# IT-Sicherheit im Wettstreit um die erste autonome Fahrzeugflotte: ein Diffusionsmodell

Zander, Tim; Birnstill, Pascal; Kaiser, Florian; Wiens, Marcus; Beyerer, Jürgen; Schultmann, Frank

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

**Empfohlene Zitierung / Suggested Citation:**
Zander, T., Birnstill, P., Kaiser, F., Wiens, M., Beyerer, J., & Schultmann, F. (2020). IT-Sicherheit im Wettstreit um die erste autonome Fahrzeugflotte: ein Diffusionsmodell. *TATuP - Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis / Journal for Technology Assessment in Theory and Practice*, *29*(1), 16-22. https://doi.org/10.14512/tatup.29.1.16

# IT-Sicherheit im Wettstreit um die erste autonome Fahrzeugflotte

## Ein Diffusionsmodell



**Tim Zander**, *Institut für Anthropomatik und Robotik, Lehrstuhl für Interaktive Echtzeitsysteme Karlsruher Institut für Technologie (KIT), c/o Technologiefabrik, Haid-und-Neu-Str. 7, 76131 Karlsruhe (tim.zander@kit.edu)*
**Pascal Birnstill**, *Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung (IOSB) (pascal.birnstill@iosb.fraunhofer.de)*
**Florian Kaiser**, *Institut für Industriebetriebslehre und Industrielle Produktion (IIP), Karlsruher Institut für Technologie (KIT) (florian-klaus.kaiser@kit.edu)*
**Marcus Wiens**, *Institut für Industriebetriebslehre und Industrielle Produktion (IIP), Karlsruher Institut für Technologie (KIT) (marcus.wiens@kit.edu)*
**Jürgen Beyerer**, *Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung (IOSB) (juergen.beyerer@iosb.fraunhofer.de)*
**Frank Schultmann**, *Institut für Industriebetriebslehre und Industrielle Produktion (IIP), Karlsruher Institut für Technologie (KIT) (frank.schultmann@kit.edu)*

In der Fahrzeugindustrie halten aktuell eine Reihe von Neuerungen Einzug. So sorgen neben dem Umstieg auf E-Mobilität hochtechnologische Assistenzsysteme in Fahrzeugen für einschneidende Veränderungen. Eine weitere mit diesen neuen Systemen einhergehende Neuerung ist, dass Autos nun wie Smartphones mit regelmäßigen Updates versorgt werden. Der Hersteller Tesla behauptet sogar, seine Autos in Zukunft per Softwareupdate zum vollautonomen Fahrzeug upgraden zu können. Diese Entwicklung kann zu einer nicht nachhaltigen und risikoreichen Entwicklung der IT-Security und der Umweltbilanz des Fahrzeugsektors führen.

*IT security and competition in the automotive industry*
*A diffusion model*

*Today's automotive industry is changing rapidly. The slow movement toward electric mobility and highly technical assistant systems challenge old hierarchies. Another innovation associated with the latter is that cars now receive regular software updates, just like smartphones. Tesla even claims to be able to upgrade their cars to fully autonomous driving in the future. This could lead to an unsustainable and risky development of IT security and the environmental performance of the vehicle sector.*

**Keywords:** *IT security; autonomous mobility; diffusion model*


https://doi.org/10.14512/tatup.29.1.16
Submitted: 23. 09. 2019. Peer reviewed. Accepted: 17. 12. 2019

## Motivation

Durch den Einzug von Software mit regelmäßigen Updates in Fahrzeugen wird die IT-Security zunehmend relevant für Autobauer. Oftmals fehlt beim Anwender im Diskurs um die Bedeutung der IT-Security das Bewusstsein über die Möglichkeiten, welche Sicherheitslücken einem Angreifer bieten (Bordonali et al. 2017). Entsprechend vulnerabel sind viele modernen Automobile. Dabei sei, glaubt man Elon Musk, ein flottenweiter Hack eines der größten Risiken für die autonome Mobilität. Der Nachrichtendienst heise.de machte in einem Bericht auf die geringen Sicherheitsstandards in der Automobilindustrie aufmerksam, nachdem es einem Hacker gelungen war „weltweit den Verkehr beeinflussen" zu können (Scherschel 2019). Insbesondere die Motivation, eine Vorreiterposition in der autonomen Mobilität einzunehmen und so eine gute Marktposition zu erlangen, kann vor dem Hintergrund der kapitalintensiven Transformation in Richtung Elektromobilität eine weitere Gefahr für die IT-Sicherheit von Automobilen darstellen. Zusammengenommen kann die Verbindung aus Vernetzung, fehlender Erfahrung mit der neuen Technologie und hohem Wettbewerbsdruck potenziell zu hohen systemischen Risiken bzgl. der IT-Sicherheit führen.

## Deep und Fleet Learning für autonomes Fahren

In modernen Fahrzeugen stehen sämtliche Fahrer- und Bedienbefehle wie Bremsen, Lenkung, Regelung der Antriebsleistung über ein elektronisches Nachrichtenprotokoll zur Verfügung. Damit sind alle Voraussetzungen erfüllt, um ein Fahrzeug

von einem Computerprogramm autonom steuern zu lassen. Die Frage, die sich nun stellt ist, welche Sensoren und welche Informationsfusion der Daten dieser Sensoren und welche daraus abgeleiteten Steuerbefehle für ein fahrerloses Fahrzeug nötig sind (Paden et al. 2016).

