Elektronische Manipulation von Fahrzeug- und Infrastruktursystemen

Berichte der Bundesanstalt für Straßenwesen

Fahrzeugtechnik Heft F 78

Elektronische Manipulation von Fahrzeug- und Infrastruktursystemen

Gefährdungspotentiale für die Straßenverkehrssicherheit

von

Jana Dittmann
Tobias Hoppe
Stefan Kiltz
Sven Tuchscheerer

Otto-von-Guericke Universität Magdeburg
Fakultät für Informatik
Institut für technische und betriebliche Informationssysteme (ITI)

Berichte der Bundesanstalt für Straßenwesen

Fahrzeugtechnik Heft F 78

bast

Die Bundesanstalt für Straßenwesen veröffentlicht ihre Arbeits- und Forschungsergebnisse in der Schriftenreihe **Berichte der Bundesanstalt für Straßenwesen.** Die Reihe besteht aus folgenden Unterreihen:

A - Allgemeines
B - Brücken- und Ingenieurbau
F - Fahrzeugtechnik
M - Mensch und Sicherheit
S - Straßenbau
V - Verkehrstechnik

Es wird darauf hingewiesen, dass die unter dem Namen der Verfasser veröffentlichten Berichte nicht in jedem Fall die Ansicht des Herausgebers wiedergeben.

Die Hefte der Schriftenreihe **Berichte der Bundesanstalt für Straßenwesen** können direkt beim Wirtschaftsverlag NW, Verlag für neue Wissenschaft GmbH, Bgm.-Smidt-Str. 74-76, D-27568 Bremerhaven, Telefon: (04 71) 9 45 44 - 0, bezogen werden.

Über die Forschungsergebnisse und ihre Veröffentlichungen wird in Kurzform im Informationsdienst **Forschung kompakt** berichtet. Dieser Dienst wird kostenlos abgegeben; Interessenten wenden sich bitte an die Bundesanstalt für Straßenwesen, Stabsstelle Presse und Öffentlichkeitsarbeit.

Impressum

Bericht zum Forschungsprojekt FE 88.007/2009:
Analyse des Gefährdungspotentials für die Straßenverkehrssicherheit durch die elektronische Manipulation von Fahrzeug- und Infrastruktursystemen

Projektbetreuung
Marcel Vierkötter
Lutz Rittershaus

Herausgeber
Bundesanstalt für Straßenwesen
Brüderstraße 53, D-51427 Bergisch Gladbach
Telefon: (0 22 04) 43 - 0
Telefax: (0 22 04) 43 - 674

Redaktion
Stabsstelle Presse und Öffentlichkeitsarbeit

Druck und Verlag
Wirtschaftsverlag NW
Verlag für neue Wissenschaft GmbH
Postfach 10 11 10, D-27511 Bremerhaven
Telefon: (04 71) 9 45 44 - 0
Telefax: (04 71) 9 45 44 77
Email: vertrieb@nw-verlag.de
Internet: www.nw-verlag.de

ISSN 0943-9307
ISBN 978-3-86918-115-8

Bergisch Gladbach, April 2011

Kurzfassung – Abstract

Elektronische Manipulation von Fahrzeug- und Infrastruktursystemen

Elektronik und IT werden auch im Automobilbereich zunehmend Gegenstand unautorisierter Veränderungen. Diese Studie stellt einen ersten, breiteren Überblick über die praktische Relevanz elektronischer Veränderungen an Fahrzeug- und Infrastruktursystemen dar. Sie liefert einen Überblick über wesentliche bekannte und existente Beispiele von Möglichkeiten derartiger Veränderungen, das Risiko ihres Auftretens und damit verbundene Gefahren. Die Ergebnisse basieren auf einer Recherche, die neben wissenschaftlichen Quellen insbesondere das Internet als neues, interaktives Medium einbezieht. Es werden Abschätzungen zur praktischen Relevanz dieser Veränderungen vorgenommen und potenzielle Folgen insbesondere für die Verkehrssicherheit reflektiert.

Praktische Hinweise auf elektronische Veränderungen sind an 24 Fahrzeug- und Infrastruktursystemen dokumentiert, die als Ziel teils mehrerer Arten von elektronischen Veränderungen identifiziert wurden. Dies erstreckt sich über verschiedene Domänen wie u. a. den Antriebstrang, das Fahrwerk, Infotainment, Fahrerassistenz und mehrere Infrastrukturkomponenten. Diese Systematisierung enthält zudem eine Klassifikation der agierenden Personen, wobei deren individuelle Motivationen, technische Kenntnisse und Ausstattung unterschieden werden. Das Spektrum potenziell resultierender Gefahren wird einerseits theoretisch anhand der erstellten Systematisierungen aufgezeigt und andererseits an 19 Rechercheergebnissen aus verschiedenen Bereichen illustriert. Die so vorgenommene Analyse des Gefährdungspotenzials wird ergänzt durch einen Ausblick auf potenzielle zukünftige Gefährdungen, die sich insbesondere in kommenden Car-to-Car Kommunikationsnetzen ergeben könnten und die weitere Erforschung von Schutzkonzepten motivieren. Während die recherchierten Veränderungen heute noch meist vom Nutzer ausgehen und das Gefährdungspotenzial häufig unbeabsichtigt entsteht, könnte zukünftig das vorsätzliche Herbeiführen von Gefährdungen an Bedeutung gewinnen.

Electronic manipulation of vehicle and infrastructural systems

Even in the automotive domain, electronics and IT are increasingly subject to (unauthorised) changes. As a first, broader impression of the relevance of these activities in today's practice, this work presents a collection of modifications to vehicles and infrastructure systems, the associated probability of occurrence and related hazard scenarios. The results are based on a research that has been performed on related scientific literature and especially on the internet as a modern source of information. The aim is to estimate the practical relevance of such unauthorised changes and to reflect potential implications for road safety.

