Österreichisches Institut
für Medienwirtschaft

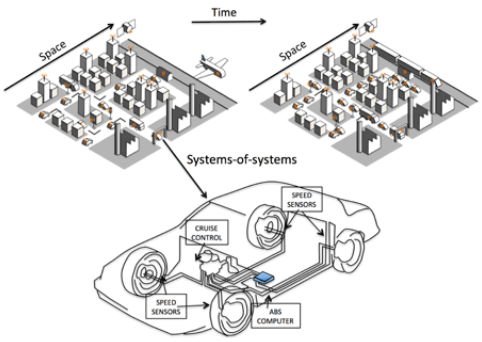
KIRAS KIF

GSK-Endbericht

Gesellschaftliche Aspekte vernetzter, autonomer Mobilität.

Eine sozialwissenschaftliche Folgenabschätzung zum KIRAS Projekt

Hochsichere, langzeitige Kryptografie für kabellose Kommunikation in der vernetzten Mobilität.



Quelle: ERCIM 2016 (CC-BY)

Autoren:
Philipp Schaumann
Tassilo Pellegrini
Barbara Seyfried

St. Pölten, am 05.11.2018

Inhalt

Executive Summary ____ *5*

1. Einleitung ____ *7*

1.1 Fragestellungen und Methode ____ 9

1.2 Aufbau der Arbeit ____ 9

2. Begriffsklärung und Erkenntnisstand ____ *11*

2.1. Vernetzte Mobilität (CASE: Connected) ____ 11

2.2. Autonome vs. Automatisierte Mobilität (CASE: Autonomous) ____ 13

2.3. Shared & Services ____ 16

2.4. Elektrische Kontroll- und Antriebssysteme (CASE: Electric) ____ 18

3. Gesellschaftliche Auswirkungen vernetzter, autonomer Mobilität ____ *19*

3.1 Unfallreduktion/-vermeidung ____ 20

3.2 Mobilitätssteigerung ____ 21

3.3 Stauvermeidung ____ 21

3.4 Siedlungsstruktur und Raumbewirtschaftung ____ 21

3.5 Eigentums- und Nutzungsmodell ____ 22

3.6 Energieverbrauch und Emissionen ____ 23

3.7 Transformationskosten ____ 23

3.8 Akzeptanz ____ 24

4. (Un-)Sicherheit und vernetzte autonome Mobilität ____ *25*

4.1 Der Schutzbedarf von IT-Systemen - Bedrohung wogegen? ____ 27

4.2 Threat Modeling – systematische Bedrohungsanalyse ____ 28

4.3 Safety und Security in modernen Fahrzeugen ____ 31

4.4 Safety und Security im “Internet of Things” ____ 33

4.5 Safety und Security in der autonomen Mobilität ____ 35

5. Safety und Security in der vernetzten Mobilität ____ *38*

5.1 Technische Integrität der Nachrichten ____ 39

5.2 Integrität und Verlässlichkeit aller Teilnehmergeräte _____39

5.3 Identität und Authentizität der Teilnehmer _____41

6. Resumé _____ 43

7. Literaturverzeichnis _____ 44

Annex 1: Geschichte der Automatisierung und Stand der Technik_____ 62

Annex 2: Artificial Intelligence in der autonomen Mobilität _____ 65

Annex 3: Service-Orientierung & Fahrzeuge als hybride Produkte _____ 69

Abbildungsverzeichnis

Abb. 1: Automatisierungsgrad des automatisierten Fahrens, eigene Darstellung in Anlehnung an VDA 2017. 14

Abb. 2: The New Threat Modeling Process nach Microsoft 2007. 29

Abb. 3: Codebases – Millions of Lines of Code (Doughty-White & Quick 2015). 32

Abb. 4: Merkmale menschlicher Intelligenz übertragen auf autonomes Fahren, eigene Darstellung in Anlehnung an Habel et al. (2003, S.349). 66

Abb. 5: Nutzung der durch autonomes Fahren gewonnenen Zeit" (Deloitte 2016, S.16). 72

Executive Summary

Dieser Report diskutiert die Frage, wie eine vertrauenswürdige und sichere Kommunikationsinfrastruktur in einem digital vernetzten Mobilitätssystem hergestellt werden kann. Hierbei behandelt der Report vornehmlich jene Aspekte, die die Sicherheit eines Fahrzeuges direkt beeinflussen. Dies betrifft den Informationsaustausch zwischen Fahrzeugen untereinander (C2C) sowie die Kommunikation des Fahrzeuges mit der Verkehrsinfrastruktur (C2I). Indirekte Einflussfaktoren, die aus der Kommunikation des Fahrzeuges mit weiteren technischen Einrichtungen entstehen (C2X), können in diesem Report nicht berücksichtigt werden.

Zur Eingrenzung und Strukturierung des Untersuchungsgegenstandes wird auf das CASE-Paradigma Bezug genommen. Das Designkonzept CASE wurde durch den Automobilkonzern Daimler geprägt und steht für ein neues Fahrzeugdesign, dass die Eigenschaften **C**onnected, **A**utonomous, **S**hared & Services und **E**lectric zu einem integrierten Produkt vereint (Daimler 2018).

Um die Wirkungsdimensionen der autonomen Mobilität im Vergleich zum herkömmlichen System besser zu verstehen, wurden die sozialen, ökonomischen und ökologischen Effekte aus der Literatur zur autonomen Mobilität zusammengetragen und gegenüberstellend diskutiert. Hierbei wird ersichtlich, dass je nach Studiendesign und Motivation die Effekte alles andere als homogen, im schlimmsten Fall sogar widersprüchlich sind, was eine effektive Folgenabschätzung erheblich erschwert.

Zusätzlich wird in dieser Studie herausgearbeitet, dass die Technologien dieses KIRAS-Projekts nur einen Teilaspekt der sicheren Kommunikation lösen: Die zwischen Fahrzeugen und mit der vernetzten Infrastruktur ausgetauschten Nachrichten können mit Hilfe der hier entwickelten Technologie als unverändert und abhörsicher betrachtet werden, leider aber nicht als vertrauenswürdig, da eine sichere Authentisierung fehlt.

Eine sichere Verschlüsselung aller Nachrichten ist Grundlage einer sicheren Vernetzung und damit eine notwendige Voraussetzung für einen vertrauenswürdigen Austausch von Nachrichten zwischen Fahrzeugen und Komponen-

ten einer vernetzten Verkehrsinfrastruktur. Es verbleiben aber für einen wirklich sicheren Nachrichtenaustausch weitere Herausforderungen, für die es in der Informationssicherheit zwar theoretische Lösungen gibt, für die aber derzeit keine praktisch mit vertretbarem Aufwand umsetzbare Lösungen existieren. Das heißt, die gegenständliche Arbeit des KIRAS-Projektes löst nur eine der drei grundlegenden Problemstellungen zur Gewährleistung einer sicheren Kommunikation, leistet jedoch einen wichtigen Beitrag um diese herzustellen.

1. Einleitung

Gesellschaft, Politik und Wirtschaft im 21. Jahrhundert sind mehr denn je geprägt von Technik und Innovation (Castells 2009). Neben vielen Lebensbereichen ist insbesondere der Mobilitätssektor durch zunehmende Digitalisierung und Vernetzung geprägt und wird in Folge um „smarte“ Funktionen angereichert. Der dabei stattfindende Prozess der *Datafizierung* (Hepp 2016) bedingt bisweilen tiefgreifende Veränderungen des bestehenden Mobilitätssystems mit weitreichenden Effekten nicht nur auf den Personen- und Güterverkehr, sondern auch die Gesellschaft als Ganzes.

Digitale Services bilden in Zukunft die Schnittstelle zwischen Fahrzeugen, der Verkehrsinfrastruktur und Menschen in ihren unterschiedlichen und funktional interdependenten Rollen – als Arbeitgeber und Arbeitnehmer, als Produzent und Konsument, als Systemanbieter und Systemnutzer (ATKearney 2016). Hierbei verspricht die Digitalisierung eine effizientere Kontrolle und Steuerung mobilitätsrelevanter Produkte sowie daran gekoppelter Folgeleistungen. Doch den erhofften Verbesserungen und positiven Effekten stehen auch unerwünschte Folgen gegenüber. Dazu gehören etwa vor dem Hintergrund der zunehmenden Vulnerabilität vernetzter Systeme bislang unzureichend bearbeitete Fragestellungen zur Herstellung eines sicheren und gesellschaftlich inklusiven Mobilitätssystems. Zusätzlich wird die Debatte von einer Reihe ethischer Fragestellungen flankiert, die sich bisher einer zufriedenstellenden Beantwortung entziehen (Nyholm & Smids 2016).[1]

Der Untersuchungsgegenstand der vernetzten Mobilität ist zu vielschichtig und komplex um alle auftretenden Problemstellungen, die an der Schnittstelle von

[1] Für eine differenzierte Diskussion der ethischen Implikationen der vernetzten Mobilität siehe den Report der Ethikkommission zur autonomen und vernetzten Mobilität des Deutschen Bundesministeriums für Transport und Digitale Infrastruktur (BMVI 2017). Eine Analyse der Deutsche Bank Research zu den Auswirkungen der Digitalisierung auf den Autoproduktionsstandort Deutschland findet sich bei Heymann & Meister (2017).

Mensch, Technik und Sicherheit kristallisieren, zu behandeln.[2] Dieser Report konzentriert sich deshalb auf Fragen der Safety und Security im Kontext autonom und vernetzt agierender Fahrzeuge und daraus resultierenden gesellschaftlichen Implikationen.

Im Kern steht damit die Frage, wie eine vertrauenswürdige und sichere Kommunikationsinfrastruktur in einem digital vernetzten Mobilitätssystem hergestellt werden kann. Dies betrifft den Informationsaustausch zwischen Fahrzeugen untereinander (C2C) sowie die Kommunikation des Fahrzeuges mit der Verkehrsinfrastruktur (C2I).[3] D.h. in diesem Report werden all jene Aspekte behandelt, die die Sicherheit eines Fahrzeuges direkt beeinflussen. Indirekte Einflussfaktoren, die aus der Kommunikation des Fahrzeuges mit weiteren technischen Einrichtungen entstehen (C2X), können in diesem Report nicht berücksichtigt werden.

Bereits diese Einteilung macht deutlich, dass die Sicherheitsanforderungen an vernetze Mobilität einen weitaus höheren Komplexitätsgrad aufweisen, als dies in konventionellen Mobilitätssituationen der Fall ist. Dieser Umstand wird auch dadurch verschärft, als Datensicherheit laut diverser Untersuchungen insbesondere aus Perspektive der Endkonsumenten ein kritischer Aspekt in der Herstellung von Akzeptanz für und Vertrauen in die vernetzte Mobilität darstellt.[4]

---

[2] Konzepte der „smarten Mobilität“ und die Eingliederung in Ansätze wie der Smart-City (Wolter 2012; Gläser & Lesko 2017), werden nicht weiter ausgeführt. Wenn im Nachfolgenden vom Service-Konzept „Autonomes Fahren“ gesprochen wird, ist dies nicht mit dem bereits existierenden Begriff des „Mobility as a service“ (Brünglingshaus 2013) zu verwechseln, welche die Zusammenfassung unterschiedlicher Formen von Transportmöglichkeiten in einen mobilen Service beschreibt.

[3] Der Vollständigkeit wegen sei erwähnt, dass ein Sicherheitskonzept auch die Kommunikation zwischen den im Fahrzeug verbauten Komponenten berücksichtigen muss. Dieser Aspekt wird jedoch in diesem Report nicht weiter berücksichtigt.

[4] Siehe dazu Kapitel 2.2.8 in diesem Report.

1.1 Fragestellungen und Methode

Vertiefend zu den bestehenden Ausführungen stehen in diesem Report folgende Fragestellungen im Mittelpunkt:

1) Welche gesellschaftlichen Effekte gehen mit der Transformation des Mobilitätswesens entlang des CASE Paradigmas einher?
2) Was sind charakteristische Sicherheitsprobleme, die sich aus dem CASE Paradigma ableiten lassen?
3) Welchen Basiskriterien muss das Design einer belastbaren Security- und Safety-Architektur für autonome, vernetzte Mobilität genügen?
4) Welche Rolle kann dabei die Technologie des gegenständlichen KIRAS-Projekts spielen?

Die Bearbeitung dieser Fragestellungen erfolgt auf Basis einer umfangreichen Literaturanalyse sowie daraus abgeleiteten Empfehlungen für das Design einer sicheren und vertrauenswürdigen Sicherheitsarchitektur.

1.2 Aufbau der Arbeit

Kapitel 2 dieses Reports widmet sich der notwendigen Begriffsklärung und dokumentiert den Erkenntnisstand zur vernetzten Mobilität. Dazu wird ausgehend vom CASE-Paradigma eine Reihe von gesellschaftlichen Aspekten der vernetzten Mobilität identifiziert und der Literaturstand dargestellt.

Kapitel 3 diskutiert gesellschaftliche Auswirkungen einer vernetzten, autonomen Mobilität und hinterfragt kritisch bestehende Annahmen zu positiven und negativen Folgeeffekten eines Mobilitätssystems neuer Prägung.

Kapitel 4 stellt die Aspekte aus Kapitel 3 in den Kontext der aktuellen Diskussion um geeignete Security-Konzepte für eine vernetzte, autonome Mobilität und identifiziert offene Fragen in Bezug auf ein geeignetes Security-Design.

Kapitel 5 diskutierte zentrale Design-Kriterien eines adäquaten Safety- und Security-Konzeptes für vernetzte, autonome Mobilität. Dabei wird herausgearbeitet, dass die Technologie des gegenständlichen KIRAS-Projekts einen der Teilaspekte dieser kritischen Sicherheitsanforderungen bearbeitet, die ande-

ren Aspekte sicherer Kommunikation und Vernetzung aber weiter offen bleiben.

Kapitel 6 schließt den Berichtsteil des Reports mit einer knappen Conclusio.

Weiters enthält der Report drei Anhänge, in denen Partikularaspekte der vernetzten Mobilität wie etwa die Geschichte der Automatisierung (Annex 1), die Rolle der künstlichen Intelligenz in der autonomen Mobilität (Annex 2) sowie die Hybridisierung autonomer Fahrzeuge als Service-Produkt (Annex 3) vertieft werden.

2. Begriffsklärung und Erkenntnisstand

Die aktuelle Erkenntnislage zur Sicherheitsrisiken der autonomen Mobilität ist umfangreich, aber nur wenig systematisiert. Der Publikationsstand ist gekennzeichnet durch eine Fülle an Industriestudien und einen lebhaften wissenschaftlichen Diskurs. Zur Eingrenzung und Strukturierung des Untersuchungsgegenstandes wird auf das CASE-Paradigma Bezug genommen. Das Designkonzept CASE wurde durch den Automobilkonzern Daimler geprägt und steht für ein neues Fahrzeugdesign, dass die Eigenschaften **C**onnected, **A**utonomous, **S**hared & Services und **E**lectric zu einem integrierten Produkt vereint (Daimler 2018). Im Folgenden wird dieses Paradigma einer vertiefenden Betrachtung unterzogen.

2.1. Connected (CASE)

Die Vernetzung von Fahrzeugen lehnt sich an das Konzept des Internet der Dinge (engl. Internet of Things, Abk. IoT) an. In diesem sollen bis zum Jahr 2020 zwischen 50 und 100 Mrd. physische Objekte miteinander verknüpft sein (vgl. IEEE Standards Association 2013). Dazu gehören auch Fahrzeuge für den Personen- und Gütertransport.

Im Internet der Dinge geht es nicht nur um die Beziehung zwischen Mensch und Maschine, sondern auch um die Kommunikation zwischen den Dingen selbst, welche in Folge eine Bedingung für die vernetzte Mobilität darstellt (Andelfinger und Hänisch 2015, S.9). Die Maschinenkommunikation bildet laut Samulat (2017, S.14) die Grundlage für eine flexiblere, effizientere Produktions- und Prozessinfrastruktur. Daten- und analysegestützte Wertschöpfungsketten würden alle Phasen des Produktlebenszyklus miteinschließen und Produkte individuell auf die Umweltbedingungen und Kundenwünsche ausrichten (ebd., S.4). Den technologischen Kern des IoT im Verkehrswesen bilden laut Samulat (2016, S.29) sogenannte „Embedded Systems“ (dt. eingebettete Systeme), die längst in die Automobilelektronik Einzug gehalten haben. In diesem Kontext spricht man vom „Internet of Vehicles“ (IoV) als Grundlage eines intelligenten Transportsystems (ITS) (APEC 2014, S.1): „The Internet of Vehicles

(IoV) is an integration of three networks: an inter-vehicle network, an intra-vehicle network, and vehicular mobile Internet."

In Kombination dieser drei Netzwerktypen wird das IoV als System beschrieben, das drahtlose Kommunikation und den Informationsaustausch zum einen zwischen den im Fahrzeug verbauten Komponenten als auch zwischen Fahrzeugen untereinander („Car2Car Communication", C2C) bzw. die Kommunikation mit der Infrastruktur (C2I) und der Umwelt des Autos bzw. anderer Einrichtungen („Car2X Communication") ermöglicht.[5]

Lee et al. (2016, S.1) weisen darauf hin, dass digitale Informationen innerhalb des Verkehrs bisher weitgehend über Plattformen bezogen wurden, die über Sender eine Verbindung zum Internet oder einer alternativen Telekommunikationsinfrastruktur herstellen. Darauf aufbauende Dienste inkludieren beispielsweise die Erfassung der aktuellen Verkehrssituation. Im IoV sollen Fahrzeuge ihre Daten unmittelbar untereinander austauschen ohne zwingend auf einen Intermediär wie einen Plattformbetreiber angewiesen zu sein. Das speziell für Fahrzeuge konzipierte Netzwerk wird in der Fachliteratur als „vehicular fog" bezeichnet (ebd., S.2): „This mobile cloud provides several essential services, from routing to content search, spectrum sharing, dissemination, attack protection, and so on to AUV [autonomous vehicles – Anm. d. A.] applications via standard, open interfaces".

Das Konzept *vehicular fog* bezeichne also die Kombination eines Fahrzeugs mit einem IT-System, welches als intelligenter Agent fungiere und die Funktionen „networking" und „computing" miteinander vereine, so Lee et al. (vgl. ebd., S.3) weiter. Dies umfasse auch das sogenannte Fahrzeug-Ad-Hoc-Netzwerk (engl. *vehicular ad hoc network*, Abk. VANET), welches in Form eines mobile ad hoc network (MANET), diverse Knotenpunkte (hier: Autos) miteinander zu kommunikativen und Information austauschenden Zwecken verknüpft (vgl. ebd., S.2).

[5] In der Literatur wird oft statt „car" der Begriff „vehicle" (dt. Fahrzeug) verwendet. Laut VDA (vgl. o.J.) werde als Überbegriff für die Vernetzung bzw. Kommunikation mit diversen Adressaten der Terminus „Vehicle-to-X" (V2X) verwendet.

2.2. Autonomous (CASE)

Schon heute wird der/die Fahrer/in durch verfügbare Fahr- und Parkfunktionen für assistiertes und teilautomatisiertes Fahren und Parken entlastet. Zusätzlich zu Fahrassistenzsystemen (FAS) wie bspw. dem *Adaptive Cruise Control* (ACC), das über einen automatischen Abstandsregeltempomat verfügt um Unfällen vorzubeugen (vgl. Volkswagen 2017), werden in den nächsten Jahren Fahrzeuge mit neuen Technologien ausgestattet, die mithilfe von Sensoren und semantischer Informationsverarbeitung eine steigende Anzahl von Fahrfunktionen unterstützen bis hin zur völlig autonomen Steuerung des Fahrzeugs ohne menschliches Zutun.

> „Unter dem automatisierten Fahren versteht man das selbstständige, zielgerichtete Fahren eines Fahrzeugs im realen Verkehr mit bordeigenen Sensoren, nachgeschalteter Software und im Fahrzeug gespeicherten Kartenmaterial für die Erfassung der Fahrzeugumgebung“ *(VDA. 2015, S.19).*

Die dafür notwendige Entwicklung und Integration künstlicher Intelligenz (KI)[6] lässt diese Thematik jedoch wesentlich komplexer werden. KI ermächtigt die im Fahrzeug implementierte Steuerungssoftware selbstständig und menschenähnlich zu entscheiden, und so das Verhalten des Fahrzeugs dynamisch an die Umweltbedingungen anzupassen.[7]

In diesem Kontext ist die Unterscheidung zwischen „Autonomie“ und „Automatisierung“ essenziell. Während „automatisiert“ das Vorhandensein von Fahrassistenzsystemen bezeichnet, die den/die Fahrerin bei der Fahraufgabe unterstützen können, bedeutet „autonom“ die vollständige Übernahme der Fahr-

[6] Siehe dazu auch Annex 2 in diesem Report.