Ein modernes Auto besitzt eine Vielzahl von Sensoren. Als Beispiel dafür kann das seit 2011 vorgeschriebene Electronic Stability Control-System dienen, das durch gezieltes Verzögern einzelner Räder ein Ausbrechen des Wagens zu verhindern versucht. Dafür werden u. a. Sensoren für den Lenkwinkel, Drehrate, Radgeschwindkeits- sowie die Längs- und Gierachsenbeschleunigung benötigt. In einem Auto mit Autonomiestufe 2 (Perret et al. 2018; Gasser et al. 2012; Wood et al. 2019) wird zusätzlich eine Vielzahl von Sensoren für die Beobachtung der Strecke und der anderen Verkehrsteilnehmer benötigt (Gasser et al. 2012).

In der Folge gehen wir exemplarisch auf die Autonomisierungsbemühungen des elektrischen Fahrzeugherstellers Tesla ein. Die einzelnen Wettbewerber unterscheiden sich bezüglich ihres Vorgehens zwar in einigen Aspekten, diese unterschiedlichen Herangehensweisen sind jedoch für unsere Diskussion und für das weitere Verständnis der Thematik nicht weiter relevant. So hat Tesla seit 2016 für den „Autopilot" acht Kamera-, zwölf Sonar- und einen Radarsensor verbaut (Tesla 2019 b). Die eingehenden Daten dieser Sensoren müssen fusioniert werden, um den für das Fahrzeug relevanten Zustand der Umwelt zu schätzen. Diese Information über die aktuelle Situation und das entsprechende Ziel müssen dann in entsprechende Steuerbefehle umgesetzt werden.

Für die Verarbeitung von Bilddaten hat sich Deep-Learning als zielführend erwiesen. Bei diesen Verfahren werden künstliche neuronale Netze durch Lernbeispiele angepasst. Hierbei werden große Datenmengen analysiert, um Muster zu erkennen nach denen dann Entscheidungen getroffen werden können und nach denen das Verhalten ausgerichtet werden kann. Damit werden Maschinen befähigt, autonom ihr Verhalten zu optimieren. Mithilfe dieses Verfahrens können in neuen Bildern mit hoher Genauigkeit Objekte wie Tiere und Fußgänger erkannt werden. Passende Datensätze von Bildern zu erstellen und dann zu annotieren ist ein zeit- und kostenintensives Problem. Für den Betrieb eines autonomen Fahrzeugs ergeben sich weitere Herausforderungen bei der Sensorfusion. Unter anderem muss erkannt werden, welcher Teil der Fahrbahn wirklich frei befahrbar ist und ob etwaige bewegliche Hindernisse (wie andere Verkehrsteilnehmer) den geplanten Fahrweg versperren könnten.

Deshalb werden große Mengen an Trainingsbeispielen benötigt. Der Ansatz, auf welchen Tesla für dieses Problem zurückgreift, ist das sogenannte *Fleet Learning*. Hierbei trägt jedes Auto der Fahrzeugflotte zum Sammeln der Trainingsbeispiele bei. Als Beispiele dafür wurden am Tesla *Autonomy Investor Day* Trainingsdaten von der Flotte gesammelt und von Menschen annotiert, um richtig zu detektieren, ob Fahrräder an anderen Fahrzeugen befestigt sind oder als eigenständige Verkehrsteilnehmer am Verkehrsgeschehen teilnehmen (Tesla 2019 a). Ein weiteres Beispiel stellte die vollautomatische Generierung von Lerndaten dar, um Spurwechsel und Fahrverhalten anderer Fahrzeuge besser vorherzusagen.

*Fleet Learning ermöglicht das Sammeln großer Mengen an Trainingsbeispielen für die Software autonomer Fahrzeuge.*



Zusammenfassend kann Tesla durch Abfrage der sensorgenerierten Daten seiner Flotte und die Beobachtung der Tesla-Fahrer automatisiert Trainingsbeispiele sammeln und diese teilweise sogar automatisch annotieren (Eady 2019). Diese werden dann zur Verbesserung der Fahrzeugsoftware genutzt.

Obwohl es trotz dieser genannten Fortschritte zurzeit noch nicht klar ist, wann, bzw. ob überhaupt vollautonome Fahrzeuge existieren werden, sollte man sich darüber klarwerden, dass der Kauf eines vollautonomen Fahrzeugs viele Ähnlichkeiten mit dem Kauf von Softwarepaketen hat. So kostet zum Beispiel bei Tesla das gleiche Auto ohne die Autopilotfunktion 5.000 € weniger. Wie bei anderen Softwarelizenzen kann die kommerzielle Nutzung beschränkt werden. So enthält die Lizenz für den Autopiloten von Tesla eine Exklusivitätsklausel, die besagt, dass mit Autos im vollautonomen Modus nur im Tesla Robotaxi-Netzwerk Geld verdient werden kann (Tesla 2019 a).