The work presents practical indications for electronic modifications on 24 component classes of vehicle and infrastructure systems, that have been identified as a target of (partly multiple) electronic modifications. This covers domains like the powertrain, infotainment, driver assistance systems and several infrastructural components. This systematisation is extended by a classification of the acting persons, also taking their individual motivation into account as well as their amount of technical knowledge and equipment required. The spectrum of dangers potentially resulting from these actions is illustrated. After a theoretical analysis of potential dangers based on the systematisation developed beforehand, 19 practical examples of arising dangers (taken from the research results) are discussed. This analysis is extended by an outlook on potential future dangers which could arise especially in emerging Car-to-Car communication scenarios. One main goal is to motivate further research on the protection of automotive IT systems and infrastructure. The exemplary modifications observed mainly originate from the vehicle users themselves and hazard potentials frequently arise as unintended side-effects. However, the study also reveals first indications for an upcoming international endangerment of traffic resulting from such manipulations.

Inhalt

Glossar

Bluetooth
Ist ein Industriestandard (IEEE 802.15.1) für die Funkübertragung zwischen Geräten über kurze Distanz.

C2C (Car-to-Car Kommunikation)
Oberbegriff für zukünftige drahtlose Kommunikation zwischen Fahrzeugen untereinander. Insbesondere im Amerikanischen oft auch V2V (Vehicle-to-Vehicle).

C2I (Car-to-Infrastructure Kommunikation)
Oberbegriff für zukünftige drahtlose Kommunikation zwischen Fahrzeugen und Infrastrukturkomponenten. Insbesondere im amerikanischen oft auch V2I (Vehicle-to-Infrastucture).

C2X (Car-to-X Kommunikation)
Oberbegriff für zukünftige drahtlose Kommunikation. Deckt sowohl C2C als auch C2I ab. Insbesondere im amerikanischen oft auch V2X (Vehicle-to-X).

Car-Jacking (auch: Hijacking)
Bezeichnet die Entwendung eines Fahrzeuges unter Androhung von Gewalt. Dabei werden die Insassen eines Fahrzeuges, z. B. in der Wartezeit vor einer roten Ampel, von den Tätern unter Androhung von Gewalt gezwungen, ihr Fahrzeug zu verlassen und es den Tätern zu überlassen. Oft werden hierbei Waffen eingesetzt. In Deutschland erfüllt dieser Delikt die Voraussetzungen des § 316a StGB (unter Ausnutzung der besonderen Bedingungen des Straßenverkehrs), sonst § 249 StGB, § 252 StGB und § 255 StGB.

CERT (Computer Emergency Response Team)
Vereinigungen/Abteilungen etc. zur Aufklärung und Behandlung von IT-Sicherheitsvorfällen, vornehmlich in der Desktop-IT. Aus diesem Umfeld stammt auch die sog. CERT-Taxonomie zur Analyse und Beschreibung von Security-Vorfällen.

DoS (Denial of Service)
Bezeichnet eine Klasse von Angriffen, die die Erreichbarkeit eines Systems (bzw. eines von diesem angebotenen Dienstes) unterbinden. Dies erfolgt häufig durch die gezielte Überlastung mit einer Vielzahl von Anfragen.

ECU (Electronic Control Unit)
Zu Deutsch: Steuergerät. Elektronische Komponenten, die in modernen Automobilen eine Vielzahl von Funktionen (elektronisch) realisieren.

EDGE (Enhanced Data Rates for GSM Evolution)
Bezeichnet eine Technik zur Erhöhung der Datenübertragungsrate in GSM-Mobilfunknetzen. Realisiert wird dies durch ein zusätzliches Modulationsverfahren.

Gateway
Zentrale Steuergerät (→ ECU), das in einem Automobil digitale Informationen zwischen verschiedenen Busnetzwerken teils unterschiedlicher Technologien vermittelt.

GPS (Global Positioning System)
Ist ein globales Navigationssatellitensystem zur Positionsbestimmung und Zeitmessung.

GSM (Global System for Mobile Communications)
Ist ein Standard für volldigitale Mobilfunknetze. Es dient der Telefonie, für leitungsvermittelte und paketvermittelte Datenübertragung sowie Kurzmitteilungen (Short Messages).

Jamming (Jammer)
Bezeichnet das gezielte Stören von Kommunikation insbesondere über Funkmedien. Der Begriff „Jammer" bezeichnet dabei den eingesetzten Störsender.

Keyless Entry and Go
Bezeichnet ein System, um ein Fahrzeug ohne aktive Benutzung eines Autoschlüssels (also „schlüssellos") zu entsperren und mittels Betätigung eines Knopfes zu starten. Ermöglicht wird dies durch den Keyless & Go-Schlüssel mit Chip, den der Fahrzeughalter mit sich führt.

Mapping/Remapping
Mapping bezeichnet einen Vorgang, bei dem eine Software auf ein Steuergerät geschrieben wird. Remapping ist entsprechend das „Überschreiben" oder Neu Beschreiben von Steuergeräten.

POI (Points of Interest)
Dt. „Ort von Interesse", bezeichnet im Zusammenhang mit Navigationssystemen geografische Punkte, die für den Nutzer von Interesse sein könnten. Beispiele wären: Tankstellen, Restaurants, Einkaufsmöglichkeiten oder Hotels in der Nähe des aktuellen Standortes.

RDS (Radio Data System)
Bezeichnet eine Technologie zur Übermittlung von Zusatzinformationen beim Hörfunk. In Autoradios kommen dabei Funktionen wie Programmkennung (Anzeigen des Sendernamens), Verkehrsfunk (Lautstärkenanpassung) und Alternativfrequenzen (automatischer Frequenzwechsel) zum Einsatz. Daneben gibt es die Möglichkeit, weitere Informationen zu übertragen, wie TMC.

Spoofing
Senden von Informationen (z. B. Nachrichten in draht- oder funkbasierten Netzwerken) unter Nutzung/Vortäuschen einer falschen (Absender-)Identität. Dieser Vorgang wird im Deutschen umgangssprachlich teils auch als „Spoofen" bezeichnet.

TMC (Traffic Message Channel)
Digitale Informationen werden nicht hörbar auf einer UKW-Frequenz des Hörfunks gesendet (siehe RDS). Vornehmlich sind dies Verkehrsinformationen wie Stauwarnungen oder Unfallwarnungen.

Tracking
(dt. Spurenbildung) bezeichnet das Verfolgen von bewegten Objekten während deren Bewegung. Im Gegensatz dazu bezeichnet Tracing die Verfolgung zeitlich nach der Bewegung des Objektes (z. B. auf Basis von aufgezeichneten Daten).