[7] Im wissenschaftlichen Diskurs (Görz et al. 2003, S. 25) wird jedoch angezweifelt, ob eine ausreichende Lernfähigkeit überhaupt erreicht werden kann, da trotz diverser Methoden des maschinellen Lernens und speziell entwickelter Lernverfahren die Verlässlichkeit und Adaptionsfähigkeit bestehender Systeme vor dem Hintergrund der real gegebenen Umweltkomplexität (noch) unzureichend sind.

und Parkfunktionen und die damit verbundene Kommunikation zwischen Fahrzeugen und der umliegenden Verkehrsinfrastruktur (vgl. VDA 2015).

Die US-amerikanische Branchenvertretung der Automobilindustrie SAE (SAE International 2016) sowie der deutsche Verband der Automobilindustrie (VDA 2015) definieren sechs Stufen der Automatisierung (siehe Abb.1), die im internationalen Vergleich die Entwicklung von assistiertem und teilautomatisiertem Fahren und Parken zusammenfasst (vgl. VDA 2015).

Stufe 0	Stufe 1	Stufe 2	Stufe 3	Stufe 4	Stufe 5
Driver Only	Assistiert	Teilautomatisiert	Hochautomatisiert	Vollautomatisiert	Fahrerlos
Fahrer führt dauerhaft Längs- **und** Querführung aus	Fahrer führt dauerhaft Längs- **oder** Querführung aus	Fahrer **muss** das System **dauerhaft** überwachen	Fahrer muss das System **nicht** mehr **dauerhaft** überwachen	Kein Fahrer erforderlich im spez. Anwendungsfall	Von **"Start"** bis **"Ziel"** ist kein Fahrer erforderlich
			Fahrer muss potenziell in der Lage sein zu übernehmen		
Kein eingreifendes Fahrzeugsystem aktiv	System übernimmt die jeweils andere Funktion	System übernimmt Längs- und Querführung in einem spez. Anwendungsfall	System übernimmt Längs- **und** Querführung in einem spez. Anwendungsfall (erkennt Systemgrenzen und fordert den Fahrer zur Übernahme mit ausr. Zeitreserve auf	System **kann im spez. Anwendungsfall** alle Situationen automatisch bewältigen	Das System übernimmt die Fahraufgabe vollumfänglich bei allen Straßentypen, Geschwindigkeiten und Umfeldbedingungen

Abb. 1: Automatisierungsgrad des automatisierten Fahrens, eigene Darstellung in Anlehnung an VDA 2017.

In der ersten Stufe, **Stufe 0**, sind noch keinerlei automatisierte Funktionen vorhanden. Die Längsführung (Geschwindigkeit halten, Gas geben und Bremsen), sowie die Querführung (Lenken) obliegen dem Fahrer/der Fahrerin. Fahrzeugsysteme sind noch nicht dazu in der Lage einzugreifen, sondern haben lediglich eine Warnfunktion.

Auf **Stufe 1** übernimmt das System eine der beiden Führungen, entweder längs oder quer, die Verantwortung für die jeweils andere bleibt aber dem Fahrer/der Fahrerin überlassen, weshalb man von vom assistierten Fahren spricht.

Ab **Stufe 2** ist von teilautomatisiertem Fahren die Rede: Hier kann das System die Längs- und Querführung in einem spezifischen Anwendungsfall übernehmen. Diese Fälle beziehen sich auf Straßentypen, Geschwindigkeitsbereiche und die Reaktion auf Umfeldbedingungen. Jedoch muss der Fahrer/die Fahrerin das System dauerhaft überwachen und in einer Gefahrensituation jederzeit eingreifen können.

Dies unterscheidet das teilautomatisierte vom hochautomatisierten Fahren, der **Stufe 3**. Das System ist in der Lage Längs- und Querführung in einem spezifischen Anwendungsfall komplett zu übernehmen. Zusätzlich jedoch erkennt es Systemgrenzen, die durch die Umgebung beeinträchtigt werden können und fordert den Fahrer/die Fahrerin früh genug zur Übernahme auf. Zu diesem Zeitpunkt muss der Fahrer/die Fahrerin in der Lage sein seine/ihre Funktion als solche/r wieder wahrzunehmen. Die Überwachung des Systems durch den Menschen muss nicht dauerhaft erfolgen, sollte aber dennoch ausgeübt werden. Nebentätigkeiten des Fahrers/der Fahrerin sind daher begrenzt möglich.

Mit **Stufe 4** erfolgt schließlich die Vollautomatisierung: Ein/e Fahrer/in ist im spezifischen Anwendungsfall nicht mehr erforderlich, da das System die jeweilige Situation automatisch und selbstständig bewältigen kann.

Stufe 5 beschreibt das bereits definierte fahrerlose, vollständig autonome Fahren. Vom Start bis Ziel ist kein/e menschliche/r Fahrer/in mehr erforderlich, der/die das Auto lenkt und kontrollieren müsse. Das System ist dazu fähig, die Fahrfunktion vollumfänglich auf allen Straßentypen, in allen Geschwindigkeitsbereichen und unter sämtlichen Umfeldbedingungen zu übernehmen.

Im Gegensatz zu den sechs Automatisierungsgraden des VDA, die im Dialog oft nur als die „5 Stufen“ bezeichnet werden (Stufe 0 wird als solche nicht anerkannt, da keinerlei Autonomie besteht und die volle Verantwortung beim Fahrer liegt), stuft die US-amerikanische „National Highway Traffic Safety Administration“ (NHSTA) in nur vier Stufen ab (vgl. Knott 2016). Da sich die Stufen 4 und 5 kaum unterscheiden, werden diese hier zusammengefasst. Der entscheidende Unterschied liegt jedoch in den beschriebenen Anwendungsfällen, die in Stufe 4 noch beschränkt sind, im weiteren Schritt jedoch

ohne Einschränkung übernommen werden würden. Die US-amerikanische RAND Corporation (Anderson et al. 2016) wiederum schlägt ein fünf-stufiges Modell vor, dass die Stufen 4 und 5 der VDA-Klassifikation zusammenfasst.

Diese abweichenden Klassifikationsmodelle belegen unter anderem die fehlende Systematik im Diskurs.[8] Umso wichtiger ist es darauf zu achten, dass bei der Beschreibung und Analyse von automatisierten bzw. autonomen Fahrzeugen auf die exakte Definition geachtet werden muss, um Unklarheiten im Diskurs zu vermeiden. Diesem Report liegt im Weiteren das Klassifikationsmodell der VDA zugrunde.

2.3. Shared & Services (CASE)

Mobilitätskonzepte der Zukunft verstehen das Fahrzeug als Bestandteil eines umfassenden Ökosystems bestehend aus personalisierten Dienstleistungen und Produktangeboten.

Der Bundesverband für Digitale Wirtschaft e.V. (BVDW 2016a, 2016b, o.J.) fasst die wesentlichen Aspekte des „Ökosystems Connected Cars“ in drei Diskussionspapieren zusammen. Dabei wird der Wandel des Autos im Kontext der Serviceorientierung, Chancen und Risiken der Anbieter im Automobilmarkt als auch auf neu entstehende Geschäftsmodelle betrachtet. Als bezeichnendes Merkmal rücken Sharing-Modelle sowie Info- und Entertainment laut BVDW (2016b) immer weiter in den Vordergrund, wobei der Konsum von Mobilitätsdiensten und Inhalten elementarer Bestandteil des Fahrererlebnisses sei („Driving vs. User Experience“).[9]

[8] Dieses Problem wird unter anderem von Cabrall et al. (2017) aufgegriffen, die ein generisches Klassifikationsschema der Automatisierung vorschlagen, das den Grad der Autonomie entlang folgender Dimensionen ableitet: (1) Location (from local to remote), (2) Identity (between human and computer), (3) Number of agents (degree of centralization of control), (4) adaptive optimization over Time.

[9] Für eine vertiefende Diskussion des Begriffes „Service-Orientierung“ siehe Annex 3 in diesem Report.

Insbesondere private Sharing-Modelle haben das Potenzial bestehende Mobilitätskonzepte, die auf dem persönlichen Besitz eines Fahrzeuges aufbauen, radikal zu verändern (Clewlow & Mishra 2017). Vor allem im urbanen Bereich entwickeln sich Sharing-Modelle zu einer tragfähigen Geschäftsgrundlage sowohl für kommerzielle (Giffi et al. 2017) als auch gemeinnützige (Clewlow & Mishra 2017) Anbieter. So nutzen laut einer aktuellen Befragung (Giffi et al. 2017) in den urbanen Metropolen Indiens bereits 85% der Bevölkerung sogenannte Shared Mobility Services und 61% der Befragten sehen keinen Bedarf mehr für den persönlichen Ankauf eines Fahrzeuges. Ähnliche Befunde, allerdings auf einem geringeren Niveau, finden sich für die USA. Dort nehmen bereits 21% der urbanen Bevölkerung sogenannte Ride-Hailing-Services in Anspruch, wobei die Nutzungsintensität sowie die Einstellung zum persönlichen Besitz eines Fahrzeuges sehr stark von Faktoren wie Alter, Bildung und Wohnort abhängig sind (Clewlow & Mishra 2017). Giffi et al. (2017, S. 4) folgern:

> "Such statistics point toward a growing trend of mass urbanization happening in many countries and a potential future where personal vehicle ownership is drastically reduced in favor of shared mobility fleets—a significantly different global market reality to which traditional manufacturers, suppliers, and other stakeholders may find it difficult to adjust."

In Bezug auf die Kommerzialisierung neuer Mobilitätsdienste ist erkennbar, dass IT-Unternehmen für die Automobilhersteller immer wichtiger werden. Interessant in diesem Zusammenhang ist die Bezeichnung autonomer Fahrzeuge als „hybride Produkte", also die „intelligente und innovative Verknüpfung von Sach- und Dienstleistungen" (Wassmus 2014, S. VII.). Dazu arbeiten Johanning & Mildner (vgl. 2015, S.5) mithilfe diverser SWOT-Analysen die Stärken und Schwächen sowie Chancen und Risiken einer zunehmenden Service-Orientierung im Mobilitätswesen heraus. Daraus lassen sich drei we-

sentliche Service-Dimensionen ableiten: Sicherheit, Effizienz und Infotainment.[10]

Die Kombination dieser drei Dimensionen macht vernetzte Fahrzeuge „das disruptive Potenzial eines GameChangers im Automobilmarkt“ (vgl. BVDW 2016a S.9) und verwandeln konventionelle Fahrzeuge zu „mobilen ‚Infotainment'-Vehikeln, so der BVDW im Diskussionspapier zum Thema Services im Bereich der Connected Cars. Gängige Verkaufs- bzw. Kaufargumente von Fahrzeugherstellern wie Fahreigenschaften, Beschleunigungsleistung u.Ä. würden an Bedeutung verlieren und neue Funktionen wie etwa die Display-Auflösung, das Betriebssystem, die gegebene Content- und Service-Vielfalt an Bedeutung gewinnen.

2.4. Electric (CASE)

Die Digitalisierung der Mobilität geht einher mit einer umfangreichen Elektrifizierung der Antriebssysteme und Digitalisierung der Kontrollsysteme. So erklärt der Vorstandschef des deutschen Chipherstellers *Infineon,* Reinhard Ploss, dazu im Interview mit der FAZ (vgl. Lindner 2017), dass die Elektronik bei der Entwicklung von Autos bereits für 80 bis 90 Prozent des Innovationsanteils stehe. Dies bezieht sich nicht nur auf neue bzw. alternative Antriebsformen, sondern schließt auch den zunehmenden Ersatz mechanischer Komponenten durch elektronische Steuerungs- und Kommunikationseinheiten (Electronic Control Units - ECUs) mit ein. Diese ECUs bilden im Wesentlichen die technologische Grundlage für die vorhergehenden Ausführungen des CASE-Paradigmas und sollen im Folgenden nicht weiter vertieft werden. Aus Security-Perspektive ist jedoch darauf hinzuweisen, dass laut Koscher et al. (2010) es insbesondere diese ECUs sind, welche die Sicherheitsanforderungen an Fahrzeuge der nächsten Generation definieren und teilweise radikal

[10] Bei der Lektüre diverser Studien fällt auf, dass der Service-Charakter eines autonomen Fahrzeuges vorwiegend über den Infotainment-Aspekt argumentiert wird (z.B. Feng et al. 2014, Diewald et al. 2011, Bose 2010), wobei die Aspekte Sicherheit und Effizienz nachgelagert sind.

neue Ansätze in der Sicherheitsarchitektur notwendig machen (siehe dazu Kapitel 5).

Eine weitere Konsequenz der Digitalisierung besteht in der nahtlosen Überwachbarkeit der Fahrzeugnutzung sowohl für private als auch kommerzielle oder staatliche Zwecke, woraus diverse datenschutzrechtliche Probleme entstehen. Mittels vom Fahrzeugproduzenten bereitgestellter Software können je nach Autonomiestufe Fahrstil, Kraftstoff- bzw. Energieverbrauch, Materialverschleiß u.v.a.m. aufgezeichnet, aggregiert und weiterverarbeitet werden. Dies ermöglicht den Herstellern, Service-Providern (inkl. Versicherungsunternehmen) und Endnutzern zum einen die Konfiguration personalisierter Mobilitätsprodukte und eine verbesserte Planungsgrundlage für mobile Aktivitäten, schließt jedoch zum anderen die Weitergabe der oftmals sensiblen Daten an Dritte für Zwecke des Profilings mit ein. Dieses auch unter dem Begriff „Mobilitätsdilemma“ bekannte Problem (Kreuzbauer 2018) kann u.U. weitreichende Folgen für die Akzeptanz vernetzter, autonomer Mobilität zugrundeliegender Geschäfts- und Service-Modelle haben.[11]

3. Gesellschaftliche Auswirkungen vernetzter, autonomer Mobilität

Um die Wirkungsdimensionen der autonomen Mobilität im Vergleich zum herkömmlichen System besser zu verstehen, werden im Folgenden zusammenfassend die sozialen, ökonomischen und ökologischen Effekte beschrieben, die in die Literatur zur autonomen Mobilität Eingang gefunden haben. Die folgenden Auswahl an Wirkungsdimensionen orientiert sich, wenn nicht anders angegeben, auf eine Policy-Empfehlung der RAND Corporation zu autonomen Fahrzeugen (Anderson et al. 2016), die Scoping Studie des britischen UCL Transport Insititute (Cohen et al. 2017) sowie eine Metastudie zur autonomen Mobilität des kanadischen Victoria Transport Policy Institute (Litman 2018).

[11] Siehe dazu auch die Ausführungen unter Punkt 3.8.

3.1 Unfallreduktion/-vermeidung

Breite Einigkeit herrscht zu der Auffassung, dass bereits eine Teilautomatisierung wie Spurhaltesysteme, Abblend- oder Ausweichassistenten zu einer signifikanten Reduktion von Straßenunfällen beitragen können. Nach wie vor ist menschliches Versagen eine der Hauptursachen für Verkehrsunfälle. Durch den vermehrten Einsatz sogenannter utilitaristischer Algorithmen, welche ein autonomes Fahrzeug dazu befähigen moralische Dilemmasituationen aufzulösen (Bonnefon et al. 2016), und darauf basierende kognitive Assistenzsysteme[12] bis hin zu Vollautomatisierung können auch menschlich bedingte Unfallursachen signifikant reduziert werden. Dies ist laut Studien von Kalra & Paddock (2016) und Kalra & Groves (2017) selbst dann, wenn der Wirkungsgrad dieser Systeme im Vergleich zum menschlichen Verhalten nur um 10% verbessert wird, was bereits jetzt in vielen Bereichen gegeben ist. Entsprechend argumentieren die Autoren, dass ein weiteres Zuwarten für die gesetzliche Zulassung sogenannter „highly automated vehicles“ (HAVs) nicht mehr gerechtfertigt ist, zumal eine stete Verbesserung von Simulationssystemen (Zhao & Peng 2017) u.a. durch die aktive Einbindung der Endnutzer in den Softwareentwicklungsprozess (Dietvorst et al. 2015) stattfindet. Relativiert werden diese Annahmen durch den Umstand, dass eine belastbare empirische Grundlage, die diese Annahmen bestätigt, bisher fehlt (Townsend 2016; Favarò et al. 2017; Favarò et al. 2018). Weiters kritisieren Banks et al. (2018), dass bestehende Assistenzsysteme, die eine sichere und situationsgerechte Übernahme manueller Kontrolle in vollautomatisierten Fahrzeugen gewährleisten sollen, ergonomisch noch unausgereift sind und tendenziell eine neue Gefahrenquelle darstellen, zumal es hier zu Reaktionsverzögerungen von bis zu 10 Sekunden kommen kann.

[12] Exemplarisch soll hier auf das Non-Line-Of-Sight-Prinzip verwiesen werden, eine Kameratechnik, die verborgene Objekte detektieren kann (vgl. Heide et al. 2017).

3.2 Mobilitätssteigerung

Vollautomatisierte Mobilität ist dazu geeignet die Mobilitätssituation jener zu verbessern, die bisher aus gesundheitlichen, altersbedingten oder anderen persönlichen Gründen vom Mobilitätssystem ausgeschlossen sind. Insbesondere für Personen mit körperlichen oder kognitiven Einschränkungen sowie für Kinder und Jugendliche bedeutete eine Vollautomatisierung einen Gewinn an Unabhängigkeit, eine Reduktion der sozialen Isolation sowie den vereinfachten Zugang zu Basisdienstleistungen wie etwa die medizinische Versorgung. Durch den Wegfall von Kostenfaktoren wie Chauffeure oder Begleitpersonal wird es zusätzlich möglich auch bisher nicht lukrative Regionen mit Mobilitätsdienstleistungen zu erschließen. Jedoch würde laut einer Studie von Harper et al. (2016) für die USA dies in Summe zu einem gesteigerten Verkehrsaufkommen von 14% führen und damit insbesondere in metropolitanen Regionen die Verkehrsbelastung signifikant steigern.

3.3 Stauvermeidung

Obwohl anzunehmen ist, dass etwaige geringere Mobilitätskosten in Zukunft zu einem stärkeren Verkehrsaufkommen führen werden, kann ein softwareunterstütztes Verkehrsmanagement bei zentraler Steuerung der autonomen Fahrzeuge eine besser Auslastung der Straßenkapazitäten durch effizientere Fahrweise und Reduktion von verhaltensinduzierten Verzögerungen (z.B. Rückstaueffekte) bedingen (Ge et al. 2018). Zusätzlich können im Falle eines Stillstands die Fahrzeuginsassen die verfügbare Zeit für andere Tätigkeiten als das Lenken des Fahrzeuges nutzen. Dennoch zeigen Studien (z.B. WEF 2017), dass aufgrund des generell höheren Verkehrsaufkommens insbesondere in Zentrumsnähe metropolitaner Regionen die Staugefahr zunimmt, wobei periphere Regionen vom Verkehr weiter entlastet werden.

3.4 Siedlungsstruktur und Raumbewirtschaftung

Die durch Teil- und Vollautomatisierung „gewonnene“ Lebenszeit kann dazu führen, dass Erwerbstätige bereit sind längere Anfahrtszeiten zum Arbeitslatz

in Kauf zu nehmen, was wiederum zu mehr Verkehrsaufkommen führt. Dies kann in Folge signifikante Auswirkungen auf die bestehende Siedlungs- und Raumstruktur haben, indem urbane Ballungszentren entlastet und stadtnahe bzw. rurale Wohngebiete aufgewertet werden. Trotz der höheren Zahl an Verkehrsteilnehmern wird aufgrund der autonomen Fahrweise der Parkraumbedarf in den Zentren geringer bzw. durch On-Demand-Nutzung derart verlagert, dass die bestehenden Flächen in der Stadt effizienter genutzt oder sogar umgewidmet werden können (WEF 2017), jedoch mit Folgen für die Flächenwidmung am Stadtrand. So könnten autonome Fahrzeuge zur Parkplatzvermeidung entweder „Kreise drehen“, an den Stadtrand oder gar bis zur Garage des Besitzers zurückfahren. Jede dieser Optionen wäre mit einer Erhöhung des Verkehrs verbunden, wie z.B. eine Simulation von Forschern der TU Wien zeigt (N.N. 2018; Pfaffenbicherl et al. 2018).