## IT-Sicherheit autonomer Fahrzeuge

Die Anbindung an das Internet zum Zwecke der Versorgung mit Updates, Verkehrs- und Mediendaten führt zu der Gefahr des Remotezugriffs durch unautorisierte Personen. So konnten Forscher 2014 demonstrieren, wie über das Mobilfunknetz ein Auto von der Ferne aus angegriffen wurde und unter anderem die Bremsen deaktiviert werden konnten (Miller und Valasek 2014). Es ist zu erwarten, dass elementare Funktionen wie Bremsen, Lenken und Beschleunigen evtl. sogar gewollt noch für längere Zeit über das Internet zur Verfügung stehen werden, da autonome Fahrzeuge vermutlich noch lange nicht auf alle Situationen selbstständig reagieren können (Wood et al. 2019). Ein menschlicher Operator müsste somit per Fernzugriff eingreifen, um z. B. ein

Wendemanöver zu vollführen, zu dem das Fahrzeug selbst nicht in der Lage ist.

Ein weiteres Problem ist ein starkes Wachstum der Softwaregröße und damit der Komplexität. So erhöhte sich die durchschnittliche Softwaregröße in Fahrzeugen von ca. 10 Mio. Codezeilen im Jahr 2010 auf ca. 150 Mio. Codezeilen im Jahr 2016. Als Konsequenz wurden in letzter Zeit vermehrt softwarebedingte Rückrufe von ausgelieferten Fahrzeugen durchgeführt. Die Sicherstellung hoher Softwarequalität nimmt insofern eine Schlüsselrolle ein, da sie maßgeblich die Sicherheit des Fahrzeugbetriebs bestimmt und für den breiten Gebrauch unerlässlich ist (Consumer Watchdog 2019). Eine weitere große Gefahr besteht für die Privatheit aller Verkehrsteilnehmer, da Fahrzeuge Kameras, andere Sensoren und entsprechende Hardware haben, mit denen eine Überwachung sowie Verarbeitung der Daten stattfinden kann. Von ihnen geht also mindestens die gleiche Gefahr für Persönlichkeitsrechte (u. a. Recht auf freie Entfaltung der Persönlichkeit sowie informationelle Selbstbestimmung) der Bürger aus wie von Überwachungskameras im öffentlichen Raum, die durch das Internet erreichbar sind. Darüber hinaus sind Datenschutzproblematiken bezüglich der Datenaggregation sowie der Analyse von Daten der gesamten Fahrzeugflotte zu nennen.



*Ähnlich wie im Softwaremarkt ist auch eine Monopolisierung des Marktes für autonome Mobilität zu erwarten.*

## Auswirkungen auf den wirtschaftlichen Wettbewerb

Der dargestellte technologische Schock in der Automobilbranche durch autonomes Fahren verändert die Wettbewerbssituation erheblich. Hierbei ist die Verlagerung der Differenzierungsmerkmale und Veränderung der Wahrnehmung des Automobils von einer maßgeblich durch ihre Hardware bestimmten Maschine hin zu einer sich durch Software definierenden Maschine von großer Bedeutung (Teece 2018). So verschiebt sich durch autonomes Fahren der Fokus des Kunden vom Fahrerlebnis hin zur fahrzeuginternen Multimediaerfahrung (Aboagye et al. 2017). Dies hat zur Folge, dass sich die Regeln des Wettbewerbs grundlegend verändert und dadurch den Markt für neue Wettbewerber geöffnet haben. Dementsprechend drängen viele neue Wettbewerber auf den Automobilmarkt (Teece 2018). Hierbei ist nicht nur eine vertikale, sondern auch eine horizontale Integration vieler Unternehmen zu beobachten (Burkacky et al. 2018). Dies führt temporär zu einer Steigerung der Wettbewerbsintensität. Ermöglicht wird dies dadurch, dass die etablierten Unternehmen durch die veränderte Bedeutung der Software eines Automobils an Wettbewerbsfähigkeit sowie technologischem Vorsprung verloren haben und somit Markteintrittsbarrieren gesunken sind (Aboagye et al. 2017). Die Auswirkungen des technologischen Schocks verdeutlicht auch die Prognose einer Verringerung des Wertanteils traditioneller Technologien auf dem Automobilmarkt von 98 % im Jahr 2017 auf ca. 50 % im Jahr 2030 (Aboagye et al. 2017).

Die technologischen Rahmenbedingungen der Entwicklung des autonomen Fahrens bestimmen die neue Wettbewerbssituation. Hierbei nimmt die Erlangung eines technologischen Vorsprungs gegenüber den Konkurrenten bei der hohen Komplexität der Software, welche autonomes Fahren ermöglicht, eine entscheidende Rolle ein (Aboagye et al. 2017). Technologischer Vorsprung gegenüber den Wettbewerbern erhöht dabei die Wettbewerbsfähigkeit und damit die potenzielle Marktmacht sowie Marktdurchdringung eines Anbieters. Mit einer gesteigerten Marktdurchdringung verringern sich wiederum die Informationskosten (Charette 2009). Es sei dabei auf das *Fleet Learning* verwiesen, bei dem durch eine größere Marktausbreitung zusammen mit Netzwerkeffekten vereinfacht Trainingsdaten durch sich im Betrieb befindliche Fahrzeuge generiert werden können. Die geringeren Informationskosten gegenüber den Wettbewerbern mit schlechterer Marktposition ermöglichen es den Unternehmen nochmals, ihren technologischen Vorsprung weiter auszubauen (Bertoncello et al. 2016).