Tuning (Tuner)
Bezeichnet individuell vorgenommene Modifikationen und Nachrüstungen mit dem Ziel der Erhöhung eines subjektiven Zugewinns für den Fahrzeugnutzer. Ein „Tuner" ist eine Person, die das Tuning durchführt.

UMTS (Universal Mobile Telecommunications System)
Bezeichnet einen Mobilfunkstandard der dritten Generation (3G). Mit diesem sind deutlich höhere Datenübertragungsraten (bis zu 7,2 Mbit/s) als mit dem Mobilfunkstandard der zweiten Generation (2G) möglich.

Verkehrsleitsysteme
Ein System zur Lenkung des Straßenverkehrs mit Hilfe von statischen Verkehrszeichen oder Wechselverkehrszeichen. Dies kann neben Infrastruktureinrichtungen auch in Fahrzeugen realisiert werden. Dazu ist eine Technologie innerhalb von Fahrzeugen notwendig, zum Empfang dieser Informationen.

WIFI
Abkürzende Bezeichnung der im Bereich der WLAN Technologie (s. u.) tätigen „Wireless Ethernet Compatibility Alliance", dier vielerorts als Synonym für WLAN verwendet wird.

WLAN (Wireless Local Area Network)
Deutsch: drahtloses lokales Netzwerk. Bezeichnet eine Funknetztechnologie, die besonders im Bereich der Desktop-IT verbreitet ist.

Wurm, Computer-Wurm
Schadsoftware mit dem primären Ziel der Verbreitung, die hierzu insbesondere (drahtgebundene oder drahtlose) Kommunikationsverbindungen nutzt.

1 Einleitung

Einleitend werden die Zielstellung und die zur Bearbeitung gewählte Vorgehensweise vorgestellt. Anschließend wird ein Überblick über die weitere Gliederung dieses Berichtes geliefert.

1.1 Motivation/Zielstellung

Ähnlich zur heutigen Situation bei Systemen der Desktop-IT („PC-Welt“) werden zunehmend auch Elektronik und Informationstechnik (IT) im Automobilbereich (die durch die technologische Weiterentwicklung, z. B. im Kontext des intelligenten Straßenverkehrs der Zukunft, an Komplexität gewinnen) zum Ziel unautorisierter Veränderungen. Während auch in der bestehenden Forschung anhand praktischer Beispiele die Machbarkeit unterschiedlich komplexer Eingriffe in auf automotive IT demonstriert wurde, werden zunehmend auch Informationen zu automotiver Elektronik und Möglichkeiten ihrer Veränderung insbesondere im Internet verbreitet. Dieser Trend lässt daher befürchten, dass Eingriffe in automotive IT zukünftig eine ähnliche Verbreitung erfahren, wie dies im PC-Bereich nach der erfolgten Entwicklung bereits heute der Fall ist. Hierdurch könnten neuartige Gefährdungen für die Straßenverkehrssicherheit entstehen.

Einerseits sind bereits einzelne Beispiele für Veränderungen an elektronischen Systemen im Straßenverkehr bekannt. Andererseits ist jedoch bisher auch angesichts der bisherigen Informationen aus Berichterstattung und Forschungsprojekten kein breiter Überblick über die tatsächliche Relevanz und Verbreitung derartiger Möglichkeiten zur Veränderung in der heutigen Praxis verfügbar. Dieser wäre als Grundlage für zielgerichtete Forschungsaktivitäten allerdings sehr hilfreich. Ziel ist es daher, eine hierfür geeignete Basis zu legen, indem ein erster Überblick über die Relevanz derartiger Veränderungen in der Praxis geschaffen wird. Dazu wird durch eine breite Recherche in wissenschaftlichen und öffentlichen Quellen ein Überblick über wesentliche bekannte und existente Beispiele derartiger Möglichkeiten zur Veränderung im Straßenverkehr geschaffen. Es werden als Quellen neben bekannten nationalen und internationalen themenrelevanten Forschungsprojekten insbesondere auch neue Medien wie z. B. Internetforen einbezogen. Dadurch sollen möglichst quantitative Abschätzungen zu Faktoren der praktischen Relevanz der betrachteten Aktivitäten und potenziellen Folgen für die Verkehrssicherheit ermöglicht werden. Die Ergebnisse stellen somit einen ersten Schritt dar, um weitere Forschungsaktivitäten gezielt auf solche Teilprobleme ausrichten zu können, zu denen gleichzeitig eine hohe praktische Relevanz sowie erhebliche Risiken und Gefahren für die Praxis zu erwarten sind.

1.2 Vorgehensweise

Basierend auf umfassenden Recherchen insbesondere in neuen Medien setzt sich die verfolgte Vorgehensweise zum Ziel, Aussagen und Abschätzungen zu folgenden Faktoren zu erzielen:

- Bedrohungslage: Wie intensiv ist die Nachfrage nach einer Veränderung bzw. wie viele Informationen sind diesbezüglich verfügbar?
- Schwachstellen: Gibt es Systemeigenschaften, die diese Veränderung möglich machen, und wer kann diese ausnutzen?
- Risiko: Wie wahrscheinlich ist es, dass Veränderungen betrieben werden?
- Gefahren: Welche Gefahren können aus erfolgten Veränderungen entstehen?

Bezüglich der ersten drei Punkte wird innerhalb der verfolgten Vorgehensweise der aus der Literatur bekannte Zusammenhang Bedrohungslage x Schwachstellen = Risiko (engl.: Threat x Vulnerability = Risk) verwendet, der z. B. WRIGHT, 2007, S. 34 zu entnehmen ist.

Zur Ermittlung der Bedrohungslage wird insbesondere die Verbreitung verfügbarer Informationen herangezogen, die Möglichkeiten zur Veränderung elektronischer automotiver Systeme in der Literatur (abgeschlossene/aktuelle nationale/internationale Projekte) und neuen Medien (Internet, z. B. themenrelevante Foren) beschreiben. Dies erfolgt entlang von automotiven Teilsystemen, die in der Recherche als Ziel von Veränderungen ermittelt werden konnten. Die identifizierten Einzelkomponenten werden zudem allgemeinen, übergreifenden Komponentenklassen zugeordnet.

Danach werden hierzu wesentliche Schwachstellen identifiziert und kategorisiert, welche die recherchierten Veränderungen ermöglichen. Im Rahmen dieser Systematisierungen werden die Rechercheergebnisse gleichzeitig u. a. auch bezüglich des Angreiferspektrums untersucht.

