Themenpapier Cluster Elektromobilität Süd-West

Automotive Cybersecurity

elektromobilität süd-west

Inhaltsverzeichnis

Management Summary

Eine Prognose, wie sich das Thema Cybersecurity in Zukunft exakt entwickeln wird, ist nach heutigem Stand noch mit einigen Unsicherheiten verbunden. Sicher ist jedoch: Das digitale Auto macht Cybersecurity zunehmend zu einem zentralen Bestandteil des nachhaltigen Erfolgs in der Automobilwirtschaft. Deshalb beschreibt das vorliegende Themenpapier in zwei Kategorien – Einfallstore sowie Wertschöpfungskette –, wo und für wen Cybersecurity relevant wird, und gibt anschließend Handlungsempfehlungen. Diese sollen nicht nur, aber speziell kleinen und mittelständischen Unternehmen (KMU) aus der Branche als Leitfaden dienen.

Da das moderne Automobil über seinen gesamten Lebenszyklus ein potenzielles Angriffsziel für Cyberkriminalität darstellt, muss die Betrachtung dementsprechend umfassend sein.

Die Entwicklung stellt hierbei das Einfallstor mit dem größten Schadenspotenzial dar, wobei sie gleichzeitig auch den physisch bestgeschützten Bereich repräsentiert. Gefahr geht hier mehr von einem Informationsabgriff statt von einem -zugriff aus. OEM haben in diesem Feld zumeist bereits geeignete Maßnahmen entwickelt; die gängige Regulatorik, im Speziellen UNECE R-155 in Kombination mit der ISO-Norm 21434, bietet eine gute Orientierung bei der Gestaltung einschlägiger Entwicklungsprozesse.

Dagegen ist der physische Zugriff auf das Fahrzeug während der Produktion deutlich weniger restriktiv und ein möglicher Eingriff dementsprechend leichter. So können zusätzliche Komponenten in das Fahrzeug gebracht oder bestehende Komponenten manipuliert werden – oder über die On-Board-Diagnose(OBD)-Schnittstellen kann Zugriff auf das Fahrzeug erlangt werden. Ebenso sind Manipulationen aus der Ferne über WLAN- oder Mobilfunk-Schnittstellen möglich. Für all diese Eingriffe ist jedoch umfangreiches Wissen notwendig, um eine Erkennung in nachfolgenden Prozessschritten zu vermeiden. Gleichzeitig sind unbeabsichtigte Fehler in der Produktion häufiger ein Grund für etwaige Störungen. Daher ist grundsätzlich für all diese Eventualitäten eine entsprechende Sensibilisierung der Mitarbeiter:innen dringend zu empfehlen. Durch die Einführung der Software-Identifikationsnummern basierend auf UNECE R-156 werden Hersteller von Steuergeräten und Bauteilen verpflichtet, entsprechende Software-Update-Management-Systeme zu entwickeln. Dadurch soll sichergestellt werden, dass erstens nur homologierte Software auf die verbauten Steuergeräte gespielt werden kann, zweitens gezielt Updates („Over-the-Air"/OTA) im Feld durchgeführt werden können und drittens manipulierte Software zeitnah erkannt wird. Da das Gesamtsystem immer nur so stark ist wie sein schwächstes Glied, stehen im Speziellen auch die Bauteile der Zulieferer im Fokus. KMU stellt es zuweilen vor Herausforderungen, ausreichend Kapazitäten für diese Bereiche ihres Geschäfts abzustellen.

Durch OTA-Updates und die Zunahme digitaler Services, beispielsweise aus der Produktwelt des Connected Car, bleiben Fahrzeuge jedoch auch jederzeit nach Auslieferung, also im Feld, angreifbar. Wie auch in der Produktion sind Angriffe auf das Fahrzeug über Mobilfunk- und andere Kommunikationsschnittstellen zu erwarten. Es müssen Fehlerspeicher ausgelesen, Störungen behoben und aus etwaigen Angriffen schnell die richtigen Schlüsse gezogen werden. Trotz der noch bestehenden Unklarheit hinsichtlich der Länge der Bereitstellungspflicht von Sicherheitsupdates müssen Cybersecurity-Konzepte diese Aspekte berücksichtigen. Dabei muss zu jeder Zeit ein zertifizierungsfähiges Fahrzeugverhalten aufrechterhalten werden – trotz der steigenden Zahl an Updates sowie der bereits vorhandenen Menge an Fahrzeugkonfigurationen.

Unabhängig davon, ob Zulieferfirmen analoge Produkte, Elektronikbauteile oder Software herstellen, bilden Managementsysteme für Informationssicherheit (Information Security Management Systems, ISMS) nach der ISO-Norm 27001 und der darauf basierende TISAX-Standard eine Grundvoraussetzung, um weiter von OEM als Lieferant in Betracht gezogen zu wer-

den. Bedingt durch das große Wertschöpfungsnetzwerk und die Variantenvielfalt in der Automobilindustrie ist vor allem dem Schnittstellenmanagement große Beachtung zu schenken. Dies stellen OEM sicher, indem sie die Einhaltung der Sicherheitsstandards und der Schnittstellenanforderungen bei ihren Lieferfirmen regelmäßig überprüfen. Zusätzlich empfiehlt sich der Aufsatz architektonischer Abstraktionsebenen mit klar definierten Schnittstellen.

Um Monopolstellungen im Datenbesitz aufzubrechen, wurden von der Europäischen Union (EU) erste Schritte eingeleitet, im Zuge derer neue Geschäftsmodelle in der After-Sales-Industrie entstehen können. Mit der EU-Initiative Secure Remote Maintenance Information (SERMI) sind Hersteller nun aufgerufen, Dritten die Möglichkeit zu geben, sicherheitskritische Dienstleistungen anzubieten. Hierfür müssen auch geeignete Werkzeuge entwickelt und bereitgestellt werden, um unter anderem einen kryptographischen Schutz gewährleisten zu können. Dabei ist speziell Augenmerk auf die Absicherung der Diagnosefunktionen zu legen, die eine Aktualisierung der Fahrzeugsoftware ermöglichen.

Da sich die verschiedenen Teilbereiche der Sicherheit interdependent zueinander verhalten, müssen einzelne Komponenten wie funktionale Sicherheit und Cybersecurity integriert gedacht und entwickelt werden. Dazu gehört zwingend, dass Entwicklungsprozesse gem. ISO 21434 (Cybersecurity), ISO 26262 (funktionale Sicherheit) sowie ISO 21448 (SOTIF; Safety Of The Intended Functionality) und idealerweise der Gebrauchssicherheit gestaltet werden. Zudem sollten sie eng miteinander verzahnt arbeiten, um ein sicheres E/E-System gewährleisten zu können. Durch den Einsatz zentraler Rechner im Fahrzeug wird die Anzahl an Steuergeräten minimiert. Damit geht eine Verringerung der Anzahl an Schnittstellen und potenziellen Angriffsvektoren einher. Da das Risiko bei Angriffen auf die zentrale Steuerung jedoch im Vergleich zu verteilten Systemen steigt, ist diese umso intensiver zu sichern.

Dieses Themenpapier erklärt die einfachsten und gängigsten Hebel im Bereich Cybersecurity speziell für KMU und legt dar, weshalb auch Konzerne von deren Produktsicherheit abhängen und warum das Thema Automotive Cybersecurity eine Chance darstellt.

1.
Motivation und Hintergrund des Themenpapiers

Ein Fall aus dem Jahr 2015 belegt, dass in der Öffentlichkeit kursierende Schreckensszenarien zur Automotive Cybersecurity längst Realität sind. Mit einfachen Mitteln gelang es Forscher:innen, Zugriff auf das Modell Jeep Cherokee und all seine Systeme (inkl. Motor, Bremse, Lenkung, Getriebe etc.) zu erlangen. Der Beweis des fernsteuerbaren Automobils hatte unter anderem den Rückruf von 1,4 Millionen Fahrzeugen zur Folge. Bei einem Angriff durch eine kriminelle Vereinigung statt durch Forscher:innen hätte es zu schwerwiegenden Folgen kommen können.

Folglich rückt das Thema Cybersecurity zum Schutz der Kund:innen, der Bevölkerung im weiteren Sinne, aber auch der Unternehmen und ihrer Beschäftigten immer mehr in den Fokus und genießt wachsende Aufmerksamkeit. Gleichermaßen wächst die Bedeutung des Themas Cybersecurity für Regulierungsbehörden und Standardisierungsinitiativen, die sowohl Vorgaben als auch Empfehlungen für Produkte und Organisationsstrukturen von Unternehmen im Hinblick auf Cybersecurity definieren.

Für Unternehmen sind der Aufbau und die Etablierung von ISMS entsprechend der ISO 27001 zu empfehlen. Diese Vorgaben haben den Anspruch, alle Unternehmensbereiche hinsichtlich kritischer Angriffsszenarien abzusichern – die überarbeitete Fassung der ISO 27001 ist 2018 in deutscher Sprache erschienen. Daraus abgeleitet veröffentlicht das BSI die IT-Grundschutzkataloge, die konkrete Handlungsempfehlungen für die Umsetzung der Anforderungen der ISO 27001 liefern. Ziel des IT-Grundschutzkataloges ist es, mit geringem Aufwand wirksame und zertifizierungsfähige ISMS entsprechend ISO 27001 aufbauen zu können. Der Aufbau und Betrieb von ISMS ist branchenübergreifend zu empfehlen. In der deutschen Automobilindustrie sind ISMS bereits weit verbreitet. Im weiteren Verlauf des Themenpapiers erfolgt eine Fokussierung auf automobilspezifische Standards und Regularien, die sich in erster Linie auf die Absicherung der IT-Sicherheit in Fahrzeugen richten.

Sowohl die Internationale Organisations für Standardisierung mit der Norm ISO 21434 als auch die Wirtschaftskommission für Europa der Vereinten Nationen mit den Regulierungen UN-ECE R-155 (Cyber Security and Cyber Security Management System) und UNECE R-156 (Software Update Management System) stehen derzeit im Fokus der Automobilindustrie, da bei mangelnder Umsetzung ab Mitte 2022 für neue Fahrzeugtypen und ab Mitte 2024 für Typerweiterungen ein Zulassungsstopp zu erwarten ist.

Die Regularien bergen sowohl für Automobilhersteller als auch für die Zuliefer- und Dienstleistungsindustrie eine Fülle an neuen Herausforderungen – aber auch Chancen. Prozessuale und organisatorische Anforderungen, wie z. B. die Feldbeobachtung oder die Einführung von Cybersecurity- und Software-Update-Management-Systemen bedürfen neuer Kompetenzen, Denkweisen, Prozesse und Strukturen. Durch die verpflichtende Gültigkeit der UNECE R-155 und R-156 in mehr als 50 Ländern als Voraussetzung zur Homologation von Fahrzeugen und ähnliche zu erwartende Vorschriften in weiteren Kernmärkten (z. B. USA und China) erscheint die Nichteinhaltung der ab 2022 für neue Fahrzeugtypen und ab 2024 für alle Fahrzeugtypen gültigen Regulierung nicht als Option. Durch den steigenden Bedarf an Entwicklungs- und Testservices rund um das Thema Cybersecurity können sich jedoch auch Chancen ergeben, neue Geschäftszweige auf- und auszubauen und eine Vorreiterrolle einzunehmen.

Darüber hinaus existieren bzw. entstehen zahlreiche weitere, fachspezifische Normen, die das Thema Security primär oder im Zusammenhang mit weiteren Themen regeln. Insbesondere

für den Bereich des automatisierten bzw. autonomen Fahrens sind hier die Vorschrift UNECE R-157 Automated Lane Keeping Systems und die Norm ISO 4804 Safety and Cybersecurity for Automated Driving Systems zu nennen.

In Baden-Württemberg werden ein Viertel des Gesamtumsatzes der deutschen Automobilindustrie erwirtschaftet (Baden-Württemberg International 2021) – somit spielt eine fundierte und nachhaltige Betrachtung der Thematik eine wichtige Rolle. Über 300 Unternehmen sind in dieser Branche tätig, über 70 Prozent ihrer Umsätze sind exportorientiert. Weiterhin weist die Strukturstudie 2019 der e-mobil BW aus, dass etwa 11 Prozent aller sozialversicherungspflichtigen Arbeitnehmer:innen in Baden-Württemberg (rund 470.000 Personen) im Umfeld der Automobilindustrie tätig sind. Um auch in Zukunft diese hohe Anzahl an Arbeitskräften in der Branche beschäftigen zu können, ist es Konsens, dass der Industrie- und Wirtschaftsstandort Baden-Württemberg auch beim Thema Cybersecurity in der Automobilbranche nachhaltig eine führende Rolle anstreben und sich als Innovationscluster im stark wachsenden Markt für vernetztes Fahren und digitale Infrastruktur positionieren soll. Dafür ist es notwendig, neue Wertschöpfungspotenziale sowie prozessuale und technische Herausforderungen zu analysieren, um geeignete Maßnahmen für industriebezogene Anreizsysteme und bedarfsgerechte Kompetenzentwicklungsmöglichkeiten zu schaffen.

Um als Wirtschaftsstandort zukunftsfähig zu bleiben, ist es aus baden-württembergischer Sicht notwendig, das Thema Cybersecurity als relevantes Wirtschaftsfeld zu betrachten und basierend auf bestehenden Kompetenzen der ansässigen Wirtschaft gezielt zu entwickeln.

Weil die relevanten Regulierungen bereits in Kürze gelten werden, ist jedoch schnelles Handeln nötig, um mögliche negative Auswirkungen für die ansässige Industrie zu verhindern.

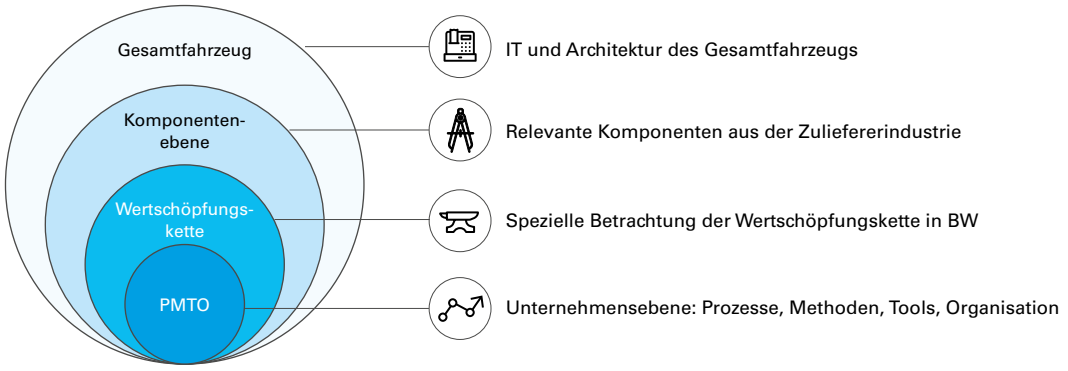
2.
Vorgehen und Aufbau des Themenpapiers

Die vorliegende Analyse soll einen umfassenden Überblick über die Relevanz von Automotive Cybersecurity in der Industrie geben und den Leser:innen konsistente Handlungsanleitungen an die Hand geben. Eine Erläuterung wichtiger in Fachkreisen verwendeter Abkürzungen und Begriffe ist im Stichwortverzeichnis (Seite 34) zu finden.

Dieses Papier dient der Einführung ins Thema. Die Zusammenhänge werden aus unterschiedlichen Perspektiven beleuchtet: von den technischen Rahmenparametern des Gesamtfahrzeugs über die Ebene der Unternehmen selbst bis hin zu Handlungsempfehlungen für Geschäftsprozesse. Zur Untermauerung der Ergebnisse wurden neben P3-internen Expert:innen auch Dr. Ingmar Baumgart vom Karlsruher Forschungszentrum Informatik (FZI) sowie Dennis Heusser vom Verband der Elektrotechnik Elektronik Informationstechnik e. V. (VDE) mit ihrer Expertise hinzugezogen.

Nach einer umfassenden thematischen Einleitung befasst sich das Themenpapier zuerst mit dem technischen Gesamt-Ökosystem des Fahrzeugs, analysiert grundsätzliche Gefahrenpotenziale und beleuchtet potenzielle Einfallstore von Cyberangriffen entlang des kompletten Lebenszyklus. Im zweiten Fokusteil des Papiers geht es speziell um die an der gesamten Fahrzeugwertschöpfung beteiligten Unternehmen. Mit einer Unterscheidung zwischen zuliefernder Industrie, automobilherstellenden Unternehmen und dem After-Sales-Markt wird versucht, speziell das automobile Unternehmensspektrum in Baden-Württemberg konsequent abzudecken. Entlang der automobilen Wertschöpfungskette analysiert das Papier dann dementsprechend die wichtigsten Fokusthemen für die betreffenden Branchen.