Die Entwicklung der Technologie des autonomen Fahrens führt dabei nicht nur zu einem technologischen Vorsprung, sondern verursacht auch hohe Fixkosten. Diese Fixkosten verteilen sich dabei auf alle Fahrzeuge, wodurch sich Skaleneffekte ergeben. Aufgrund der Skaleneffekte (Fixkostendegression) und Netzwerkeffekte (sinkende Informationskosten) steigt der Wert einer Flotte, wie bei Software-Produkten (Anderson 2008), überproportional zu der Zahl seiner Fahrzeuge. Dies wiederum impliziert Lock-In-Effekte, da mit steigender Größe des Netzwerks der Austritt aus dem Netzwerk für jeden Nutzer unattraktiver wird und durch die Exklusivitätsklausel in der Lizenz noch verstärkt wird. Aufgrund der hohen Entwicklungskosten für autonomes Fahren sowie der dargestellten Besonderheiten der Technologie erhöhen sich nun wieder die Markteintrittsbarrieren für neue Marktteilnehmer, welche die Marktposition bestehender Anbieter langfristig sichern. Ähnlich wie im Softwaremarkt (Anderson 2008) ist somit auch eine Monopolisierung des Marktes für autonome Mobilität zu erwarten.

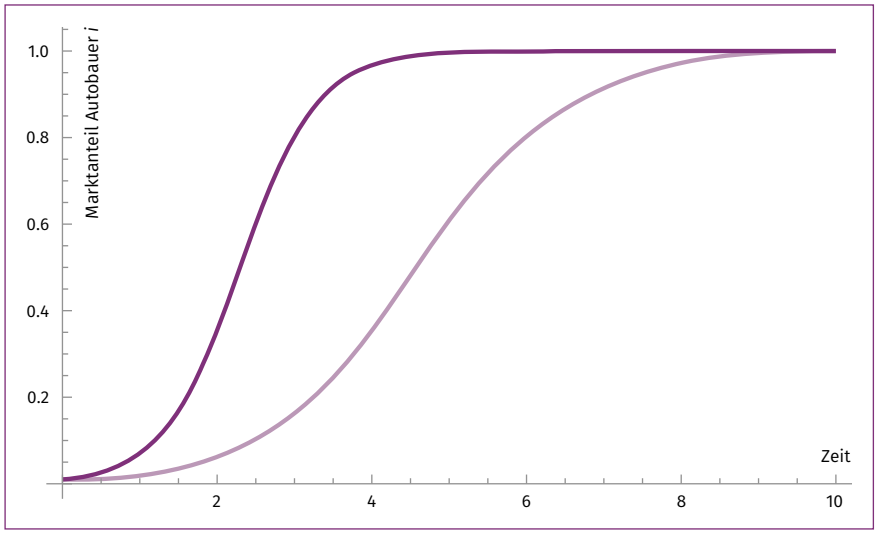



**Abb. 1:** Marktdurchdringung in Abhängigkeit von IT-Sicherheitsinvestitionen. *Quelle: Eigene Darstellung*

## Diffusionsmodell für autonome Fahrzeuge

Um die Marktdurchdringung durch autonome Fahrzeuge und damit den Wettstreit um die erste autonome Fahrzeugflotte zu beschreiben, erscheint die Diffusionstheorie als besonders geeignet, da sie die Adoption neuer Technologien auf einem Markt und damit den Prozess der Marktdurchdringung beschreibt (Geroski 2000). Gemäß Rogers (2010) können die Nutzer neuer Technologien nach dem Grad ihrer Bereitschaft, diese zu nutzen, klassifiziert werden. Hierbei hängen Adoptionsentscheidungen von Informationen über den Nutzen dieser Technologie ab. Die Informationen können dabei aus direktem Erleben aber auch indirekt durch Erzählen erlangt werden. Unter der Annahme einer konstanten Penetrationsrate α kann der Marktanteil $f(t)$ bestimmt werden, der sich als sogenannte Sigmoidfunktion darstellen lässt.

$$f(t) = \frac{1}{1+\frac{1-f(t_0)}{f(t_0)} \cdot e^{-\alpha \cdot (t-t_0)}}$$

Dabei wird für den initialen Marktanteil $f(t_0)$ die Bedingung $f(t_0) > 0$ angenommen, das heißt, das Modell liefert eine Erklärung für die Diffusion autonomer Fahrzeuge nach bereits erfolgtem Markteintritt der Unternehmen. Die Penetrationsrate α beschreibt dabei die Geschwindigkeit der Marktdurchdringung beziehungsweise Diffusion autonomer Fahrzeuge. Sie stellt damit die wichtigste Komponente der Analyse des Wettstreits um die erste autonome Fahrzeugflotte dar.

Davies (1979) bestimmt hierbei als zentrale Determinante den pekuniären Nutzen der Technologie, d. h. die Höhe der Penetrationsrate wird maßgeblich durch den finanziellen Mehrwert durch die Adoption der neuen Technologie bestimmt. Hierbei gilt: je höher der Gewinn für den Nutzer, desto höher seine Priorität der Adoption der neuen Technologie und umso höher die Penetrationsrate. Somit stellt die Erhöhung des Gewinns für den Nutzer beziehungsweise die Vorteilhaftigkeit der neuen Technologie die Priorität für das Handeln der Unternehmen dar, wenn die Erlangung eines möglichst großen Marktanteils in möglichst kurzer Zeit das Ziel ist. Diese Ausrichtung unternehmerischen Handelns scheint in der dargestellten Wettbewerbssituation um die erste autonome Fahrzeugflotte plausibel zu sein.

