierungsverfahren dokumentiert. | 5,00 | 3,00 |

## Prüfkatalog UNECE R156 SUMS

Auswertung & Ergebnis der Erfüllungsgradmessung

**Offene Anforderungen SUMS & Produktion**

*Folgende Anforderungen erreichen noch nicht den Zielerfüllungsgrad:*

| Kapitel: | Kontrollfrage: | Ergebnis: |
|---|---|---|
| **1** | **Vorschriften beim Fahrzeughersteller** | **2,77** |
| 1.1.3 | Inwieweit können Zielfahrzeuge für ein Software-Update identifiziert werden? | 2,00 |
| **1.2** | **Auswirkungen von Software Updates** | **2,00** |
| 1.2.1 | Inwieweit können Abhängigkeiten zwischen dem zu aktualisierenden System und anderen Systemen identifiziert werden? | 1,00 |
| 1.2.2 | Inwieweit wird die Kompatibilität eines Software-Updates mit der bestehenden Konfiguration auf dem Zielfahrzeug überprüft? | 1,00 |
| 1.2.3 | Inwieweit wird der Einfluss eines Software-Updates auf bestehende typgenehmigte Software-Systeme überprüft? | 1,00 |
| 1.2.4 | Inwieweit wird der Einfluss eines Software-Updates auf die Genehmigung von bestehenden Software-Systemen überprüft? | 2,00 |
| 1.4.2 | Inwieweit werden Informationen innerhalb verschiedener RXSWINs dokumentiert? | 2,00 |
| 1.4.6 | Inwieweit werden Informationen zu den Bedingungen, unter denen ein Update ausgeführt werden darf, dokumentiert und befolgt? | 2,00 |
| **1.5** | **Informationssicherheit** | **2,00** |
| 1.5.1 | Inwieweit wird sichergestellt, dass ein Software-Update vor Beginn des Aktualisierungsprozesses ausreichend geschützt ist? | 1,00 |
| 1.5.3 | Inwieweit wird sichergestellt, dass Software-Updates ausreichend geprüft und gestest werden? | 2,00 |
| **1.6** | **Over-The-Air Software Updates** | **2,50** |
| 1.6.1 | Inwieweit wird sichergestellt, dass ein OTA-Update die Fahrzeugsicherheit während der Fahrt nicht beeinträchtigt? | 2,00 |
| **2** | **Vorschriften für den Fahrzeugtyp** | **2,62** |
| 2.2.5 | Inwieweit sind die RXSWINs und Softwareversionen am Fahrzeug geschützt? | 2,00 |
| **2.3** | **Over-The-Air Software Updates** | **1,50** |
| 2.3.1 | Inwieweit ist die Fahrzeugsicherheit im Falle fehlgeschlagener oder abgebrochener Updates gewährleistet? | 1,00 |
| 2.3.2 | Inwieweit wird überprüft, ob ausreichend Energie zur Beendigung des Software-Updates vorhandes ist? | 1,00 |
| 2.3.3 | Inwieweit wird sichergestellt, dass die Ausführung eines Software-Updates die Fahrzeugsicherheit nicht beeinträchtigt? | 2,00 |
| 2.3.4 | Inwieweit werden notwendige Voraussetzungen für die Durchführung des Updates überprüft? | 2,00 |
| **2.4** | **OTA-Updates: Information des Fahrzeugnutzers** | **2,57** |
| 2.4.4 | Inwieweit wird der Fahrzeugnutzer über mögliche während der Ausführung nicht zur Verfügung stehende Fahrzeug-funktionen informiert? | 2,00 |
| 2.4.6 | Inwieweit wird der Fahrzeugnutzer nach Beendigung über den Status des Updates informiert? | 2,00 |
| 2.4.7 | Inwieweit wird der Fahrzeugnutzer nach Beendigung des Updates über vorgenommene Änderungen informiert? | 2,00 |
| 3.1.2 | Inwieweit werden die Ergebnisse der Kontrolle der Konformität dokumentiert und aufbewahrt? | 2,00 |

**UNECE R156 SUMS Prüfkatalog – Tabellenblatt 8:**

Infolge des großen Umfangs werden nicht alle Inhalte aus Tabellenblatt 8 abgebildet.