Im Schlussteil folgen Empfehlungen und Handlungsleitungen für die Unternehmen: Welche Schlüsse sollten gezogen werden, worauf muss besonders Acht gegeben werden, welche Regularien waren in dieser Form bisher noch unbekannt?



Quelle: eigene Darstellung

Abbildung 1: Struktur des Themenpapiers

3.
Einführung: Relevanz der Automotive Cybersecurity

Die Automobilindustrie befindet sich im größten Wandel ihrer Geschichte. Insbesondere die Digitalisierung von Geschäftsprozessen, das autonome und vernetzte Fahrzeug und der Einsatz neuer Antriebstechnologien sind Treiber des Wandels, der auf breiter Front etablierte Strukturen in der Automobilindustrie ändert. Mit dem Bedarf an neuen Strukturen und mit zunehmender Komplexität in Produkten, Dienstleistungen, Unternehmensstrukturen und Schnittstellen ergeben sich Potenziale, die Unternehmen und ihre Produkte anzugreifen. Mit dem Begriff Cybersecurity meint die Industrie konsequenterweise den allumfassenden Schutz jeglicher mit dem Internet verbundener Systeme, Software, Daten und Hardware gegen den Zugriff von Kriminellen. Vereinfacht lassen sich die einzelnen Disziplinen wie in Tabelle 1 dargestellt abgrenzen.

Exemplarische Zahlen aus Großbritannien zeigen, dass fast die Hälfte aller betrachteten Firmen (46 Prozent) und ein Viertel aller Wohltätigkeitsorganisationen im Vereinigten Königreich 2020 Cybersecurity-Attacken erlitten haben.[1] Auch die Automobilindustrie bleibt davon nicht verschont, wie das Beispiel des Ingenieurdienstleisters EDAG Engineering Group aus dem Frühjahr 2021 zeigt, bei dem aufgrund eines Hacker-Angriffes alle IT-Systeme heruntergefahren werden mussten, um sensible Kundendaten zu schützen.[2] Es zeigt sich also, dass die Security-Thematik direkten und nachhaltigen Einfluss auf den Geschäftsbetrieb hat.

Die Bedrohung richtet sich jedoch nicht nur gegen die Unternehmen im Allgemeinen, sondern greift auch auf deren Produkt, das Automobil, und damit auf die Endkundschaft über.

Cybersecurity	Schützt Fahrzeug-, Backend- und Servicefunktionen vor äußeren und funktionalen Einflüssen (z. B. Hackerangriff)
Funktionale Sicherheit	Schützt Fahrzeugnutzer:in und die Umwelt vor Fehlfunktionen des E/E-Systems des Fahrzeugs
Gebrauchssicherheit	Schützt Fahrzeugnutzer:in und Umwelt vor Gefahren durch reguläre Nutzung und vorhersehbare (Fehl-) Nutzung
SOTIF (Safety of The Intended Functionality)	Schützt Fahrzeug, Bediener:in und Umwelt vor den Auswirkungen falsch oder unzureichend konstruierter oder spezifizierter Funktionen

Tabelle 1: Disziplinen der Fahrzeugsicherheit

Quelle: eigene Darstellung

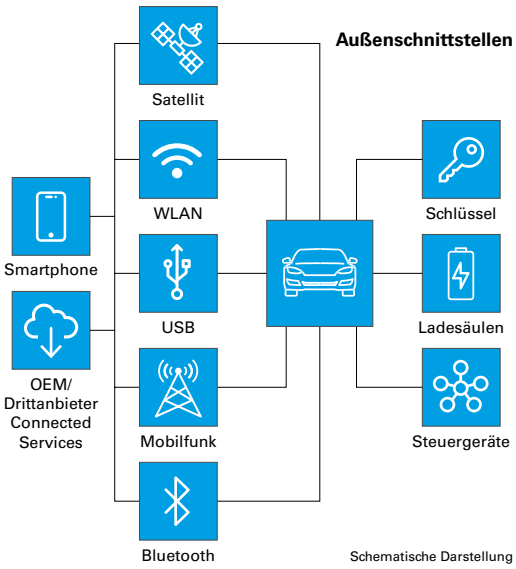
1 | *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/893399/Cyber_Security_Breaches_Survey_2020_Statistical_Release_180620.pdf*, Zugriff am 21.07.2021.

2 | *https://www.handelsblatt.com/unternehmen/industrie/cyberangriff-hacker-legen-autozulieferer-edag-lahm/27005604.html*, Zugriff am 21.07.2021.

Ein modernes Fahrzeug verfügt über eine Vielzahl von Kommunikationsschnittstellen – z. B. USB-Schnittstellen, die Smartphone-Anbindung via Bluetooth, WLAN, GPS, eine eigene SIM-basierte Internetverbindung inkl. App-Store, den Funkschlüssel oder die E-Ladesäule – und bietet so potenzielle Einfallstore für Manipulation und Schadsoftware. Im Vergleich zu „klassischen" Domänen der Cybersecurity sind im Bereich des Automobils weitaus mehr und vielseitigere Schnittstellen zu betrachten, die eine Absicherung dementsprechend erschweren und eine detaillierte Betrachtung der Thematik umso nötiger machen.

Dies gilt ebenso im Hinblick auf das mögliche Schadenspotenzial. Als Hauptrisiko kann die Gefährdung von Leib und Leben der Endkund:innen, aber auch von außenstehenden Dritten genannt werden. Im Extremfall können Angreifende auf alle Systeme des Fahrzeugs zugreifen und es durch einen Eingriff in die Längs- und Querführung zu einer Waffe, z. B. für einen Terroranschlag, werden lassen. Darüber hinaus bietet die Vernetzung des Fahrzeugs mit Internet und Mobiltelefon das Potenzial für den Verlust vertraulicher Daten. (Industrie-)Spionage durch Abhören ist dabei genauso vorstellbar wie z. B. der Verlust von Kreditkartendaten oder ein Identitätsdiebstahl. Die Liste der möglichen Schadenspotenziale ist lang und lässt sich in die folgenden Cluster einteilen: finanziell, materiell, Leib und Leben, rechtlich/Intellectual Property/Image. Die Vielzahl der möglichen Schadensszenarien unterstreicht die Wichtigkeit und den möglichen Einfluss des Themas Cybersecurity.

Heutige Fahrzeuge verfügen über einen **hohen Vernetzungsgrad** und ein stetig wachsendes Angebot an Funktionen zur Verbesserung des Fahrerlebnisses



Die große Vielfalt an Funktionen und Konnektivität führt zu einer **größeren Systemkomplexität,** die das Fahrzeug anfällig für bösartige Cyberangriffe macht.

Die Relevanz dieser Problematik wächst mit dem Aufkommen von **autonomen Fahrzeugfunktionen,** deren Sicherheit und Zuverlässigkeit nur durch korrekte Funktionalität ihrer digitalen Systeme sichergestellt werden kann.

Quelle: eigene Darstellung

Abbildung 2: Außenschnittstellen eines Fahrzeugs

4.
Technische Betrachtung: Fahrzeug-Ökosystem und Lebenszyklus

4.1 Neue Herausforderungen durch wachsende Relevanz der Cybersecurity im Fahrzeug

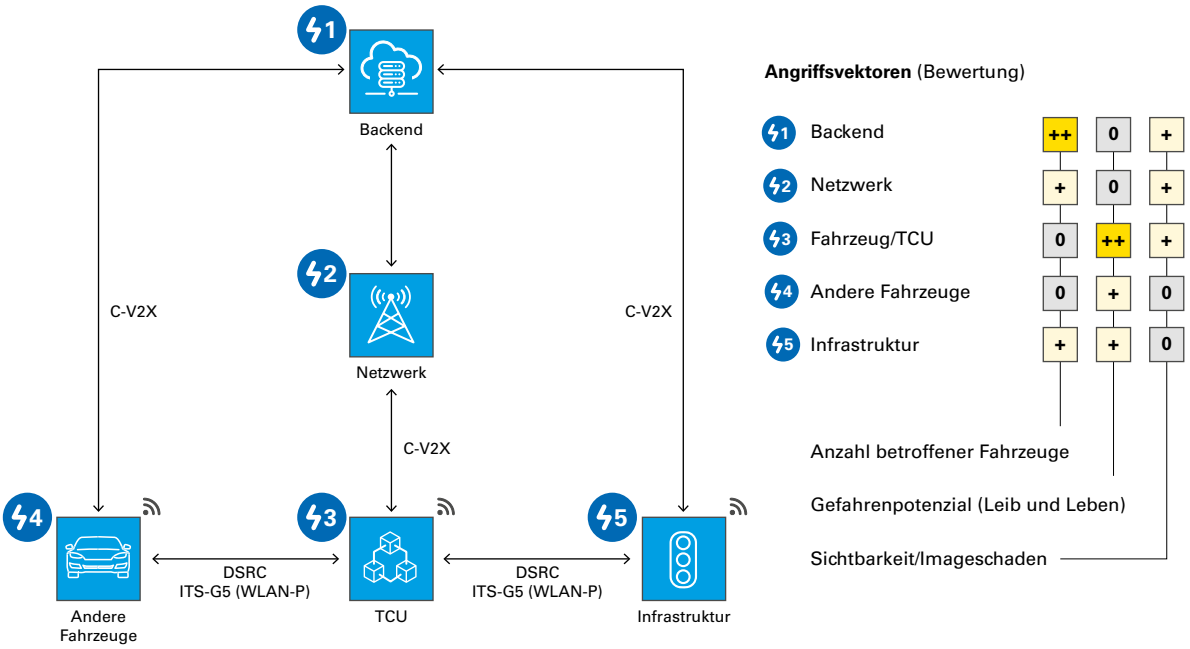
Der bewusste Umgang mit Cybersecurity im Fahrzeug wird in der Automobilindustrie erst seit wenigen Jahren vorangetrieben und Mitarbeiter:innen werden mit hoher Dringlichkeit für das Thema sensibilisiert. Dabei führen die zunehmend komplexeren Fahrzeuge mit ihrer erhöhten Konnektivität dazu, dass auch die Risiken eines nicht autorisierten Zugriffs wachsen. Insbesondere bezüglich Vehicle-to-X (V2X)-Kommunikation verfügen Fahrzeuge im Gegensatz zu vielen anderen „klassischen" Domänen der Cybersecurity über weitaus mehr und vielseitigere Schnittstellen, die potenziell Angriffe ermöglichen (SIM, WLAN, Bluetooth, USB, Funkschlüssel, Diagnoseschnittstelle usw.). Zudem befindet sich in einem modernen Fahrzeug eine Vielzahl an Steuergeräten (mitunter über 100), die miteinander kommunizieren, um Mehrwert für die Kund:innen zu schaffen und gewünschte Funktionen zu realisieren. Obwohl Hersteller an einer zentralisierten E/E-Architektur mit High-Performance-Computing-Plattformen arbeiten, erhöht die historisch gewachsene dezentrale E/E-Architektur jedoch die Komplexität und erschwert eine Absicherung der zahlreichen Kommunikationskanäle gegen Angriffe wie Sniffing und Spoofing. Eine Einschränkung der Angriffsvektoren, also der Konnektivität, ist vor dem Hintergrund neuer digitaler Geschäftsmodelle keine denkbare Option, vielmehr sind z. B. OTA-Software-Updates und V2X-Kommunikation ein Muss im kompetitiven Umfeld. Grundsätzlich ist es möglich, dass softwarerelevante Sicherheitsmechanismen durch eine Manipulation beeinträchtigt werden und die Maßnahmen zur Sicherstellung der funktionalen Sicherheit durch einen externen Einfluss unterlaufen werden. Diese breite Angriffsfläche resultiert, in Kombination mit dem zunehmenden Verbau von Technologien des automatisierten Fahrens, in einem hohen Risiko für schwerwiegende Folgen bei Cyberattacken, wenn die Mechanismen der funktionalen Sicherheit durch Kriminelle überwunden werden.

Neben dem Datenaustausch mit der Umwelt stellen insbesondere die Vielzahl an Steuergeräten im Fahrzeug sowie deren Verknüpfung in diversen Kommunikationsnetzwerken essenzielle Herausforderungen dar.

Durch die Vielzahl an zuliefernden Unternehmen für Hard- und Software der eingebetteten Systeme ist allein die Vermeidung von absichtlich und unabsichtlich entstandenen Sicherheitslücken im Fahrzeug – und zwar über den gesamten Produktlebenszyklus hinweg – eine enorme Herausforderung.

Neben präventiven Security-Maßnahmen haben auch detektivische und reaktive Aspekte eine tragende Rolle in der Sicherstellung der Cybersecurity im Ökosystem moderner Fahrzeuge; Cyberattacken müssen in Echtzeit erkannt werden, damit vordefinierte Fall-back-Routinen effektiv zur Abwehr der Angriffe aktiviert werden können.

Die UNECE hat daher neue Regelungen aufgesetzt, die im Wesentlichen die Überwachung von Fahrzeugen anhand von Security Updates, ein ausgiebiges Risikomanagement sowie das Erkennen und Behandeln von Cyberbedrohungen für Fahrzeuge und deren Daten- und Telematik-Dienste über ihren gesamten Lebenszyklus verlangen.



Quelle: eigene Darstellung

Abbildung 3: Bewertung des Gefahrenpotenzials verschiedener Angriffsvektoren

Im Rahmen der Automotive Cybersecurity geht es regelmäßig um hohe Risiken für Leib und Leben: Kein anderes Produkt, das im alltäglichen Leben in einer solchen Vielzahl vertreten ist, birgt derart hohe Gefahrenpotenziale für Leib und Leben im Falle eines Hackerangriffs. Deshalb ist es wichtig, die potenziellen Einfallstore hinsichtlich ihrer zu erwartenden Auswirkungen zu klassifizieren (siehe Abbildung 3). Die Anforderungen an die Cybersecurity sind dementsprechend hoch, das bedeutet folglich erhöhten Aufwand bei steigender Bewertung.

Im Vergleich zur „klassischen" IT, die sich vorwiegend mit der Sicherheit von Unternehmensnetzwerken, VPN-Verbindungen, On-Premise-Servern und Cloud Solutions auseinandersetzt, sind moderne Automobile und ihre Ökosysteme darüber hinaus mit der Sicherstellung der Cybersicherheit von Embedded Systems, Sensor-Systemen, Telekommunikation und z. B. Schnittstellen wie Ladebuchsen an E-Fahrzeugen konfrontiert. Kritische Systeme können im Bereich der klassischen IT gekapselt werden (z. B. befinden sich Server in Unternehmen möglichst in separaten Netzwerken, die durch Firewalls getrennt sind). Insbesondere Verbindungen ins World Wide Web werden, wenn möglich, vermieden. Für Automobile steht die Reduzierung potenzieller Einfallstore im Zielkonflikt mit „Connected Car"-Funktionalitäten und dem Trend hin zum autonomen Fahren.

Automobile in Kundenhand können nur OTA dauerhaft und zeitnah mit sicherheitsrelevanten Software-Updates versorgt werden, da den Kund:innen zu häufige Werkstattaufenthalte nicht zu vermitteln sind. OTA-Software-Updates als potenzielles Einfallstor sind folglich unvermeidbar. In der klassischen IT ist der Zugriff auf die Systeme meist dauerhaft gewährleistet. Der Zugang zur Hardware ist bei Automobilen ungleich leichter als bei der IT-Infrastruktur, z. B. auf Betriebsgeländen; insbesondere Serverräume sind hinsichtlich „Physical Access Control", also physischem Eindringen, klar besser geschützt als Automobile. Eine besondere Herausforderung ist die Sicherstellung der Cybersicherheit über eine Lebensdauer von 15 Jahren, da der technologische Fortschritt das Hacken veralteter Hardware deutlich erleichtert; das Risiko und gleichzeitig das Schadenpotenzial der Nutzer:innen ist im Falle eines unsicheren Fahrzeugs deutlich höher. Eine Kapselung in einem sicheren, kabelgebundenen Netzwerk, wie z. B. bei alten Produktionssteueranlagen, kann für Automobile jedoch nicht realisiert werden. Das könnte auch erheblichen Einfluss auf die Hardware in den Fahrzeugen haben, da für zukünftige Security-Updates „Puffer" notwendig sein könnten. Dies bedeutet,

dass beispielsweise Vorhalte für Speicherplatz und Rechenleistung in einzelnen Steuergeräten oder der Vorhalt eines Komponentenaustauschs gesichert sein müssen, falls verbaute Komponenten nach einem gewissen Zeitraum ein Sicherheitsrisiko darstellen sollten. Dies könnte zu höheren Kosten führen, die einkalkuliert und an anderer Stelle ausgeglichen werden müssen. Zudem muss eine Vielzahl von zuliefernden Unternehmen die Aktualität der Software einzelner Steuergeräte über diesen langen Zeitraum gewährleisten. Weitere Herausforderungen, denen sich Unternehmen hier zu stellen haben, sind:

- Optimierung der Datenmenge
- Optimierung der Analyse
- Personalplanung und Vermeidung von Personal- und Fachkräftemangel
- Sicherstellung der Optimierung automatisierter und manueller Analyse
- Threat Intelligence (schnellere Abwendung von Cyberangriffen)
- klare Identifikation der betroffenen Datenquelle
- Produktlebenszyklus (Gewährleistung bis zum Ende des Software-Lebenszyklus)
- Regulatorik (Multi-Compliance-Ansatz zur Bewältigung des regulatorischen Aufwands)

Durch die starke Verbreitung von Automobilen im täglichen Leben, ihre große Stückzahl und Verfügbarkeit ergeben sich Unterschiede zu anderen Branchen und Produkten.