Als Auftrittswahrscheinlichkeit von Veränderungen wird anschließend das Risiko abgeschätzt, das sich aus oben genanntem Zusammenhang ergibt. Als Verifikation und Ergänzung der so erhaltenen Abschätzungen werden weitere Kenngrößen und Kontextinformationen diskutiert und in die Abschätzungen einbezogen, die bezüglich der Wahrscheinlichkeit des praktischen Auftretens von Eingriffen vorgenommen werden.

Daraufhin erfolgt eine Gefahrenanalyse, um die potenziell resultierenden Gefahren abschätzen zu können. Ausgehend von den zuvor abgeschätzten Risiken für das Auftreten von Vorfällen der Veränderung wird hier das Spektrum der recherchierten Vorfälle bezüglich daraus resultierender Gefahren aufgezeigt. Dies erfolgt in zwei Schritten.

Im ersten, konzeptuellen Teil wird zur Abschätzung potenziell resultierender Gefahren zunächst exemplarisch das theoretische Spektrum entstehender Gefahren beleuchtet, wobei Auswirkungen von Veränderungen potenziell Einbußen nach sich ziehen, die in die Bereiche Komfort, Security (Zugriffsschutz) und Safety (funktionale Sicherheit und Sicherheit von Leib und Leben) fallen können. Mit Fokus auf die Straßenverkehrssicherheit werden schwerpunktmäßig Gefahren der letztgenannten Domäne betrachtet. In dieser Domäne wurde zusätzlich zwischen direkten Auswirkungen derartiger Veränderungen (Funktionswirkungen) und indirekten Nebeneffekten auf die Peripherie (Strukturwirkungen) unterschieden. Auch stehen neben Gefahren für das einzelne Fahrzeug bzw. die einzelne Infrastrukturkomponente potenzielle Gefahren für den gesamten Straßenverkehr als Verbünde von Fahrzeugen und Infrastrukturkomponenten im Kontext der Untersuchungen (Interaktionen zweiter Ordnung).

Dieses, zunächst konzeptuell behandelte Spektrum von Gefahren wird anschließend im zweiten Schritt an ausgewählten praktischen Beispielen aus der Recherche substantiviert, um eine Abschätzung der realen Gefährdung des Straßenverkehrs vornehmen zu können. Dies erfolgt mit Blick auf Anzeichen für in der Praxis existierende Gefährdungspotenziale nach elektronischen Veränderungen, die sich als Ergebnis der Recherchen und Beobachtungen identifizieren und einordnen lassen. Basierend hierauf erfolgt die abschließende Abschätzung des Gefährdungspotentials für die Straßenverkehrssicherheit.

Abschließend erfolgt in einem Ausblick zusätzlich eine Diskussion weiterer Komponentenklassen, bei

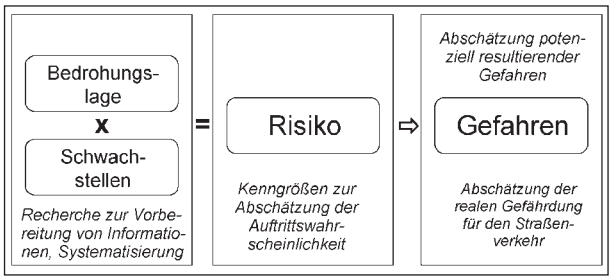


Bild 1: Die zugrunde liegende Vorgehensweise

denen zunehmend Eingriffe zu erwarten sein sollten. In diesem Kontext werden potenzielle Tendenzen in der praktischen Entwicklung der Bedrohungslage ebenfalls beleuchtet.

Bild 1 veranschaulicht die beschriebene zugrunde gelegte Vorgehensweise.

Die erarbeiteten Ergebnisse haben neben einem großen Rechercheteil hauptsächlich konzeptionellen und beurteilenden Charakter und orientieren sich an einer Recherche in öffentlich zugänglichen deutsch- und englischsprachigen (sowie teils auch russischsprachigen) Quellen in Literatur und neuen Medien (z. B. Internetforen). Die Dokumentation der erzielten Resultate wurde sorgfältig und nach bestem Wissen der bearbeitenden Personen erstellt, erhebt jedoch keinen Anspruch auf Vollständigkeit.

1.3 Überblick über den vorliegenden Schlussbericht

Die Ergebnisse werden in den Kapiteln 2 bis 6 entlang der vorgestellten Vorgehensweise (vgl. Bild 1) dokumentiert: Kapitel 2 befasst sich hierbei mit der Abschätzung der Bedrohungslage und Kapitel 3 mit den zugrunde liegenden Schwachstellen. Das Risiko des Auftretens entsprechender Vorfälle wird in Kapitel 4 abgeschätzt. Die Ergebnisse werden mit der Analyse potenziell resultierender Gefahren (Kapitel 5) vervollständigt und in Kapitel 6 ein Ausblick auf die potenzielle zukünftige Entwicklung der Problematik gegeben. Eine Einschätzung der Ergebnisse wird in Kapitel 7 geliefert, durch einen abschließenden Überblick über ausgewählte Gefahren elektronischer Manipulationen für die Straßenverkehrssicherheit ergänzt und ein Ausblick auf weitere zu erwartende Trends gegeben.

Allgemeine Literaturverweise sind in Kapitel 8 aufgelistet und werden im Text über die groß geschrie-

benen Autorennamen referenziert (z. B.: vgl. WALLENTOWITZ, 2006, S. 134). Zusätzlich dazu werden im Text (insbesondere bei den Ergebnissen in den Kapiteln 2.1 und 5.2.1) einzelne Rechercheergebnisse referenziert. Diese Verweise sind in der Form [R123] notiert, wobei die enthaltene Zahl auf eine eindeutige Indexnummer jedes zusammengetragenen Rechercheergebnisses verweist. Eine kurze tabellarische Übersicht mit einer Aufstellung der Rechercheergebnisse und ihrer Titel findet sich in der „Kompaktübersicht Rechercheergebnisse“ am Ende dieses Dokumentes.

1.4 Einleitende Begriffsklärungen und Konventionen

Vor der Dokumentation der Ergebnisse folgen vorausgehend noch Erklärungen einzelner Begriffe und Vorstellung genereller Konventionen, wie sie im Kontext dieses Dokuments zu verstehen sind.