Dennoch ist zu berücksichtigen, dass die Umsetzbarkeit autonomer Mobilitätskonzepte immer vor dem Hintergrund der regionalen Gegebenheiten beurteilt werden muss, wie eine Scoring-Studie des US-amerikanischen Beratungsunternehmens INRIX auf Basis der Faktoren Parkraumverfügbarkeit, geographische Ausdehnung und demographischer Faktoren wie Alter und Wohlstandniveau darlegt (Ash et al. 2017).

3.5 Eigentums- und Nutzungsmodell

Das On-Demand-Modell bedingt bisweilen eine Verschiebung in der Eigentümerstruktur von Fahrzeugen, welches weniger als bisher durch den Besitz eines Fahrzeuges als durch die (zusätzliche) Inanspruchnahme von Car-Sharing und personalisierten Mobilitätsdienstleistungen gekennzeichnet ist (Clewlow and Gouri 2017). In Regionen mit einer hohen Dienstleistungsdichte kann der Bedarf nach persönlichem Besitz eines Fahrzeuges sinken, wohingegen in unterversorgten Regionen der Individualbesitz nach wie vor einen hohen Stellenwert einnehmen wird, wobei auch hier eine Mehrfachnutzung von Fahrzeugen begünstigt wird. Die Gesamteffekte dieser Entwicklung müssen jedoch differenziert betrachtet und interpretiert werden. So kommt das World Economic Forum (WEF 2017, S. 4) in einer Studie zur Auswirkung au-

tonomer Fahrzeuge im Großraum Boston (USA) zu dem Befund, dass Shared Mobility Services zu einer Reduktion von Fahrzeugen von 15% führen werden, wobei die Anzahl der gefahrenen Kilometer um 16% steigt. Der Zeitgewinn für den Mobilitätsteilnehmer schlägt mit einer Verbesserung von 4% zu Buche

3.6 Energieverbrauch und Emissionen

Einige Berechnungen gehen davon aus, dass es aufgrund der effizienteren Fahrweise, der effektiveren Infrastrukturnutzung sowie einer leichteren und verbrauchoptimierenden Bauweise autonomer Fahrzeuge zu einer Reduktion des Kraftstoffverbrauches als auch der Emissionen beitragen werden (Gläser & Lesko 2017), wobei diese Effekte laut einer Studie der University of Leeds (Wadud, o.J.; Wadud et al. 2016) bei teilautonomen Fahrzeugen sogar größer wären als bei vollautonomen. Eine Emissionsreduktion kann u.a. auch durch die intelligente Kombination alternativer Antriebsarten erreicht werden, wobei insbesondere der elektrischen Mobilität ein wichtiger Stellenwert eingeräumt wird. Reichweiteneinschränken, die beschränkter Stromspeicherkapazitäten geschuldet sind, könnten durch die allgemeine gesteigerte Effizienz und Effektivität des Verkehrswesens entschärft werden. Ein autonomes Energiemanagement zum Laden bzw. Betanken der Fahrzeuge entlastete zudem die notwendige Dichte an benötigten Lade- bzw. Tankstationen. Doch je nach Berechnungsmodell fällt die Ökobilanz unterschiedlich aus. So machen Giffi et al. (2018) und Greenblatt & Shaheen (2015) darauf aufmerksam, dass aufgrund der höheren Laufleistung und in Abhängigkeit der zugrundliegenden Stromproduktion die Umweltbelastung durch gesteigerten Energieverbrauch und erhöhte Emissionen sogar zunehmen könnte.

3.7 Transformationskosten

Der Übergang zu einer autonomen Mobilität verursacht Kosten, die zum einen dem Umbau der bestehenden Verkehrsinfrastruktur geschuldet sind (Townsend 2016, S. 17), bisweilen aber auch als nicht intendierte Sekundär- und Tertiäreffekte der zuvor beschriebenen Veränderungen auftreten (Fag-

nant & Kockelman 2015; Gruel & Stanford 2016; Milakis et al. 2017). So könnten die tendenziell geringeren Mobilitätskosten zu einem überproportionalen Bedarf an Mobilitätsdienstleistungen führen, was in Folge mit einem signifikant höheren Verkehrsaufkommen, höherem Kraftstoffverbrauch und höheren Emissionen einherginge (Wadud, o.J.). Weiters könnte die autonome Mobilität disruptive Effekte in Bezug auf bestehende private und öffentliche Dienstleister und deren Erlöskanäle zur Finanzierung derselben haben.[13] Insbesondere öffentliche Mobilitätsdienstleister könnten gezwungen sein durch die geringere Nachfrage und stärkere Konkurrenz durch private Anbieter ihr Leistungsportfolio signifikant einzuschränken, wie etwa eine Studie der ETH Zürich für die Schweiz prognostiziert (Meyer et al. 2017). Durch den Wegfall der Einnahmen aus der Parkraumbewirtschaftung verlören viele Städte und Gemeinden eine Einkommensquelle. Durch die Rationalisierung von Berufsfahrern durch autonom agierende Softwaresysteme wird einem ganzen Berufsstand seine Existenz- und Einkommensgrundlage entzogen.

Weitere dramatische Transformationskosten könnten sich aus einer möglichen Umsetzung von kostspieligen Infrastrukturveränderungen durch Private Public Partnerships (PPP) ergeben (z.B. Digitalisierung alles Ampeln und Verkehrszeichen, digitale Markierung von Fahrspuren, Bereitstellung von Elektrizität durch Oberleitungen und Induktionsschleifen in der Fahrbahn, etc.). Beispiele zeigen sich derzeit in den USA, z.B. bei dem Angebot von flächendeckendem WLAN in New York (Pinto 2016), bei der Diskussion im kostenlosen Internetzugang in Indien (N.N. 2016) oder der kostenlosen Auswertung der britischen Gesundheitsdaten durch Google (Naughton 2017).

3.8 Akzeptanz

Der Erfolg der autonomen Mobilität steht und fällt mit der Akzeptanz, die dieses Konzept in der breiten Bevölkerung genießt. Diese ist für Fahrassistenzsysteme der zweiten und dritten Ebene bereits relativ gut ausgeprägt, jedoch

[13] Exemplarisch seien etwa Effekte auf die Nahrungsmittelzustellung durch Food Delivery Services in ruralen Gebieten genannt (Heard et al. 2018).

zeigt sich für höhere Ebenen der Autonomie ein signifikanter Vertrauensschwund (Blanco et al. 2015; Bansal et al. 2016). In der aktuellen *Global Automotive Consumer Study* des Beratungsunternehmens Deloitte (Giffi et al. 2018) ist weltweit ein signifikanter Rückgang der Vertrauenswerte in selbstfahrende Autos dokumentiert, was u.a. die Ergebnisse einer früheren Ad-Hoc-Studie des MIT zum Konsumentenvertrauen in autonome Mobilität bestätigt (Abraham et al. 2017). Hierbei geht es nicht nur um das Vertrauen in die Technologie – und in diesem Kontext die Vorhersagbarkeit des Verhaltens maschinell gesteuerter Fahrzeuge (Surden & Williams 2016) -, sondern ebenso in Sicherheitsfragen (Kyriakidis et al. 2015; Abraham et al. 2017) als auch neue Geschäfts- und Versicherungsmodelle, die auf den neuen Produkten und Dienstleistungen aufbauen (Townsend 2016, S. 19).[14] Entsprechend existiert laut Giffi et al. (2018) keine bis nur eine geringe Zahlungsbereitschaft für Zusatzfunktionen und Dienste, die zum Service-Portfolio der autonomen Mobilität zählen, wenngleich es laut einer Studie der Bitkom für Sicherheitschecks eine hohe Zahlungsbereitschaft gibt (Bühler und Rohleder 2018). Das damit gekoppelte, nach wie vor starke Vertrauen in tradierte Autohersteller und konventionelle Antriebe macht es insbesondere für Startup-Unternehmen und neuartige Mobilitätsdiensteanbieter schwierig im Markt Fuß zu fassen.

4. (Un-)Sicherheit und vernetzte autonome Mobilität

Die Digitalisierung von Fahrzeugen und deren Einbettung in eine kommunikationsfähige Verkehrsinfrastruktur führen zu „vernetzten Fahrzeugen“ bzw.

[14] Eine Folgenabschätzung zu neuen Versicherungsmodellen für autonome Fahrzeuge wurde etwa durch AXA in Zusammenarbeit mit dem Beratungsunternehmen Burges Salmon für das United Kingdom erstellt (AXA 2018). Im Kern der Analyse scheint sich abzuzeichnen, dass die Versicherungsbeiträge mit zunehmender menschlicher Kontrolle des Fahrzeuges steigen werden, wohingegen vollautonom operierende Fahrzeuge den geringsten Versicherungstarif haben werden. Vor dem Hintergrund, dass mit zunehmender Autonomie der Fahrzeuge Produkthaftungsfragen stärker in den Mittelpunkt rücken, empfiehlt The Institution of Mechanical Engineers (IME 2016), dass Versicherungsleistungen zu Zukunft zu einem dominanteren Geschäftsfeld der Automobilhersteller werden sollten und der Kunde diese quasi mit der Erwerb bzw. der Nutzung eines Fahrzeuges automatisch erwirbt.

„connected cars“ (Johanning & Mildner (2015). Eine solche Vernetzung wirft jedoch eine ganze Reihe von Sicherheitsfragen auf.

Eine Studie der Bitkom (Bühler und Rohleder 2018) unter deutschen Autofahrern dokumentiert ein hohes Interesse an Sicherheitsthemen in Zusammenhang mit dem autonomen Fahren und einer vernetzten Mobilität. So sind technisches Versagen, Hackerangriffe und die unberechtigte bzw. exzessive Datennutzung durch Dritte die größten Sorgenpunkte. Entsprechend ist der Wunsch nach einer kontinuierlichen Sicherheitsüberprüfung auf Datenschutz und Datensicherheit stark ausgeprägt, ebenso die dafür notwendige Zahlungsbereitschaft.

In der hier zitierten Studie werden unterschiedliche Aspekte von „Sicherheit“ der technischen Systeme miteinander vermischt. Für eine bessere Systematisierung werden im Folgenden die Sicherheitsaspekte eines autonomen, vernetzten Mobilitätssystems einzeln vorgestellt und systematisch diskutiert.

Der deutsche Begriff „ Sicherheit“ wird im Englischen in zwei sehr deutlich getrennte Themen separiert, die „Safety“ und die „Security“. Dies gilt nicht nur bei IT- und anderen technischen Systemen, sondern in allen Bereichen die sicherheits-relevant sind. So ist z.B. die Arbeitssicherheit ein Bereich der Safety, Schutz gegen externe Eindringlinge jedoch ein Bereich der „Security“.

Unter **Safety** wird die Absicherung gegen technische Gebrechen subsumiert, die ohne gezielte Fremdeinwirkung, d.h. ohne das Mitwirken eines zielgerichteten böswilligen Angreifers geschehen. Bedrohungen der Sicherheit im Bereich Safety sind z.B. der technische Ausfall von Geräten oder Komponenten durch Verschleiß, Witterungseinflüsse oder Schädigung der Infrastruktur (wie Versorgung mit Energie, Kühlung und Daten). Zu den Bedrohungen im Bereich Safety gehören auch unvollständig implementierte oder gelebte Prozesse, unzureichende Schulung von Mitarbeitern und/oder Nutzern, Fehlentscheidungen (z. B. beim Design oder der Implementierung) ohne „böse Absicht“, nicht ausreichendes Testen und fehlerhafte Konzepte (z.B. im Bereich Ausfallsicherheit). Im Bereich Safety ist i.d.R. (durch entsprechend erfahrene Spezialisten) eine vollständige Aufzählung der Bedrohungen auf Grund früherer Erfahrungen mit ähnlichen Systemen gut möglich.

Unter **Security** wird die Absicherung gegen gezielte böswillige Angriffe gesehen, die zumeist zur Erzielung eines Eigennutzens des Angreifers, zum Teil aber auch durch reine Schädigungsabsicht (Stichwort Sabotage) passieren. Da hier der Angriff durch Menschen geplant wird, sind der Kreativität der Angreifer kaum Grenzen gesetzt. D.h. eine komplette Auflistung aller Angriffsmöglichkeiten ist regelmäßig unvollständig. Durch geeignete Methoden wie eine Bedrohungsanalyse (Threat Modelling) oder „Attack Landscapes" muss versucht werden, möglichst viele der Optionen der Angreifer selbst zu entdecken und geeignete Schutzmaßnahmen zu implementieren. Bei diesen Methoden können, bzw. sollten die Bedrohungen der Safety ebenfalls einbezogen werden.

4.1 Der Schutzbedarf von IT-Systemen - Bedrohung wogegen?

Der Schutzbedarf von IT-Systemen wird in folgende grundlegenden Kategorien eingeteilt und oft unter dem Stichwort „CIA" zusammengefasst:

1. Confidentiality – Vertraulichkeit. Diese Anforderung bedeutet, dass nur authentisierte und autorisierte Personen oder Systeme Zugriff auf Daten haben dürfen. Dies setzt natürlich voraus, dass es einen Weg zur sicheren Authentifizierung und Autorisierung der Teilnehmer des Gesamtsystems geben muss – wie wir sehen werden, ist dies bei vernetzten Systemen eine erhebliche Herausforderung
2. Integrity – Integrität. Diese Anforderung bedeutet, dass Veränderungen von Daten (oder Systemzuständen) nur durch authentisierte und autorisierte Personen oder Systeme herbeigeführt werden dürfen.
3. Availability – Verfügbarkeit. Diese Anforderung bedeutet, dass die Systeme und Komponenten immer dann zur Verfügung stehen müssen, wenn sie benötigt werden. Dies beinhaltet den Schutz gegen technische Gebrechen wie verschleißbedingte Ausfälle oder Ausfälle wegen Verlust der Daten oder der Stromversorgung ebenso wie bewusste Denial-of-Service Angriffe durch Angreifer, z.B. durch Störung von Datenübertragungen.

Dazu kommen zumeist noch weitere Anforderungen. Diese sind

- Auditability – Nachvollziehbarkeit. Diese Anforderung beinhaltet, dass eine sichere Protokollierung möglich ist, d.h. eine Protokollierung, die die CIA-Anforderungen erfüllt. Eine solche Protokollierung ermöglicht es, beim Eintreten von Sicherheitsvorfällen, z.B. Unfällen, herauszufinden, was genau passiert ist, wer, bzw. welche Komponente eine bestimmte Aktionen gesetzt hat oder ob eine Fremdeinwirkung vorliegt.
- Authenticity und Non-Repudiation. Hier geht es darum, dass nicht nur eine vollständige Protokollierung vorliegt, sondern dass handelnde Personen, Systeme oder Sub-Systeme eindeutig und nachweisbar identifiziert werden können. Nur auf diese Weise ist bei komplexen Sicherheitsverletzungen, z.B. Unfällen, eine Korrektur für die Zukunft möglich.
- Compliance – Einhaltung von Gesetzen und Vorschriften. Auch dies ist bei Fahrzeugen relevant, z.B. die Einhaltung der Verkehrsregeln, der Datenschutzgesetze, Zulassungsauflagen, etc. Um dies sicher zu gewährleisten müssen alle vorigen Anforderungen eingehalten werden.

4.2 Threat Modeling – systematische Bedrohungsanalyse

Um die Sicherheit von IT-Systemen zu bewerten, gibt es leider keine formale wissenschaftliche Methode, sondern es wird unter Zuhilfenahme von bewährten Vorgehensweisen versucht, alle Bedrohungen zu identifizieren und dann gegen jede der Bedrohungen geeignete Schutzmaßnahmen zu implementieren. Eine dieser Methoden wird als Threat Modeling bezeichnet.

Als Threats werden alle Formen von Bedrohungen verstanden, die zur Verletzung der im vorigen Abschnitt gelisteten Schutzbedarfsaspekte führen können. Bedrohungen sind systemimmanent und können nicht sicher „entfernt“ werden. Verschleiß passiert und Angriffe finden überall dort statt, wo Angreifer ausreichend Motivation haben.

Der Schutz gegen Bedrohungen besteht darin, möglichst alle Schwachstellen zu identifizieren, durch die eine gegebene Bedrohung schlagend werden

kann. Das heißt, Sicherheit (sowohl Safety wie auch Security) wird hergestellt, indem ALLE Bedrohungen identifiziert werden und für jede einzelne eine geeignete ausreichende Gegenmaßnahme gefunden und implementiert wird. Diese Vorgehensweise wird Bedrohungsanalyse genannt.Die Systematik der Bedrohungsanalyse wird als Threat Modeling bezeichnet.

Eine mögliche Vorgehensweise kann wie folgt dargestellt werden:[15]

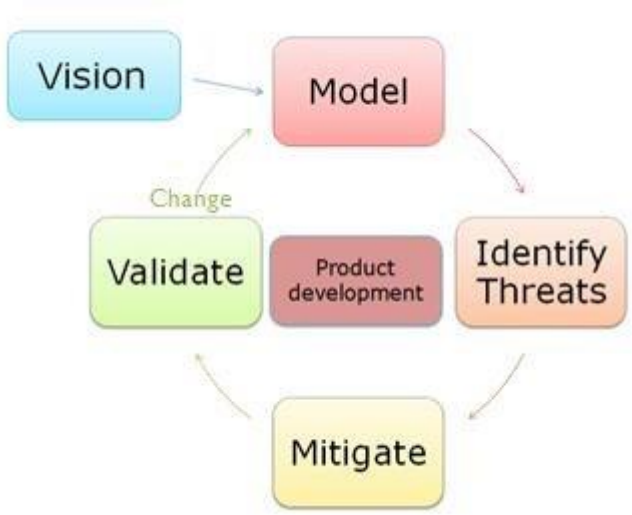


Abb. 2: The New Threat Modeling Process nach Microsoft 2007.

Vision beschreibt die Sicherheitsanforderungen und die Erwartungen oder Befürchtungen aller Stakeholder.

Model. Die technischen und nicht-technischen Komponenten des Systems werden in dem „Model“ zusammengefasst, einschließlich ihrer sog. „trust boundaries“, d.h. der Schnittstellen zu anderen Systemen, von denen sie abhängen und deren Integrität sie z.B. nicht direkt kontrollieren können. Im Fall vernetzter autonomer Mobilität sind dabei alle Systeme innerhalb des Fahrzeugs mit ihren Interaktionen zu betrachten, aber auch alle externen Systeme, die mit dem Fahrzeug interagieren, sei es elektronisch/digital wie auch in der realen Welt z.B. durch Begegnung auf der Straße. Ebenso Teil des Models

[15] Siehe dazu https://cloudblogs.microsoft.com/microsoftsecure/2007/10/01/the-new-threat-modeling-process/ (Zugriff 09.09.2018)

sind Daten, die entweder intern generiert und/oder gespeichert sind oder die von extern bezogen werden.

Identify Threats. Hierfür gibt es leider keine bessere Methode als den systematischen Einsatz der eigenen und fremden Phantasie. Für den Bereich „Security“ kann das durch die STRIDE Methode[16] systematisiert geschehen (STRIDE listet die zu betrachtenden Security-Verletzungen als: "Spoofing", "Tampering", "Repudiation", "Information disclosure", "Denial of service", and "Elevation of privilege".

Im Fall der vernetzten autonomen Fahrzeuge kommen aber zu den Security-Verletzungen noch die Verletzungen im Bereich Safety, d.h. der Ausfall oder das Fehlverhalten von Komponenten des Systems ohne böse Absicht. Vermutlich muss man auch unachtsames Verhalten der Verkehrsteilnehmer hier noch ergänzen.

Mitigate Threats. Hier muss für jede der auf diese Weise gefundenen Bedrohungen eine hinreichende Gegenmaßnahme, bzw. ein Redesign geplant werden, so dass eine Verletzung der 6 Sicherheitsanforderungen, die in „Schutzbedarf von IT-Systemen“ gelistet sind, sichergestellt ist.

Validate. Sicherstellen, dass keine Bedrohungen der Safety oder Security übersehen wurden, dass die Mitigationen alle effektiv implementiert sind und dass durch die Mitigationen keine neuen Schwachstellen entstanden sind.

Das Model ist als Kreis konzipiert – mit jeder Änderung, auch den ganz kleinen, muss der Kreislauf neu durchlaufen werden. Dies ist auch dann der Fall, wenn neue Erkenntnisse über Angriffsmöglichkeiten, neue Verwundbarkeiten in verwendeten Komponenten oder ähnliches bekannt werden.