Das Unternehmen muss also versuchen, autonome Fahrzeuge so günstig wie möglich auf den Markt zu bringen, um in der Phase des intensiven Wettbewerbs möglichst schnell eine ausreichend große Fahrzeugflotte (kritische Schwelle, ab der die Netzwerkeffekte und Skaleneffekte einsetzen) zu erreichen. Unter der Bedingung, dass das Unternehmen kurzfristig keinen Verlust macht, kann die kurzfristige Preisuntergrenze als Veräußerungspreis angenommen werden. Ein tieferer Preis würde das Unternehmen in finanzielle Schieflage bringen, während ein höherer Preis mit dem Unternehmensziel der schnellen Marktdurchdringung nicht konform wäre.

Die Penetrationsrate von Unternehmen $i$ kann bei der Beschränkung der Bestimmung des Nutzens auf den monetären Mehrwert mit der Differenz aus Zahlungsbereitschaft und variablen Kosten gleichgesetzt werden.

$$\alpha_i = Z - k_{v,i}$$

Während im Allgemeinen Ansatz zur Bestimmung der Penetrationsrate ein Nutzenvergleich mit Konkurrenzprodukten erforderlich ist, genügt für den Monopolfall die hier vorgestellte einfache Version, die keine Interaktion mit Konkurrenten erfasst. Unter der Annahme einer konstanten Zahlungsbereitschaft der potenziellen Nutzer stellt sich die Marktdurchdringung in Abhängigkeit von $k_v$ wie in Abb. 1 dar.

Im Hinblick auf die IT-Sicherheit kann es nun erstrebenswert erscheinen Kosten einzusparen, um mit einem geringeren Preis an den Markt zu gehen, insbesondere wenn man die IT-Sicherheit weder als Leistungsmerkmal noch als Begeisterungsmerkmal sieht (Kano et al. 1984). Dies kann am Beispiel der Verbindung von Infotainmentsystemen mit Controller Area Netzwerken erläutert werden, welche sicherheitsrelevante Fahrzeugsysteme steuern (Consumer Watchdog 2019). So stellt das Infotainmentsystem eine Leistungsanforderung und damit ein zentrales Differenzierungsmerkmal dar, während die IT-Sicherheit ein Basismerkmal darstellt. Um eine herausragende Leistung im Bereich des Infotainments zu erreichen, wird hierbei das Controller Area Network zulasten der Sicherheit mit dem Infotainmentsystem verbunden (Consumer Watchdog 2019). Dies hat den Vorteil, dass intelligente Lautstärkeregelungen in Abhängigkeit von

der Geschwindigkeit sowie der Motorgeräusche ermöglicht werden (Consumer Watchdog 2019). Darüber hinaus schränken Sicherheitsmaßnahmen die Funktionalität ein, welches den wahrgenommenen Nutzen bei den Kundinnen und Kunden und damit deren Zahlungsbereitschaft negativ beeinflusst. Es kann für die Firma also sinnvoll sein, in einem kurzfristigen Betrachtungshorizont auf Investitionen in Maßnahmen zur IT-Sicherheit zu verzichten, um eine gute Marktposition zu erreichen (Anderson 2008). Da Kundinnen und Kunden ein sicheres Automobil zunächst nicht von einem nicht sicheren unterscheiden können, kann es aufgrund dieser asymmetrischen Information sogar langfristig zum Marktversagen kommen (Akerlof 1970), wenn zeitversetzt die Sicherheitsdefizite bekannt werden und die Kunden dadurch schließlich verunsichert bzw. abgeschreckt werden. Hierbei unterstreicht das Beispiel der Firma Microsoft, bzw. deren Vorgehen zur Erlangung eines hohen Marktanteils, die angemerkte Ähnlichkeit der Softwarebranche zur Branche der autonomen Mobilität. So hatte Microsoft in den 1990er-Jahren das Motto „Ship it on Tuesday and get it right by version 3“ mit der bekanntermaßen schlechten IT-Sicherheit des Produkts in dieser Zeit. Um eine Monopolstellung zu erreichen war es also nicht nötig, ein von Anfang an sicheres Produkt zu entwerfen (Anderson 2008). Einsparungen bei den Ausgaben für IT-Sicherheit würden also zu einer schnelleren Durchdringung und Beherrschung des Marktes, jedoch langfristig zu steigenden Risiken führen.



*Die Wartung von Software in autonomen Fahrzeugen muss langfristig sichergestellt werden.*

## Auswirkungen auf die IT-Sicherheit

Falls es möglich sein wird, ein vollautonomes Auto zu entwickeln, zur Marktreife zu führen und zeitnah eine entsprechende Marktposition zu erlangen (schnelles Szenario), wird die Bedeutung der IT-Sicherheit durch die große Verbreitung derselben Software an Bedeutung gewinnen. So steigert sich auch die Attraktivität eines Hacks durch die Möglichkeit, mehrere Fahrzeuge zu beeinflussen. Entsprechend wachsen die Anforderungen an die IT-Sicherheit der Fahrzeuge.