1.4.1 Klärung der hier vorgenommenen Verwendung des Veränderungsbegriffs

Im Kontext dieses Dokuments werden unter dem zentralen Begriff „Veränderung“ verschiedene Arten von (elektronischen) Eingriffen an Fahrzeug- und Infrastruktursystemen verstanden:

- (Unfachmännisch durchgeführte) Nachrüstung
  Darunter fallen alle Handlungen, bei denen zusätzliche Komponenten oder Funktionen in ein bestehendes System eingebracht werden.
- Modifikation
  Darunter fallen alle Handlungen, bei denen bestehende Komponenten oder Funktionen in einem bestehenden System verändert werden.
- Tuning
  Bezeichnet individuell vorgenommene Modifikationen und Nachrüstungen mit dem Ziel der Erhöhung eines subjektiven Zugewinns für den Fahrzeugnutzer (siehe auch Glossar).
- Unautorisierte Manipulation
  Bezeichnet sämtliche Veränderungen, die durch einen Hersteller, Versicherungen und gesetzliche Regelungen und weitere berechtigte Dritte (z. B. Flottenbetreiber) sanktioniert sind.
- Missbrauch
  Bezeichnet das Nutzen von autorisierten Möglichkeiten zur Veränderung von Komponenten oder Funktionen in einer nicht für diesen Nutzungskontext vorgesehene Weise.

Speziell die unautorisierte Manipulation und der Missbrauch stehen im Fokus. Aber auch (unfachmännisch durchgeführte) Nachrüstungen, Modifikationen und Tuningmaßnahmen werden als relevante Veränderungen referenziert, insofern sie für die Zielstellung (potenzielle Gefährdung des Straßenverkehrs) von Bedeutung sind. Die Begriffe „Angriff“ und „Angreifer“ sowie („Basis-)Angriffe” werden wertneutral verwendet und bezeichnen entsprechende Eingriffe, die agierenden Personen bzw. die eingesetzten Techniken.

1.4.2 Aspekte der Sicherheit

Bzgl. des Begriffs „Sicherheit“ wird im Englischen zwischen „Safety“ und „Security“ unterschieden. Obwohl sie beide im Deutschen mit „Sicherheit“ übersetzt werden, ist die Unterscheidung in der wissenschaftlichen Verwendung oft von besonderer Bedeutung. Zur Klarstellung der jeweiligen Ausprägung werden in diesem Dokument daher häufig die englischen Begriffe, Safety und Security, verwendet.

Safety wird im Deutschen teils auch als „Funktionssicherheit“ oder „funktionale Sicherheit“ bezeichnet. Nach ECKERT, 2004 umfasst sie damit die Eigenschaft eines Systems, dass die realisierte Ist-Funktionalität mit der spezifizierten Soll-Funktionalität übereinstimmt, d. h., dass es unter allen (normalen) Betriebsbedingungen funktioniert. Damit nimmt ein funktionssicheres System keine unzulässigen Zustände an.

Security dagegen ist nach ECKERT, 2004 die Eigenschaft eines (funktionssicheren) Systems, nur solche Systemzustände anzunehmen, die zu keiner unautorisierten Informationsveränderung oder -gewinnung führen.

Ein gleichzeitig gültiges Unterscheidungskriterium ist die hinter einem Vorfall stehende Absicht. Beabsichtigte, d. h. vorsätzliche, Eingriffe in ein System (z. B. zu dessen Manipulation oder dem Ausspähen von Informationen) fallen unter den Sicherheitsbegriff der Security. ELLIMS, 2007 definiert Security daher als den Schutz eines Objektes vor der Umgebung. Der Schutz vor unbeabsichtigten (i. d. R. zufälligen) Fehlfunktionen eines Systems (die z. B. im Ausfall oder Versagen einer Komponente begründet liegen) hingegen fällt unter den Begriff der

Safety. Entsprechend stehen bei der Safety oft Leib und Leben des Menschen als ein hohes Schutzgut im Vordergrund, was auch Personenschäden infolge eines Systemversagens einschließt. Fehlfunktionen der Technik sollen möglichst nicht die körperliche Unversehrtheit der Nutzer gefährden. ELLIMS, 2007 definiert Safety daher als den Schutz der Umgebung vor einem Objekt. Im Automobilbereich fällt daher insbesondere auch die Straßenverkehrssicherheit unter den Begriff der Safety. Bei entsprechenden Sicherheitsfunktionen (d. h. Systemen, die zum Schutz von Leib und Leben der beteiligten Personen dienen) wird dort zudem zwischen aktiver und passiver Sicherheit differenziert. Unter aktive Sicherheitsfunktionen fallen sämtliche Systemfunktionen, die aktiv zur Vermeidung potenzieller Unfallereignisse beitragen. Ein Beispiel hierfür ist das Elektronische Stabilitätsprogramm (ESP). Passive Sicherheitsfunktionen sind dagegen dazu bestimmt, im Falle eines Unfallereignisses die gesundheitlichen Folgen für die beteiligten Personen zu reduzieren.

1.4.3 Ableitung von Komponentenklassen aus automotiven Domänen

In der Forschung und Literatur (siehe z. B. WALLENTOWITZ, 2006) haben sich bereits verschiedene Domänen etabliert, in die automotive Komponenten/Systeme nach ihrer funktionellen und strukturellen Bedeutung eingeordnet werden. Im vorliegenden Dokument werden insbesondere die folgenden Komponentenklassen, die diesen Domänen entlehnt sind, exemplarisch betrachtet. Der Fokus liegt auf elektronischen Regelsystemen, die innerhalb der folgenden Domänen jeweils in Form von Steuergeräten, Sensorik und Aktorik realisiert sind:

- Motor und Antriebsstrang: In diese Domäne werden hauptsächlich Systeme zusammengefasst, die Aufgaben zur Motor- und Getriebesteuerung übernehmen.
- Fahrwerksysteme: Diese Domäne umfasst Lenk-, Dämpfungs- und Verzögerungsfunktionen. Beispiele für Systeme, die in diese Domäne fallen, sind Servolenkung und Niveauregulierung. Dieser Domäne wurden auch Systeme zur aktiven Sicherheit (Fahrdynamikregelsysteme wie ESP, ABS, ASR) zugeordnet.
- Passive Sicherheit: Sicherheitssysteme zur Erhöhung der passiven Sicherheit (im Sinne der Safety) werden in dieser Domäne zusammengefasst. Hierzu zählen alle Fahrzeugsysteme und -funktionalitäten, die verschiedene Maßnahmen bieten, um Unfallfolgen zu reduzieren. Sie stellen so eine wichtige Basis für die Sicherheit im Straßenverkehr dar. Darunter fallen beispielsweise kombinierte Rückhaltesysteme, im Englischen auch als Supplemental Restraint System (SRS) bezeichnet (vgl. ROSENBLUTH, 2002). Hierzu gehören u. a. Airbags und Gurtstraffer.
- Fahrerassistenzsysteme: Unter Fahrerassistenzsystemen (vgl. auch WINNER, 2009) werden insbesondere umfelderfassende Systeme zur Unterstützung des Fahrers verstanden. Diese können als informierende oder als eingreifende Systeme realisiert sein. Hierzu zählen beispielsweise Systeme zur aktiven Sicherheit (z. B. Ausweich- und Bremsassistent).
- Infotainment: Der Begriff Infotainment ist ein Kunstwort aus Information und Entertainment (Unterhaltung). In dieser Domäne werden Systeme zusammengefasst, die entweder der Information des Fahrers dienen (z. B. fahrrelevante Daten im Kombiinstrument, Navigation) oder der Unterhaltung dienen (z. B. Radio, Telefon).
- Zugriffschutz (Security): Neben Sicherheitssystemen zur Wahrung der Safety (s. o.) sind insbesondere auch Systeme zum Zugriffsschutz (Security) zu beachten. Diese richten sich explizit gegen unberechtigte Zugriffe (z. B. Zugang, Nutzung) unautorisierter Personen (z. B. Zentralverriegelung und Wegfahrsperre) und sollen explizit auch gezielten, vorsätzlichen Veränderungen bzw. Manipulationen widerstehen.
- Karosserie: In der Karosserie verbaute weitere Systeme, die nicht primär einer der übrigen Domänen zuzuordnen sind, werden im Rahmen dieses Dokuments als Komponenten der Domäne Karosserie geführt. Hierunter fallen sowohl Beleuchtungssysteme als auch Systeme wie Verdecksteuerung oder elektrisch verstellbare Außenspiegel und die Klimatisierung.
- Infrastrukturkomponenten: Verkehrsrelevante Systeme außerhalb des Fahrzeugs werden als Infrastrukturkomponenten zusammengefasst. Hierunter fallen Verkehrsleitsysteme (siehe Glossar) wie z. B. Lichtsignalanlagen („Ampeln“) und variable Anzeigen (z. B. dynamische Geschwindigkeitsbegrenzungen).

1.4.4 Überblick Fahrzeug IT und -Netze

Abschließend folgen in diesem Kapitel einige Grundlagen zu automotiven IT-Infrastrukturen, die für mehrere im weiteren Verlauf dokumentierte Beispiele elektronischer Veränderungen relevant sind.

Immer mehr Funktionen in Fahrzeugen werden elektronisch realisiert. In diesem Zuge werden zunehmend auch bewährte mechanische Systeme durch elektronische Ansteuerung ergänzt oder gänzlich durch elektronische Lösungen ersetzt. Ein Beispiel ist das Gaspedal, das in heutigen Fahrzeugen heute oft keine mechanische Verbindung zur Drosselklappe über einen Bowdenzug aufweist, sondern elektronisch abgetastet und elektromechanisch umgesetzt wird.

Die diesem zunehmend komplexen Funktionsspektrum zugrunde liegende IT findet sich in modernen Fahrzeugen verteilt in einer Vielzahl so genannter Steuergeräte (engl.: Electronic Control Units/ ECUs). Aktuelle Fahrzeuge beinhalten bereits eine Vielzahl von Steuergeräten. Dies sind kompakte, eingebettete Systeme, die auf den Einsatz im Automobil zugeschnitten sind. Über verschiedenartige Sensoren erfasste Eingaben werden durch sie elektronisch verarbeitet. Unter anderem über ebenfalls an die Steuergeräte angeschlossene Aktoren kann die Elektronik ihre Ausgaben auf verschiedenartige Weise umsetzen (z. B. mechanisch, optisch, akustisch etc.).

Sensoren und Aktoren sind in der Regel elektrische Komponenten, die über analoge Signalleitungen (Kabel) direkt an ein Steuergerät angeschlossen sind. Darüber hinaus sind die Steuergeräte untereinander vernetzt, um notwendige Informationen (wie z. B. digitalisierte Sensorwerte oder aktuelle Betriebsdaten) austauschen zu können. Dies erfolgt i. d. R. über digitale Feldbussysteme. Beispiele für entsprechende Bussysteme, die heute in Automobilen eingesetzt werden, sind CAN, LIN, MOST oder FlexRay, die z. B. in ZIMMERMANN, 2008 detailliert vorgestellt werden.

In heutigen Fahrzeugen werden in der Regel mehrere dieser Netzwerke, teils basierend auf unterschiedlichen Bussystem-Technologien, parallel betrieben. Beispielhafte Gründe hierfür können mit Blick auf die einzugliedernden Steuergeräte unterschiedliche Bandbreitenanforderungen, Kostenfaktoren und auch die gegenseitige Abschottung einzelner Funktionsgruppen sein. In der Praxis fällt diese physische Aufteilung der Fahrzeugnetwerke oft mit einzelnen der in Kapitel 1.4.3 vorgestellten logischen Fahrzeugdomänen zusammen, da die ihnen zuzuordnenden Systeme (und deren Funktionen) oft ähnliche Anforderungen aufweisen. So sind Funktionen des Antriebsstrangs (teils gemeinsam mit Funktionen des Fahrwerks) bei einigen Herstellern in einem Netzwerk zusammengelegt, die in vielen Fällen hohe Echtzeitanforderungen haben (z. B. als High-Speed-CAN-Bus). Geräte aus dem Infotainmentbereich werden auch vielfach in einem Teilnetzwerk gebündelt; diese haben oftmals größeren Bandbreitenbedarf, dem z. B. über einen – auf Glasfaser-Technologie basierenden – MOST-Bus entsprochen werden kann.