Eine alternative Systematik für Threat Identification im Bereich “Security” wird in “Eliciting Security Requirements through Misuse Cases” beschrieben (Sin-

[16] Siehe dazu https://blogs.msdn.microsoft.com/larryosterman/2007/09/04/threat-modeling-again-stride/ (zugriff 09.09.2018)

dre & Opdahl 2005). Hierbei werden die Angreifer als aktiv handelnde Personen im System selbst modelliert.

4.3 Safety und Security in modernen (nicht-autonomen) Fahrzeugen

Bevor wir uns mit der Frage von Sicherheit der vernetzten und autonomen Mobilität beschäftigen, ist zu klären, ob moderne Fahrzeuge grundsätzlich als „sicher“ betrachtet werden dürfen.

Hauptherausforderung für Safety im Bereich moderner Mobilität ist, dass wir es mit einer sehr großen Zahl elektronischer Komponenten zu tun haben und dass für ein funktionierendes Gesamtsystem alle Funktionalitäten fehlerfrei zur Verfügung stehen müssen. Dies bedeutet, dass alle kritischen Komponenten mehrfach vorliegen müssen und dass bei Fehlverhalten einer der Komponenten das System dies sicher erkennen muss und entweder geeignete Ersatzkomponenten oder einen Sicherheitsmodus aktivieren muss (z.B. „an den Straßenrand fahren und anhalten“).

Diese Anforderung ist bereits für ein einzelnes Fahrzeug bei der hohen Zahl der verbauten Komponenten eine erhebliche Herausforderung, zumal die Komponenten von sehr vielen Lieferanten kommen. Selbst das Autoradio ist heute mit kritischen Komponenten vernetzt (da z.B. Geräusche wie das Klicken des Blinkers werden durch das Entertainment System erzeugt und wiedergegeben).

Die extrem hohe Komplexität moderner (nicht-autonomer) Fahrzeuge zeigt sich auch in der Komplexität der verwendeten Software. Wenn als vereinfachter Metrix „lines of code“ genutzt wird, so liegen moderne Fahrzeuge jenseits von großen modernen Betriebssystemen mit ihrer großen Zahl von Entwicklern. Es ist (derzeit) ausgeschlossen, eine so umfangreiche Software auch nur in die Nähe von „fehlerarm“ zu bekommen.

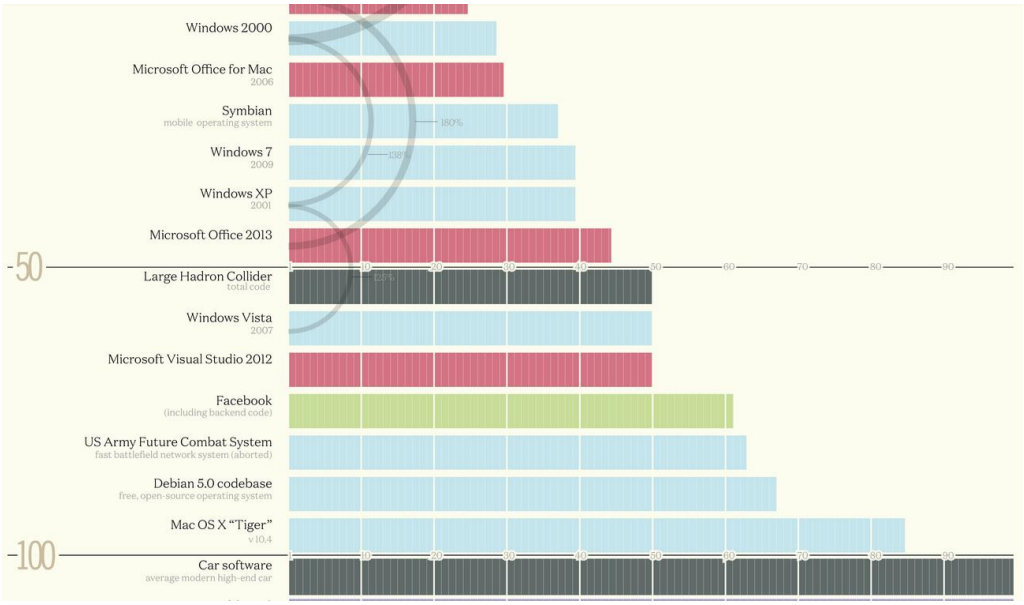


Abb. 3: Codebases – Millions of Lines of Code (Doughty-White & Quick 2015).

Die Studie "A Survey of Remote Automotive Attack Surfaces" (Miller & Valasek 2014) führt eine Bedrohungsanalyse eines modernen Fahrzeugs durch und kommt zu einer erschreckend großen Zahl von Schnittstellen, über die ein modernes Fahrzeug angegriffen werden kann. Diese Angriffe führen entweder zu einem Verlust von Vertraulichkeit, oder aber auch Verlust von Integrität, wenn der Angreifer das Fahrzeug dazu bringen kann, ein modifiziertes Verhalten zu zeigen. Die Studie listet folgende Angriffsoptionen auf.

- Passive Anti-Theft System (PATS)
- Tire Pressure Monitoring System (TPMS)
- Remote Keyless Entry / Start (RKE)
- Bluetooth
- Radio Data System / Entertainment System
- Telematics / Cellular / Wi-Fi (5 G Networks)
- Internet Access / Car Apps

Dass dies keine Theorie ist, zeigen Veröffentlichungen wie „Experimental Security Analysis of a Modern Automobile" (Koscher et al. 2010). Ausgehend von einem Threat Model, das nicht nur Angriffe aus der Ferne beinhaltet, son-

dern z.B. auch in Werkstätten, durch Mitfahrer oder Valet-Parking), findet die Studie viele Möglichkeiten tief in das System einzudringen und dort Veränderungen vorzunehmen.

Diese Probleme können aus grundsätzlichen Gründen mittelfristig nicht behoben werden. Wie bereits gezeigt wurde, setzt die Implementierung von Integrität immer zuerst eine sichere Authentisierung und Autorisierung aller Komponenten voraus. Dies ist aber in einem modernen Automobil mit Komponenten von vielen Zulieferern nicht möglich. D.h. die internen Systeme des Fahrzeugs „vertrauen“ sich gegenseitig und damit auch den Angriffswerkzeugen eines Angreifers, wenn z.B. das Angriffswerkzeug vorgibt, ein Entertainment-System zu sein.

Ein ausführliches Konzept eines sicheren Automobils und die dafür notwendigen Technologien findet sich in Ring et al. (2018). Dies sind alles Technologien wie sie derzeit entweder in PCs (z.B. Secure Boot, Hardware Trust Anchor) oder bei Internetdatenverkehr (z.B. gegenseitige Authentisierung) bereits eingesetzt werden. Die Autoren schreiben in ihrer Conclusio: „Based on our research, the automotive sector has recognized the problems that arise from missing security and is on track to develop safe and secure systems, although not for all challenges fitting solutions for the automotive sector are available. (ebd.)“

4.4 Safety und Security im “Internet of Things”

Bei jeder Vernetzung von Fahrzeugen (und innerhalb der Fahrzeuge) entstehen alle Probleme, die wir bereits jetzt im „Internet of Things“ (IoT) finden. Bereits die jetzige, kaum vernetzte Verkehrsinfrastruktur bietet eine große Zahl von Angriffsflächen wie in „Green Lights Forever: Analyzing the Security of Traffic Infrastructure“ (Ghena et al. 2014) gezeigt wird.

Je intensiver die Vernetzung wird, desto größer werden auch die möglichen Angriffsflächen sein. Kernprobleme sind, dass die Techniker, die diese Geräte entwerfen aus einer safety-orientierten Tradition kommen und keine security-relevante Ausbildung haben, verbunden mit dem Problem, dass aus wirt-

schaftlichen Gründen eine erhöhte Sicherheit nicht belohnt wird, weil die Schäden durch mangelnde Sicherheit regelmäßig nicht beim Verursacher der Probleme schlagend werden (Schneier 2018).

Lösungen lägen in einer zwingenden weltweiten Durchsetzung von Security-Anforderungen, was zwar von vielen Sicherheitsexperten seit einiger Zeit gefordert wird, für die es aber (derzeit) keinen politischen Willen gibt, vor allem nicht auf globaler Ebene, auf der diese Probleme gelöst werden müssten. Schneier (2017) und Scarfone (2018) bieten eine Zusammenstellung security-relevanter Forderungen:

1. **Starke Authentisierung:** Vor dem Konfigurieren von Fahrzeug-Komponenten muss eine Authentisierung und Autorisierung des Menschen der „Administratoren“ verlangt werden um sicherzustellen, dass keine un-autorisierten Veränderungen vorgenommen werden. Bei allen Kommunikationen zwischen den Komponenten des Fahrzeugs muss zuerst eine Authentisierung der Komponenten verlangt werden.
2. **Aktualisierbarkeit:** Gibt es eine einfache (d.h. automatische) Möglichkeit, neue Firmware-Versionen zu installieren, wenn z.B. Verwundbarkeiten im Gerät gefunden wurden?
3. **Integrität und Authentizität:** Wird die Integrität der Komponente sichergestellt, z.B. bei einer Aktualisierung der Software die Authentizität der neuen Firmware geprüft?
4. **Verschlüsselung:** Verschlüsselt das Gerät alle seine Verbindungen (Standort-Daten, Video-Daten, Telemetriedaten, ...), aber auch z.B. die Übertragung einer neuen Firmware? Wird vor jedem Verbindungsaufbau die Identität und Integrität der beiden Gegenstellen durch gegenseitige Authentisierung sichergestellt?
5. **Reduktion der Angriffsflächen, z.B. „offene Ports“:** Viele dieser Geräte und Komponenten haben offene Ports wie Telnet, damit sie einfach gewartet werden können. Zumeist stehen dann die dazu gehören Zugangscodes im Internet (und lassen sich über eine Suchmaschine leicht finden).

Diese Anforderungen müssten von allen Komponenten erfüllt werden, die innerhalb der vernetzten Infrastruktur genutzt werden. Das heißt, dass neben den Fahrzeugen auch jede vernetzte Ampel, jedes vernetzte Verkehrsschild, jede vernetzte Stau-, Baustellen- oder Verkehrswarnung diese Anforderungen erfüllen müsste.

4.5 Safety und Security in der autonomen Mobilität

Zusätzlich zu den in den vorigen Kapiteln aufgezeigten zahlreichen Herausforderungen und Problemen hat die Sicherheit im Fall der autonomen Fahrzeuge zwei zusätzliche Voraussetzungen:

a) **Safety:**
Die Entwickler müssen in der Lage sein, die KI in ihren Fahrzeugen auf ein ausreichend sicheres Niveau zu heben, so dass in allen Situationen, für die das jeweilige Fahrzeug ausgelegt ist, die notwendige Fahrsicherheit erreicht werden kann. Das Erreichen dieses Sicherheitsniveaus muss durch Zertifizierungsstellen durch ausreichende Tests geprüft werden. Letztes stellt eine erhebliche Herausforderung dar (Greis 2016; Lutz 2014).

b) **Security:**
Durch geeignete Schutzmaßnahmen muss sichergestellt werden, dass das elektronische Innenleben der Fahrzeuge nicht durch Angriffe gestört oder modifiziert wird. Diese Angriffe können von außerhalb des Fahrzeugs kommen oder auch von innen. Angriffe von außen sind überall dort möglich, wo Komponenten Schnittstellen mit der Außenwelt haben. Dies ist z.B. bei der drahtlosen Reifendruckübermittlung der Fall, aber auch alle Verbindungen zur Verkehrsinfrastruktur und zum Internet, z.B. für die Übermittlung von Daten an die Info- und Entertainment Systeme. Angriffe von innen können durch Insassen erfolgen, die Geräte drahtlos oder über die Wartungsstecker mit der Fahrzeugelektronik verbinden oder auch durch Systemkomponenten, z.B. Entertainment-Systeme, die fehlerhaft sind oder „bösartig“ agieren.

> Diese Absicherung gegen Veränderungen schließt auch Veränderungen ein, die der Fahrzeughalter eventuell selbst durchführen möchte, die aber die Sicherheit anderer Verkehrsteilnehmer gefährden könnten, z.B. Stichwort „Tuning“(Kotrba 2017; Doctorow 2015).

Zu den bisherigen (und bisher ungelösten) Herausforderungen die Komponenten eines Fahrzeugs gegeneinander abzusichern kommen bei autonomen Fahrzeugen zusätzliche Herausforderungen dadurch, dass KI-basierte Komponenten eine extrem hohe Komplexität haben und auf Grund ihrer Technologien keine Nachvollziehbarkeit der Grundlage ihrer Entscheidungen erlauben. D.h. die Anforderung nach Auditability – Nachvollziehbarkeit aus Kapitel 4.1 ist grundsätzlich durch die genutzte Technologie nicht gegeben. Lernende Systeme wie neuronale Netze können zwar protokollieren zu welchen Entscheidungen sie gekommen sind, aber nicht, warum diese Entscheidung gefallen ist (Knight 2016). Diese Einschränkung ist bei Brettspielen wie Schach und Go leicht zu tolerieren, aber wenn es um die Analyse eines Verkehrsunfalls zur zukünftigen Vermeidung geht, sehr problematisch.

Die nächste Problematik besteht darin, dass das Verhalten dieser KI-Systeme nicht auf einer geschlossenen und verifizierbaren Theorie beruhen sondern auf mehr oder weniger zufällig zusammengestellten Daten. Dies wird bezeichnet als “the unreasonable effectiveness of data” (Cristianini 2016). Diese Systeme lernen nur, was sie gelehrt bekommen und dabei gilt: Garbage-in - Garbage-out. Fehlerhafte oder unvollständige Lerndatensätze führen zu Lücken im Verhalten der KI-basierten Systeme. Wenn die Lerndatensätze gewisse Kombinationen von Witterungsverhältnissen, Lichtverhältnissen und Straßenverkehrssituationen nicht enthalten, so kann das KI-basierte System in diesen Situationen nicht adäquat reagieren. Prominente Beispiele sind etwa Teslas Verwechseln eines querenden Lastwagens mit einer Autobahnüberführung (Yadron & Tynan 2016; Vlasic & Boudette 2016) oder der Uber-Unfall, bei dem das Fahrzeug zuerst „verwirrt“ war, weil die Sensoren die Frau, die das Fahrrad geschoben hatte, zwar „gesehen“, aber die KI-Systeme sie falsch eingeordnet hatten (Wakabayashi 2018). Eine weitere Analyse des Unfalls besagt, dass das Unfallopfer als “false positive”, d.h. als nicht sicherheitsrelevant eingestuft worden war (Efrati 20189). Solche Probleme werden (vermut-

lich) auf Dauer weniger werden, aber werden sich auf Grund der inhärenten Eigenschaften von KI nicht verhindern lassen. Erschwerend kommt hinzu, dass die Entwickler nicht aus den Erfahrungen und Datensätzen der anderen Entwickler „lernen“ können und beim „Anlernen“ ihrer AI immer wieder von vorn anfangen müssen. D.h. eine Welt gänzlich ohne Unfälle ist nicht zu erwarten.

Noch dramatischer wirken sich die inhärenten Schwächen der AI-basierten Systeme im Bereich „Security“, d.h. der gezielten Angriffe aus (Sitawarin et al. 2018; Reynolds 2017). Drastisch demonstriert wird dies z.B. in vielen Experimenten, in denen Verkehrszeichen leicht modifiziert werden und dann von KI-basierten Systeme als vollkommen andere Verkehrszeichen wahrgenommen werden (Nickel 2018; Goodfellow et al. 2018).

Das führt dazu, dass das Vermeiden von Unfällen bei voller Autonomie immer Grenzen haben wird. In diesen Situationen müsste der Mensch aufmerksam genug sein um eingreifen zu können. Dies stößt aber auf grundsätzliche Probleme, denn das Übernehmen der Kontrolle erfordert eine Zeitspanne zwischen 8 Sekunden und 15 Sekunden, in der das Fahrzeug einen erheblichen Weg zurückgelegt (Brunnert 2018).

Ein Ergebnis der Problematik, dass eine wirkliche Unfallfreiheit vermutlich nur bei 100% autonomen und vernetzten Fahrzeugen möglich sein wird, ist die bereits öffentlich geäußerte Forderung nach separaten Fahrbahnen für autonome Fahrzeuge (mit geeigneter Absicherung gegen Tiere, Fußgänger und Radfahrer), was zu einem erhöhtem Landverbrauch führen würde und zu weiteren Einschränkungen in der Mobilität für bestimmte Mobilitätsarten (McLean 2017; Rocque 2017).

5. Safety und Security in der vernetzten Mobilität

Wir kommen jetzt zum Kern des gegenständlichen KIRAS-Projekts. Als „vernetzte Mobilität“ wird in diesem Abschnitt eine Kommunikation eines autonomen Fahrzeugs mit anderen Fahrzeugen und/oder der Verkehrsinfrastruktur verstanden. Ziel dieser Kommunikation ist eine Erhöhung der Sicherheit der autonomen Fahrzeuge. Diese Vernetzung mit anderen Fahrzeugen und der Verkehrsinfrastruktur ist zusätzlich zu den im vorigen Abschnitt behandelten bisherigen Vernetzungen im Fahrzeug selbst (z.B. Reifendrucksensoren), zwischen dem Fahrzeug und den Smartphones der Insassen, sowie zwischen dem Fahrzeug und dem Internet (Telematik, Diebstahlsicherung, etc.).

Zu diesen Herausforderungen bei der Vernetzung gehören auf jeden Fall die Verkehrsampeln, aber auch andere Verkehrszeichen, möglicherweise Fahrbahnmarkierungen und Informationen über den Zustand des Verkehrs einige Kilometer weiter (wie in dieser KIRAS Studie konzipiert).

Für diese Kommunikationen gelten von den sechs Aspekten des Schutzbedarfs (siehe Kapitel 4.1) vor allem die Integrität der Geräte und Nachrichten (fehlende oder falsche Signale von Ampeln könnten zu dramatischen Unfällen führen). Aber auch die damit eng verbundene Nachvollziehbarkeit (d.h. das sichere Protokollieren der Kommunikation) ist für die Rekonstruktion von Unfällen wichtig. Ohne Integrität von Geräten und Nachrichten kann keine sichere Protokollierung erreicht werden.

Zusätzlich sind noch die Safety-Aspekte zu befriedigen. Dabei muss natürlich die Verfügbarkeit dieser Systeme (d.h. die Ausfallsicherheit und ihr Schutz gegen Denial of Service-Angriffe) garantiert werden.

Aspekte der Vertraulichkeit können bei der Kommunikation mit der Infrastruktur in dem Augenblick relevant werden, wo die Fahrzeuge (z.B. für die Authentisierung) eine Kennung ihrer Identität senden, die zum Tracking des Fahrzeugs verwendet werden könnte. Eine sichere Authentisierung ist eine Vo-

raussetzung für die sichere Kommunikation, wobei folgende Teilaspekte sicherer Kommunikation zu unterscheiden sind:

- Technische Integrität der Nachrichten,
- Integrität und Verlässlichkeit aller Teilnehmergeräte und
- sichere Authentisierung der Teilnehmer, d.h. die Feststellung ihrer Identität.

Die folgenden Unterkapitel behandeln jeden dieser drei Punkte.

5.1 Technische Integrität der Nachrichten

Bei der technischen Integrität der Nachrichten geht es darum, dass die ausgetauschten Nachrichten weder safety-bezogene (d.h. technisch bedingte) noch security-bezogene (d.h. durch Angreifer erzeugte) Modifikationen erleiden. Dies kann grundsätzlich durch Verschlüsselung gelöst werden. Die Herausforderungen liegen jedoch darin, dass die Zeitverzögerung durch Schlüsselaustausch, Schlüsselgenerierung und Verschlüsselung gering sein soll und die Verschlüsselungsalgorithmen auch in leistungs- und energieschwachen Komponenten leicht zu implementieren sind.

Diese Herausforderungen werden in der gegenständlichen KIRAS Studie durch eine sichere Verschlüsselung auf Grund von temporären Schlüsseln, die jeweils nur die beiden Teilnehmer einer Kommunikation kennen behandelt und gelöst. Diese Lösung behandelt eine der Herausforderungen der sicheren Kommunikation zwischen den Kommunikationspartnern. Leider ist dies jedoch nur eine von mehreren Problemstellungen.