Falls sich autonomes Fahren in nächster Zeit nicht verwirklichen lassen sollte, bzw. eine schnelle Marktdurchdringung nicht erreicht werden kann (langsames Szenario) und sich die Investitionen in Techniken des autonomen Fahrens wie *Fleet Learning* als langfristig nicht rentabel erweisen, würden gegensätzliche Effekte eintreten (Porter 2019). So kann das investierte Kapital nicht mehr zurückgewonnen werden, was zur Abwicklung ganzer Unternehmen führen könnte oder diesen zumindest einen rigiden Sparkurs diktieren würde. In diesem Fall könnte es zum Problem werden, dass es dann keinen Verantwortlichen mehr gibt, der die Software warten kann oder will. Diese Gefahr wird durch die steigende Wettbewerbsintensivität in der Automobilbranche sowie durch das Eintreten vieler kleiner Unternehmen immer präsenter. Es wäre also dann unter Umständen unmöglich, etwaige Schwachstellen zu reparieren, da evtl. niemand mehr Zugriff auf den Quelltext der Software hat.

Mindestens würden jedoch Lebenszyklusprobleme auftreten, sollte sich herausstellen, dass die aktuelle Fahrzeuggeneration auch nicht mit Umrüstung für autonomes Fahren geeignet ist. So würde die Softwarewartung bei dieser veraltenden Flotte eine Externalität darstellen, da ökonomische Investitionen ohne zukünftigen Nutzen erforderlich wären. Dies kann damit erklärt werden, dass die Kosten für unterlassene Wartung nicht beim Automobilhersteller anfallen, sondern direkt beim Kunden. Dadurch finden diese Kosten in Marktpreisen keine Berücksichtigung. So wäre es denkbar, dass die Unternehmen den Softwaresupport für Altfahrzeuge einstellen oder den Betrieb derartiger Fahrzeuge künstlich verteuern (Wiens und Chamberlain 2018). Besonders plausibel werden diese Lebenszyklusprobleme, wenn man bedenkt, dass das Durchschnittsalter eines Autos in der Europäischen Union elf Jahre beträgt. So stellt sich die Frage, mit welchen Softwareentwicklungskonzepten man in 20 Jahren Updates für ein heutiges Fahrzeug zur Verfügung stellen kann (Anderson 2018).

## Vorschläge zur Vermeidung

Um Bedrohungen durch softwaremäßig nicht mehr gewartete Altfahrzeuge zu vermeiden, wäre es denkbar, diese durch die einschneidende technische Maßnahme des *„Kill Switch“* hart vom Internet zu trennen (Consumer Watchdog 2019). Auch scheint die geforderte Trennung von Infotainment- und Kontrollsystemen in den Fahrzeugen im Hinblick auf die IT-Sicherheit begrüßenswert.

Als Mechanismus für die Erhöhung der IT-Sicherheit könnten Strafen für deren Vernachlässigung dienen. Natürlich stellen sich hier Fragen nach funktionierenden Strafverfahren und Durchsetzbarkeit, die noch überhaupt nicht geklärt sind. Der Vorschlag, sich an den Best Practices der Flugzeugindustrie zu orientieren und sich von allzu komplexer Software zu verabschieden, scheint im Sinne der Wartbarkeit und IT-Sicherheit wünschenswert (Consumer Watchdog 2019). Jedoch steht dies im Gegensatz zum Interesse der Autobauer, die neuesten Assistenzsysteme zu verbauen.

Da Softwarewartung wie gezeigt eine Externalität darstellt, könnten Anbieter zumindest im Falle wirtschaftlicher Schwie-

rigkeiten die Wartung einstellen, den Weiterbetrieb der Fahrzeuge verhindern, die Fähigkeit zur Wartung meistbietend verkaufen oder etwaige Gläubiger des Unternehmens könnten versuchen, durch die künstliche Verteuerung von Updates ihr Kapital zurückzuholen. Dies würde dazu führen, dass sich die Kosten für den Weiterbetrieb eines Fahrzeuges sehr erhöhen oder dieser schlicht unmöglich wird, sodass sich in der Folge die Lebensdauer eines Fahrzeugs verkürzt. Wenn man nun bedenkt, dass ungefähr die Hälfte des gesamten emittierten $CO_2$ eines Verbrennerfahrzeuges durch die Herstellung erzeugt wird – bei Elektrofahrzeugen ist der absolute Wert und der Anteil noch höher – so ist das vorzeitige Betriebsende eines Automobils aus IT-Sicherheitsproblemen bereits aus ökologischen Gründen untragbar (unter der Vorrausetzung, dass das Fahrzeug dann durch ein neues ersetzt wird). Eine Regulierung, die den Weiterbetrieb der Fahrzeuge über mindestens 20 Jahre sicherstellt, scheint insbesondere aufgrund der gesteigerten Lebenserwartung von Elektroautos wünschenswert. Dass das Interesse an IT-Sicherheit und am günstigen Weiterbetrieb von Altfahrzeugen geringer sein wird als bspw. von Flugzeugen, wird maßgeblich daran liegen, dass es sich bei den Betroffenen um eine deutlich weniger einflussreiche und zahlungskräftige Käufergruppe handelt (Anderson 2008). Da Fahrzeughersteller Gebrauchtwagenmärkte als Wachstumshindernis sehen (Bavier et al. 2019), liegt die Vermutung nahe, dass die mit Kontrolle über die in Fahrzeugen installierte Software einhergehende Macht irgendwann dazu genutzt wird, besonders in wirtschaftlich schwierigen Zeiten den Weiterbetrieb der Fahrzeuge zu erschweren, um damit künstlich Nachfrage zu erzeugen. Zumindest aber sollte nicht darauf gehofft werden, dass die Industrie selbst für eine nachhaltige Softwareentwicklung sorgt und so ein langfristiger Weiterbetrieb der Fahrzeuge mit sicherer Software möglich wird. Ein langfristiger Weiterbetrieb der Fahrzeuge würde einen Teil zur zukünftigen $CO_2$-Vermeidung beitragen. Aufgrund der bevorstehenden Klimakatastrophe sollten sich Wirtschaft, Wissenschaft und Politik zusammenzuschließen (Anderson 2001), um den IT-Sicherheit und sicheren Weiterbetrieb von Fahrzeugen über die geplante Obsoleszenz hinaus zu gewährleisten.