Die Sensibilität moderner Automobile bezüglich der Datenschutz-Aspekte ist vergleichbar mit der von Unterhaltungs- und Verbraucherelektronik, da durch das Hacken eines Fahrzeugs oder Sicherheitslücken einer Fahrzeugbaureihe potenziell eine großflächige Verletzung von Persönlichkeitsrechten im Bereich der informationellen Selbstbestimmung denkbar ist – durch die Vernetzung mit dem Smartphone und Internet of Things (IoT) können gegebenenfalls sogar weitere Daten über eine Sicherheitslücke im Auto abgegriffen werden. Sowohl das Umfeld von Fahrzeugen kann betroffen sein – durch die vorhandenen Außenkameras – als auch einzelne Fahrer:innen durch die im Fahrzeug erhobenen Daten (Bewegungsprofile etc.).

Auch der Blick auf eine weitere Industrie des Mobilitätssektors, die Flugindustrie, lohnt sich in diesem Zusammenhang. Aufgrund der weniger starken Präsenz von Flugreisen in unserem täglichen Leben sind die Risiken von Flugzeugen für die informationelle Selbstbestimmung im Vergleich deutlich geringer zu bewerten. Bezüglich der potenziellen Gefahren für Leib und Leben, analog zu den Inhalten, mit denen sich die funktionale Sicherheit befasst, haben aber auch die Luftfahrzeuge herstellenden Firmen ein erhöhtes Interesse, ihre Beförderungsmittel gegen Cyberrisiken abzusichern. Genauso wie im Automobilbereich müssen sich diese Unternehmen durch die ständig voranschreitende Entwicklung hin zu E/E-Systemen immer stärker mit der Informationssicherheit auseinandersetzen. Da Flugzeuge einen ähnlich langen Lebenszyklus wie Fahrzeuge aufweisen, geht damit einher, dass Systeme mit der Zeit veralten und für Angriffsszenarios anfälliger werden. Vorteilhaft für die Luftfahrt ist jedoch, dass der physische und digitale Zugang zu ihren Maschinen im Vergleich zum Automobil deutlich erschwert ist. Wie auch der Autoverkehr bewegen sich die zu überwachenden Gegenstände einer Fluggesellschaft, die Flugzeuge, grenzüberschreitend, weshalb ein Stör- und Notfallmanagement enorme Kapazitäten und Fähigkeiten benötigt. Parallelen liegen dabei nicht nur in der globalen Verteilung der zu überwachenden Posten, sondern auch in den IT-Systemen. Fluggesellschaften bieten heutzutage ebenfalls einen externen Internetzugang für die Passagiere an, was wiederum dazu führt, dass die steigende Konnektivität als Angriffsvektor auf die IT-Systeme des Flugzeugs dienen könnte. Auch im Flugverkehr werden Passagiere befördert, die in Folge eines sicherheitsrelevanten Ereignisses einem hohen Risiko ausgesetzt sind. Ebenso wie in der Automobilindustrie gelten in der Luftfahrt Regularien, die in aktuellen Avionik-Systemen zum Beispiel die Protokollierung von Sicherheitsereignissen fordern. Anders als es die UNECE WP.29 für Fahrzeuge verlangt, wird für Flugzeuge aber noch keine Echtzeit-Überwachung vorausgesetzt.

Natürlich ist die geforderte Sicherheit für Flugzeugsysteme ähnlich, auch durch die gesellschaftliche Erwartung an dieses Ökosystem. Viele Passagiere fühlen einen Kontrollverlust innerhalb eines Flugzeugs und vertrauen ihm weniger im Vergleich zu einem Automobil, in dem der bzw. die Fahrer:in das Steuer noch selbst in der Hand hält. Dabei verwenden Flugzeughersteller gar bis zu fünf parallele Steuersoftwaresysteme, die alle von unterschiedlichen Softwareherstellern zur Verfügung gestellt werden und so das Risiko verteilen sollen.

Der Austausch der Sicherheitsexpert:innen über die Branchengrenzen hinweg muss daher in den kommenden Jahren intensiviert werden, um Erfahrungen und Abwehrprinzipien beim gemeinsamen Kampf gegen Cyberangriffe auszutauschen und deren Effektivität und Effizienz auf das geforderte Niveau zu bringen.

Die Automobilindustrie steht exemplarisch für alle Industrien, die diverse, teils gegenläufig erscheinende Herausforderungen zu den Themen funktionale Sicherheit und Datensicherheit bewältigen müssen.

4.2 Risiken und Einfallstore für einen Cyberangriff entlang des Produktlebenszyklus

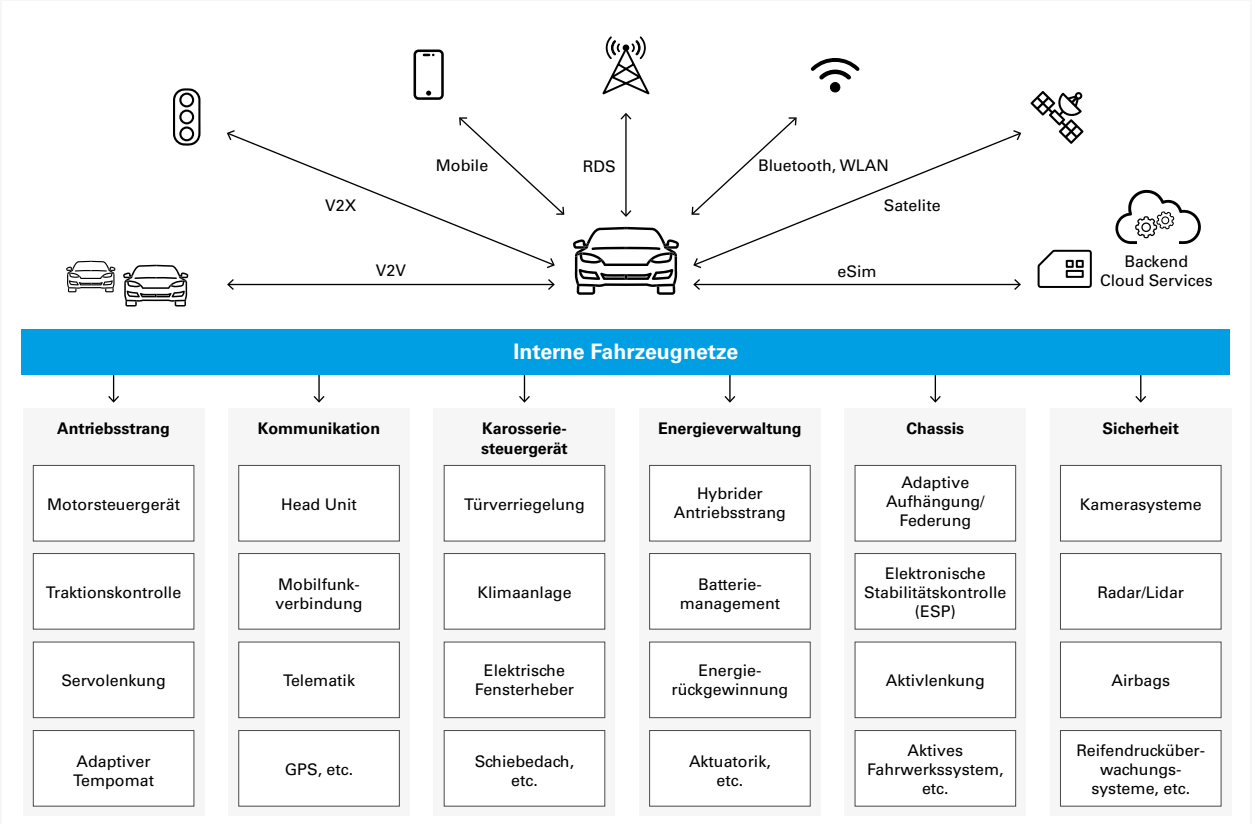
Um hochintegrierte Kundenfunktionen zu realisieren, sind moderne Fahrzeuge durch zahlreiche Schnittstellen und einen hohen Vernetzungsgrad innerhalb des Bordnetzes und darüber hinaus geprägt. Bedingt durch den hohen Vernetzungsgrad ergibt sich ebenfalls eine hohe Systemkomplexität, die im Widerspruch zu funktional und informationell sicheren Fahrzeugen steht. Um diesen Widerspruch aufzulösen, ist ein breiter Trend zur Steigerung der Systemintegration erkennbar, der u. a. die Anzahl an Schnittstellen und Einfallstoren mindern soll. Jedoch resultiert aus der zunehmenden Zentralisierung von Funktionen auch ein erhöhter Schweregrad der Angriffsszenarien.

Die untenstehende Abbildung zeigt eine ganze Reihe potenzieller Angriffskanäle, die das moderne vernetzte Fahrzeug Kriminellen über seine Schnittstellen bietet.

Die potenziellen Angriffskanäle lassen sich zusammenfassen als Angriffe auf lokale Schnittstellen des Fahrzeugs, Angriffe über das Backend/Ökosystem, das Mobilfunknetz und „Point-to-Point"(P2P)-Verbindungen.

Schnittstellen und Einfallstore können an zahlreichen Stellen des Fahrzeug-Systemverbundes und des Fahrzeug-Ökosystems entstehen, die unterschiedliche Risikograde in Bezug auf die Anzahl der betroffenen Fahrzeuge, das Gefahrenpotenzial für Leib und Leben und die Sichtbarkeit bzw. den Reputationsschaden des Herstellers haben können.

Zu den lokalen Fahrzeugschnittstellen gehören insbesondere OBD-, Bluetooth- und WLAN-Schnittstellen zur Integration von Infotainment-Funktionen unter Einbezug weiterer Geräte der Fahrzeugnutzer:innen. Weniger offensichtlich sind weitere Diagnoseschnittstellen einzelner Steuergeräte (z. B. JTAG) als auch die Möglichkeit von „Man-in-the-Middle"-Attacken im



Quelle: eigene Darstellung

Abbildung 4: Externe Einflüsse auf das Fahrzeug-Netzwerk

Bordnetz bei nicht ausreichender kryptografischer Härtung der Onboard-Kommunikation. Lokale Attacken haben das höchste Schadenspotenzial für Leib und Leben, setzen jedoch physischen Zugriff oder Nähe zum Fahrzeug voraus.

Mit zunehmender Verbreitung von V2X-Anwendungen rücken P2P-Verbindungen vermehrt in den Fokus von Sicherheitsbetrachtungen. Diese können zwischen einzelnen Fahrzeugen oder zwischen Fahrzeugen und Infrastruktur aufgebaut werden. Hierzu werden Technologien wie WLAN-P und „Cellular P2P" eingesetzt. Mit zunehmender Mobilität der Verkehrsteilnehmer:innen steigt die Zahl der Kommunikationskontakte, sodass einzelne manipulierte Teilnehmer:innen in kurzer Zeit Verbindung zu zahlreichen weiteren Teilnehmer:innen aufbauen können. Die tiefe Integration von V2X-Funktionen in den Fahrzeug-Systemverbund und den Einfluss von V2X-Anwendungen auf das Fahrzeugsystemverhalten machen P2P-Schnittstellen zu attraktiven Einfallstoren für Angriffe mit erheblichem Schadenspotenzial.

Über die Mobilfunkverbindung können erhebliche Teile von Fahrzeugflotten angegriffen werden. Hierzu stehen verschiedene Generationen an Kommunikationsprotokollen zur Verfügung, die teilweise veraltete Sicherheitsstandards nutzen. Die fahrzeugspezifischen Rahmenbedingungen, wie z. B. eingeschränkte Konnektivität und Beschränkungen des Ruhestroms, erfordern den Einsatz von Steuerungsprotokollen, wie z. B. OMA Device Management (OMADM) zum Aufwecken einzelner Steuergeräte. Auch wenn erhebliche Teile von Fahrzeugflotten über Netzwerke angegriffen werden können, ist aufgrund der fahrzeuginternen Kapselung von einem geringeren Schadenspotenzial als bei Angriffen über die anderen hier genannten Kommunikationskanäle auszugehen.

Insbesondere mit der Einführung von autonomen und assistierten Fahrfunktionen werden Backend-Systeme integraler Bestandteil des Fahrzeug-Systemverhaltens. Exemplarisch sind hier das Training von neuronalen Netzen für das autonome Fahren im Backend und OTA-Updates zu nennen. Angriffe über das Fahrzeugbackend stellen eine Gefahr für gesamte Fahrzeugflotten dar. Daher ist durch spezifische Maßnahmen der Durchgriff aus dem Backend auf kritische Systemanteile im Fahrzeug zu vermeiden und eine Überwachung des Backends und der Fahrzeuge in Bezug auf Vulnerabilitäten und Störungen zu realisieren. Die UNECE R-155 schreibt geeignete Maßnahmen zur Abwendung dieser Angriffsszenarien vor.

Die genannten V2X-Technolgien führen in Verbindung mit den steigenden Absatzzahlen vernetzter Automobile dazu, dass die Menge an generierten Daten und Eintrittspunkten unbedingt auch ein erhöhtes Potenzial für unterschiedlichste Arten von Hackerangriffen zur Folge hat. Unter anderem könnten fremde Nationen durch eine Überwachung die nationale Sicherheit gefährden oder politische Aktivist:innen ihre potenziellen Ziele ausspähen. Weitere Motivationsmöglichkeiten neben terroristischen Risiken sind aber auch forschende Erkenntnisse von Whitehat-Hackern, die sich darüber definieren, einen gemeinnützigen Zweck zu verfolgen. Zählt man all diese verschiedenen Arten von Attacken zusammen, könnte man schlussfolgern, dass die Mehrzahl von Cyberattacken auf die Fahrzeugindustrie in den letzten Jahren keinesfalls zufälliger Natur war. Es lässt sich allerdings lediglich vermuten, welche kriminellen Ideen ganz grundsätzlich als Motivation zugrunde lagen. Klar ist jedoch auf jeden Fall eines: Daten sind in der heutigen Zeit, auch in der Welt der Automobile, zur Schlüsselressource aufgestiegen und müssen dringend gut geschützt werden.

Da mögliche Schnittstellen bzw. der Zugriff auf sie und entsprechende Angriffsszenarien über den Produktlebenszyklus sehr verschieden sein können, gehen wir im Folgenden konkret auf einzelne Lebenszyklusphasen ein. Dabei wollen wir beispielhaft Schnittstellen und Einfallstore beschreiben, wie sie in der Entwicklung, der Produktion und Logistik und im Feld typisch sind.

4.2.1 Entwicklung

Grundsätzlich bietet die Fahrzeugentwicklung das größte Einflusspotenzial, um Cyberangriffe auf Fahrzeuge durchzuführen oder vorzubereiten. Beispielsweise, indem gezielt Einfallstore für einen späteren Angriff in die Fahrzeuge eingebracht werden. In der Entwicklung besteht theoretisch direkter Zugriff auf sämtliche Hard- und Software eines Fahrzeugs, dadurch sind die Möglichkeiten für einen Angriff sehr zahlreich und die Anzahl betroffener Fahrzeuge und der mögliche resultierende Schaden ist enorm. Allerdings sind insbesondere die Entwicklungsbereiche in der Automobilindustrie bereits heute in der Regel gut gesichert (Gebäudezutritte, Toolzugriffe etc.) und üblicherweise durchläuft die Entwicklung mehrere Test- und Iterationsschleifen, bei denen mutwillige Manipulationen entdeckt werden können. Zusammen mit dem notwendigen, umfangreichen Expertenwissen über Entwicklungsprozesse, Systeme, Komponenten etc. erscheint ein gezielter Angriff auf Kundenfahrzeuge in der Entwicklung eher unwahrscheinlich.