Die weiteren (ungelösten) Problemstellungen werden im Folgenden behandelt. Diese Problemstellungen sind in der Theorie bereits alle gelöst, wie warten jedoch noch auf praktikable Lösungen für einen flächendeckenden Einsatz bei einer extrem großen Zahl von Kommunikationsteilnehmern.

5.2 Integrität und Verlässlichkeit aller Teilnehmergeräte

Jede Teilnehmerkomponente soll (nur) genau das tun, für das sie konzipiert wurde – nicht mehr und nicht weniger. Dies zu verifizieren ist ein grundsätzli-

ches Problem der Informatik und für komplexe Software nicht gelöst. Eine solche Prüfung ist aber die Grundlage von Zertifizierungen wie diese bei Medizintechnik gefordert sind.

Aber auch bei der Zulassung von Fahrzeugen tritt dieses Problem auf. Traditionell wurde bei der Fahrzeugzulassung das Verhalten von Fahrzeugen durch ausreichende Tests geprüft und das Fahrzeug dann zugelassen. Der „Dieselskandal“ hat jedoch gezeigt, dass konkrete Funktionalitäten sich jederzeit durch Veränderung der Software, bzw. von Software-Parametern drastisch ändern lassen.

Im Medizinbereich wird daher bei jeder Änderung der Software, auch beim sog. Patchen von Verwundbarkeiten, eine Re-Zertifizierung notwendig. Bei der riesigen Zahl von Komponenten in einem Fahrzeug und zusätzlich der Verkehrsinfrastruktur ist diese Herausforderung extrem groß und daher nicht praktikabel.

D.h. die fortlaufende Gültigkeit einer Zertifizierung (bzw. Zulassung) setzt (eigentlich) die Unversehrtheit des Programmcodes voraus. Das heißt, ein sicherer Schutz gegen Hacking durch Fremde, aber auch durch den Eigentümer des Geräts muss gewährleistet sein. Technisch ließ sich eine solche Prüfung der Nicht-Veränderung der Software zwar durch eine digitale Signatur implementieren. Bei Personal Computern wird versucht, dieses Prinzip für das Stadium des Systemstarts in den Startkomponenten UEFI (BIOS) umzusetzen (Olzak 2011) (Olzak, 2011). In der Praxis zeigen sich jedoch immer wieder Probleme.

Eine der Kernproblematiken liegt darin, dass durch die Entdeckung immer neuer Verwundbarkeiten die Sicherheit von IT-Systemen immer nur temporär gegeben ist und daher ein zeitnahes Aktualisieren bei der Entdeckung neuer Verwundbarkeiten möglich sein muss.

In der Medizintechnik führt dies zu erheblichen Problemen. Durch eine Aktualisierung der Software (das Patchen gegen Verwundbarkeiten) in Steuerungscomputern großer Medizingeräte wie MRT führt dazu, dass die Zulassung der medizinischen Großgeräte durch die Behörden (z.B. FDA) wiederholt werden müsste. Dies ist bei älteren Großgeräten, die nur noch in wenigen Stückzahlen im Einsatz sind, ein wirtschaftlich kaum vertretbarer Aufwand. Deswegen

wird auf vielen der Steuerungscomputer immer noch Windows XP eingesetzt, was zu erheblichen Schäden z.B. durch Ransomware-Angriffen führt (Larson 2017; Krafty Librarian 2014; Messmer 2004).

Um eine wirkliche Sicherheit des Gesamtsystems aus Fahrzeugen und Infrastruktur sicherzustellen, müsste eine Zertifizierung und ständige Re-Zertifizierung (staatlich oder nicht-staatlich) aller Komponenten eingeführt werden.

Das Fehlen von Lösungen für eine sichere automatische Aktualisierung von IT-Systemen führt bereits jetzt zu einer extrem unsicheren Internet of Things-Infrastruktur. Diese Probleme würden auch bei dem Versuch einer Sicherstellung einer überprüften Integrität der Komponenten einer vernetzten Verkehrsinfrastruktur eintreten.

Rein informationstheoretisch ist das Problem der Sicherstellung eines bestimmten Zustands einer Software lösbar: Um sich auf die Integrität der anderen Geräte im Datenaustausch verlassen zu können, braucht „lediglich“ jede Komponente eine digitale Signatur ihres Software-Codes zu senden, die dann vom jeweiligen Empfänger gegen ein zentrales Repository dieser Signaturen geprüft wird. Nach jeder notwendigen Software-Aktualisierung ist eine neue digitale Signatur notwendig und zu verifizieren. Der Verwaltungsaufwand für die kontinuierliche Pflege dieser Signaturen wäre jedoch so erheblich, dass so etwas derzeit nicht einmal angedacht ist.

5.3 Identität und Authentizität der Teilnehmer

Der Austausch der im vorigen Abschnitt geforderten digitalen Signatur ist jedoch für die Feststellung der Integrität der anderen Teilnehmer noch nicht ausreichend. Eine grundlegende Eigenschaft von Computern ist, dass ein Computer grundsätzlich jede andere Maschine emulieren kann, d.h. auch jeden anderen Computer. So könnte eine „böse“ Komponente im Gesamtnetz natürlich die digitale Signatur eines anderen (zertifizierten) Gerätes aussenden („replay attack“).

Die Sicherheit von ausgetauschten Nachrichten hängt daher auch davon ab, ob die wirkliche Identität und Authentizität jedes Teilnehmers festgestellt wer-

den kann. Auch dieses Problem kann theoretisch gelöst werden, z.B. durch zentrale Zertifizierungsstellen, die nicht-fälschbare digitale Zertifikate verteilen (Beispiele sind die Bürgerkarte oder SIM-Karte eines Mobilfunkgeräts). Dies muss so implementiert sein, dass ein „Klonen“ dieser Identitäten nur mit sehr erheblichem Aufwand möglich ist. Dies kann z.B. erreicht werden, indem diese digitale Identität in sog. TPMs (Trusted Platform Modules) in jeder der Komponenten implementiert wird. (Es reicht dafür nicht aus, dass jedes Fahrzeug eine fälschungssichere (aber mobile) SIM-Karte enthält, denn die kann jederzeit leicht von einem Fahrzeug in ein anderes übertragen werden. Diese TPMs müssten fest in jeder Komponente verbaut sein).

Ohne eine solche sichere Feststellung der Identität und Authentizität der jeweiligen Teilnehmer kann kein sicherer „Trust“ zwischen den Teilnehmern hergestellt werden. Der Aufwand für die Implementierung von TPMs in jeder Komponente ist vielleicht noch machbar, der Aufwand der Verwaltung und ständigen Aktualisierung einer zentralen Datenbank aller Signaturen aller dieser Komponenten übersteigt unsere heutigen Möglichkeiten deutlich.

6. Resumé

Zusätzlich zu den in den Kapitel 2 und 3 diskutierten und weitgehend ungeklärten gesellschaftlichen Konsequenzen einer autonomen und vernetzten Mobilität, speziell was die Auswirkungen zweiter und höherer Ordnung betrifft, haben wir es auch noch mit ungelösten technischen Problemen zu tun.

Insbesondere in den Kapiteln 3 und 4 wurden für moderne nicht-autonome Fahrzeuge, alle Komponenten im Internet of Things, für die autonome und für die vernetzte Mobilität jeweils eine ganze Reihe von derzeit noch ungelösten Herausforderungen in den Bereichen Safety und Security aufgezeigt.

Wie die Ausführungen in Kapitel 5 zeigen, ist eine sichere Verschlüsselung aller Nachrichten zwar Grundlage einer sicheren Vernetzung und damit eine der Grundlagen für einen vertrauenswürdigen Austausch von Nachrichten zwischen Fahrzeugen und Komponenten einer vernetzten Verkehrsinfrastruktur. Es verbleiben aber für einen wirklich sicheren Nachrichtenaustausch weitere erhebliche Herausforderungen, für die es in der Informationssicherheit zwar theoretische Lösungen gibt, für die aber derzeit keine praktisch mit vertretbarem Aufwand umsetzbare Lösungen existieren. Das heißt, die gegenständliche Arbeit löst leider nur eine der drei grundlegenden Problemstellungen bei der sicheren Kommunikation.

Dies bedeutet, dass die mit Hilfe dieser Technologien dieser KIRAS-Studie zwischen Fahrzeugen und mit der vernetzten Infrastruktur ausgetauschten Nachrichten zwar als unverändert und abhörsicher betrachtet werden können, leider aber nicht als vertrauenswürdig eingestuft. D.h. es dürfen auf Grundlage dieser Nachrichten keine Entscheidungen getroffen werden, die möglicherweise zu einer Gefährdung anderer Verkehrsteilnehmer führen könnten. Ein Beispiel für eine solche Entscheidung wäre das Auslösen einer Vollbremsung rein auf Grund der Kommunikation eines (angeblich) vorausfahrenden Fahrzeugs. Allerdings könnte eine solche Nachricht sehr wohl zu einer vorsichtigen Reduktion der Geschwindigkeit genutzt werden.

7. Literaturverzeichnis

[1.] Abraham, H., Reimer, B., Seppelt, B., Fitzgerald, C., Mehler, B., Coughlin, J.F., 2017. Consumer Interest in Automation: Preliminary Observations Exploring a Year's Change. MIT. Online: agelab.mit.edu/sites/default/files/MIT%20-%20NEMPA%20White%20Paper%20FINAL.pdf (Zugriff: 28.06.2018)

[2.] ADL (Arthur D Little) (o. J.) Zukunft der Mobilität 2020. Die Automobilität im Umbruch? Online:

[3.] Andelfinger V.P., Hänisch T. (Hrsg.) (2015) Internet der Dinge. Technik, Trends und Geschäftsmodelle. Wiesbaden: Springer.

[4.] Anderson, J.M., Kalra, N., Stanley, K.D., Sorensen, P., Samaras, C., Oluwatola, O.A., 2014. Autonomous vehicle technology: a guide for policymakers. Rand Corporation, Santa Monica, CA.

[5.] APEC (2014) White Paper of Internet of Vehicles (IoV). Online: http://mddb.apec.org/Documents/2014/TEL/TEL50-PLEN/14_tel50_plen_020.pdf (Zugriff: 24.03.2017).

[6.] Ash, A., Pishue, B., Weiser, B., 2017. INRIX Identifies Top U.S. Cities for Shared Highly Autonomous Vehicle Deployment. INRIX. Online: http://inrix.com/resources/autonomous-vehicles-study-2017/ (Zugriff: 12.06.2018)

[7.] ATKearney, 2016. How can automakers survive the self-driving era. Online: https://www.atkearney.de/documents/856314/8689007/How+Automakers+Can+Survive+the+Self-Driving+Era.pdf/323574cc-0357-46cc-95f4-934d3fe5d997 (Zugriff: 18.06.2018)

[8.] AXA, 2018. Are we ready to 'handover' to driverless technology? VENTURER Insurance and Legal Report 2017/18. Online: https://www.axa.co.uk/uploadedFiles/Content/Newsroom_v2/Media_Resources/Reports_and_Publications/Downloads/Driverless_Cars/VENTURER_Insurance_and_Legal_Report_2018.pdf (Zugriff: 20.06.2018)

[9.] Banks, V.A., Eriksson, A., O'Donoghue, J., Stanton, N.A., 2018. Is partially automated driving a bad idea? Observations from an on-road

study. Applied Ergonomics 68, 138–145. https://doi.org/10.1016/j.apergo.2017.11.010

[10.] Bansal, P., Kockelman, K.M., Singh, A., 2016. Assessing public opinions of and interest in new vehicle technologies: An Austin perspective. Transportation Research Part C: Emerging Technologies 67, 1–14. https://doi.org/10.1016/j.trc.2016.01.019

[11.] Blanco, M., Atwood, J., Vasquez, H. M., Trimble, T. E., Fitchett, V. L., Radlbeck, J. & Morgan, J. F. (2015, August). *Human factors evaluation of level 2 and level 3 automated driving concepts*. (Report No. DOT HS 812 182). Washington, DC: National Highway Traffic Safety Administration.

[12.] BMVI, 2017. Ethics Commission - Automated and Connected Driving. Federal Minister of Transport and Digital Infrastructure. Online: www.bmvi.de/SharedDocs/EN/publications/report-ethics-commission.pdf?__blob=publicationFile (Zugriff: 20.05.2018)

[13.] Bonnefon, J.-F., Shariff, A., Rahwan, I., 2016. The social dilemma of autonomous vehicles. Science 352, 1573–1576. https://doi.org/10.1126/science.aaf2654

[14.] Bose R., Brakensiek J., Park K. (2010) Terminal Mode- Transforming Mobile Devices into Automotive Application Platforms. Automotive UI 2010. Online: https://www.auto-ui.org/10/proceedings/p148.pdf. (Zugriff: 12.05.2017).

[15.] Bruhn M. (2007) Integrierte Kundenorientierung. Wiesbaden. zit.n. Coenen C. (2010) „Hierarchieübergreifende Umsetzung von Serviceorientierung - Eine handlungsbezogene Betrachtung aller Unternehmensebenen“. In: M. Bruhn, B. Stauss (Hrsg) Serviceorientierung im Unternehmen. Forum Dienstleistungsmanagement. S. 33-61. Wiesbaden: GWV.

[16.] Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Roff, H., Allen, G.C., Steinhardt, J., Flynn, C., Ó hÉigeartaigh, S., Beard, S., Belfield, H., Farquhar, S., Lyle, C., Crootof, R., Evans, O., Page, M., Bryson, J., Yampolskiy, R., Amodei, D., 2018. The Malicious

Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. Future of Humanity Institute, University of Oxford; Centre for the Study of Existential Risk, University of Cambridge; Center for a New American Security; Electronic Frontier Foundation; OpenAI. Siehe auch: https://img1.wsimg.com/blobby/go/3d82daa4-97fe-4096-9c6b-376b92c619de/downloads/1c6q2kc4v_50335.pdf (Zugriff am 18.06.2018)

[17.] Brunnert, M., 2018. Unfallforscher warnen vor Risiken des teilautomatisierten Fahrens [WWW Document]. heise online. URL https://www.heise.de/newsticker/meldung/Unfallforscher-warnen-vor-Risiken-des-teilautomatisierten-Fahrens-3949696.html (accessed 9.10.18).

[18.] Brünglingshaus C. (2013) „Smart Mobility- Verkehrsangebote intelligenter vernetzen“. Online: https://www.springerprofessional.de/fahrzeugtechnik/carsharing/smart-mobility-verkehrsangebote-intelligent-vernetzen/6561560. (Zugriff: 16.03.2017)

[19.] Buriánek F. (2009) Vertragsgestaltung bei hybriden Produkten – Eine ökonomische Betrachtung. Wiesbaden: Gabler.

[20.] Bühler J. und Rohleder B. (2018). Autonomes Fahren und vernetzte Mobilität. In: https://www.bitkom.org/Presse/Anhaenge-an-PIs/2018/Bitkom-Charts-Autonomes-Fahren-und-vernetzte-Mobilitat-18-04-2018-final.pdf, accessed: 2018-06-10

[21.] BVDW (Hrsg.) (2016a) Connected Cars - ein Diskussionspapier zum Thema Services. Online: http://www.bvdw.org/presseserver/ConnectedCars/Finalversion_Diskussionspapier_Services_15.06.pdf (Zugriff:12.05.2017)

[22.] BVDW (Hrsg.) (2016b) Connected Cars- Geschäftsmodelle. Online: http://www.bvdw.org/medien/connected-cars--geschaeftsmodelle?media=7792 (Zugriff: 12.05.2017).

[23.] BVDW & Hochschule Reutlingen (o.J.) Connected Cars. Interaktive Infografik. Online: http://www.bvdw.org/fileadmin/connectedcars/. (Zugriff:13.05.2017).

[24.] Cabrall, C.D.D., Sheridan, T.B., Prevot, T., de Winter, J.C.F., Happee, R., 2018. The 4D LINT Model of Function Allocation: Spatial-Temporal Arrangement and Levels of Automation, in: Karwowski, W., Ahram, T. (Eds.), Intelligent Human Systems Integration. Springer International Publishing, Cham, pp. 29–34. https://doi.org/10.1007/978-3-319-73888-8_6

[25.] Castells, M., Castells, M., 2010. The rise of the network society, 2nd ed., with a new pref. ed, The information age : economy, society, and culture. Wiley-Blackwell, Chichester, West Sussex ; Malden, MA.

[26.] Cawsey A. (2003) Künstliche Intelligenz im Klartext. München: Pearson Studium.

[27.] Clewlow, R.R. and Gouri S.M. (2017) Disruptive Transportation: The Adoption, Utilization, and Impacts of Ride-Hailing in the United States. Institute of Transportation Studies, University of California, Davis, Research Report UCD-ITS-RR-17-07

[28.] Coenen C. (2001) Serviceorientierung und Servicekompetenz von Kundenkontakt-Mitarbeitern. In: Bruhn M., Stauss B. (Hrsg.) Jahrbuch Dienstleistungsmanagement 2001- Interaktionen im Dienstleistungsbereich.Wiesbaden.S.341-374. zit.n. Coenen C. (2010) „Hierarchieübergreifende Umsetzung von Serviceorientierung- Eine handlungsbezogene Betrachtung aller Unternehmensebenen“. In: M. Bruhn, B. Stauss (Hrsg) Serviceorientierung im Unternehmen. Forum Dienstleistungsmanagement. S. 33-61. Wiesbaden: GWV.

[29.] Coenen C. (2010) „Hierarchieübergreifende Umsetzung von Serviceorientierung- Eine handlungsbezogene Betrachtung aller Unternehmensebenen“. In: M. Bruhn, B. Stauss (Hrsg) Serviceorientierung im Unternehmen. Forum Dienstleistungsmanagement. S. 33-61. Wiesbaden: GWV.

[30.] Cohen, T., Jones, P. & Cavoli, C., 2017. Social and behavioural questions associated with automated vehicles. Scoping study by UCL Transport Institute. Final report, London: Department for Transport.

[31.] Cristianini, N., 2016. The road to artificial intelligence: A case of data over theory [WWW Document]. New Scientist. URL

https://www.newscientist.com/article/mg23230971-200-the-irresistible-rise-of-artificial-intelligence/ (accessed 9.10.18).

[32.] Dabrock P. (2017) „Ethik und Autonomes Fahren. Ethische Dilemmata unterlaufen oft Akzeptanz von autonomen Fahrzeugen.“ Online: https://causa.tagesspiegel.de/gesellschaft/autonomes-fahren-sind-wir-bereit-fuer-selbstfahrende-autos/ethische-dilemmata-unterlaufen-oft-akzeptanz-von-autonomen-fahrzeugen.html. (Zugriff: 03.05.2017).

[33.] Daimler (o. J. b) „Autonom unterwegs. Ein Mehr an Komfort, Sicherheit und Effizienz.“ Online: https://www.daimler.com/innovation/autonomes-fahren/special/veraenderungen.html. (Zugriff: 04.05.2017).

[34.] Daimler (2018). CASE - Intuitive Mobilität. In: https://www.daimler.com/case/ (Zugriff: 10.06.2018)

[35.] Deloitte (2016) Autonomes Fahren in Deutschland- wie Kunden überzeugt werden. Online: https://www2.deloitte.com/content/dam/Deloitte/de/Documents/consumer-industrial-products/Autonomes_Fahren_komplett_safe.pdf. (Zugriff: 18.05.2017).

[36.] Deloitte (2017a) Mobilität 2.0: Erfolg neu denken. Sonderveröffentlichung in der Automobilwoche. Online: https://www2.deloitte.com/de/de/pages/consumer-industrial-products/articles/mobilitaet-2-0-erfolg-neu-denken.html. (Zugriff: 27.04.2017).

[37.] Deloitte (2017b) „Autonomes Fahren: Knackpunkt Sicherheit.“ Online: http://www.presseportal.de/pm/60247/3579241. (Zugriff:28.04.2017).

[38.] Dietvorst, B.J., Simmons, J.P., Massey, C., 2015. Overcoming Algorithm Aversion: People Will Use Algorithms If They Can (Even Slightly) Modify Them. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2616787

[39.] Diewald S., Möller A., Roalter L., Kranz M. (2011) Mobile Device Integration and Interaction in the Automotive Domain. Automotive UI 2011. Online: http://www.eislab.fim.uni-

passau.de/files/publications/2011/AutoNUI_Mobile_Device_Integration.pdf. (Zugriff: 03.05.2017).

[40.] Doctorow, C., 2015. The problem with self-driving cars: who controls the code? [WWW Document]. The Guardian. URL https://www.theguardian.com/technology/2015/dec/23/the-problem-with-self-driving-cars-who-controls-the-code (accessed 9.10.18).