## Literatur


Aboagye, Aaron; Baig, Aamer; Hensley, Russel; Kelly, Richard; Padhi, Asutosh; Shafi, Danish (2017): Facing digital disruption in mobility as a traditional auto player. Online verfügbar unter https://www.mckinsey.com/~/media/McKinsey/Industries/Automotive%20and%20Assembly/Our%20Insights/Facing%20digital%20disruption%20in%20mobility%20as%20a%20traditional%20auto%20player/Facing-digital-disruption-in-mobility-as-a-traditional-auto-player.ashx, zuletzt geprüft am 17. 12. 2019.

Akerlof, Georg (1970): The market for „lemons". Quality uncertainty and the market mechanism. In: The Quarterly Journal of Economics, 84 (3), S. 488–500.

Anderson, Ross (2001): Why information security is hard. An economic perspective. Seventeenth Annual Computer Security Applications Conference, 10–14 December 2001. New Orleans: IEEE Computer Society. DOI: 10.1109/ACSAC.2001.991552.

Anderson, Ross (2008): Security engineering. A guide to building dependable distributed systems. New York: John Wiley & Sons.

Anderson, Ross (2018): Making security sustainable. In: Communications of the ACM, 61 (3), S. 24–26.

Bavier, Joe; Rumney, Emma; Miriri, Duncan (2019): Auto giants battle used car dealers for Africa's huge market. Online verfügbar unter https://www.reuters.com/article/us-africa-autos/auto-giants-battle-used-car-dealers-for-africas-huge-market-idUSKCN1RO0OJ, zuletzt geprüft am 19. 11. 2019.

Bertoncello, Michele et al. (2016): Monetizing car data new service business opportunities to create new customer benefit. Online verfügbar unter https://www.mckinsey.com/~/media/McKinsey/Industries/Automotive%20and%20Assembly/Our%20Insights/Monetizing%20car%20data/Monetizing-car-data.ashx, zuletzt geprüft am 19. 11. 2019.

Bordonali, Corrada; Ferraresi, Simone; Richter Wolf (2017): Shifting gears in cyber security for connected cars. Online verfügbar unter https://www.mckinsey.com/~/media/McKinsey/Industries/Automotive%20and%20Assembly/Our%20Insights/Shifting%20gears%20in%20cybersecurity%20for%20connected%20cars/Shifting-gears-in-cybersecurity-for-connected-cars.ashx, zuletzt geprüft am 19. 11. 2019.

Burkacky, Ondrej; Deichmann, Johannes; Doll, Georg; Knochenhauer, Christian (2018): Rethinking car software and electronics architecture. Online verfügbar unter https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/rethinking-car-software-and-electronics-architecture, zuletzt geprüft am 19. 11. 2019.

Charette, Robert (2009): This car runs on code. Online verfügbar unter https://spectrum.ieee.org/transportation/systems/this-car-runs-on-code, zuletzt geprüft am 19. 11. 2019.

Consumer Watchdog (2019): Kill switch. Why connected cars can be killing machines and how to turn them off. Online verfügbar unter https://www.consumerwatchdog.org/sites/default/files/2019-07/KILL%20SWITCH%20%207-29-19_0.pdf, zuletzt geprüft am 19. 11. 2019.

Davies, Stephen (1979): The diffusion of process innovations. Cambridge, U. K.: Cambridge University Press.

Eady, Trent (2019): Tesla's deep learning at scale. Using billions of miles to train neural networks. What Tesla can do that Waymo can't. Online verfügbar unter https://towardsdatascience.com/teslas-deep-learning-at-scale-7eed85b235d3, zuletzt geprüft am 19. 11. 2019.

Gasser, Tom et al. (2012): Rechtsfolgen zunehmender Fahrzeugautomatisierung. Gemeinsamer Schlussbericht der Projektgruppe. In: Berichte der Bundesanstalt für Straßenwesen. Fahrzeugtechnik Heft F83. Bremerhaven: Wirtschaftsverlag NW. Online verfügbar unter https://bast.opus.hbz-nrw.de/frontdoor/index/index/docId/541, zuletzt geprüft am 14. 01. 2020.