Dennoch müssen in vielen Fällen auch Informationen zwischen Komponenten ausgetauscht werden, die in unterschiedlichen Teilnetzwerken lokalisiert sind. Damit beispielsweise das Navigationssystem im Infotainment-Netzwerk die aktuell gefahrene Geschwindigkeit als Eingabewert verarbeiten kann,

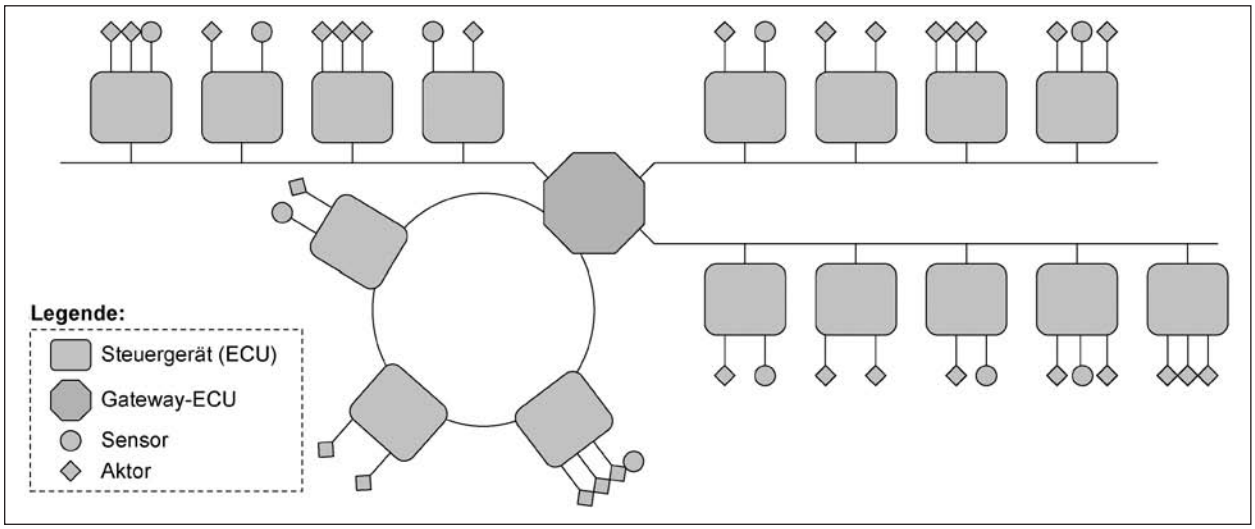


Bild 2: Beispielhafte Topologie eines Bussystem-Netzwerks

muss diese aus dem Antriebsstrang-Netzwerk übermittelt werden. Damit dies möglich ist, sind i. d. R. ein oder mehrere zentrale Gateway-Steuergeräte vorhanden, die Informationen zwischen unterschiedlichen Bussystemen vermitteln.

Bild 2 skizziert beispielhaft eine mögliche Netzwerktopologie eines Fahrzeuges.

2 Abschätzung der Bedrohungslage: Recherche zur elektronischen Veränderung von Kfz- und Infrastruktursystemen

In diesem und den folgenden Kapiteln werden die nach der in Kapitel 1.2 vorgestellten Vorgehensweise erhaltenen Ergebnisse zusammengefasst. Im Kontext dieser Kapitel wird jeweils mit eckigen Klammern auf die Rechercheergebnisse verwiesen (z. B. [R17] für das mit Index 17 versehene Rechercheergebnis, vgl. Kapitel 1.3 sowie „Kompaktübersicht Rechercheergebnisse" am Ende dieses Dokumentes).

Im Folgenden wird mit der Analyse der Bedrohungslage begonnen. In Kapitel 2.1 wird zunächst das potenzielle Spektrum derjenigen Komponenten aufgezeigt, die im Rahmen der Recherchen als Ziel elektronischer Veränderungen identifiziert werden konnten. Dabei wird nach Fahrzeug- und Infrastrukturkomponenten unterschieden, was getrennt in den Kapiteln 2.1.1 und 2.1.2 erfolgt. Anschließend folgt in Kapitel 2.2 eine systematisierte Aufbereitung der Rechercheergebnisse, bevor in Kapitel 2.3 die abschließende Abschätzung der Bedrohungslage vorgenommen wird.

2.1 Analyse der Bedrohungslage: Recherche zu veränderten Komponenten

Bei der Analyse der Bedrohungslage werden Komponenten aus dem automotiven Umfeld identifiziert, die bereits heute Ziel elektronischer Veränderungen sind. Im Fokus stehen dabei Veränderungen an heute verfügbaren Systemen, zu denen sich in der Recherche konkrete Hinweise auf die Veränderbarkeit oder zumindest entsprechende Bestrebungen finden ließen. Eine zusätzliche Abhandlung zur potenziellen Veränderbarkeit zukünftiger Fahrzeug- und Infrastruktursysteme bzw. denkbarer Motivationen dazu erfolgt separat in Kapitel 6.

2.1.1 Kfz-Systeme als Ziel elektronischer Veränderungen

In diesem Kapitel werden die wesentlichen Kfz-Komponenten (d. h. die internen Systeme eines Fahrzeugs) kurz vorgestellt, die im Rahmen der Recherchen als Ziel bestehender oder beabsichtigter elektronischer Veränderungen identifiziert werden konnten.

Es handelt sich bei den recherchierten Beispielen in vielen Fällen um Eingriffe durch den Besitzer bzw. Nutzer des Fahrzeuges, der dieses aus seiner Sicht optimieren will (dies wird meist auch als „Tuning" bezeichnet). An dieser Stelle sei bereits im Vorfeld betont, dass entsprechende Aktivitäten allein durch ihre Nennung in diesem Dokument nicht automatisch als gefährlicher und/oder unerlaubter Eingriff verstanden werden sollten. Viele dieser Änderungen können, fachmännisch vorgenommen, auch durch Gutachter als unbedenklich bescheinigt und über eine entsprechende Eintragung offiziell festgehalten werden. Die Rechercheergebnisse verdeutlichen jedoch, dass entsprechende Eingriffe häufig unfachmännisch durchgeführt werden und zum Teil auch ungewollte Nebenwirkungen haben können, die sich bis auf die Straßenverkehrssicherheit auswirken können (vgl. Kapitel 5 und 5.2.1). Auch kann durch einen nicht eingetragenen Eingriff formal die Allgemeine Betriebserlaubnis (ABE) erlöschen (vgl. BORGEEST, 2008, Kap. 10), was auch rechtliche Konsequenzen nach sich ziehen könnte – z. B. in Haftungsfragen (selbst wenn der Eingriff selbst nicht ursächlich für den Streitfall war). Entsprechend ist das Prüfen auf Tuningmaßnahmen auch im Rahmen der Verkehrsunfallrekonstruktion als ein wichtiger Aspekt zu sehen (siehe auch BURG, 2009, S. 826 und 833).