[41.] Doughty-White, P., Quick, M., 2015. Million Lines of Code [WWW Document]. Information is Beautiful. URL https://informationisbeautiful.net/visualizations/million-lines-of-code/ (accessed 11.4.18).

[42.] Fagnant, D.J., Kockelman, K., 2015. Preparing a nation for autonomous vehicles: opportunities, barriers and policy recommendations. Transportation Research Part A: Policy and Practice 77, 167–181. https://doi.org/10.1016/j.tra.2015.04.003

[43.] Favarò, F.M., Nader, N., Eurich, S.O., Tripp, M., Varadaraju, N., 2017. Examining accident reports involving autonomous vehicles in California. PLOS ONE 12, e0184952. https://doi.org/10.1371/journal.pone.0184952

[44.] Favarò, F., Eurich, S., Nader, N., 2018. Autonomous vehicles' disengagements: Trends, triggers, and regulatory limitations. Accident Analysis & Prevention 110, 136–148. https://doi.org/10.1016/j.aap.2017.11.001

[45.] FAZ (2017) „Intel kauft israelisches Start-up Mobileye. Kameras für Roboterwagen". Online: http://www.faz.net/aktuell/wirtschaft/neue-mobilitaet/kameras-fuer-roboterwagen-intel-kauft-israelisches-start-up-mobileye-14922462.html. (Zugriff: 28.03.2017).

[46.] Feng, F., Liu, Y., Chen, Y., Filev, D., & To, C. (2014) Computer-aided usability evaluation of in-vehicle infotainment systems, Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 58, 2285-2289.

[47.] Fraunhofer IAO, Horváth & Partners (2016) ‚The Value of Time' Nutzerbezogene Service- Potenziale durch autonomes Fahren, Stutt-

gart. Online: https://blog.iao.fraunhofer.de/images/blog/studie-value_of_time.pdf. (Zugriff: 28.03.2016)

[48.] Frost & Sullivan (2016a) „Global Autonomous Driving Market Outlook 2016“ Online: http://www.frost.com/sublib/display-report.do?id=MBD3-01-00-00-00, (Online: 21.03.2017)

[49.] Frost & Sullivan (2016b) „Autonomes Fahren: Steigende Akzeptanz ermöglicht Wachstum und treibt Erstausrüster zu Entwicklung neuer Geschäftsmodelle an.“ Online: https://ww2.frost.com/news/press-releases/autonomes-fahren-steigende-akzeptanz-ermoglicht-wachstum-und-treibt-erstausruster-zur-entwicklung-neuer-geschaftsmodelle/. (Zugriff: 21.03.2017).

[50.] Futurezone (2017) „Tag: Selbstfahrende Autos“. Online: https://futurezone.at/tag/Selbstfahrende+Autos/5. (Zugriff: 17.3.2017).

[51.] Ge, J.I., Avedisov, S.S., He, C.R., Qin, W.B., Sadeghpour, M., Orosz, G., 2018. Experimental validation of connected automated vehicle design among human-driven vehicles. Transportation Research Part C: Emerging Technologies 91, 335–352. https://doi.org/10.1016/j.trc.2018.04.005

[52.] Ghena, B., Beyer, W., Hillaker, A., Pevarnek, J., Halderman, J.A., 2014. Green Lights Forever: Analyzing the Security of Traffic Infrastructure, in: Proceedings of the 8th USENIX Conference on Offensive Technologies, WOOT'14. USENIX Association, Berkeley, CA, USA

[53.] Gläser, N., Lesko, P., 2017. Smart City Applikationen für die Verbesserung der Luftqualität in deutschen Städten am Beispiel Smart Parking. Ernst & Young. Online: www.ey.com/Publication/vwLUAssets/ey-smart-city-beispiel-smart-parking/$File/ey-smart-city-beispiel-smart-parking.pdf (Zugriff: 20.06.2018)

[54.] Giffi C.A., Vitale J., Schiller T., Robinson R. (2018). A reality check on advanced vehicle technologies. In: https://www2.deloitte.com/insights/us/en/industry/automotive/advanced

-vehicle-technologies-autonomous-electric-vehicles.html., January 05, 2018, accessed: 2018-06-10

[55.] Goodfellow, I., McDaniel, P., Papernot, N., 2018. Making machine learning robust against adversarial inputs. Communications of the ACM 61, 56–66. https://doi.org/10.1145/3134599

[56.] Görz G., Rollinger C.-R., Schneeberger J. (Hrsg.) (2003) Handbuch der Künstlichen Intelligenz, 4. Auflage. München/Wien: Oldenbourg.

[57.] Greenblatt, J.B., Shaheen, S., 2015. Automated Vehicles, On-Demand Mobility, and Environmental Impacts. Current Sustainable/Renewable Energy Reports 2, 74–81. https://doi.org/10.1007/s40518-015-0038-5

[58.] Greis F. (o.J.) „Autonomes Fahren- Die Ära der Kooperitis“. Online: https://www.golem.de/news/autonomes-fahren-die-aera-der-kooperitis-1702-125945.html. (Zugriff: 29.03.2017).

[59.] Greis, F., 2016. Zulassung autonomer Autos: Die längste Fahrprüfung des Universums - Golem.de [WWW Document]. golem.de. URL https://www.golem.de/news/zulassung-autonomer-autos-die-laengste-fahrpruefung-des-universums-1611-124139.html (accessed 9.10.18).

[60.] Gruel, W., Stanford, J.M., 2016. Assessing the Long-term Effects of Autonomous Vehicles: A Speculative Approach. Transportation Research Procedia 13, 18–29. https://doi.org/10.1016/j.trpro.2016.05.003

[61.] Habel C., Herweg M., Pribbenow S., Schlieder C. (2003) Wissen über Raum und Zeit. In: G. Görz et al. (Hrsg.) Handbuch der Künstlichen Intelligenz, 4.Aufl., München: Oldenbourg. (2003). (349-405).

[62.] Harper, C.D., Hendrickson, C.T., Mangones, S., Samaras, C., 2016. Estimating potential increases in travel with autonomous vehicles for the non-driving, elderly and people with travel-restrictive medical conditions. Transportation Research Part C: Emerging Technologies 72, 1–9. https://doi.org/10.1016/j.trc.2016.09.003

[63.] Heard, B.R., Taiebat, M., Xu, M., Miller, S.A., 2018. Sustainability implications of connected and autonomous vehicles for the food supply chain. Resources, Conservation and Recycling 128, 22–24. https://doi.org/10.1016/j.resconrec.2017.09.021

[64.] Heide, F., O'Toole, M., Zang, K., Lindell, D., Diamond, S., Wetzstein, G., 2017. Non-line-of-sight Imaging with Partial Occluders and Surface Normals. arXiv:1711.07134 [cs].

[65.] Hepp, A., 2016. Kommunikations- und Medienwissenschaft in datengetriebenen Zeiten. Publizistik 61, 225–246. https://doi.org/10.1007/s11616-016-0263-y

[66.] Heymann, E., Meister, J., 2017. Das „digitale Auto" - Mehr Umsatz, mehr Konkurrenz, mehr Kooperation. Deutsche Bank Research. Online: https://www.dbresearch.de/PROD/RPS_DEPROD/PROD0000000000445411/Das_%E2%80%9Edigitale_Auto%E2%80%9C%3A_Mehr_Umsatz%2C_mehr_Konkurrenz%2C.PDF (Zugriff: 10.06.2018)

[67.] IEEE Standards Association (2013) „Standards are Making the Internet of Things come alive". Online: http://beyondstandards.ieee.org/iot/standards_iot/. (Zugriff: 22.03.2017).

[68.] IME, 2016. Autonomous and driverless cars. Online: www.imeche.org/docs/default-source/1-oscar/reports-policy-statements-and-documents/driverless-cars-case-study.pdf?sfvrsn=0 (Zugriff: 20.06.2018)

[69.] Johanning V., Mildner R. (2015) Car IT kompakt. Das Auto der Zukunft - Vernetzt und autonom fahren. Wiesbaden: Springer.

[70.] Kalra, N., Paddock, S.M., 2016. Driving to safety: How many miles of driving would it take to demonstrate autonomous vehicle reliability? Transportation Research Part A: Policy and Practice 94, 182–193. https://doi.org/10.1016/j.tra.2016.09.010

[71.] Kalra, N., Groves, D.G., 2017. The enemy of good: estimating the cost of waiting for nearly perfect automated vehicles. RAND, Santa Monica, Calif.

[72.] Kaluza, B., Blecker, T. (2005) „Flexibilität- State of the Art und Entwicklungstrends“. In: B. Kaluza, T. Blecker (Hrsg.) Erfolgsfaktor Flexibilität- Strategien und Konzepte für wandlungsfähige Unternehmen. Berlin: Erich Schmidt.

[73.] Khalifa, A.S. (2004) Customer Value- A Review of Recent Literature- An Integrative Configuration. In: Management Decision. Ausg. 42 (5), 645-666.

[74.] Knight, W., 2016. Undurchschaubare Autopiloten [WWW Document]. Technology Review. URL https://www.heise.de/tr/artikel/Undurchschaubare-Autopiloten-3264689.html (accessed 9.10.18).

[75.] Knott, M. (2016) „Autonomes Fahren: In fünf Stufen zum Roboterauto. Automatisierungsgrade erklärt“. Online: https://www.netzwelt.de/automobil/159354-autonomes-fahren-fuenf-stufen-roboterauto.html. (Zugriff: 15.3.2017)

[76.] Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., 2010. Experimental Security Analysis of a Modern Automobile. IEEE, pp. 447–462. https://doi.org/10.1109/SP.2010.34

[77.] Kotrba, D., 2017. US-Farmer hacken vermehrt ihre eigenen Traktoren [WWW Document]. futurezone. URL https://futurezone.at/digital-life/us-farmer-hacken-vermehrt-ihre-eigenen-traktoren/253.677.084 (accessed 9.10.18).

[78.] Krafty Librarian, 2014. Hospitals Still on Windows XP Could Mean Loss of HIPAA Compliance – Krafty Librarian [WWW Document]. Krafty Librarian. URL http://www.kraftylibrarian.com/hospital-still-on-windows-xp-could-mean-loss-of-hipaa-compliance/ (accessed 9.18.18).

[79.] Kreuzbauer, H.M., 2018. The Connected Car and Data Protection: A Dilemma of Legal Ethics, in: Jusletter IT 22. Februar 2018

[80.] Kumpf, A. (1999) Servicekultur als Erfolgsfaktor: Strategien und Maßnahmen auf dem Weg zur Serviceorientierung. Wien: Linde.

[81.] Kyriakidis, M., Happee, R., de Winter, J.C.F., 2015. Public opinion on automated driving: Results of an international questionnaire among 5000 respondents. Transportation Research Part F: Traffic Psychology and Behaviour 32, 127–140. https://doi.org/10.1016/j.trf.2015.04.014

[82.] Lee E.-K, Gerla M., Pau G., Lee U., Lim J.-H. (2016) „Internet of Vehicles: From intelligent grid to autonomous cars and vehicular fogs“. International Journal of Distributed Sensor Networks. 12/9. 1-14.

[83.] Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., 2010. Experimental Security Analysis of a Modern Automobile, in: 2010 IEEE Symposium on Security and Privacy. Presented at the 2010 IEEE Symposium on Security and Privacy, IEEE, Oakland, CA, USA, pp. 447–462. https://doi.org/10.1109/SP.2010.34

[84.] Larson, S., 2017. Why hospitals are so vulnerable to ransomware attacks [WWW Document]. CNN. URL https://money.cnn.com/2017/05/16/technology/hospitals-vulnerable-wannacry-ransomware/index.html (accessed 9.18.18).

[85.] Lindner, R. (2017) “Ohne uns fährt kein Auto autonom“ Online: http://www.faz.net/aktuell/wirtschaft/unternehmen/infineon-chef-im-gespraech-ohne-uns-faehrt-kein-fahrzeug-autonom-14607425-p2.html. (Zugriff: 29.03.2017).

[86.] Litman, T., 2018. Autonomous Vehicle Implementation Predictions - Implications for Transport Planning. Victoria Transport Policy Institute. Siehe auch: https://www.vtpi.org/avip.pdf (Zugriff: 20.06.2018)

[87.] Lünendonk GmbH, AutomotiveIT (2011) IT- Dienstleistungen für eine veränderte Automobilindustrie, Ein neues Automotive- Eco-System fordert interne IT und externe IT- Provider heraus. Online: http://luenendonk-shop.de/out/pictures/0/lue_branchendossier_automotiveit_f141211_fl.pdf. (Zugriff: 3.4.2017).

[88.] Lutz, L.S., 2014. Rechtliche Hürden auf dem Weg zu autonomen Fahrzeugen [WWW Document]. Telepolis. URL

https://www.heise.de/tp/features/Rechtliche-Huerden-auf-dem-Weg-zu-autonomen-Fahrzeugen-3364605.html (accessed 9.10.18).

[89.] Maurer M., Gerdes J.C., Lenz B., Winner H. (Hrsg.) (2015) Autonomes Fahren. Technische, rechtliche und gesellschaftliche Aspekte. Heidelberg: Springer.

[90.] McLean, A., 2017. Innovation committee toys with separate lanes for autonomous vehicles in Australia [WWW Document]. ZDNet. URL https://www.zdnet.com/article/innovation-committee-toys-with-separate-lanes-for-autonomous-vehicles-in-australia/ (accessed 9.10.18).

[91.] Messmer, E., 2004. Fed up hospitals defy patching rules [WWW Document]. Network World. URL https://www.networkworld.com/article/2324260/lan-wan/fed-up-hospitals-defy-patching-rules.html (accessed 9.18.18).

[92.] Meyer, J., Becker, H., Bösch, P.M., Axhausen, K.W., 2017. Autonomous vehicles: The next jump in accessibilities? Research in Transportation Economics 62, 80–91. https://doi.org/10.1016/j.retrec.2017.03.005

[93.] Milakis, D., van Arem, B., van Wee, B., 2017. Policy and society related implications of automated driving: A review of literature and directions for future research. Journal of Intelligent Transportation Systems 21, 324–348. https://doi.org/10.1080/15472450.2017.1291351

[94.] Miller, Ch., Valasek, C., 2014. A Survey of Remote Automotive Attack Surfaces. Online: https://ioactive.com/pdfs/IOActive_Remote_Attack_Surfaces.pdf. (Zugriff: 09.09.2018)

[95.] Münchener Kreis e.V. (Hrsg.) et al. (2009) Zukunft und Zukunftsfähigkeit der Informations- und Kommunikationstechnologien und Medien, Internationale Delphi-Studie 2030. Online: http://informationszentrum-mobilfunk.de/zukunft-und-zukunftsfaehigkeit-der-informations-und-kommunikations-technologien-und-medien. (Zugriff: 12.05.2017)

[96.] N., N., 2016. Indien verbietet Facebook kostenlosen Internet-Service [WWW Document]. Futurezone. URL https://futurezone.at/netzpolitik/indien-verbietet-facebook-kostenlosen-internet-service/179.782.942 (accessed 11.4.18).

[97.] N., N., 2018. Selbstfahrende Autos könnten Verkehrsaufkommen sogar erhöhen [WWW Document]. derStandard.at. URL https://derstandard.at/2000089537030/Selbstfahrende-Autos-koennten-Verkehrsaufkommen-sogar-erhoehen (accessed 11.4.18).

[98.] Naughton, J., 2017. Giving Google our private NHS data is simply illegal | John Naughton. The Guardian.

[99.] Nickel, O., 2018. Autonomes Fahren: Forscher täuschen Straßenschilderkennung mit KFC-Schild - Golem.de [WWW Document]. golem.de. URL https://www.golem.de/news/autonomes-fahren-forscher-taeuschen-strassenschilderkennung-mit-kfc-schild-1802-132874.html (accessed 9.10.18).

[100.] Nilsson N.J. (2014) Die Suche nach Künstlicher Intelligenz. Eine Geschichte von Ideen und Erfolgen. Aus dem Englischen von Hinrichs R., Koch A., Reinecke R., Schemala D., Bibel W., Schmidt N., Seemann I. Berlin: Akademische Verlagsgesellschaft AKA

[101.] Nyholm, S., Smids, J., 2016. The Ethics of Accident-Algorithms for Self-Driving Cars: an Applied Trolley Problem? Ethical Theory and Moral Practice 19, 1275–1289. https://doi.org/10.1007/s10677-016-9745-2

[102.] Olzak, T., 2011. UEFI and the TPM: Building a foundation for platform trust [WWW Document]. InfoSec Resources. URL https://resources.infosecinstitute.com/uefi-and-tpm/ (accessed 9.18.18).

[103.] Pfaffenbichler, Paul & Emberger, Günter & Shepherd, Simon & May, A.D.. (2018). The potential impacts of automated cars on urban transport: an exploratory analysis. Working Paper - Extended Abstract, presented at the Vienna Special Interest Group Workshop SIG 2 – Regional and National Transport Policy World Conference on Transport

Research (WCTRS SIG G2) TU Vienna, Austria, 24-25 September 2018.

[104.] Pinto, N., 2016. Google Is Transforming NYC's Payphones Into a 'Personalized Propaganda Engine' [WWW Document]. The Village Voice. URL https://www.villagevoice.com/2016/07/06/google-is-transforming-nycs-payphones-into-a-personalized-propaganda-engine/ (accessed 11.4.18).

[105.] Rademacher, P. (2012) „Das vernetzte Auto: Der Begriff der Car-IT gewinnt in der Automobilindustrie massiv an Bedeutung- die künftige Rolle der Business- IT". Online: http://www.car-it.com/der-begriff-car-it-gewinnt-in-der-automobilindustrie-massiv-an-bedeutung-die-kunftige-rolle-der-business-it/id-0031942. (Zugriff: 17.3.2017).

[106.] Reichardt D. (1996) Kontinuierliche Verhaltenssteuerung eines autonomen Fahrzeugs in dynamischer Umgebung. Diss. Universität Kaiserslautern. Online: http://wwwlehre.dhbw-stuttgart.de/~reichardt/content/person/doc/diss-all.pdf. (Zugriff: 12.05.2017)

[107.] Reynolds, M., 2017. Sneaky attacks trick AIs into seeing or hearing what's not there [WWW Document]. New Scientist. URL https://www.newscientist.com/article/2142059-sneaky-attacks-trick-ais-into-seeing-or-hearing-whats-not-there/ (accessed 9.10.18).

[108.] sCybersecurity Evaluation of Automotive E/E Architectures. In: https://cscs.mpi-inf.mpg.de/files/2018/09/02-Cybersecurity-Evaluation-of-Automotive-E_E-Architectures.pdf, accessed 2018-10-30

[109.] Rocque, M., 2017. Make way for autonomous vehicles: infra-structure considerations for urban environments by Michelle Caulfield-Harris [WWW Document]. Smart Cities World. URL https://www.smartcitiesworld.net/opinions/opinions/make-way-for-autonomous-vehicles-infrastructure-considerations-for-urban-environments-by-michelle-caulfield-harris (accessed 9.10.18).

[110.] Samulat P. (2016) Top-Down zum Digitalen Unternehmen. Handlungsempfehlungen für die erfolgreiche Transformation, BoD: Books on Demand, Norderstedt.

[111.] Samulat P., (2017) Die Digitalisierung der Welt. Wie das Industrielle Internet der Dinge aus Produkten Services macht. Wiesbaden: Springer.

[112.] SAE International, 2016. Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles, SAE International. Available at: http://standards.sae.org/j3016_201609/ [Accessed November 23, 2016].

[113.] Scarfone, K., 2018. Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks. NIST, Draft NISTIR 8228. https://doi.org/10.6028/nist.ir.8228-draft

[114.] Schneier, B., 2017. Security and Privacy Guidelines for the Internet of Things - Schneier on Security [WWW Document], 09.02.2017. URL https://www.schneier.com/blog/archives/2017/02/security_and_pr.html (Zugriff: 09.09.2018).

[115.] Schneier, B., 2018. Click here to kill everybody: security and survival in a hyper-connected world, First edition. ed. W.W. Norton & Company, New York.

[116.] Sindre, G., Opdahl, A.L., 2005. Eliciting security requirements with misuse cases. Requirements Engineering 10, 34–44. https://doi.org/10.1007/s00766-004-0194-4

[117.] Sitawarin, C., Bhagoji, A.N., Mosenia, A., Chiang, M., Mittal, P., 2018. DARTS: Deceiving Autonomous Cars with Toxic Signs. arXiv:1802.06430 [cs].