Geroski, Paul (2000): Models of technology diffusion. In: Research Policy 29 (4–5), S. 603–625.

Kano, Noriaki; Seraku, Nobuhiko; Takahashi, Fumio; Tsuji, Shin-Ichi (1984): Attractive quality and must-be quality. In: Journal of the Japanese Society for Quality Control 14 (2), S. 147–156.

Miller, Charlie; Valasek, Chris (2014): Adventures in automotive networks and control units. Online verfügbar unter https://ioactive.com/pdfs/IOActive_Adventures_in_Automotive_Networks_and_Control_Units.pdf, zuletzt geprüft am 19. 11. 2019.

Paden, Brian; Cap, Michal; Yong, Sze Zheng; Yershov, Dmitry; Frazzoli, Emilio (2016): A survey of motion planning and control techniques for self-driving urban vehicles. In: IEEE Transactions on Intelligent Vehicles1 (1), S. 33–55.

Perret, Fabienne; Fischer, Remo; Frantz, Holger (2018): Automated driving as a challenge to cities and regions. In: TATuP – Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis 27 (2), S. 31–37. DOI: 10.14512/tatup.27.2.31.

Porter, Jon (2019): Elon Musk says free self-driving chip upgrade could come to older Teslas this year. Online verfügbar unter https://www.theverge.com/2019/7/8/20685873/tesla-fsd-chip-upgrade-2019-install-hw2-full-self-driving, zuletzt geprüft am 19. 11. 2019.

Rogers, Everett (2010): Diffusion of innovations. New York: The Free Press.

Scherschel, Fabian (2019): Hacker knackt Auto-GPS-Tracker. „Ich kann weltweit den Verkehr beeinflussen". Online verfügbar unter https://heise.de/-4408466, zuletzt geprüft am 19. 11. 2019.

Teece, David (2018): Tesla and the reshaping of the auto industry. In: Management and Organization Review 14 (3), S. 501–512.

Tesla (2019 a): Tesla Autonomy Investor Day. Online verfügbar unter https://ir.tesla.com/events/event-details/tesla-autonomy-investor-day, zuletzt geprüft am 19. 11. 2019.

Tesla (2019 b): Support Autopilot. Online verfügbar unter https://www.tesla.com/support/autopilot, zuletzt geprüft am 19. 11. 2019.

Wiens, Kyle; Chamberlain, Elizabeth (2018): John Deere just swindled farmers out of their right to repair. Online verfügbar unter https://www.wired.com/story/john-deere-farmers-right-to-repair, zuletzt geprüft am 19. 11. 2019.

Wood, Matthew et al. (2019): Safety first for automated driving. Online verfügbar unter https://www.daimler.com/documents/innovation/other/safety-first-for-automated-driving.pdf, zuletzt geprüft am 19. 11. 2019.



### DR. TIM ZANDER

ist wissenschaftlicher Mitarbeiter des Lehrstuhls für Interaktive Echtzeitsysteme (IES) sowie des Kompetenzzentrums für angewandte Sicherheitstechnologie (KASTEL) und forscht im Bereich der Modellierung und Quantifizierung von IT-Security und Privacy.

### DR.-ING. PASCAL BIRNSTILL

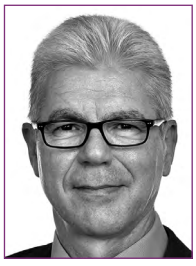
ist wissenschaftlicher Mitarbeiter am Fraunhofer IOSB und KASTEL. Seine Forschungsschwerpunkte liegen im technischen Datenschutz, der Datensouveränität und dem Trusted-Computing.

### FLORIAN KAISER

ist wissenschaftlicher Mitarbeiter in der Forschungsgruppe Risikomanagement am Institut für Industriebetriebslehre und Industrielle Produktion (IIP) sowie KASTEL. Er forscht im Bereich des Cyberrisikomanagements und der Analyse sowie Modellierung von Wirtschaftssystemen.

### DR. RER. POL. MARCUS WIENS

ist Leiter der Forschungsgruppe Risikomanagement am IIP sowie Mitarbeiter in KASTEL. Seine Forschungsschwerpunkte liegen im Bereich des ökonomischen Risikomanagements, der Analyse von System- und Verhaltensrisiken sowie der Akzeptanz- und Vertrauensforschung.



### PROF. DR.-ING. JÜRGEN BEYERER

ist der Leiter des Fraunhofer IOSB sowie des IES Lehrstuhls sowie Mitarbeiter in KASTEL. Seine Forschungsschwerpunkte umfassen u. a. die Automatischen Sichtprüfung und Bildverarbeitung, die Mustererkennung und die semantische Umweltmodellierung.

### PROF. DR. RER. POL. FRANK SCHULTMANN

ist Leiter des IIP, des Deutsch-Französischen Instituts für Umweltforschung sowie Inhaber des Lehrstuhls für Betriebswirtschaftslehre, insbesondere Produktionswirtschaft und Logistik und Mitarbeiter in KASTEL. Seine Forschungsschwerpunkte umfassen u. a. stoffstrombasiertes Produktionsmanagement, Konzeption und Optimierung industrieller Kreislauwirtschaftssysteme sowie die techno-ökonomische Bewertung nachhaltig orientierter Investitionen und Innovationen.