Ein mögliches Ziel für direkte Angriffe in der Entwicklung könnten Prototypen und Erprobungsfahrzeuge sein, die noch nicht über serientaugliche Sicherheitsmechanismen verfügen und damit theoretisch ein leichteres Ziel darstellen als spätere Serienfahrzeuge. Die geringe Anzahl an Fahrzeugen und die stärkere Beobachtung insbesondere außerhalb der Werksgelände erschweren in diesem Szenario allerdings einen Angriff.

Ein wahrscheinlicheres, aktives Angriffsszenario in der Entwicklung ist die gezielte Informationsbeschaffung über Fahrzeuge und deren mögliche Schwachstellen durch Infiltration des Unternehmensnetzwerkes. Auf diesem Wege könnten sensible Informationen beschafft werden, um spätere Angriffe auf Fahrzeuge zu planen und durchzuführen. Die Sicherung der Unternehmensnetzwerke steht im Rahmen dieses Themenpapiers aber nicht im Fokus, daher sei dieser Punkt nur kurz angerissen. Er verdeutlicht aber, dass Automotive Cybersecurity und die Sicherheit der Fahrzeuge eng mit der Cybersecurity der Unternehmensnetzwerke zusammenhängen.

Das größte Einfallstor für Cyberangriffe in der Entwicklung ist der Entwicklungsprozess selbst. Zwar sind aktive Angriffe aufgrund oft bereits bestehender Hürden eher unwahrscheinlich, aber im Laufe des Entwicklungsprozesses können aus unterschiedlichsten Gründen Schwachstellen in das Fahrzeug integriert werden, die für einen späteren Angriff ausgenutzt werden können. Zu nennen sind hierbei Fehler im Code, fehlende Verschlüsselungen, veraltete oder zu leistungsschwache Hardware, Software von Drittanbietern und vieles mehr. Deswegen muss es das Ziel der Entwicklung sein, mögliche Schwachstellen zu kennen und bestmöglich zu vermeiden. Der Entwicklungsprozess sollte so gestaltet sein, dass mögliche Bedrohungen und Schwachstellen identifiziert werden, z. B. über externe Quellen wie Datenbanken, Konferenzen oder Foren, aber auch interne Quellen wie Rückmeldungen aus dem Feld. Darauf basierend sollte konkret für alle Bestandteile des Fahrzeugs analysiert werden, ob diese ein mögliches Risiko für die Cybersecurity darstellen. Erkannte Risiken sollten analysiert und durch geeignete Maßnahmen auf ein vertretbares Restrisiko gemindert werden. Die UNECE R-155 in Kombination mit der ISO 21434 bietet eine gute Orientierung, wie ein solcher Entwicklungsprozess gestaltet werden sollte, um ein Höchstmaß an Cybersecurity in der Entwicklung zu gewährleisten.

4.2.2 Produktion

Die Produktion stellt eine weitere Phase im Produktlebenszyklus eines Fahrzeugs dar, in der Schnittstellen und Einfallstore für Cyberangriffe bestehen und ausgenutzt werden könnten. Im Vergleich zur Entwicklung sind hier die Sicherheitsvorkehrungen üblicherweise deutlich weniger restriktiv, d. h. insbesondere der physische Zugriff auf Fahrzeuge und/oder deren Steuergeräte ist auch für Unbefugte deutlich einfacher. Zudem durchlaufen Fahrzeuge in der Produktion aufgrund des späteren Zeitpunkts im Lebenszyklus deutlich weniger Test- und Prüfschleifen als dies in der Entwicklung der Fall ist, wodurch Manipulationen am Fahrzeug schwieriger erkannt werden können. Es ist allerdings wichtig, an diesem Punkt zwischen unabsichtlichen Fehlern und aktiven Angriffsszenarien durch kriminelle Angestellte zu unterscheiden. Unabsichtliche Fehler passieren offensichtlich regelmäßig in Produktionsprozessen und ziehen dann jeweils feste Prozesse der Bekämpfung und Abwendung der jeweiligen Konsequenzen nach sich – zumindest im Idealfall. Grundsätzlich ist an dieser Stelle zu erwähnen, dass es den entsprechenden Firmen ein wichtiges Anliegen sein sollte, alle betreffenden Produktionsmitarbeiter:innen auf die speziellen Risiken der Cybersecurity, die Einfallstore und mögliche Schwachstellen und vor allem den Umgang mit Problemen ausreichend zu trainieren. Eine gute Handlungsanleitung bieten hier die bereits erwähnten ISO-Normen. Da absichtliche Manipulationen aller Art an verschiedenen Punkten im Produktionsprozess möglich sind, werden diese im Folgenden genauer betrachtet.

Mögliche Einfallstore in der Produktion sind sehr vielfältig. Theoretisch können Angreifende über die gleichen Schnittstellen Zugriff auf ein Fahrzeug oder eine Reihe von Fahrzeugen erlangen, wie es auch im Feld möglich ist, d. h. physisch beispielsweise über OBD-Software oder aus der Ferne, sofern entsprechende Schnittstellen wie WLAN oder Mobilfunk im Fahrzeug bereits während der Produktion aktiv sind. Darüber hinaus könnten in der Produktion auch gezielt zusätzliche Komponenten in das Fahrzeug eingebracht werden, die einen späteren Angriff ermöglichen oder unterstützen können, indem z. B. die CAN-Kommunikation abgefangen oder „Man-in-the-Middle"-Angriffe initiiert werden. Es könnten auch Bauteile platziert werden, die z. B. gezielt Sensoren beeinträchtigen und damit unbrauchbar machen oder falsche Daten erzeugen. Genauso könnten theoretisch Bauteile entfernt oder Verbindungen unterbrochen werden.

Es ist auch denkbar, direkt Bauteile in der Produktion zu manipulieren oder auszutauschen, während sich diese im Lager oder auf dem Transportweg von einem zuliefernden Unternehmen befinden. Einzelne Bauteile oder ganze Chargen könnten auf diesem Weg zu einem Einfallstor für spätere Angriffe im Feld werden. Auch während der Produktion sind einzelne Bauteile oder ganze Fahrzeuge oft für längere Zeiträume gegen unbefugten Zugriff nur unzureichend geschützt, wenn z. B. Fahrzeuge für die Nacharbeit geparkt werden. Ähnliches gilt für den Transport produzierter Fahrzeuge zum Handel oder zur Kundschaft.

Des Weiteren ist auch eine Manipulation von Fahrzeugen in der Produktion mit dem Ziel eines späteren Angriffs absolut denkbar. Mit dem nötigen Wissen über die produzierten Fahrzeuge könnten z. B. unbemerkt kleine Bauteile in die Produktion eingeschleust werden, die in der Montage nicht weiter auffallen, aber bspw. für aktive Angriffe genutzt werden oder Steuergeräte/Sensoren stören könnten. Außerdem sind z. B. Steuergeräte in der Produktion oft so präsent, dass sie unauffällig mitgenommen und manipuliert oder ausgetauscht werden könnten. Auch hier ist aber umfangreiches Wissen über die zu manipulierenden Produktionsprozesse nötig, um zu wissen, wie und was manipuliert werden kann, damit es bei späteren Prozessschritten nicht erkannt wird. Mit Zugriffen auf Systeme, die Steuergeräte programmieren, können theoretisch auch direkt an dieser Stelle Angriffe erfolgen.

Steuergeräte- und bauteilherstellende Unternehmen werden durch die UNECE R-156 in die Verantwortung genommen, entsprechende Software-Update-Management-Systeme zu implementieren, um homologationskonforme Produkte zu entwickeln. Mit dieser Regulierung werden Software-Identifikationsnummern „RxSWIN“ eingeführt (Rx steht in diesem Fall für das regulierte Bauteil mit der Nummer x, SWIN ist die Abkürzung für „Software Identification Number“). Mit dieser fortlaufenden RxSWIN wird sichergestellt, dass nur homologisierte Software auf die verbauten Steuergeräte gespielt ist. In weiterer Folge sind fahrzeugherstellende Unternehmen und solche aus dem After-Sales-Bereich in der Lage, den Softwarestand von einzelnen Fahrzeugen bis hin zu Flotten zu erheben, gezielt Updates in das Feld auszuspielen oder manipulierte Software zu erkennen.

4.2.3 Fahrzeug im Feld

Über den Fahrzeuglebenszyklus sind sowohl Schwachstellen als auch Störungen zu identifizieren und geeignet abzuschwächen. Aktuell hat sich keine einheitliche Meinung etabliert, wie lange die Hersteller zur Bereitstellung von Updates verpflichtet sind. Es werden mögliche Einschränkungen des Supportzeitraums entsprechend der Ersatzteilversorgung bzw. in Abhängigkeit von den Supportzeiträumen der Connected Services diskutiert. Zusätzlich stellt sich die Herausforderung, dass möglicherweise ein Vorrat an einschlägiger Hardware eingeplant werden muss, um zukünftige Security Features bei veränderter Bedrohungslage jederzeit bereitstellen zu können. Andernfalls besteht das Risiko, dass relevante Steuergeräte unter erheblichen Kosten getauscht werden müssen – sofern dies für Bauteile der neuen 5G-Generation technisch überhaupt möglich ist.

Schwachstellen werden anhand öffentlicher Quellen, z. B. der CVE-Datenbank des National Institute of Standards and Technology (NIST), identifiziert. Basierend auf diesen Informationen sind die Relevanz für die eingesetzten Komponenten und das Risiko für den automobilen Anwendungsfall zu bestimmen. Die Bewertung ermöglicht die Festlegung geeigneter Maßnahmen in Form von Software-Updates oder Änderungen für laufende und zukünftige Entwicklungsvorhaben. Die Verfahren zur Identifikation und Bewertung von Schwachstellen werden jeweils im Asset Management des jeweiligen Unternehmens zusammengefasst.

Auch für die Überwachung von Störungen und aktiv ausgenutzten Schwachstellen sind teilweise gänzlich neue Überwachungsstrukturen zu etablieren. Diese Strukturen erzeugen neue organisatorische und technologische Anforderungen. In Bezug auf die Organisation sind Organisationseinheiten, Prozesse und Methoden zur Etablierung der Security Operations aufzubauen. Die Überwachung von Fahrzeugen kann über die Analyse der Fehlerspeicher erfolgen, in denen Störmeldungen basierend auf der Analyse deterministischer Angriffsmuster hinterlegt werden. Als bevorzugte Variante sind hier allerdings dedizierte Angriffserkennungssysteme in den Fahrzeugen zu empfehlen, da diese Systeme flexibel auf nicht deterministische Angriffe reagieren können und zumeist eine Online-Verbindung zur zentralisierten Konsolidierung der Analyseergebnisse aus der Fahrzeugflotte besitzen. In ähnlicher Weise sind nicht nur die Fahrzeuge selbst, sondern auch deren Ökosysteme zu überwachen.

Durch den Einsatz von Software-Updates stellt sich zusätzlich die Herausforderung, dass ein zertifizierungsfähiges Fahrzeugverhalten auch bei zahlreichen Änderungen über den gesamten Fahrzeuglebenszyklus aufrechterhalten werden muss. Mit

steigender Anzahl der Updates steigt die Anzahl der im Feld befindlichen Fahrzeugkonfigurationen exponentiell. So sind Angriffe auf das Fahrzeug nicht nur über die Mobilfunkschnittstelle zu erwarten, sondern auch über die übrigen Kommunikationsschnittstellen des Fahrzeugs. Die wachsende Bedeutung der direkten Kommunikation des Fahrzeugs mit seiner Umgebung und deren Terminologien werden in Tabelle 2 erläutert.

Grundsätzlich ist festzuhalten, dass das automobile Umfeld eine besondere Herausforderung in Bezug auf das Hardening von Fahrzeugen darstellt. Gegenüber anderen Industrien ist die Automobilwirtschaft durch außergewöhnlich hohe Komplexität sowohl hinsichtlich der Produktstrukturen als auch in Bezug auf die Wertschöpfungsnetzwerke geprägt. Darüber hinaus liegt während der Nutzung oft eine eingeschränkte Konnektivität vor, was die Überwachung, die Bereitstellung von Software-Updates und den Einsatz von zentralen Zertifizierungsstellen erschwert.

Generell lassen sich viele Angriffsszenarien auf Fahrzeuge und deren Ökosystem übertragen. Diese Angriffsszenarien sind in zahlreichen Katalogen gelistet und bewertet (z. B. MITRE, OWASP). Darüber hinaus wurde durch die WP.29 der UNECE der ANNEX 5 der UNECE R-155 zu Cybersecurity Management Systems erarbeitet. Dieser Katalog stellt typische Angriffsszenarien für den automobilen Anwendungsfall dar und kennt sieben Angriffskategorien, siehe Tabelle 3.

Bisherige Geschäftsmodelle in der Automobilindustrie waren insbesondere fokussiert auf die Generierung von Umsätzen durch den Absatz von Fahrzeugen. Mit zunehmender Verbreitung von Connected-Car-Technologien ergeben sich neue Möglichkeiten sowohl zur nachträglichen Bereitstellung neuer Kundenfunktionen als auch zur Analyse des Nutzerverhaltens, um kundenspezifische Angebote zu gestalten. Die zunehmende Fokussierung auf den gesamten Produktlebenszyklus produziert neue Herausforderungen auch in Bezug auf die Cybersecurity.

Abk.	Begriff	Erklärung
V2X	Vehicle to Everything	V2X bezeichnet den Datenaustausch und jede Kommunikation zwischen einem Fahrzeug und diversen anderen Objekten oder Verkehrsteilnehmer:innen.
V2I	Vehicle to Infrastructure	Definiert den drahtlosen Austausch von Daten zwischen dem Fahrzeug und der Straßeninfrastruktur, um Informationen über Parkflächen, Behinderungen wie Baustellen oder Unfälle und weitere Ereignisse zu erhalten.
V2V	Vehicle to Vehicle	Hiermit wird der Datenaustausch unter Fahrzeugen selbst beschrieben, der typischerweise Stau- und Unfallinformationen anhand des Standorts kommuniziert.
V2P	Vehicle to Pedestrian	V2P versteht sich als die Kommunikation von Fahrzeugen, der Infrastruktur und mobilen Endgeräten, bisher eher eine Vision, um Informationen über die Umgebung zu verarbeiten.
V2C	Vehicle to Cloud	V2C bezeichnet den Informationsaustausch von Fahrzeugen und Cloud-Systemen, die beispielsweise auf Backend-Server der OEM verweisen und es ermöglichen, Befehle zu verarbeiten, die zwischen verwendeten Diensten übertragen werden.

Quelle: eigene Darstellung

Tabelle 2: Schnittstellen im Fahrzeug

Nr.	Kategorie
1	Backend-Server
2	Fahrzeugkommunikationskanäle
3	Fahrzeugupdateprozeduren
4	unbeabsichtigtes menschliches Handeln
5	externe Konnektivität sowie Verbindungen
6	Fahrzeugdaten und -code
7	Verletzlichkeiten aufgrund nicht ausreichender Systemsicherheit

Quelle: eigene Darstellung

Tabelle 3: Sieben Kategorien typischer Angriffsszenarien in der Automobilindustrie

Im Vergleich zu anderen Branchen, in denen Security Updates bereits stärker verbreitet sind, stellen sich für die Automobilindustrie besondere Herausforderungen. Zum einen sind Fahrzeuge durch einen längeren Nutzungszeitraum geprägt, zum anderen bietet die Automobilindustrie eine höhere Variantenvielfalt als beispielsweise die Konsumgüterindustrie. Diese Vielfalt entsteht durch unzählige Kombinationsmöglichkeiten hinsichtlich technischer Ausstattung sowie durch die Verwendung verschiedener Steuergeräte. Zusätzliche Komplikationen entstehen regelmäßig dadurch, dass Varianten der Fahrzeugarchitektur oft historisch gewachsen sind und je nach Bedarf marginal angepasst wurden, anstatt zentral geplant zu werden.

Diese Faktoren treiben den erforderlichen Aufwand für die Bereitstellung von Security Updates mit herkömmlichen Entwicklungsmethoden in teilweise nur schwer handhabbare Höhen. Hinzu kommen die nach wie vor vorherrschenden technischen Probleme mit den sogenannten OTA-Updates, mithilfe derer OEM in Zukunft befähigt wären, Software-Updates schnell und reibungslos auf Autos aufzuspielen, ohne dass deren Halter:innen beispielsweise eine Werkstatt aufsuchen müssen. Das Problem hier ist jedoch die vorliegende Komplexität, wenn Software im Auto auf verschiedene Steuergeräte verteilt oder an verschiedene Netzwerke angebunden ist. Hinzu kommen schlechte Netzabdeckung in ländlichen Gebieten und die oftmals zeitkritische Natur dieser Vorhaben – eine schwierige Kombination. Die Möglichkeit, Updates so während der Fahrt aufzuspielen, ist dementsprechend noch einige Schritte entfernt. Um diesen Herausforderungen angemessen zu begegnen, sind neue methodische, prozessuale Entwicklungsvorgehen zu implementieren und standardisierte, modulare Bordnetzarchitekturen einzusetzen. In Bezug auf die Entwicklung sind vermehrt analytische und automatisierte Absicherungsmethoden gegenüber bisherigen empirischen Tests einzusetzen. Hierzu ist umfangreiches Wissen über die technischen Abhängigkeiten innerhalb von und zwischen Systemkomponenten erforderlich.