[118.] Spehr M. (2015) „Wozu braucht man das Internet im Auto?“ Online: http://www.faz.net/aktuell/technik-motor/auto-verkehr/aufregung-nach-hackerangriffen-wozu-braucht-man-das-internet-im-auto-13740804.html. (Zugriff: 03.05.2017).

[119.] SZ (Süddeutsche Zeitung) (2016) Das Vertrauen in das autonome Fahren ist durch den Tesla-Unfall dahin. Online: http://www.sueddeutsche.de/wirtschaft/tesla-das-vertrauen-in-das-autonome-fahren-ist-durch-den-tesla-unfall-dahin-1.3058621. (Zugriff: 16.05.2017)

[120.] Surden, H., Williams, M.-A., 2016. Technological Opacity, Predictability, and Self-Driving Cars. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2747491

[121.] Townsend, A., 2016. Prioritising the Safety Potential of Automated Driving in Europe. Policy Briefing. European Transport Safety Councel. Online: etsc.eu/wp-content/uploads/2016_automated_driving_briefing_final.pdf (Zugriff: 20.06.2018)

[122.] Vandermerwe S., Rada J., (1988) Servitization of Business: Adding Value by Adding Services. European Management Journal. Ausg. 6(4).314-324.

[123.] VDA (2015a) Automatisierung. Von Fahrerassistenzsystemen zum automatisierten Fahren. VDA Magazin. Online: https://www.vda.de/dam/vda/publications/2015/automatisierung.pdf. (Zugriff:12.05.2017).

[124.] Voeth M. & Bertels V. (2014) „Service Value von produktbegleitenden Dienstleistungen“ In: M. Bruhn, K. Hadwich(Hrsg.) Service Value als Werttreiber. Konzepte, Messung und Steuerung. Forum Dienstleistungsmanagement. S. 283- 300. Wiesbaden: Springer Gabler.

[125.] Volkswagen (2017) „Adaptive Cruise Control (ACC). Volkswagen’s safe distance technology“. Online: http://www.volkswagen.co.uk/technology/adaptive-cruise-control-acc. (Zugriff: 15.03.2017).

[126.] Wadud, Z. (o.J.). Self-Driving Cars. Will they reduce Energy Use?. University Leeds, Mobility & Energy Futures Series. Online: http://www.its.leeds.ac.uk/about/news/driverless-cars-could-increase-reliance-on-roads/, accessed: 2018-06-10

[127.] Wadud, Z., MacKenzie, D., Leiby, P., 2016. Help or hindrance? The travel, energy and carbon impacts of highly automated vehicles. Transportation Research Part A: Policy and Practice 86, 1–18. https://doi.org/10.1016/j.tra.2015.12.001

[128.] Wassmus A., (2014) Serviceorientierung als Erfolgsfaktor und Komplexitätstreiber beim Angebot hybrider Produkte. Wiesbbaden: Springer Gabler.

[129.] WEF (2018). Reshaping Urban Mobility with Autonomous Vehicles - Lessons from the City of Boston. Online: www3.weforum.org/docs/WEF_Reshaping_Urban_Mobility_with_Autonomous_Vehicles_2018.pdf (Zugriff: 16.06.2018)

[130.] WHO (World Health Organization) (2015) „Global Status Report on Road Safety“. Online: http://www.who.int/violence_injury_prevention/road_safety_status/2015/en/. (Zugriff: 16.05.2017).

[131.] Vlasic, B., Boudette, N., 2016. Self-Driving Tesla Was Involved in Fatal Crash, U.S. Says - The New York Times [WWW Document]. The New York Times. URL https://www.nytimes.com/2016/07/01/business/self-driving-tesla-fatal-crash-investigation.html (accessed 9.10.18).

[132.] Wakabayashi, D., 2018. Emergency Braking Was Disabled When Self-Driving Uber Killed Woman, Report Says [WWW Document]. The New York Times. URL https://www.nytimes.com/2018/05/24/technology/uber-autonomous-car-ntsb-investigation.html (accessed 9.10.18).

[133.] Wolter S. (2012) Smart Mobility - Intelligente Vernetzung der Verkehrsangebote in Großstädten. In: H. Proff, J. Schönharting, D. Schramm, J. Ziegler (Hrsg.) Zukünftige Entwicklungen in der Mobilität. Betriebswirtschaftliche und technische Aspekte. S.527-548. Wiesbaden: Springer Gabler.

[134.] Yadron, D., Tynan, D., 2016. Tesla driver dies in first fatal crash while using autopilot mode [WWW Document]. The Guardian. URL https://www.theguardian.com/technology/2016/jun/30/tesla-autopilot-death-self-driving-car-elon-musk (accessed 9.10.18).

[135.] Yağdereli E., Gemci C., Aktas A. Z. (2015) A study on cyber-security of autonomous and unmanned vehicles. Journal of Defense

Modeling and Simulation: Applications, Methodology, Technology, 2015, Ausg. 12(4), S. 369.

[136.] Zhao,D., Peng, H., 2017. From the Lab to the Street: Solving the Challenge of Accelerating Automated Vehicle Testing. M-City. UNiversity of Michigan. Online: https://mcity.umich.edu/wp-content/uploads/2017/05/Mcity-White-Paper_Accelerated-AV-Testing.pdf (Zugriff: 10.06.2018)

Annex 1: Geschichte der Automatisierung und Stand der Technik

Bereits Anfang des 20. Jahrhunderts wurde der Gedanken an ein automatisiertes Fahren öffentlich (vgl. VDA 2015, S.5). Im Jahr 1939 wurde die Vision des fahrerlosen Fahrzeugs auf der New Yorker Weltausstellung „Futurama" präsentiert und die Realisierung bereits für das Jahr 1960 vorausgesehen. Daraufhin entwickelten, laut VDA, Ingenieure/Ingenieurinnen in den 1950er-Jahren die ersten Konzepte für vollautomatisierte Langstreckenfahrten in den USA. Die Verbindung zwischen Infrastruktur und Fahrzeugtechnologie sollte dafür sorgen, dass eine reine Meldung an die Verkehrsleitzentrale ausreiche, um ans gewünschte Ziel zu kommen.

Das erste autonome Fahrzeug stelle schließlich 1977 das *Mechanical Engineering Laboratory* im japanischen *Tsukub*a vor, was mithilfe zweier Kameras die Straße „wahrnehmen" konnte. Daraufhin folgten Entwicklungen in den USA, bspw. im *Artificial Intelligence Lab* der *University of Stanford* (vgl. Maurer et al 2015, S.59 f). Schließlich markierte die Vorstellung des *Antiblockiersystems* (ABS) 1978 den Anfang von ins Fahrgeschehen eingreifender FAS.

Grundlegende Basis für die Entwicklung selbstfahrender Autos bildet das wahrscheinlich bekannteste europäische Programm zur Fahrzeugautomatisierung (vgl. ebd. S. 4): „**Pro**gra**m**me for a **E**uropean traffic with **h**ighest **e**fficiency and **u**nprecedented **s**afety (*PROMETHEUS*) von 1987 bis 1994. Laut Reichardt (1996, S. 2) wurde ein steigendes Verkehrsaufkommen in Westeuropa als Ursache für unzählige Unfälle mit Todesfällen und Verletzten bezeichnet. Dieser Fakt und die Angst vor einer wirtschaftlichen und technologischen Rückständigkeit gegenüber Japan und den USA werden als die ausschlaggebende Motivation für die Initiierung des Forschungsprogramms genannt. Der Name des Programms erkläre, nach Reichardt, auch die Intention des Projekts: Hauptziel sollte es sein, das Auto sicherer zu machen und den Verkehr effizienter zu organisieren. Dafür erfolgte die Konzentration auf die Integration und Weiterentwicklung von Techniken wie Mikroelektronik, neue Sensoren und die Informations- und Kommunikationstechnik.

In den Bereichen Sicherheit und Verkehrssystem-Management umfasste das Programm sieben verschiedene Schwerpunkte. Unter den Bezeichnungen „PRO-CAR“, „PRO-NET“ und „PRO-ROAD“ führten industrielle Partner Entwicklungen direkt am Fahrzeug selbst durch wie bspw. Frühwarnsysteme in Gefahrensituationen, Kommunikationswege zwischen Fahrzeugen oder mit Informationssystemen im Straßenverkehr. Die Bereiche „PRO-ART“, „PRO-GEN“, „PRO-CHIP“ und „PRO-COM“ beschäftigten sich mit dem Einsatz von Künstlicher Intelligenz (KI) im Straßenverkehr, Datenaustausch oder rechtlichen Fragen (vgl. ebd., S.4). Auffällig ist hierbei die wachsende Integration des Faktors der Kommunikation in den Bereich der Automobilbranche, welche später noch näher thematisiert werden soll.

Das Beratungsunternehmen *Frost & Sullivan* thematisierte in der Studie „Global Autonomous Driving Market Outlook, 2016“ (vgl. Frost & Sullivan 2016a) die Veränderungen im zukünftigen automobilen Ökosystem. Dabei seien (vgl. Frost & Sullivan, 2016b) bereits 80 Prozent der Erstausstatter (engl. original equipment manufacturers, Abk. OEMs) der Automobilindustrie dabei ihre Automatisierungstechnik zu planen bzw. diese umzusetzen. Das autonome Fahren könne demnach nur durch die schrittweise Annäherung durch Fahrassistenzsysteme entstehen. Nachdem das Auto mithilfe von Sensoren und Kameras nun „Fühlen und Sehen“ könne, so Johanning und Mildner (2015, S.1) in ihren Ausführungen, werde die „Intelligenz“ des Autos durch die Vernetzung von Fahrzeugen und Infrastruktur um ein Vielfaches erhöht.

So werden mithilfe der Automatisierung Funktionen, die früher noch von Menschen ausgeführt wurden, auf technische Systeme übertragen. Im Flugverkehr werden bereits autonom funktionsfähige Systeme, wie etwa Flight-Management-Systeme oder Autopilot eingesetzt (vgl. Maurer et al. 2015, S.105). Ebenfalls zu autonomen Systemen hinzuzuzählen sind, laut Yağdereli et al. (2015, S. 369), Raumsonden, Raumfahrzeuge, unbemannte Luftfahrzeuge (UAV), unbemannte Landfahrzeuge (UGV), unbemannte Seefahrzeuge (USV) sowie unbemannte Unterwasserfahrzeuge (UUV).

Im Straßenverkehr haben es die Systeme jedoch mit einer viel höheren Umgebungskomplexität und -dynamik zutun (vgl. Maurer et al. 2015, S.107),

weshalb die Einführung der Systeme in den Alltag und die Nutzung der autonomen Fahrzeuge in Serie derzeit noch in der Zukunft liege.

Dennoch schreitet die Entwicklung rasch voran: Sowohl Automobilkonzerne (z. B. *Ford, Audi/Volkswagen, Daimler, BMW, Nissan, Hyuandai* u.v.m.), wie auch große Chiphersteller (z. B. *Intel, Nvidia, Mobileye, Qualcomm*) oder andere Technikkonzerne (z. B. *Bosch*) sowie Firmen der Telekommunikationsbranche (*Google/Alphabet*, *Apple, Baidu*) oder aus anderen Branchen (z.B. *Uber, Airbus*) engagieren sich intensiv seit Jahren im Bereich des autonomen Fahrens (vgl. Futurezone 2017). Zunehmend ergeben sich hier Betriebszusammenschlüsse zwischen Unternehmen aus unterschiedlichen Branchen: Erst kürzlich übernahm der amerikanische Chip-Gigant *Intel* den israelischen Kameratechnik- und Softwarehersteller *Mobileye* (vgl. FAZ 2017), der schon jetzt eine Vorreiterrolle im Bereich der Roboterwagen, Fahrassistenzsysteme und der künftig selbstfahrenden Autos übernehme.

> Diese Kooperation ist nur ein Beispiel für diverse Zusammenarbeiten zwischen Automobilherstellern und Softwareherstellern im weiteren Sinne. Aufgrund von hohen Entwicklungskosten im IT- und Softwarebereich werden Kooperationen angestrebt, die rascher zu einem Fortschritt im Bereich des autonomen Fahrens führen sollen (vgl. Greis 2017). Betrachtet man sich in weiterer Folge die führenden Unternehmen in diesem, neuen Geschäftsfeld, so kristallisiert sich vor allem eine Auffälligkeit heraus: Obwohl das autonome Fahren auf den ersten Blick ein Anwendungsgebiet der Automobilbranche zu sein scheint, sind es gerade die Technologiekonzerne, die die Vorreiterrolle übernehmen. Automobilhersteller im klassischen Sinn, wie z.B. *Volkswagen* oder *Daimler* konzentrieren sich auf Kooperationen mit Chipherstellern. Der Grund dafür stellt der wachsende Anteil an Informations- und Kommunikationstechnologie im Fahrzeug dar, weshalb der Fokus von der Hardware auf die Software gelegt wird.

Annex 2: Artificial Intelligence in der autonomen Mobilität

Für die autonome Mobilität reicht die Integration simpler Informations- und Kommunikationstechnologien nicht aus, sie erfordert vor allem die Schaffung einer künstlichen Intelligenz (KI) (engl. artificial intelligence, Abk. AI).[17] Mithilfe von KI kann eine Software insoweit optimiert werden, dass sie autonom agieren kann. Ohne die Fähigkeit, lernen zu können, wäre das Fahrzeug weiterhin auf eine menschliche Steuerungsfunktion angewiesen und könnte somit nicht als völlig autonom bezeichnet werden.

Das von Günther Görz et al. in Kooperation mit dem Fachbereich 1 „Künstliche Intelligenz“ der Gesellschaft für Information e.V. herausgegebene „Handbuch der Künstlichen Intelligenz“ definiert den Terminus wie folgt:

> „’Künstliche Intelligenz’ (KI) ist eine wissenschaftliche Disziplin, die das Ziel verfolgt, menschliche Wahrnehmungs- und Verstandesleistungen zu operationalisieren und durch Artefakte, kunstvoll gestaltete technische- insbesondere informationsverarbeitende- Systeme verfügbar zu machen“ *(Görz et al. 2003, S.1).*

KI beschäftige sich, laut Cawsey (vgl. 2003, S.13) also damit, die Aufgaben menschlichen Handelns auf Computer zu übertragen. Um den Begriff abgrenzen zu können, muss jedoch der Terminus der Intelligenz selbst betrachtet werden, der sich in der Literatur nur bedingt eindeutig definieren lässt. Auf der Grundlage der Begriffsdefinition von Intelligenz, der das Erkenntnisvermögen bzw. die Urteilsfähigkeit und das Erfassen von Möglichkeiten und das Vermögen, Zusammenhänge zu begreifen (vgl. Görz et al. 2003, S.2) beschreibt, werden dem komplexen, menschlichen Verhalten drei grundlegende Fähigkeiten zugeschrieben (vgl. Habel et al. 2003, S.349):

[17] Eine umfangreiche gesellschaftliche Analyse der Missbrauchspotenziale durch den Einsatz künstlicher Intelligenz findet sich bei Brundage et al. (2018).

[1.] Die Fähigkeit die Welt, sowohl auf visueller, auditiver und taktiler Ebene wahrzunehmen und zu verstehen,

[2.] Probleme lösen, handeln und sich bewegen zu können und

[3.] die Fähigkeit mit anderen Menschen, bzw. mit anderen kognitiven Systeme zu kommunizieren.

Die von der menschlichen Intelligenz ausgehende Definition setzt Wissen voraus, um kognitiv agieren zu können. Dies gelte laut Habel et al. (2003) für Menschen sowie auch für leistungsfähige Computersysteme. Betrachtet man die Merkmale menschlicher Intelligenz in Bezug auf den Einsatz von KI im Bereich des autonomen Fahrens so ergibt sich Folgendes:

Die Funktionen, die das Automobil beim autonomen Fahren für den Menschen übernimmt, sind vielfältig. Diese reichen von der Fähigkeit die Straße zu scannen bzw. die Umgebung wahrzunehmen und entsprechend zu reagieren, über die Navigation, selbstständige Start- und Fahrfunktionen sowie autonomes Einparken und sich mit der Umwelt (Umfeldbedingungen) zu verständigen. Inwiefern diese beispielhaft den Merkmalen der menschlichen Intelligenz nach Habel et al. (2003) zugeordnet werden können, soll folgende Graphik (siehe Abb. 3) darstellen:

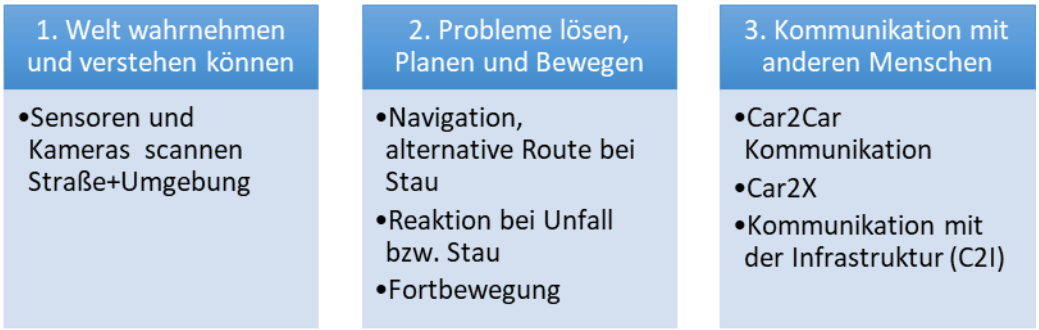


Abb. 4: Merkmale menschlicher Intelligenz übertragen auf autonomes Fahren, eigene Darstellung in Anlehnung an Habel et al. (2003, S.349).

Dabei kann die Sensorik, sowie diverse Kameras, die zur Wahrnehmung des Umfelds dienen, mit dem ersten Merkmal der menschlichen Intelligenz verglichen werden. Das Auto übernimmt hierbei die Aufgabe der Wahrnehmung und das Verständnis dessen, was im Umkreis passiert.

Das zweite Merkmal nach Habel et al. (2003), Probleme lösen zu können, zu planen und sich bewegen zu können, würde beim autonomen Fahrzeug die Fähigkeit darstellen, selbstständig zu navigieren sowie Alternativrouten vorzuschlagen und bei unvorhergesehenen Situationen reagieren zu können. Dies erfordert die Merkmale der dritten Ausprägung: der Kommunikation. Um Informationen zu erhalten, ist der Empfang und Austausch mit Infrastruktur und anderen Automobilen notwendig, was der Kommunikation der Menschen untereinander ähnelt.

Die Anwendung von KI im Bereich des autonomen Fahrens ist demnach grundlegend, um die erforderliche Autonomie des Autos zu schaffen. Dennoch wird diese vor allem im Hinblick auf eine ethische Auseinandersetzung oft diskutiert.

Während Anwendungen wie Navigationssysteme oder Spracherkennungssoftware in der Differenzierung zur „schwache[n] KI“ gezählt werden und das kognitive, menschliche System lediglich unterstützen, soll die Entwicklung der „starke[n] KI“ dieses nachahmen (vgl. Nilsson 2014, S.309) und wie bereits erwähnt, eigene intellektuelle Fähigkeiten aufweisen bzw. den menschlichen Intellekt übertreffen.

Trotz der hohen Anzahl von Unfällen im Straßenverkehr, die für durchschnittlich 1,2 Millionen Menschen pro Jahr tödlich endet (vgl. WHO 2015), ist das Vertrauen in die Technologie in der Gesellschaft nur begrenzt vorhanden und das, obwohl als größter Risikofaktor im Straßenverkehr der Mensch gelte (vgl. SZ 2016).

Aus ethischer Perspektive ergibt sich deshalb die Frage, ob es generell sinnvoll wäre, stärker in die Entwicklung unterstützender, schwacher KI-Systeme (z. B. FAS) zu investieren, statt zu versuchen, mithilfe des Roboterautos den kognitiven Apparat des Menschen obsolet zu machen. Das Ziel der Entwicklung sollte viel eher sein eine neue Definition vom Mensch-Maschine-Team zu schaffen und so die Beziehung zwischen Fahrzeuginsasse/Fahrzeuginsassinnen und Auto neu zu definieren. Im Zusammenhang mit dem autonomen Fahren erscheint deshalb der Gebrauch des Terminus der

„Smartness“ als sinnvoller, da mit dem Begriff der „Künstlichen Intelligenz“ ein noch sehr viel emotionalerer Diskurs einhergeht.