## PRÜFKATALOG UNECE R156 SUMS

Beispiele zu KPIs

| | | | |
|---|---|---|---|
| **Kapitel im Prüfkatalog** | 1.1.4 Inwieweit existiert ein Verfahren, mit dem Fahrzeugnutzer über das bevorstehende Update informiert werden? | | 1.2.2 Inwieweit wird die Kompatibi der bestehenden Konfiguration a |
| **Bereich** | ABDECKUNG | EFFEKTIVITÄT | ABDECKUNG |
| **ID** | **1.1** | **1.2** | **2.1** |
| **Bezeichnung** | **Abdeckungsgrad Vorabinformation Fahrzeugnutzer** | **Effektivität der Tools zur Informationsübermittlung** | **Abdeckungsgrad Kompatibilitätsprüfungen** |
| **Beschreibung** | Software-Updates können zu Änderungen am Fahrzeug führen und ein bestimmtes Verhalten der Fahrzeugnutzer verlangen. Die Fahrzeugnutzer sollten deshalb im Vorfeld über Updates informiert werden. Der Abdeckunsgrad misst den Anteil jener Fahrzeugnutzer, die vorab über das Update informiert wurden. | Die Übermittlung der Informationen über ein bevorstehendes Update kann über unterschiedliche Kommunikationskanäle erfolgen. In jedem Fall muss der Zugriff auf die Informationen seitens der Fahrzeugnutzer gewährleistet sein. Der KPI misst die Effektivität der Verfahren durch Erfassung aller Zugriffe, die nicht erfolgreich waren. | Bevor ein Update installiert wird, muss die Kompatibilität mit den bestehenden Systemen überprüft werden. Dies erfolgt auf Basis einer Kompatibilitätsprüfung. Der KPI misst die durchgehende Anwendung von Kompatibilitäts-prüfungen bei Software-Updates. |
| **Ziel** | Alle Fahrzeugnutzer werden im Vorfeld über ein anstehendes Update informiert. | Die Fahrzeugnutzer haben jederzeit Zugriff auf die Informationen über ein bevorstehendes Update. | Für jedes Software-Update wird im Vorfeld eine Kompatibilitätsprüfung durchgeführt. |
| **Messung** | KPI Quotient = Anzahl der Verständigungen über Updates an Fahrzeugnutzer / Anzahl aller durchgeführten Updates | KPI = Erfassung der nicht erfolgreichen Zugriffe auf Vorabinformationen | KPI Quotient = Anzahl der durchgeführten Kompatibilitätsprüfungen / Anzahl aller durchgeführten SW-Updates |
| **Angestrebter Zielwert** | 100% | 0 | 100% |
| **Schwellwerte** | individuell zu bestimmen (z. B. Grün: > 90%, Gelb: 70-90%, Rot: < 70%) | individuell zu bestimmen (0-20...gering, 20-50 mittel, 50+ hoch) | individuell zu bestimmen (z. B. Grün: > 90%, Gelb: 70-90%, Rot: < 70%) |
| **Durchführungsintervall** | individuell zu bestimmen (z.B. quartalsweise) | individuell zu bestimmen (z.B. quartalsweise) | individuell zu bestimmen (z.B. quartalsweise) |
| **Bemerkung** | | | |

| | | | |
|---|---|---|---|
| b jedes hergestellte Fahrzeug dem ıigten Typ entspricht? | 3.1.2 Inwieweit werden die Ergebnisse der Kontrolle der Konformität dokumentiert und aufbewahrt? | 3.2.1 Inwieweit ist das Vorgehen bei Abweichungen der Produktion definiert? | 3.2.2 Inwieweit ist das Vorgehen bei Einstellung der Produktion definiert? |
| EFFEKTIVITÄT | ABDECKUNG | ABDECKUNG/EFFEKTIVITÄT | ABDECKUNG |
| **17.2** | **18.1** | **19.1** | **20.1** |
| **Effektivität der Konformitätsüberprüfungen** | **Abdeckungsgrad Dokumentation der Konformitätsüberprüfung** | **Wiederherstellung der Konformität** | **Abdeckungsgrad Einstellung der Produktion** |
| Die Konformitätsüberprüfungen sollen sicherstellen, dass Fahrzeuge und Komponenten so hergestellt werden, dass sie dem ursprünglich genehmigten Typ entsprechen. Der KPI erfasst alle durch die trotz Konformitätsüberprüfung im Feld entdeckten nicht konforme Fahrzeuge und Komponenten. | Die Ergebnisse der Konformitätsüberprüfungen der Produktion müssen von Fahrzeugherstellern sorgfältig dokumentiert und aufbewahrt werden. Der Abdeckungsgrad erfasst den Anteil der dokumentierten Ergebnisse bezogen auf alle durchgeführten Konformitätsüberprüfungen | Wird eine Abweichung in der Produktion festgestellt, müssen die Fahrzeughersteller Maßnahmen ergreifen, um die Konformität wiederherzustellen. Der KPI misst den Anteil jener Fahrzeuge bzw. Komponenten, bei den die Konformität erfolgreich wiederhergestellt werden konnte. | Nach Ende der Produktionslaufzeit eines Fahrzeugtyps muss der Fahrzeughersteller die Genehmigungbehörde über die Einstellung informieren. Der KPI misst den Anteil aller Verständigungen an die Behörde bezogen auf die Anzahl aller eingestellter Produktionen. |
| Durch die Konformitätsüberprüfung werden nicht konforme Fahrzeuge und Komponenten entdeckt. | Die Ergebnisse aller Konformitätsüberprüfungen der Produktion sind dokumentiert. | Bei einer festgestellten Abweichung wird die Konformität wiederhergestellt. | Die Genehmigungsbehörde wird über alle Produktionseinstellungen informiert. |
| KPI = Anzahl aller entdeckten nicht konformen Fahrzeuge und Komponenten im Feld | KPI Quotient = Anzahl der dokumentierten Ergebnisse / Anzahl aller durchgeführten Konformitätsüberprüfungen | KPI Quotient = Anzahl der Fahrzeuge bzw. Komponenten, bei denen die Konformität wiederhergestellt wurde / Anzahl aller entdeckten nicht-konformen Fahrzeuge bzw. Komponenten | KPI Quotient = Anzahl Verständigungen an die Behörde / Anzahl aller eingestellten Produktionen (eines best. Fahrzeugtyps) |
| 0 | 100% | 100% | 100% |
| individuell zu bestimmen (0-20...gering, 20-50 mittel, 50+ hoch) | individuell zu bestimmen (z. B. Grün: > 90%, Gelb: 70-90%, Rot: < 70%) | individuell zu bestimmen (z. B. Grün: > 90%, Gelb: 70-90%, Rot: < 70%) | individuell zu bestimmen (z. B. Grün: > 90%, Gelb: 70-90%, Rot: < 70%) |
| individuell zu bestimmen (z.B. quartalsweise) | individuell zu bestimmen (z.B. quartalsweise) | individuell zu bestimmen (z.B. halbjährlich) | individuell zu bestimmen (z.B. jährlich) |