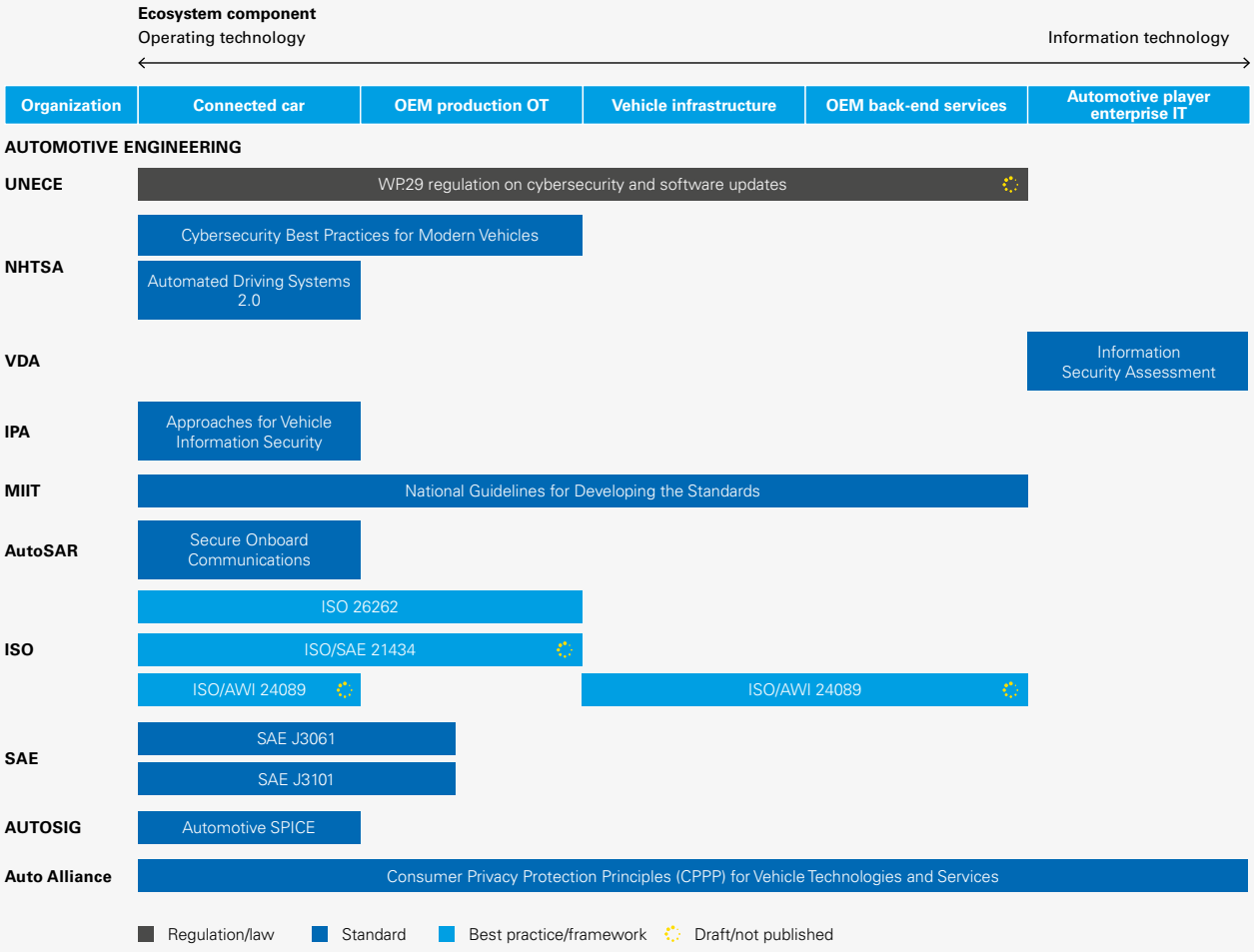
Dieser Wandel, insbesondere in den Entwicklungsmethoden, wird durch neue regulatorische Vorgaben begleitet. Hierzu zählen insbesondere die UNECE-Regulierung zum Software-Update-Management-System und die zugehörige Norm ISO 24089 Software Update Engineering.

Während der Entwicklung müssen umfangreiche Security-Konzepte, Hardware-Security-Untersuchungen sowie Pen Testing durchgeführt werden.

Die Entwicklung von Anwendungssoftware erfordert teilweise als Standard die Erfüllung der Anforderungen nach „Privacy by Design“ und „Privacy by Default“ der DSGVO.

5.
Automobile Wertschöpfungskette: Welche Auswirkungen hat Cybersecurity für einzelne Akteure?

Cybersecurity ist eine Herausforderung für den gesamten Produktlebenszyklus bzw. die gesamte Liefer- und Wertschöpfungskette. Dementsprechend intensivieren sich die Security-Anforderungen an Lieferfirmen, das beginnt bei den Forderungen nach zertifizierten ISMS nach TISAX/ISO 27001 als generelle Voraussetzung für eine Zusammenarbeit.



Quelle: Burkacky et al., 2020, S. 13

Abbildung 5: Regularien zu den verschiedenen Entwicklungszeitpunkten

Es müssen auch klare Schnittstellen zwischen liefernden Unternehmen und OEM bei der Entwicklung definiert werden, um Sicherheitslücken bei der Integration zu vermeiden. Das stellt je nach Kontext eine nicht unerhebliche Herausforderung dar, da für ein hohes Maß an Sicherheit gegebenenfalls auch ein höheres Maß an Informationsaustausch zwischen Lieferfirma und OEM notwendig sein kann, als es bisher üblich ist. Dies wiederum kann zu Problemen im Bereich Intellectual Property führen, wenn beispielsweise ein OEM zur Gewährleistung der Cybersecurity detaillierteren Einblick in Hard- und Software der zugelieferten Steuergeräte benötigt oder die Lieferfirma genauere Kenntnis über die Integration ihrer Steuergeräte in die Hardware- und Software-Architektur der Belieferten einfordert.

Cybersecurity-Entwicklungsumfänge unterliegen einer Vielzahl an Gesetzen, Regulierungen und Normen, die sich meist ergänzen. Die UNECE-Regulierungen bilden vor allem im europäischen Raum die höchste gesetzliche Ebene. In den vergangenen beiden Jahren sind hierbei vor allem für die Cybersecurity-Umfänge die UNECE R-155 für Cybersecurity und die R-156 für Software-Updates inklusive erwarteter ähnlicher Initiativen in China und USA in den Fokus gekommen. Sie fordern unter anderem die Umsetzung von Managementsystemen und entsprechenden Prozessen zur Sicherstellung der gesetzlichen Anforderungen.

Die UNECE-Regulierungen werden durch nationale Gesetze (z. B. nationaler deutscher Gesetzesrahmen zur Umsetzung von SAE-L4-Applikationen) vertieft oder weiter spezifiziert. Normen und Standards, wie die bereits erwähnte ISO 21434 Cybersecurity oder die ISO 20077 Extended Vehicle, bieten standardisierte spezifizierte Entwicklungsrahmen, Artefakte und Prozesse, die es bei einer sicherheitsrelevanten Entwicklung umzusetzen gilt.

Handlungsempfehlungen

Firmen jeder Größe müssen Wert auf die Erschaffung eines sogenannten Multi Compliance Framework legen, dann lassen sich alle Prozesse im Produktlebenszyklus einhalten; hier dargestellt im Bezug auf das autonome Fahren

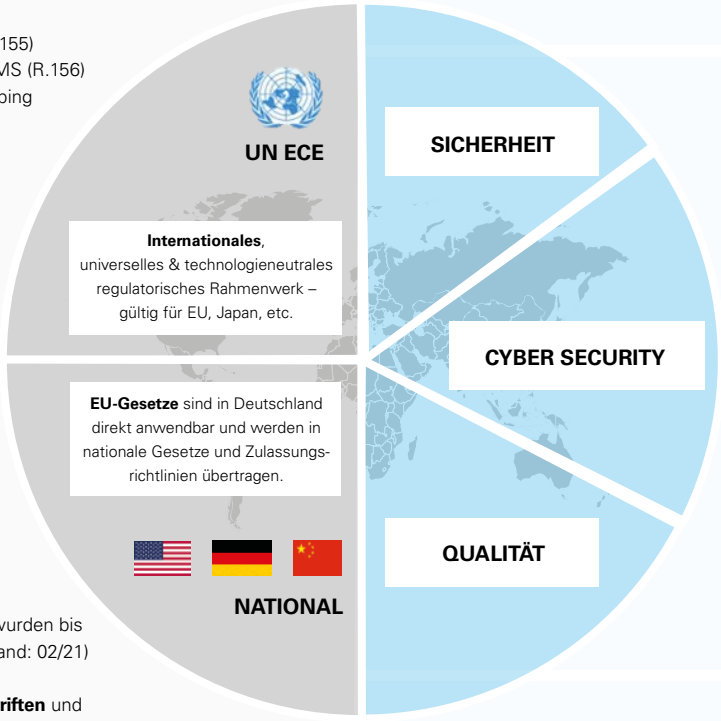
(Nationale) Regeln & Vorschriften	Produktsicherheit, (Nationale) Regeln & Vorschriften Haftung & Qualität

UNECE ist aktuell das zentrale Thema für die Homologation und Zulassung. Eine UNECE Zertifizierung ist Grundvoraussetzung für die Zulassung im europäischen und asiatisch/pazifischen (ausgenommen USA China). Für das autonome Fahren relevant sind v.a. folgende UNECEs:

- Uniform Provisions Concerning the Approval of: Vehicles with Regard to Steering Equipment (R.79-01)
- Cybersecurity MS (R.155)
- Software Update SUMS (R.156)
- Automated Lane Keeping Systems (R.157)

Produktsicherheit umfasst alle konstruktiven Maßnahmen und Aktivitäten, die einen Schaden oder ein Risiko für einen Menschen oder eine Sache verhindern.
Das oberstes Ziel sind robuste und sichere Produkte herzustellen. Relevante Vorschriften sind:

- Funktionale Sicherheit **(ISO 26262)**
- SOTIF **(ISO/PAS 21448** oder UL 4600)



Product-Security beschreibt die Fähigkeit, die Nutzung von cyber-physischen Netzwerken vor externen Manipulationen und Attacken zu schützen und zu verteidigen. Automobilrelevante Vorschriften sind:

- **ISO 27001** Information Security
- **ISO 21434** Automotive Cyber Security
- **ISO 20077** Extended Vehicle
- **ISO 15408** Evaluation criteria for IT security
- **ISO/TR 4804** Safety and cybersecurity for automated driving systems
- Software Updates etc.

Deutschland erlaubt **derzeit** autonome Fahrfunktionen bis SAE-Level 4 (generelle Fahrzeugzulassungen wurden bis zu SAE-L2 gegeben; Stand: 02/21)

US-Zulassungsvorschriften und Gesetze für autonome Fahrfunktionen **variieren von Staat zu Staat** (max. SAE-L4) – **UNECE gilt nicht**

China erlaubt derzeit Prototypen-Test bis SAE-L3 & SAE-L4 – eine angepasste ICV Gesetzgebung mit einem erweiterten V2I-Ansatz wird jedoch dieses Jahr in Kraft treten – **UNECE gilt nicht**

Auch die Automobilbranche erfordert eine breite Abdeckung weiterer Normen:

- Qualitätsmanagement **ISO 900x/IATF 16949**
- Prozessreife **ISO 15504/ASPICE**
- Energiemanagement/Umweltmanagement (z. B. **ISO 50001/14001**)

Pre-Development Phase → **Development** → **Operations** → **End of Life**

Quelle: eigene Darstellung

Abbildung 6: Multi-Compliance-Ansatz zur Sicherstellung vielfältiger Anforderungen am Beispiel autonomes Fahren

Bei der Entwicklung von sicherheitsrelevanten Kundenfunktionen ist es wichtig, die Gesetze integriert über den gesamten digitalen Software-Lebenszyklus zu denken.

In der Umsetzung der Gesetze und der Normen gilt es, parallele Entwicklungen zu vermeiden und an die gesamte End to End (E2E)-Wirkkette zu denken.

Im Bereich des autonomen Fahrens wurde z. B. ein integrierter Systemrahmen für alle sicherheitsrelevanten Umfänge über den gesamten digitalen Produktlebenszyklus hinweg entwickelt – im Rahmen eines AD Management System Framework. Dieser umfasst sowohl die Gedanken des System Engineering als auch die Anforderungen der Regulierungen und Normen.

5.1 Zulieferfirmen (Tier 1 bis Tier x)

Die Zulieferindustrie steht im Allgemeinen vor der Herausforderung, dass Implementierung und Betrieb eines zertifizierten ISMS zur Grundvoraussetzung werden, um als zulieferndes Unternehmen der Automobilhersteller agieren zu dürfen. Dies betrifft alle Lieferfirmen, unabhängig davon, ob analoge Produkte oder Elektronikbauteile und Software zugeliefert werden.

Die relevanten Standards, nach denen Lieferfirmen zertifiziert sind, sind die branchenunabhängige ISO 27001 und der auf ISO 27001 basierende TISAX-Standard, der vom Verband der Automobilindustrie entwickelt wurde. Betreibt ein Unternehmen ein ISMS, das den Anforderungen nach ISO 27001 oder TISAX genügt, kann grundsätzlich von einem soliden Grundgerüst für die Themen Informationssicherheit, Cybersecurity und Datenschutz ausgegangen werden, das mindestens die folgenden Bereiche umfasst:

- Unternehmensweite Vorgaben und Ziele zur Informationssicherheit sind definiert und werden kontinuierlich überprüft und nachgehalten.
- Organisatorische Strukturen zur Sicherstellung der Informationssicherheit inkl. aller notwendigen Rollen und Verantwortlichkeiten sind implementiert und werden gemanagt.
- Alle sogenannten „Assets“, d. h. sowohl Hardware zur Informationsverarbeitung als auch Informationen selbst, unterliegen definierten und überwachten Prozessen.
- Risiken, die die Informationssicherheit betreffen, werden systematisch gemanagt, d. h. standardisierte Verfahren zur Bewertung von Risiken sind etabliert, ebenso wie Vorgaben und Prozesse zum Umgang mit den Risiken.
- Weitere Kernthemen sind u. a.:
  - Notfall- und Störmanagement
  - Mitarbeitersicherheit
  - physische Sicherheit an den Standorten
  - Zugangskontrolle (physisch und elektronisch)
  - technische IT-Sicherheit wie z. B. kryptografische Verfahren
  - Betriebssicherheit der IT-Systeme
  - Supplier Security, d. h. die Sicherstellung der Einhaltung von Standards zur Informationssicherheit bei den eigenen (Sub-)Lieferanten
  - Compliance
  - Datenschutz
  - Anforderungen an den Schutz von Testfahrzeugen und Teilen (Prototypenschutz)
  - Informationssicherheit in Projekten

Diese Themen können als Grundanforderungen für alle Lieferfirmen und Sub-Lieferfirmen verstanden werden. Für Hersteller und Lieferanten von Elektronik und/oder Software-Komponenten gelten grundsätzlich weiterführende Anforderungen hinsichtlich sicherer Entwicklung, z. B. mit Blick auf Prozesse wie den „Secure Software Development Lifecycle“.

5.2 Automobilhersteller (OEM)

Das Geschäftsmodell von Automobilherstellern war bisher stark auf die Integration und Produktion von komplexen Fahrzeugen ausgerichtet. Hierdurch ergab sich eine stark arbeitsteilige Lieferkette, die zusammen mit dem Hersteller fast ausschließlich auf den Zeitpunkt der Fahrzeugproduktion ausgerichtet war. Cybersecurity-Aktivitäten beschränkten sich vornehmlich auf Absicherung von Schwachstellen zum Zeitpunkt der Fahrzeugproduktion. Zukünftig müssen Hersteller und ihre Lieferanten Strukturen etablieren, die von Beginn der Produktentwicklung an auf eine kontinuierliche Absicherung des gesamten Produktlebenszyklus ausgerichtet sind. Dabei steht das automobile Umfeld gegenüber anderen Branchen vor besonderen Herausforderungen. Hierbei sind insbesondere vier Teilaspekte zu nennen:

1. Langer Produktlebenszyklus

   Fahrzeuge sind typischerweise über längere Zeiträume in Benutzung als beispielsweise Produkte der Konsumgüterindustrie. Entsprechend länger ist ein Fahrzeug etwa mit Sicherheitsupdates zu versorgen. Aus regulatorischer Sicht herrscht bei diesem Thema Ungewissheit, da noch keine rechtssichere Interpretation der aktuellen Regularien in Bezug auf das Ende des Supportzeitraums vorliegt.