Annex 3: Service-Orientierung & Fahrzeuge als hybride Produkte

Aus dem Terminus „Service“ lässt die Ausrichtung auf den Kunden/die Kundin ableiten (vgl. Coenen 2010, S.38). Eine Orientierung am Kunden/an der Kundin (Kundenorientierung) kann daher auch eine höhere Serviceorientierung bedeuten. Aufgrund des Wettbewerbs sind Unternehmen dazu angehalten, einen Mehrwert für den Kunden/die Kundin bereitzustellen, um sich von den Leistungsangeboten der Konkurrenz abzuheben (vgl. Khalifa 2007, S.1). Durch produktbezogene Differenzierung allein ist dies jedoch wegen oft zu ähnlicher Qualitätsmerkmale kaum möglich, weshalb eine immer größere Fokussierung auf Service und Dienstleistungen stattfindet (vgl. Voeth & Bertels, S.285).

Während man den Ursprung des automobilen Service in der Fortbewegung sehen kann, also dem Dienst der Mobilität, ist im Laufe der Jahre und mithilfe des technischen Fortschritts eine Vielzahl an zusätzlichen Services entstanden. Über die Funktion eines Transportmittels hinweg entwickelte sich das Automobil zum Status- und Luxusgut mit technischen Raffinessen wie den Fahrassistenzsystemen (FAS), die dem Fahrer/der Fahrerin das Steuern erleichtern und die Autofahrt zu einem angenehmen Erlebnis machen sollen.

> „Bis zu 80 eingebettete Rechensysteme, 400 Sensoren und ein Gigabyte Software steuern die technischen Extras in Fahrzeugen, vom Bremsspurassistenten über das Navigationsgerät bis zum CD- Player“ (Lünendonk, 2011, S.15).

Eine im Jahr 2016 erschienene Studie, „The Value of Time“, des *Fraunhofer-Instituts für Arbeitswirtschaft und Organisation* (IAO) in Zusammenarbeit mit *Horváth & Partners Management Consultants* (vgl. Fraunhofer IAO 2016) befasst sich mit dem Potenzial, welches Service-Angebote beim automatisierten Fahren entstehen lassen. Im Rahmen dieser Studie wurden Ende des Jahres 2015 in Deutschland, Japan und den USA (Kalifornien) insgesamt 1.500 Pro-

banden und Probandinnen nach der zukünftigen Angebotslandschaft für Services im autonomen bzw. automatisierten Fahrzeug befragt. Demnach haben die Insassen und Insassinnen autonomer Fahrzeuge, Zeit und Bedarf sich anderweitig zu beschäftigen, was die neu gewonnene Zeit zu einer wichtigen Ressource macht, um Service-Leistungen anzubieten. Die Service-Welt „Automobil“ sei der Studie zufolge jedoch in Bezug auf die Form von Diensten bzw. ihrer Nachfrage noch weitgehend undurchsichtig. Mithilfe der Ergebnisse der Umfrage kreiert die Studie den Entwurf eines potenziellen Service-Marktes, der durch die gegebenen Antworten zur Beschäftigung während des Fahrens entstehen könnte. Dies bestätige ein betriebswirtschaftliches Potenzial von Service-Angeboten, so die Studie weiter.

Die Komplexität der Service-Angebote, die aus dem gewonnen Freiheitsgrad des Fahrers/der Fahrerin entstehe, sei jedoch abhängig vom Automatisierungsrad. Zwischen hochautomatisierten Fahren (Stufe 3) und autonomen Fahren (Stufe 5) bestehe klarerweise ein Unterschied in den Möglichkeiten der Inanspruchnahme von Services für den Fahrer/die Fahrerin. Bezüglich der noch unsicheren Entwicklung der Automobilindustrie unterscheidet die Studie hier zwischen zwei Szenarien. In der folgenden Betrachtung sollen jedoch die Antworten der ersten Variante „Hands off- feet off“ (vgl. ebd. S.6) ausgeblendet und nur die vollautonome Variante „Hands off- feet off- brain off“ miteinbezogen werden.

Die möglichen (Neben-) Tätigkeiten ließen sich auf die Erfüllung diverser Bedürfnisse zurückführen, so die Studie. So werden bestimmte Servicegruppen z.B. „Arbeiten“ wollen, was Tätigkeiten wie bspw. E-Mails lesen beinhaltet, dem Bedürfnis „Produktivität“ zugeordnet. Erfordere die Tätigkeit z.B. technologische Unterstützung (z.B. Lizenz oder ein Medium), so ergebe sich die Möglichkeit einer umsatzgenerierenden Service-Leistung, was bereits auf den Faktor der markt- und profitorientierten Wertschöpfung hindeutet.

Die definierten Bedürfnisse sind zusätzlich zur **Produktivität** (Arbeiten, Weiterbildung, Organisation, Einkäufe für den täglichen Bedarf), das Bedürfnis nach ***Kommunikation*** (Soziale Netzwerke/Interessengruppen, Beratungsgespräche, Privatkommunikation), **Grundbedürfnisse** (Waschen/Reinigen, Es-

sen/Trinken, Schlafen, Kleidung an/aus/umziehen), **Wohlfühlen** (Wellness, Schönheit, Gesundheit, Fitness), **Information** (Umgebungs-/ Routeninformationen, Produktinformationen, Informationssuche im Internet) und das Bedürfnis nach **Unterhaltung** (Spiele, Künstlerische Tätigkeiten, Passive Unterhaltung).

Die definierten Service-Gruppen beinhalten im autonomen Fahrzeug beispielsweise (Neben-)Tätigkeiten wie (vgl. ebd. S.8) Gespräche führen, Steuererklärungen zu erledigen, Online Shopping zu betreiben, zu bügeln, Essen zubereiten, zu schlafen, Kleindung zu wechseln, Ganzkörperpflege zu betreiben, intensiver sportlicher Betätigung nachzugehen, zu musizieren oder Entertainment in virtueller Realität zu genießen.

Mit der zunehmenden Automatisierung werde die Ausübung einer Vielzahl an zusätzlichen und komplexeren Tätigkeiten während der Autofahrt möglich. Tätigkeiten denen zuvor in der Arbeits- bzw. Freizeit nachgegangen werden musste, könnten nun während der Fahrt erledigt werden, was zusätzlich Freiräume im Tagesablauf schaffe (vgl. ebd. S. 10). Diese (Neben-)Tätigkeiten, die während der Fahrt erledigt werden können, werden im Rahmen der Studie als Services definiert.

Was die Zahlungsbereitschaft für die angebotenen Services betreffe, so korreliere diese mit dem „Value of Time“: Demnach liege der Bereitschaftsgrad für das Angebot zusätzlich zu investieren bei durchschnittlich 75 Prozent der befragten Studienteilnehmer/innen. Dies gelte vor allem für die Erfüllung der Bedürfnisse Kommunikation, Produktivität und von Grundbedürfnissen.

Weitere Erkenntnisse sind bspw. die Unterschiede der Rankings der Service-Gruppen zwischen den befragten Ländern bzw. ihre Zahlungsbereitschaft und die Differenzen zwischen Befragten bzgl. Alter, Einkommen und Fahrzeugsegment.

Auch Deloitte (2016; 2017a; 2017b) (siehe Abb. 4) stellte im Rahmen einer Studie die Frage nach der Nutzung der freien Zeit, wenn das Auto eigenständig fährt:

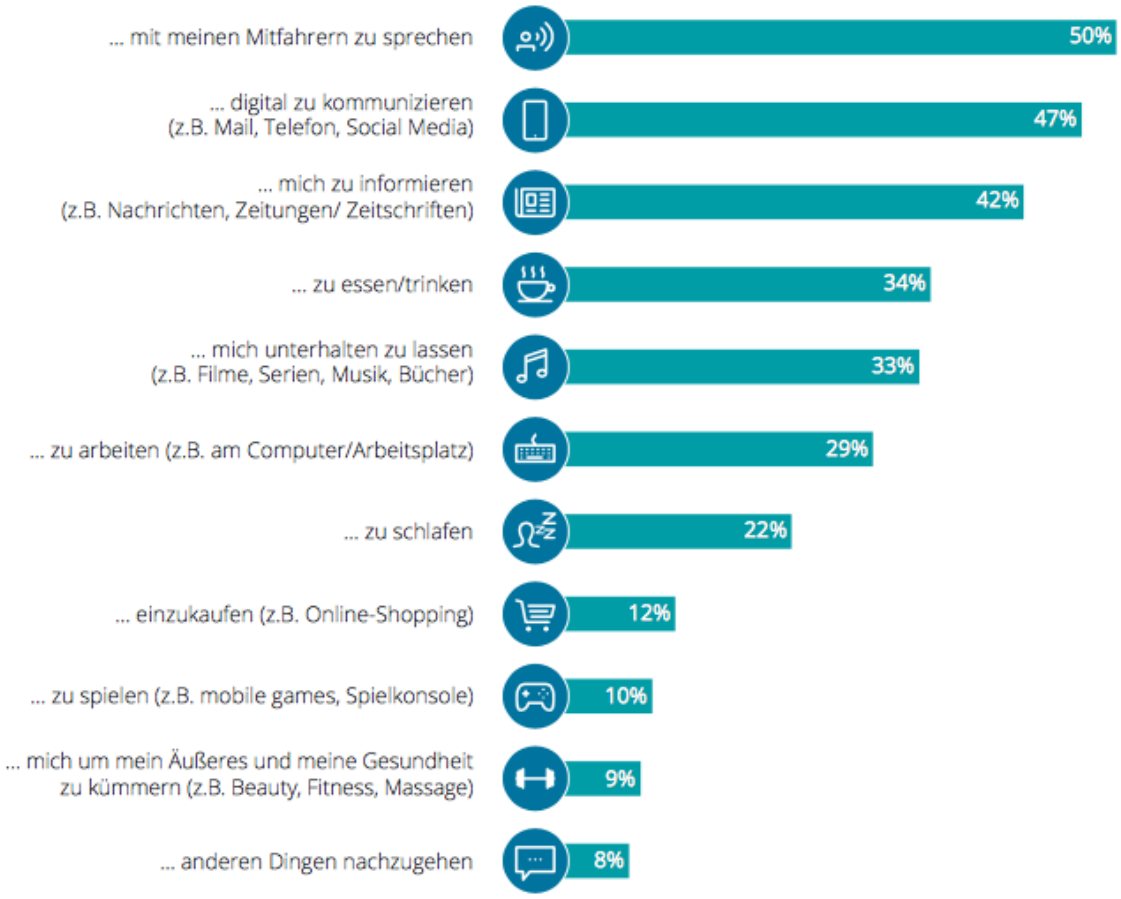


Abb. 5: Nutzung der durch autonomes Fahren gewonnenen Zeit" (Deloitte 2016, S.16).

Verglichen mit der Studie „Value of Time“ sind auch hier die Bereiche der Kommunikation, Produktivität und der Grundbedürfnisse betroffen.

Aus den Erkenntnissen lasse sich im wirtschaftlichen Kontext vor allem folgende These formulieren (vgl. ebd. S. 35): „Service-Leistungen, die die Durchführung von (Neben-)Tätigkeiten beim automatisierten Fahren ermöglichen, können kostenpflichtig angeboten werden.“ Dabei erscheine es sinnvoll, vor allem Services, die eine effiziente Nutzung der im Auto verbrachten Zeit gewährleisten, in den Mittelpunkt der Betrachtung zu rücken. Services steigern demnach die Attraktivität von automatisierten Fahrzeugen gegenüber dem Endkunden/der Endkundin, was ein enormes Marktpotenzial bzw. Möglichkeit zur Wertschöpfung bereithalte.

Während die Studie jedoch nur die angebotenen Services während der Fahrt thematisiert, so wird die Technologie des autonomen Fahrens weitgehend außer Acht gelassen, bzw. nur als die Basis für die Bereitstellung der Mehrwertdienste interpretiert. Anders als die genannten Studien soll hier jedoch die Funktion des Autos als „Chauffeur“ betont werden und ebenfalls als Service analysiert werden.

Die menschliche Wahrnehmung wurde (vgl. Daimler o. J. a) in den Vorstufen des autonomen Fahrens mithilfe diverser FAS und der Bereitstellung von Informationen zwar unterstützt, benötigte aber die selbstständige Reaktion des Fahrers/der Fahrerin. Diese werde nun mithilfe von Algorithmen nicht mehr benötigt, das Auto könne in naher Zukunft selbst reagieren. „Ein Mehr an Komfort, Sicherheit und Effizienz“ verspricht Daimler (vgl. o. J. b) und ist überzeugt: Das Auto könne mehr sein als nur ein Mittel zum Transport, nämlich ein privater Rückzugsraum mit mehr Freiheit.

Daraus lässt sich das Nutzenversprechen (engl. value proposition) des autonomen Fahrens ableiten und definieren (vgl. ebd.): Die Fahraufgabe abgeben können, um die Zeit effizienter nutzen zu können, begleitet von Faktoren wie Umweltschutz und Sicherheitssteigerung im Straßenverkehr. Auch Kinder, Senioren/Seniorinnen oder Menschen mit Behinderung wären mithilfe des autonomen Fahrens mobil, so das Versprechen der Daimler AG.

Der Nutzen entstehe also nicht nur aus den Services, die während der Fahrt in Anspruch genommen werden können, sondern die Value Proposition bildet sich vor allem auch durch die Tatsache des Fahrservices selbst.

Der Bundesverband für Digitale Wirtschaft e.V. (BVDW) unterteilt in Kooperation mit der Hochschule Reutlingen (vgl. o. J.) die gebotenen Services für „Connected Cars“ in vier Gruppen, wobei der Service des Fahrens als eigene Service-Gruppe unter dem Punkt „Sicherheit“ angeführt wird. Die anderen drei Gruppen bilden das Infotainment, individuelle Services und intelligente Navigation. Dabei umfasse das Infotainment die Multimediafunktionen Entertainment, Internet, Internet Radio und das Mobile Büro. Die individuellen Services stellen dem Nutzer/der Nutzerin durch einen sog. Concierge Service, der dem Fahrzeuginsassen/der Fahrzeuginsassin ohne Aufforderung als persönlicher

Assistent diene dem Zustellservice sowie der Funktion des Fahrzeugmanagements via Applikation, einen erhöhten Komfort zur Verfügung. Der Service der Sicherheit sei durch FAZ, Head-up-Display, Car2x Kommunikation, eCall, Diebstahlsicherung, Nothaltesystem und das autonome Fahren selbst gegeben. Hinzu kommen Services der Navigation wie ortsgebundene Dienste und Verkehrsinformationen.

Immer mehr Unternehmen entscheiden sich die Serviceorientierung als oberstes Gebot in der Unternehmensphilosophie zu verankern (vgl. Kumpf 1999). Der Begriff lasse sich, laut Kumpf, jedoch nicht eindeutig definieren. Meist werde aber der klassische Dienst am Kunden bzw. der Kundin (sog. Kundendienst) eines Industrieunternehmens gemeint. Dabei gelten als wichtigste Kriterien für den Kunden/die Kundin vor allem die Zuverlässigkeit sowie die Kompetenz der Mitarbeiter (vgl. Kumpf 1999, S.1032).

Coenen (2010) fasst in Anlehnung an Coenen (2001, S.347) und Bruhn (2007, S.17) den Terminus wie folgt zusammen: Demnach sei die Serviceorientierung als ständige Ausrichtung an der Zielgröße des Dienens zu definieren, die sich anhand der Ermittlung und Analyse individueller dienstleistungsbezogener Kundenerwartungen und einer internen sowie externen Umsetzung in Serviceangebote und individueller Interaktionen zeige. Dies führe zu einer Festigung der Kundenbeziehung.

Betrachtet man den Begriff der Serviceorientierung in der Automobilindustrie, spricht man hier zunächst, wie bereits erwähnt, hauptsächlich vom klassischen Kundendienst. Dabei steige die Nachfrage nach umfassenden Service- und Supportangeboten zum Fahrzeug und darüber hinaus, immer weiter (vgl. ADL, o.J., S.5). Dazu gehören unter anderem z.B. die Medienintegration und die Konnektivität, so die Arthur D. Little (ADL) Studie „Zukunft der Mobilität 2020“. Was Apple als Hauptakteur in der Mobiltelefonindustrie vormache, so streben auch in der Automobilmarktindustrie die Wettbewerber danach aus dem eigentlichen Produkt des Autos mehrere Umsatzströme zu generieren. Aktuell ist dies, wie bereits erwähnt, über neue Formen der Mobilität wie z.B. Car-Sharing schon möglich. Die Nachfrage nach Sicherheit, Komfort und

Nachhaltigkeit gibt im Hinblick auf neue Geschäftsmodelle darüber hinaus Raum für neue Servicekonzepte.

Die steigenden Mobilitätsanforderungen ließen sich der ADL Studie nach jedoch nicht mithilfe spezialisierter Produkte befriedigen, sondern würden die Kombination vielfältiger Mobilitätsservices erfordern. Das Konzept des selbstfahrenden Autos wurde in der Studie noch nicht ausreichend berücksichtigt. Die Idee des autonomen Fahrzeugs versucht die Befriedigung sämtlicher Kundenbedürfnisse bzgl. Mobilität, Individualität, Komfort etc. in einem hybriden Produkt zu vereinen.

Die Integration von IKT in die Automobilbranche lasse laut der *Internationalen Delphi-Studie 2030 „Zukunft und Zukunftsfähigkeit der Informations- und Kommunikationstechnologien und Medien*“ (vgl. Münchener Kreis e.V. 2009, S.193) neue Kooperationsformen zwischen Herstellern und Zulieferern entstehen, wodurch das Produktspektrum in der Branche einen höheren Grad an Dienstleistungen aufweise. Grund dafür sei die Erweiterung der klassischen Wertschöpfungskette auf den Bereich der Service- und Informationsbereiche. Eine solche Kombination IKT-basierter Dienste mit Sachleistungen kann als hybrides Produkt bezeichnet werden, so die Studie weiter.

> „’Vom Automobilbauer zum Mobilitätsanbieter’, die Umsetzung dieser Formel zeigt sich in zahlreichen Varianten bei allen großen Konzernen. Kennzeichnend für diese Entwicklung ist dabei die Ausweitung der klassischen Wertschöpfungskette auf die Service- und Informationsbereiche bzw. die anhaltende Tendenz zum so genannten ‚hybriden Produkt’, einer Kombination von IKT- basierten Diensten mit Sachleistungen“. (ebd., S.273)

Hybride Wettbewerbsstrategien haben zum Ziel durch einen zusätzlichen Nutzen für den Abnehmer/die Abnehmerin eine hohe Differenzierung zu erreichen (vgl. Kaluza & Blecker 2005, S.4). Dies sei in Bezug auf die Sicherstellung der sechs strategischen Erfolgsfaktoren, zu denen neben Kosten, Qualität, Flexibi-

lität, Zeit und Erzeugnisvielfalt auch der Service gehört, zu verstehen, so Kaluza und Blecker.

Um Kundenwünschen nachzukommen, integrieren Unternehmen bzw. ganze Märkte den Faktor Dienstleistung immer tiefer in ihr Angebot: Innovative Kundenlösungen werden mithilfe hybrider Dienstleistungsbündel, also die Kombination von Industriewaren und Dienstleistungen, geschaffen. Dieser Trend wird in der Fachliteratur als „Servitization of Business“ bezeichnet (vgl. Vandermerwe & Rada 1988, S.315ff).

Wassmus (vgl. 2014, S.2f) definiert in seinen Ausführungen zur „Serviceorientierung als Erfolgsfaktor und Komplexitätstreiber beim Angebot hybrider Produkte“ den Begriff der Serviceorientierung folgendermaßen: „Wenn Problemlösungen von Unternehmen ein hohes Maß an Individualität, einen umfangreichen Problemlösungsprozess mit hoher Kundenintegration sowie eine technische Integration von Sach- und Dienstleistungsbestandteilen aufweisen, spricht man von hybriden Produkten.“ Industrieunternehmen können hierbei einen Wandel von einem Sachgutthersteller zu einem dienstleistenden Produzenten vollziehen.

Dabei sind nach Buriánek (vgl. 2009, S.16) dienstleistende Produzenten, deren Sachleistung noch die Basis ihres Produkts bilden, vom produzierenden Dienstleister, bei dem diese den elementaren Bestandteil ausmacht, zu unterscheiden.

In der Automobilbranche zeigt sich, laut *Frost & Sullivan* (vgl. 2016), ein eindeutiger Wandel von einer produktzentrierten Industrie hin zum serviceorientierten Markt, was als Ausgangspunkt der Untersuchungen zur Service-Ökonomie der Automobilbranche und ihrer Wertschöpfung dienen kann.