2. Hohe Variantenvielfalt

   Einer der Erfolgsfaktoren der Automobilindustrie war insbesondere in europäischen Märkten die Verfügbarkeit einer hohen Variantenvielfalt kundenspezifischer Produkte, die in hohem Maße auf die Bedürfnisse der Kund:innen zugeschnitten waren. Mit den neuen Regularien sind systemübergreifende, funktionale Abhängigkeiten verstärkt unter eine Änderungskontrolle zu stellen und hinsichtlich informationeller und funktionaler Sicherheit zu untersuchen. Die hohe Anzahl möglicher Konfigurationen macht die Absicherung zu einem äußerst komplexen Problem, das nur durch Einsatz neuartiger Methoden zu lösen ist. Eine dieser Methoden ist die Einführung von architektonischen Abstraktionsebenen mit klaren Schnittstellen. Die stringente Konzeption und Steuerung von Absicherungsprogrammen und der Einsatz von Simulationsmethoden an einem „digitalen Zwilling" des Bordnetzes helfen gleichermaßen in diesem Unterfangen.

3. Verteilte Verantwortung im Lieferanten- und Partnernetzwerk

   Aufgrund des Wettbewerbs- und Kostendrucks haben sich Zulieferketten mit hochspezialisierten Lieferanten in der Automobilwirtschaft etabliert. Neuartige Geschäftsmodelle zur Umsatzgenerierung über den Produktlebenszyklus hinweg, wie beispielsweise Connected Services, erfordern die Interaktion mit zahlreichen Partnern im Wertschöpfungsnetzwerk. Die große Anzahl an Wertschöpfungspartnern erfordert ein umfangreiches Schnittstellenmanagement in Bezug auf die Entwicklung sicherer Produkte und die Gewährleistung der Reaktionsfähigkeit im Fall von neu identifizierten Schwachstellen und Angriffen.

   Automobilhersteller müssen im Zuge der Supplier Security alle notwendigen Rechte vertraglich festschreiben, die ihnen z. B. durch „Right for Audits" die regelmäßige Überprüfung der Einhaltung der Security-Standards durch die Lieferfirmen ermöglichen. Hierzu werden Schnittstellenanforderungen u. a. im Rahmen des ISMS festgeschrieben.

   Lösungen müssen auch für Hersteller von Aufbau- und Umbaufahrzeugen (z. B. Krankenwagen) gefunden werden, damit diese die Anforderungen an ein Cybersecurity Management System erfüllen, wie beispielsweise das Flottenmonitoring. Zumindest für kleinere Hersteller kann dies eigentlich nur in Kooperation mit dem Hersteller des Grundfahrzeugs (z. B. in Form neuer „Services" des OEM für den Aufbauhersteller) gewährleistet werden.

4. Eingeschränkte Konnektivität

   Aufgrund der Beweglichkeit von Fahrzeugen können heutige Mobilfunktechnologien keine vollständige Konnektivität von gesamten Flotten gewährleisten. Zudem fordern viele Kund:innen, oft aus mangelnder Transparenz hinsichtlich des Datenschutzes, die Abschaltung von Funktionalitäten der Konnektivität. Beide Aspekte verhindern, dass der Hersteller Sicherheitsupdates bei neuen Bedrohungslagen bereitstellt. Wie die zuvor beschriebenen Beispiele demonstrieren, erfolgen Angriffe jedoch oft gerade nicht über die Mobilfunkschnittstelle, sondern beispielsweise über die V2X-Schnittstellen oder auch die Reifendrucksensoren (vgl. Kapitel 4.2.3).

„Firmware Over-the-Air" ist eine der Voraussetzungen für Software-over-the-Air-Updates. Insbesondere für diesen Vorgang muss eine sichere End-to-End-Verbindung vom Backend-Server des OEM über das Mobilfunknetz und den fahrzeuginternen CAN-BUS hin zum entsprechenden Steuergerät gewährleistet sein, weshalb die Lieferfirmen auch in diesem Fall erhöhten technischen Anforderungen genügen müssen.

5.3 After-Sales-Industrie

Die automobile After-Sales-Industrie ist durch diverse Geschäftsmodelle und Angebote geprägt, die unterschiedliche Anforderungen an informationelle Sicherheit und Zugänglichkeit von Kundendaten stellen. Herstellereigene Werkstätten und Drittwerkstätten gehören zur After-Sales-Industrie, die spezielle Bedarfe an Produkt-, Fahrzeug- und Kundendaten hat. Darüber hinaus gibt es ein breites Spektrum an Umbau- und Aufbauherstellern sowie Equipment-Anbietern mit ähnlichen Interessen an Daten.

Als weitere Vertreter der After-Sales-Industrie sind auch Versicherungen, Fahrdienst- und Mietwagen- Anbieter zu nennen. Mit zunehmender Verbreitung vernetzter Dienste werden Flottendaten für die unterschiedlichen Anbieter zugänglicher. Dies ermöglicht die Digitalisierung von Geschäftsmodellen der After-Sales-Industrie. Als aktuelle Beispiele sind hier Dienste für Ride Sharing (Gemeinschaftsfahrt) und Free Floating (Carsharing ohne Stationen) zu nennen.

Die genannten Geschäftsmodelle werden zumeist von herstellereigenen und Drittanbietern mit unterschiedlicher Größe angeboten. Fahrzeughersteller haben dabei einen besseren Zugang zu vielen der erforderlichen Daten. Um dieses informationelle Ungleichgewicht auszugleichen, erlässt die Europäische Union Vorgaben zum „Extended Vehicle". Die Vorgaben werden durch Empfehlungen der ISO 20077, ISO 20078, ISO 20080 und ISO 23132 flankiert.

Zielsetzung ist der diskriminierungsfreie Zugang zu Monopoldaten für die automobile After-Sales-Industrie. Hierzu können die Hersteller entweder eigene Datenplattformen bereitstellen oder die aus der Flotte gesammelten Daten über Drittplattformen verschiedenen Akteuren im Bereich After-Sales zur Verfügung stellen. Auf diese Weise sollen Wettbewerbsvorteile von herstellereigenen Betrieben vermieden werden.

Die Vorgaben und Normen beziehen sich aktuell in erster Linie auf Werkstätten und erlauben eine gezieltere Kundenansprache bei Wartungsbedarfen von Fahrzeugen. Die Standards sind jedoch modular aufgebaut. Eine Ergänzung für Versicherungsunternehmen ist in Erarbeitung. Weitere Vorgaben für andere Akteure der After-Sales-Industrie sind zu erwarten.

Sicherheitsrelevante Dienstleistungen – beispielsweise die Programmierung von Fahrzeugschlüsseln – konnten bisher vielfach ausschließlich herstellereigene Werkstätten durchführen, die besonderen Auflagen hinsichtlich des Einsatzes sicherheitskritischer Werkzeuge erfüllten und den Schutz kritischer Daten gewährleisten konnten.

Im Rahmen der EU-Initiative SERMI (Secure Remote Maintenance Information) sind Hersteller nun angehalten, Dritten die Möglichkeit einzuräumen, sicherheitskritische Dienstleistungen anzubieten. Hierzu müssen geeignete Werkzeuge (Tester, Diagnosegeräte) und Backend-Services entwickelt und bereitgestellt werden. Die Sicherheit der Kundendaten ist dabei zumeist durch eine Ende-zu-Ende-Kryptografie geschützt, die Integrität und Authentizität sicherheitsrelevanter Daten gewährleistet. Der kryptografische Schutz bezieht sich auf Informationskanäle innerhalb des Fahrzeugs (zwischen Steuergeräten) und darüber hinaus zur Umgebung (V2X) oder zum Hersteller (vernetzte Dienste). Besonderes Augenmerk ist auf die Absicherung der Diagnosefunktionen zu legen, die eine Aktualisierung der Fahrzeugsoftware ermöglichen.

Ab Mitte 2022 werden darüber hinaus im Rahmen der Vorgaben für Software-Update-Management-Systeme weitere Maßnahmen erforderlich. Diese sind die wichtigsten:

- Bereitstellung und Verarbeitung von Integritätsdaten (Integrity Validation Data (IVD) – zum Nachweis der Updateintegrität mittels kryptografischer Signaturen)
- Rückdokumentation von Software-Änderungen in kundenindividuellen Fahrzeugen über den gesamten Produktlebenszyklus
- Behördliche Dokumentation der regulatorischen Software-Identifikationsnummer (RxSWIN); Nachweis der regulatorischen Konformität und Kompatibilität von Software-Ständen

Neben technischen Maßnahmen als Reaktion auf Vulnerabilitäten können auch Kommunikationsmaßnahmen kurzfristig Angriffsrisiken reduzieren. Beispielsweise können Fahrzeugnutzer:innen gebeten werden, bestimmte Funktionen zeitweise nicht mehr zu benutzen oder ausgewählte Funktechnologien zu deaktivieren. Darüber hinaus sind ab Mitte 2022 Kund:innen über Updatemaßnahmen zu informieren – explizit über Zweck und Inhalt der Updates. Generell gilt die Informationspflicht gegenüber den Kund:innen bei Updates in der Werkstatt und bei OTA-Updates. Darüber hinaus ist bei OTA-Updates ein funktional sicherer Fahrzeugzustand zu gewährleisten.

Mit zunehmender Verfügbarkeit von OTA-Technologien ist mit einem höheren Sicherheitsniveau in der gesamten Fahrzeugflotte zu rechnen.

Den genannten Initiativen für vereinfachte Datenzugänglichkeit stehen neue Cybersecurity-Anforderungen gegenüber, die stärker integrierte, manipulationsgeschützte Software-Deployment-Prozesse im Bereich After Sales erfordern. Beide Entwicklungen erfordern eine Adaption datengetriebener Geschäftsmodelle in der automobilen After-Sales-Industrie.

6.
Organisation: Welche Schlüsselkompetenzen müssen Akteure kurzfristig entwickeln?

Die Herausforderung, sich im komplizierten Feld der Automotive Cybersecurity sowohl themen- als auch zeit- und finanzgerecht zurechtzufinden, betrifft vor allem viele kleine und mittlere Unternehmen aus der automobilen Industrie. Diese Situation ist ein Produkt verschiedener äußerer Faktoren wie auch teilweise interner Versäumnisse. Da solch aufwändige Umstellungen für KMU jedoch meist eine größere Herausforderung darstellen als für große Unternehmen, werden sie häufig aus Gründen des Zeit-, Geld- oder auch Wissensmangels aufgeschoben. Dennis Heusser vom VDE sieht hier vor allem fehlende oder anderweitig verplante Ressourcen als Hauptursache für die „Dysbalancen zwischen den OEM und den KMU, da sich kleinere Unternehmen natürlich immer wieder die Frage stellen müssen, ob sie es sich aus Ressourcensicht leisten können, Personal für solche Zwecke abzustellen."

Im Vergleich dazu seien große Unternehmen hier grundsätzlich in einer vorteilhafteren Situation und könnten dadurch auch sicherstellen, dass sie zu jeder Zeit mit den neuesten Informationen versorgt blieben. Zusätzlich zu der Problematik, die vorhandenen Ressourcen optimal einzusetzen, sind für die Firmen die Folgen des Fachkräftemangels spürbar. Sie führen dazu, dass viele Firmen nur schwerlich die richtigen Mitarbeiter:innen finden, folglich keine Expert:innen im eigenen Haus haben und so einige Themen nicht proaktiv angehen können. Hier könnte man, so auch die Meinung der befragten Experten, Dennis Heusser vom VDE und Dr. Ingmar Bauman vom FZI, durch breite Weiterbildung der Mitarbeiter:innen und durch Fachschulungen bei Branchenverbänden Positives bewirken. Des Weiteren hilft im ersten Schritt bereits eine eingehende Sensibilisierung der Mitarbeiter:innen, speziell an neuralgischen Punkten der Cybersecurity, wie beispielsweise der Produktion. Neben dem Mangel an Ressourcen und Zeit können zudem mitunter Wissenslücken vorherrschen, wodurch wichtige Entwicklungen verpasst werden könnten. Dennis Heusser stellt klar, dass „speziell Unternehmens- und Branchenverbände [hier] einen wichtigen Beitrag leisten [können], indem sie sich weiter für KMU öffnen, als zentrale Koordinierungsstelle fungieren und wichtige Informationen gebündelt weitergeben".

In der Literatur wird deutlich, dass Ideen, in welcher Form man ein automobiles Virtual Security Operations Centre (VSOC) umsetzen kann, in der Branche durchaus vorhanden sind und dass ein VSOC als das einzig richtige Mittel zum Zweck angesehen wird, um die regulatorischen Vorgaben in den kommenden Jahren einhalten zu können. Es bestätigt sich, dass es viele spezifische Herausforderungen gibt, die sich aus der Fahrzeugarchitektur und deren besonderen IT-Systemen ergeben. Dabei korrelieren diese Herausforderungen nicht nur untereinander, sondern auch mit anderen Dimensionen innerhalb von Unternehmensstrukturen. Automobilhersteller werden die Umsetzung eines VSOC allerdings nicht allein bewerkstelligen können. Es muss die gesamte Lieferkette darauf vorbereitet und mit einbezogen werden und auch die Gesetzgebung muss an einigen Stellen den Einfluss, den diese Regulierungen haben, noch genauer definieren. Dr. Ingmar Baumgart vom FZI schätzt die Lage so ein, dass „ungeachtet der teils hohen Sicherheitsstandards der OEM Schwachstellen bei den KMU das schwächste Glied des Gesamtsystems darstellen und so großflächige Auswirkungen mit sich bringen". Ein OEM ist folglich in seiner Cybersecurity-relevanten Infrastruktur am Ende konsequenterweise nur so stark wie das schwächste Glied seiner Lieferkette.

Anforderungen der Industrie hinsichtlich Automotive Cybersecurity beziehen sich regelmäßig auf die in Tabelle 4 dargestellten Beispiele:

Nr.	Kategorie
1	Technische Methode der Angriffs- und Schwachstellenerkennung
2	Erkennung der Vorfallsdaten anhand eines Systems
3	Threat-Intelligence-Strategie zur Analyse von Security-Event-Daten
4	VSOC-Strategie innerhalb einer Organisation
5	Art der Assets, die es zu überwachen gilt
6	Voraussichtliche Größe der Asset-Flotte in den kommenden Jahren
7	Personalplanungen für ein VSOC anhand der Unternehmensgröße
8	Regulierungen, auf die sich ein VSOC ausrichten soll
9	Wirtschaftsraum, in dem ein VSOC agieren soll
10	Analyseantwortzeit für Security-Events an Fahrzeuge im Feld
11	Betriebszeiten des Cybersecurity Incident Response Team (CSIRT)
12	Fokus, ab welcher Bewertung eines Vorfalls/Ereignisses ein Alarm ausgelöst wird
13	Bereich oder Sektor, für den der Lösungsansatz umsetzt werden soll

Quelle: eigene Darstellung

Tabelle 4: Anforderungen der Industrie hinsichtlich Automotive Cybersecurity

Ähnlich wichtig ist zudem die Erkenntnis, dass die Strukturen für den Aufbau eines VSOC nicht gänzlich neu sind, sondern dass viele Teilbereiche und Prozessabläufe aus dem Enterprise-SOC auf den automotive-spezifischen Verwendungszweck adaptiert werden können, solange man Ziele, Aufgaben und Einsatzzwecke anpasst bzw. neu definiert.

Mit der Ausarbeitung des IT-Artefakts (morphologischer Kasten mit differenzierenden Lösungsmöglichkeiten) als Grundlage für das Aufzeigen einer VSOC-Gesamtstrategie wurde zudem deutlich, dass es nicht „das eine" VSOC gibt, sondern dass vor allem die unterschiedlichen Use Cases großen Einfluss darauf haben, woran sich ein VSOC-Betriebsmodell orientieren kann.

Die Entwicklung einer schnellen, aber fundierten VSOC-Expertise wird entscheidend sein für den nachhaltigen Erfolg von Connected Cars und für die Reputation der Unternehmen, solchen Cyberangriffen adäquat gegenüberzutreten.

Die erforderlichen Fähigkeiten für den Betrieb eines VSOC sind am Markt kaum zu finden. Die Rekrutierung, Bindung und Schulung von Fachkräften wird ein entscheidender Faktor für den erfolgreichen und nachhaltigen Betrieb von VSOC sein. Vor allem bei der Abwägung, ein VSOC durch externe Provider betreiben zu lassen, muss klar sein, dass Outsourcing das interne Wissen meist stark reduziert und man in Zukunft über keinen Wissensvorsprung mehr verfügen wird. Dr. Ingmar Baumgart vom FZI sieht diese Frage ebenfalls kritisch, da „bei der Weitergabe des Prüfprozesses an externe Dienstleister keine Vergleichbarkeit gegeben [ist]", dies jedoch aus Gesamtprozesssicht als absolut notwendig anzusehen sei.

Künftig besteht aus wissenschaftlicher und organisatorischer Sicht Forschungsbedarf in der Entwicklung und dem Aufbau von VSOC durch regulierende Behörden und Unternehmen, um eine effektive Nutzung und einen effizienten Betrieb zu ermöglichen. In der Bearbeitung von offenen Fragen ergeben sich nicht nur durch die fachliche Weiterentwicklung, sondern zunehmend auch durch den gesellschaftlichen Wandel neue Chancen. Dr. Ingmar Baumgart sieht die zunehmende „Feedbackkultur, in welcher auch Unternehmen versuchen, in einen offeneren Austausch zu gehen", als Chance für neue „Austauschformate, [die] gefördert werden [sollten], um eine weitere Sensibilisierung und Priorisierung des Themas gewährleisten zu können". Eines der Themen, mit denen die Beteiligten umgehen müssen, wird der Druck eines frühzeitigen Markteintritts sein.

Im Versuch, sich zukünftig auf dem VSOC-Markt zu etablieren, stellt der Markteintritt eine kritische Herausforderung dar, die die Pläne der Automobilhersteller maßgeblich beeinträchtigen kann.

Denn je länger man in diesem wettbewerbsintensiven Geschäftsfeld wartet, bis man eine VSOC-Lösung am Markt bereitstellt, desto größer ist das Risiko, dass ein irreparabler Imageschaden entsteht, wenn sich ein sicherheitsrelevanter Vorfall ereignet. Positioniert man sich mit einer VSOC-Lösung früh am Markt, so wird es erforderlich sein, die implementierten Lösungsansätze nachzuschärfen und stetig an neue Erkenntnisse anzupassen. Letzten Endes geht es bei allen Angeboten jedoch darum, dass ihr Bekanntheitsgrad in der Öffentlichkeit steigt, und gleichzeitig sicherzustellen, dass ihre Bearbeitung niederschwellig anzugehen ist.

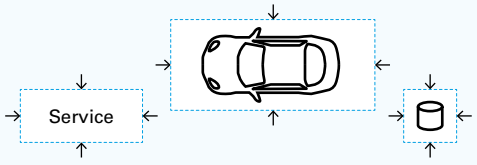
6.1 Anforderungen im Bereich der funktionalen Sicherheit

Die Produktsicherheit moderner Fahrzeuge muss aus verschiedenen Blickwinkeln betrachtet werden. Während bei Sicherheit oftmals direkt an Unfallsicherheit gedacht wird, kommt der Sicherheit während des regulären Betriebs mindestens eine gleichwertige Rolle zu. Neben der Gebrauchssicherheit, die vor allem im Produktsicherheitsgesetz geregelt wird, spielen die jungen Bereiche der funktionalen Sicherheit (ISO 26262), der Cybersecurity (ISO 21434; UNECE R-155; UNECE R-156) und der SOTIF („Safety Of The Intended Functionality"; ISO 21448) eine bedeutende Rolle. Die einzelnen Bereiche können als Disziplinen oder Teilbereiche der übergeordneten Produktsicherheit mit verschiedenem Fokus verstanden werden.

Abgrenzung zur ISO 26262 (FuSi), Prod (GeSi) und ISO 21434 (Cybersecurity)

SECURITY

Cybersecurity ISO 21434/UN ECE Cybersecurity

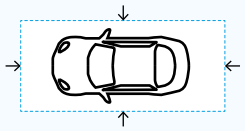


Schützt Fahrzeug-, Back-End und Servicefunktionen vor äußeren und funktionalen Einwirkungen (z.B. Hackerangriff)

&

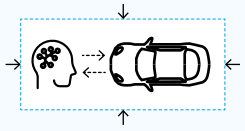
SAFETY

Funktionale Sicherheit ISO 26262



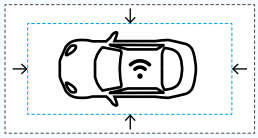
Schützt Fahrzeugnutzer und das Umfeld vor E/E-Fehlfunktionen des Fahrzeugs

Gebrauchssicherheit ProdSG



Schützt Fahrzeugnutzer und das Umfeld vor Gefahren aus bestimmungsgemäßen und vorhersehbarem (Fehl-)Gebrauch

SOTIF ISO 21448 (CD)



Schützt Fahrzeug, Bediener und das Umfeld vor Auswirkungen aus falsch oder unzureichend ausgelegten Sollfunktionen

» Neben der ISO 21434/UN R-155/UN R-156 spielen im Bereich der Safety vor allem die funktionale Sicherheit, die Gebrauchssicherheit und die Sicherzeit der Sollfunktion (SOTIF) eine Rolle bei der Entwicklung moderner Fahrzeugsysteme.

Quelle: eigene Darstellung

Abbildung 7: Abgrenzung der verschiedenen Sicherheitsdisziplinen

Die einzelnen Teilbereiche der Produktsicherheit bedingen sich nicht direkt gegenseitig, zahlen jedoch alle auf das gleiche Ziel – ein möglichst sicheres Gesamtprodukt – ein. Folglich sind die einzelnen Sicherheitsdisziplinen interdependent. So könnten beispielsweise Cybersecurity-Verstöße implementierte Maßnahmen der funktionalen Sicherheit behindern, während Maßnahmen der funktionalen Sicherheit das Risiko eines Angriffs im Sinne der Cybersecurity erhöhen könnten. Deshalb müssen die einzelnen Komponenten integriert gedacht und entwickelt werden, um mögliche Doppelarbeit und im schlimmeren Fall Zielkonflikte und gegebenenfalls resultierende gegenläufige Maßnahmen zur Risikominimierung zu vermeiden.

Dementsprechend müssen die Entwicklungsprozesse für Cybersecurity (Security) gem. ISO 21434 und funktionale Sicherheit (Safety) gem. ISO 26262 (sowie idealerweise für Gebrauchssicherheit und SOTIF gem. ISO 21448) eng miteinander verzahnt und integriert gedacht werden, um das gemeinsame Ziel eines sicheren E/E-Systems und Gesamtprodukts effektiv zu erreichen.

Vergleicht man die wesentlichen Entwicklungsphasen der zugrundeliegenden ISO-Normen von Cybersecurity, funktionaler Sicherheit und SOTIF, so ergeben sich wesentliche Parallelen, die sich in diesen Phasen beschreiben lassen.

- Generelles Konzept und Risikobewertung (z. B. Scoping; Ausgangsbasis; Hazard And Risk Analysis (HARA); CS-Risiko-Assessment)
- Design und Entwicklung eines Sicherheits- und Testkonzepts (funktionale Modifikationen; Schutzkonzepte, technische Realisierungsoptionen)
- Implementierung und technische Umsetzung inkl. Integration in das Gesamtfahrzeug
- Testing (z. B. Verification and Validation; Pen Testing etc.)
- Freigabe (Bestätigung der ISO- und UNECE-R-konformen Entwicklung und Freigabe zur Serienproduktion)
- Produktion und Feldmonitoring (Wartung; Updates; Management von auftretenden Incidents; Management von möglichen neuen Angriffsformen)

Eine Synchronisation wesentlicher Meilensteine anhand der oben aufgeführten Phasen im Produktentstehungsprozess fördert eine schlanke Entwicklung und die effektive Erreichung der gesetzten Ziele.

Wichtige Meilensteine sicherheitsrelevanter Prozesse und Aktivitäten sollten synchronisiert werden, um das gemeinsame Ziel sicherer E/E-Systeme auf wirksame Weise zu erreichen.

In den komplexen, kollaborativen Systemen moderner Autos sind Sicherheit und Gefahrenabwehr voneinander abhängig und überschneiden sich. Security-Fehler könnten Safety-Maßnahmen kompromittieren, Safety-Maßnahmen könnten die Angriffssicherheit schwächen. Daher ist die Zusammenarbeit der verantwortlichen Bereiche erforderlich.

	Generelle Herangehensweise und Risikoassessment		Design	Implementierung	Testing	Release	Post Production & Monitoring	
CS	Cybersecurity Philosophie	Risikoanalyse	CS Konzept inkl. Testkonzept	Security Entwicklung	Security Testing	Security Freigabe	Wartung & Betrieb	Management von Sicherheitsanfälligkeiten
FuSi	Assessment der Sicherheitsrelevanz	HARA	FuSi Konzept inkl. Testkonzept	FuSi Implementierung	Safety Testing (V&V)	Safety Case (Release)	Wartung & Betrieb	
SOTIF	SOTIF-bezogene Gefahrenidentifikation & Risikobewertung		Funktionale Modifikationen zur Reduzierung des SOTIF-Risikos	Funktionsmodifizierung	Verifikation und Validierung der SOTIF	SOTIF Freigabe	Feldbeobachtung	Management von Safety-Anfälligkeiten

» **Um Doppelarbeit, Konflikte und widersprüchliche Sicherheitsaktivitäten zu erkennen und zu verhindern, ist die Harmonisierung der sicherheitsrelevanten Prozesse über das ganze Projekt hinweg notwendig.**

Quelle: eigene Darstellung

Abbildung 8: Analogien und Bereiche möglicher Synergien zwischen den Sicherheitsdisziplinen

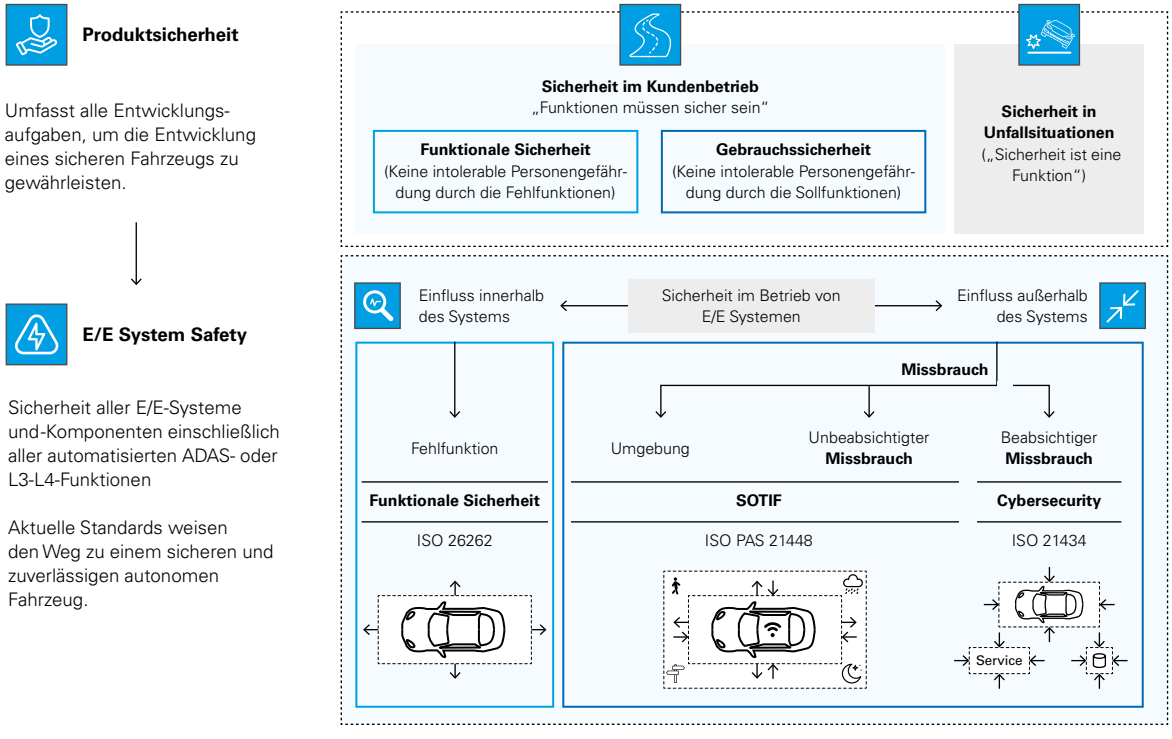
Die Entwicklungsprozesse für Cybersecurity (Security) gem. ISO 21434 und funktionale Sicherheit (Safety) gem. ISO 26262 müssen eng miteinander verzahnt und integriert gedacht werden.

Ziel sowohl in der Cybersecurity als auch in der funktionalen Sicherheit ist es, sicherheitskritische Zustände durch latente und systematische Fehler in Hardware-Software-Systemverbünden ausschließen zu können, und somit kritische Zustände durch interne E/E-Fehler oder durch eine äußere Manipulation der Hardware/Software zu vermeiden.

Ausgangsbasis für eine auf Sicherheit ausgerichtete Entwicklung (umfasst die Umfänge von Safety and Security) sind genau spezifizierte Kunden- und Fahrzeugfunktion und ein tiefes Verständnis der E2E-Wirkketten in der Fahrzeug E/E-Architektur. Sie bilden den Rahmen für eine technische Risikobetrachtung, um die Schwere der möglichen Auswirkung und die Auftrittswahrscheinlichkeiten der Fahrzeugfunktionen zu bewerten. Um dieses tiefe Verständnis zu generieren, werden vor allem zwei wichtige Arten von Analysen durchgeführt: HARA (Hazard and Risk Analysis) und TARA (Threat And Risk Analysis). Die im Rahmen der Analysen zur funktionalen Sicherheit durchgeführte HARA generiert einen Überblick über funktionale Risiken, die im Zuge der TARA berücksichtigt werden müssen. Es ist zu vermeiden, dass die funktionale Sicherheit über Cyberattacken beeinträchtigt werden kann, zudem muss ausgeschlossen werden, dass sich die jeweiligen Schutzziele gegenseitig negativ beeinflussen. Sowohl für Cybersecurity als auch für funktionale Sicherheit ist es entscheidend, die Nachverfolgbarkeit zwischen den funktionalen und technischen Anforderungen und der Verifizierung der Software-Hardware-Komponenten bzw. der Validierung der Software-Systemverbünde sicherzustellen; sie dienen als Grundlage für den Sicherheits-/Cybersecurity-Nachweis der Funktionen und deren entsprechende Release-Freigabe.

6.2 Anforderungen an die E/E-Architektur im Fahrzeug

Generell müssen IT-Systeme in Fahrzeugen deutlich robuster konzipiert werden, als das in der jüngeren Vergangenheit der



Quelle: eigene Darstellung

Abbildung 9: Sicherheitsstandards in der Produktsicherheit

Fall war. Dem IT-Hardening kommt eine größere Bedeutung zu. Um dies zu erreichen, werden verschiedene Sicherheitskonzepte onboard wie offboard eingesetzt; hierzu zählen u.a. die in Tabelle 5 genannten.

Der aktuelle Trend hin zu zentralen Rechnern im Fahrzeug führt zu einer Verringerung der Steuergeräte, was sich vorteilhaft auf die Anzahl der Schnittstellen und somit potenzieller Angriffsvektoren auswirkt. Zudem wird der Aufwand zur Sicherstellung der Hardware-Security und der Zulieferer-Security im Vergleich zu verteilten Systemen reduziert. Die Absicherung zentraler Rechner muss jedoch umso effektiver sein, weil das Risiko bei einem erfolgreichen Angriff durch die zentrale Steuerung diverser Fahrzeugfunktionen deutlich größer ist.

Nr.	Kategorie
1	Sichere Diagnose – Software-Integrität und Individualisierung der Software für einzelne Steuergeräte
2	Software-Pakete über Checksummen oder Hashwerte
3	Signatur der Software-Pakete (Integrität und Authentizität)
4	Verschlüsselung Onboard- und Offboard-Kommunikation – Transport Layer Security (TLS)
5	Authentizität der Kommunikation onboard und offboard (Signaturen)
6	Einsatz von Security Manifests
7	Mandatory Access Control/Zugriffskontrolle
8	Hardware-Schutz von Schlüsselmaterial (Hardware Security Module/Enclaves)
9	Secure Boot
10	Hardware-Beschleunigung von kryptografischen Operationen u. a. zur Aufrechterhaltung der Echtzeitfähigkeit
11	Public-Key-Infrastruktur zur Distribution von Schlüsselmaterial (Backend)

Tabelle 5: Kategorien von Sicherheitskonzepten

Quelle: eigene Darstellung

7.
Fazit und Zusammenfassung

Cybersecurity in der Automobilindustrie stellt eine enorme Herausforderung für alle Wertschöpfungsstufen dar und bedingt die Ausweitung der Produktbetreuung im Bereich Security auf den gesamten Produktlebenszyklus. Der zusätzliche Aufwand für die Etablierung und Aufrechterhaltung eines Cybersecurity-Standards nach Stand der Technik könnten sich durch die Erschließung neuer Umsatzpotenziale nach Verkauf und während der Nutzung des Fahrzeugs amortisieren.

Die Hauptrisiken für Cybersecurity Breaches werden in diesem Themenpapier innerhalb der drei essenziellen Phasen des Produktlebenszyklus kategorisiert und behandelt: der Entwicklung, der Produktion und des Feldeinsatzes.

Bereits in der Entwicklung müssen Unternehmen und ihre handelnden Personen eine Sensitivität für Schwachstellen etablieren. Bei Gesamtbetrachtung der Lieferkette wird hinsichtlich einer holistischen Cybersecurity-Strategie schnell erkennbar, dass der vermehrten Komplexität lediglich durch enge Beziehungen und weitreichende Kollaborationen zwischen OEM und Lieferfirmen beigekommen werden kann. Dazu gehören sowohl die Erstellung von Konzepten zur Sicherheits- und Risikobewertung für die initiale Entwicklung und deren Updates als auch das Sicherstellen der Regulierungskonformität inklusive einer anforderungsbasierten Absicherung.

In der Produktion ist die Software nicht nur hinsichtlich klassischer Angriffe, sondern auch gegenüber Manipulation zu schützen, während im Feld vor allem auf sichere Updateprozesse in den Werkstätten und bei den Nutzer:innen geachtet werden muss. Hier sind im Speziellen die Informations- und Rückdokumentationspflichten (Asset Management) einzuhalten. Da Cybersecurity jedoch keineswegs nach Auslieferung der Fahrzeuge endet, zählt auch das Etablieren einer Feldbeobachtung für Angriffe im gesamten Wertschöpfungsnetzwerk zu den zukünftig zu beachtenden Maßnahmen.

Trotz aller Aufwände sollte man die Fragestellungen, die sich den Unternehmen jeder Größe im Zusammenhang mit Cybersecurity stellen, nach Möglichkeit auch als Chance zur Weiterentwicklung sehen. Die Experteninterviews mit Dr. Ingmar Baumgart und Dennis Heusser haben nicht nur gezeigt, dass keine große Diskrepanz zwischen Wirtschaft und Wissenschaft hinsichtlich der Einordnung des Status quo herrscht. Sie haben auch herausgearbeitet, dass die großen Aufgaben, vor denen speziell KMU stehen, auch Chancen mit sich bringen. Besonders in den Unternehmensbereichen Produktsicherheit und Technologie wird großes Entwicklungspotenzial gesehen – auch um das Vertrauen der Kund:innen in die Produkte nicht zu gefährden. Ganzheitliche Ansätze wie das ISMS, das Zertifizierungen zu allen relevanten Bereichen der Arbeitssicherheit und der Cybersecurity (u. a. ISO 27001, TISAX, Grundschutz, DSGVO) abdeckt, müssen dringend zum Standard in den Unternehmen werden. Dies wird sich auf lange Sicht nicht nur positiv auf das externe Bild jener Firmen, sondern auch auf den Industriestandort Baden-Württemberg als Ganzes auswirken.

Stichwortverzeichnis

ADAS	Advanced Driver Assistance System
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAN	Controller Area Network
C-V2X	Cellular Vehicle-to-Everything, beschreibt eine technische Lösung zur Kommunikation zwischen Fahrzeugen und vernetzten Komponenten, die auf Mobilfunk basiert.
CVE	Common Vulnerabilities and Exposures
DSGVO	Datenschutzgrundverordnung
DSRC	Dedicated Short Range Communikation beschreibt eine technische Lösung zur Kommunikation zwischen Fahrzeugen und vernetzten Komponenten, die auf WLANp basiert
E/E-Architektur	Elektrisch/Elektronische Architektur
E2E	End to End
Embedded Systems	Digitale Systeme für Überwachungs-, Steuerungs- und Regelungsfunktionen
HARA	Hazard and Risk Analysis
Hardening	Härten – die Sicherheit eines Systems erhöhen, indem nur dedizierte Software eingesetzt wird, die für den Betrieb des Systems notwendig ist und deren korrekter Ablauf unter Sicherheitsaspekten garantiert werden kann
Internet of Things	Sammelbegriff für Technologien einer globalen Infrastruktur der Informationsgesellschaften, die es ermöglicht, physische und virtuelle Objekte miteinander zu vernetzen und sie durch Informations- und Kommunikationstechniken zusammenarbeiten zu lassen (Abk. IoT)
ISMS	Information Security Management System (Managementsystem für Informationssicherheit)
ITS	Intelligent Transport System
ITS-G5	Eine technische Lösung zur Kommunikation zwischen Fahrzeugen und vernetzten Komponenten, die auf WLANp basiert
JTAG	Joint Test Action Group
Man-in-the-Middle	Angriffsform in Rechnernetzen. Angreifende stehen dabei meist logisch zwischen den beiden Kommunikationspartnern, haben mit ihrem System vollständige Kontrolle über den Datenverkehr zwischen zwei oder mehreren Netzwerkteilnehmer:innen und können die Informationen nach Belieben einsehen und sogar manipulieren.
MITRE	Betreiber des „Federally Funded Research and Development Centers (FFRDC)“ in den USA
OBD	On-Board-Diagnose
OEM	Original Equipment Manufacturer
OMA	Open Mobile Alliance: Arbeitsgruppe führender Dienstleistungs- und Produktanbieter aus dem Bereich Mobilfunk mit dem Ziel, marktfähige, interoperable digitale Dienste zu entwickeln und als Standard weltweit zu etablieren
OMADM	OMA Device Management

OTA	Over-the-Air: Softwareaktualisierung über eine Funkschnittstelle
OWASP	Open Web Application Security Project: Non-Profit-Organisation
P2P-Verbindungen	Point-to-Point-Verbindungen; Verbindungsvariante, bei der eine direkte Verbindung zwischen zwei Netzwerkknoten oder Stationen hergestellt wird
Pen Testing	Penetration Testing; deutsch: Penetrationstests
Privacy by Default	Datenschutz als Standardeinstellung
Privacy by Design	Berücksichtigung des Datenschutzes bereits bei der Konzipierung und Entwicklung von Software und Hardware zur Datenverarbeitung
RxSWIN	Rx = reguliertes Bauteil Nummer x; SWIN = Software Identification Number
RDS	Radio Data System
Sniffing	Analyseinstrument für Datenverkehr in einem Netzwerk
SOTIF	Safety Of The Intended Functionality: Teilgebiet der technischen Produktsicherheit, das sich mit Gefahren technischer Systeme beschäftigt.
Spoofing	Eindringen in Computer oder Netzwerke, indem eine vertrauenswürdige Identität vorgetäuscht wird
TCU	Telematics Control Unit, ein Steuergerät in Kraftfahrzeugen
UNECE	United Nations Economic Commission for Europe; Wirtschaftskommission
V&V	Verification & Validation: Prüfung eines Produkts hinsichtlich seiner Übereinstimmung mit den spezifizierten Anforderungen aus dem Pflichtenheft plus Validierung mittels Feldexperiment hinsichtlich der Erfüllung der Nutzungsziele und somit die Anforderungen des Kunden auf Tauglichkeit
V2C	Vehicle to Cloud: Informationsaustausch zwischen Fahrzeugen und Cloud-Systemen, die beispielsweise auf Backend-Server der Automobilhersteller verweisen und es ermöglichen, Befehle zu verarbeiten, die zwischen verwendeten Diensten übertragen werden
V2I	Vehicle to Infrastructure: Definiert den drahtlosen Austausch von Daten zwischen dem Fahrzeug und der Straßeninfrastruktur, um Informationen über Parkflächen, Behinderungen wie Baustellen oder Unfälle und weitere Ereignisse zu erhalten
V2P	Vehicle to Pedestrian: Kommunikation von Fahrzeugen, der Infrastruktur und mobilen Endgeräten, bisher eher eine Vision, um Informationen über die Umgebung zu verarbeiten
V2V	Vehicle to Vehicle: Hiermit wird der Datenaustausch unter Fahrzeugen selbst beschrieben, der typischerweise Stau- und Unfallinformationen anhand des Standorts kommuniziert
V2X/Car2X	Vehicle to X/Car to X: Datenaustausch oder Kommunikation zwischen einem Fahrzeug und anderen Objekten oder Verkehrsteilnehmer:innen
VSOC	Virtual Security Operations Centre

Literaturverzeichnis

Argus Cyber Security Ltd. (Hrsg.). (2020). Fleet Protection. Building a effective ASOC with Argus Fleet Protection.

AT&T Cybersecurity (Hrsg.). (2020). How to Build a SOC: Threat Intelligence. Zugriff am 14.01.2022. Verfügbar unter *https://cybersecurity.att.com/solutions/security-operations-center/building-a-soc/threat-intelligence*

Baden-Württemberg International (2021): Automobilwirtschaft. Zugriff am 14.01.2022. Online: *https://www.bw-invest.de/standort/branchen-cluster/automobilwirtschaft*

Boehner, M. (2019). Security für vernetzte Fahrzeuge entlang des gesamten Lebenszyklus. ATZelektronik, 14 (1–2), 16–21.

Burkacky, O., Deichmann, J., Klein, B., Pototzky, K. & Scherf, G. (2020). Cybersecurity in automotive. Mastering the challenge (McKinsey Center for Future Mobility, Hrsg.). McKinsey & Company. Zugriff am 14.01.2022. Online: *https://www.gsaglobal.org/wp-content/uploads/2020/03/Cybersecurity-in-automotive-Mastering-the-challenge.pdf*

Crowley, C. & Pescatore, J. (2019). Common and Best Practices for Security Operations Centers. Results of the 2019 SOC Survey. (SANS Institute, Hrsg.) Zugriff am 14.01.2022. Online: *https://www.sans.org/media/analyst-program/common-practices-security-operations-centers-results-2019-soc-survey-39060.pdf*

Domínguez, J. M. L. & Sanguino, T. J. M. (2019). Review on V2X, I2X, and P2X Communications and their Applications: A Comprehensive Analysis over Time. Sensors (Basel, Switzerland), 19 (12).

e-mobil BW (2019). Strukturstudie BWe mobil 2019 – Transformation durch Elektromobilit t und Perspektiven der Digitalisierung. Zugriff am 14.01.2022. Online: *https://www.e-mobilbw.de/fileadmin/media/e-mobilbw/Publikationen/Studien/Strukturstudie2019.pdf*

Haas, R. E. & Moller, D. P. F. (2017). Automotive connectivity, cyber attack scenarios and automotive cyber security. In 2017 IEEE International Conference on Electro Information Technology (EIT) (S. 635–639). IEEE.

Huq, N., Gibson, C. & Vosseler, R. (2020). Driving Security Into Connected Cars: Threat Model and Recommendations. (Trend Micro Research, Hrsg.) Zugriff am 14.01.2022. Online: *http://documents.trendmicro.com/assets/white_papers/wp-driving-security-into-connected-cars.pdf*

Jadhav, Ashish (2021): Automotive Cybersecurity. In: M. Kathiresh, R. Neelaveni (eds.): Automotive Embedded Systems. Springer Nature Switzerland.

Johns, Emma (2020): Cyber Security Breaches Survey 2020. Zugriff am 14.01.2022. Online: *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/893399/Cyber_Security_Breaches_Survey_2020_Statistical_Release_180620.pdf*

Knauel, E., Gramm, J. & Holle, J. (2020). Automotive Cybersecurity – Effizientes Risikomanagement für den gesamten Fahrzeuglebenszyklus. ATZelektronik (11), 26–30.

Koenen, Jens (2021): Hacker legen Autozulieferer EDAG lahm. Zugriff am 14.01.2022. Online: *https://www.handelsblatt.com/unternehmen/industrie/cyberangriff-hacker-legen-autozulieferer-edag-lahm/27005604.html*

Landeslotsenstelle Transformationswissen BW (2021): Wissen kompakt. Fahrzeugdaten. Zugriff am 14.01.2022. Online: *https://www.transformationswissen-bw.de/fileadmin/media/Publikationen/e-mobil_Studien/Wissen_kompakt_Fahrzeugdaten.pdf*

Macher, G., Schmittner, C., Veledar, O. & Brenner, E. (2020). ISO/SAE DIS 21434 Automotive Cybersecurity Standard – In a Nutshell. In A. Casimiro, F. Ortmeier, E. Schoitsch, F. Bitsch & P. Ferreira (Hrsg.), Computer Safety, Reliability, and Security. SAFECOMP 2020 Workshops (Lecture Notes in Computer Science, Bd. 12235, S. 123–135). Cham: Springer International Publishing.

Nolte, Moritz (2020): OBD-Schnittstelle: Wie freien Werkstätten der Zugang zu Fahrzeugdaten erschwert wird. Zugriff am 14.01.2022. Online: *https://herthundbuss.com/branche-mehr/obd-schnittstelle-erschwerter-zugang-fuer-freie-werks-taetten/*

Olt, C. (2019). Aufbau eines Cyberabwehrzentrums für das Connected Car. ATZelektronik, 14 (5), 44–47.

Pomper, A. (2019). Vehicle Security Operation Centers: NTT Security fordert V-SOCs für digitale Fahrzeuge, funkschau.de. Zugriff am 13.04.2021. Online: *https://www.funkschau.de/markt-trends/ntt-security-fordert-v-socs-fuer-digitale-fahrzeuge.162585.html*

Roscoe, J. F., Baxandall, O. & Hercock, R. (2020). Simulation of Malware Propagation and Effects in Connected and Autonomous Vehicles. In 2020 International Conference on Computing (S. 57–62).

Schawel, C. & Billing, F. (2017). Morphologischer Kasten. In C. Schawel & F. Billing (Hrsg.), Top 100 Management Tools. Das wichtigste Buch eines Managers. Von ABC-Analyse bis Zielvereinbarung (6. Aufl., S. 219–221). Wiesbaden: Gabler.

Schmittner, C. & Macher, G. (2019). Automotive Cybersecurity Standards – Relation and Overview. In A. Romanovsky, E. Troubitsyna, I. Gashi, E. Schoitsch & F. Bitsch (Hrsg.), Computer Safety, Reliability, and Security (Lecture Notes in Computer Science, Bd. 11699, S. 153–165). Cham: Springer International Publishing.

Solms, R. von & van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97–102.

Tengler, S. (2020). Top 25 Auto Cybersecurity Hacks: Too Many Glass Houses To Be Throwing Stones, Forbes. Zugriff am 14.01.2022. Online: *https://www.forbes.com/sites/stevetengler/2020/06/30/top-25-auto-cybersecurity-hacks-too-many-glass-houses-to-be-throwing-stones/?sh=8a10f2d7f65d*

Vosseler, R., Huq, N., Gibson, C. & Kropotov, V. Cybersecurity for Connected Cars. Exploring Risks in 5G, Cloud, and Other Connected Technologies. (Trend Micro Research, Hrsg.). Zugriff am 14.01.2022. Online: *https://documents.trendmicro.com/assets/white_papers/wp-cybersecurity-for-connected-cars-exploring-risks-in-5g-cloud-and-other-connected-technologies.pdf*

Waheed, M. & Cheng, M. (2017). A system for real-time monitoring of cybersecurity events on aircraft. In 2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC) (S. 1–3).

Impressum

Herausgeber
Cluster Elektromobilität Süd-West c/o
e-mobil BW GmbH – Landesagentur für neue Mobilitätslösungen und Automotive Baden-Württemberg

Autoren
P3 group
Lucas Bublitz
Alexander Boll
Patrick Eisele
Tobias Löhr
Damian Weinzierl

Redaktion und Koordination des Themenpapiers
e-mobil BW GmbH
Valeria Kropar

Layout/Satz/Illustration
markentrieb
Die Kraft für Marketing und Vertrieb

Fotos
Umschlag: © pickup/AdobeStock, © anttoniart/AdobeStock
Die Quellennachweise aller weiteren Bilder befinden sich auf der jeweiligen Seite.

Auslieferung und Vertrieb
e-mobil BW GmbH, Leuschnerstraße 45, 70176 Stuttgart
Telefon +49 711 892385-0, Fax +49 711 892385-49, info@e-mobilbw.de, www.e-mobilbw.de

Januar 2022

www.e-mobilbw.de

e-mobil BW GmbH
Landesagentur für neue Mobilitätslösungen und
Automotive Baden-Württemberg

Leuschnerstraße 45 I 70176 Stuttgart
Telefon +49 711 892385-0 I Fax +49 711 892385-49
info@e-mobilbw.de