Bei der Entscheidung für oder gegen eine Veränderung von Funktionen kommt der subjektiven Wahrnehmung des Nutzers oftmals eine wesentliche Bedeutung zu. Nimmt der Fahrer bei der „normalen" Fahrzeugnutzung einen Zustand als subjektiv verbesserungswürdig wahr, bildet dies oft den Ausgangspunkt oder die Motivation für eine Reihe von Entscheidungen, welche die Art der Veränderung determinieren und Ansätze darstellen für Interventionen, beispielsweise auf technischer oder legislativer Ebene (vgl. Bild 3). Dabei spielen im Allgemeinen drei Fragen aus Sicht des Fahrers eine entscheidende Rolle:

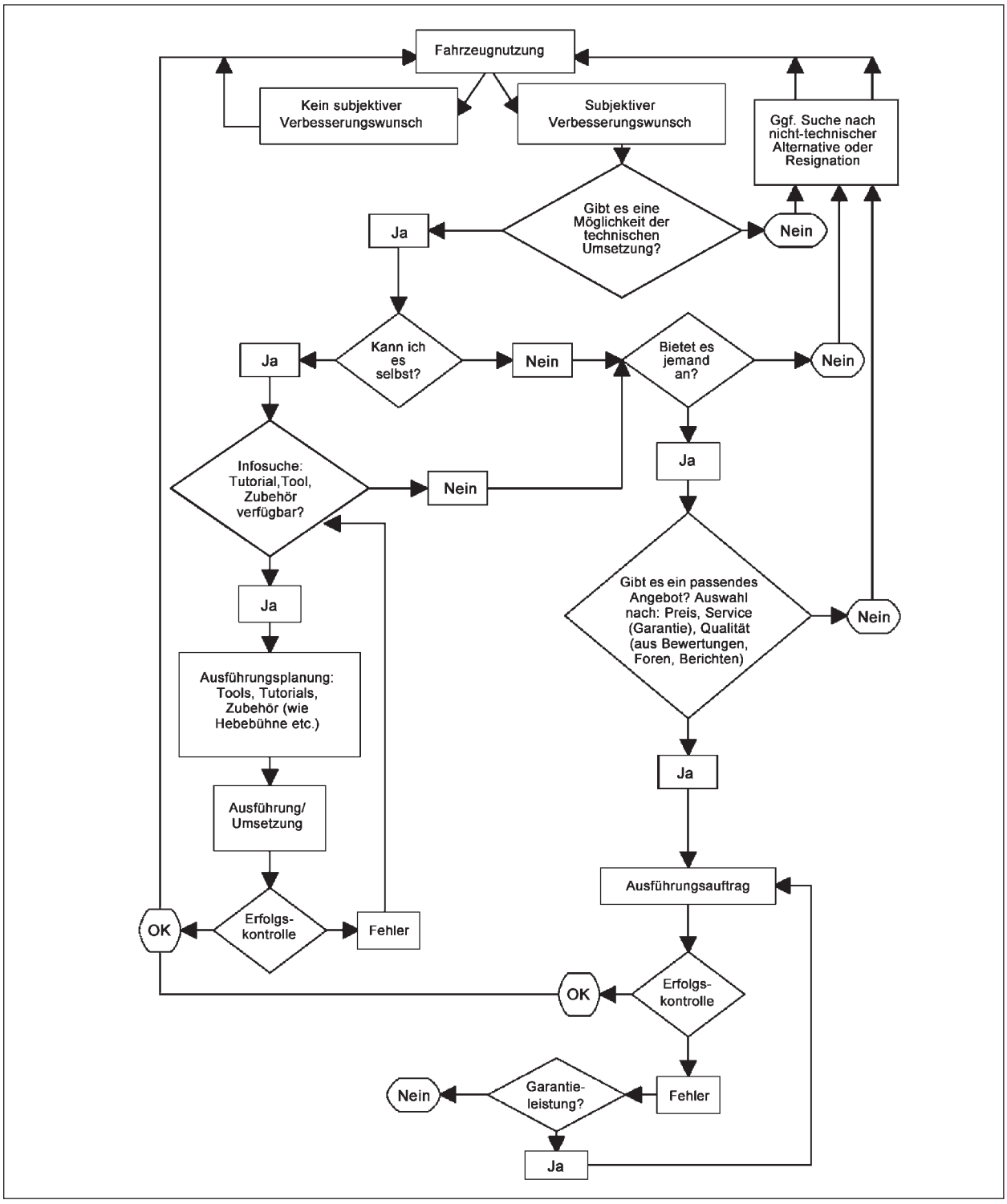


Bild 3: Exemplarisches Entscheidungsdiagramm zur Veränderung von Fahrzeugfunktionen für eine ausgewählte Komponente (z. B. Motorsteuerung)

1. Gibt es überhaupt eine technische Lösung?
2. Wenn ja, kann ich es selbst durchführen?
3. Wenn nicht, bietet es jemand anderes an?

Komponenten, bei denen sich der Fahrer für eine Veränderung entscheidet, können sehr unterschiedlicher Natur sein. Die wesentlichen Komponenten bzw. Teilfunktionen (inkl. Zuordnung der in Kapitel 1.4.3 beschriebenen Komponentenklassen), zu denen ein oder mehrere Veränderungsausprägungen recherchiert werden konnten, werden zunächst in Tabelle 1 überblicksartig aufgeführt. Im Anschluss folgt zu jeder dieser Kompo-

Komponentenklasse	Komponente
Motor und Antriebsstrang	Motorsteuerung
	Getriebesteuerung
	Startsteuerung
Fahrwerk	Servolenkung
	Adaptive Niveauregulierung
	Fahrdynamikregelsysteme
Passive Sicherheit	Airbagsystem/Gurtstraffer
Fahrerassistenz	Längsführung
	Querführung
Infotainment	Instrumentenkombination
	Radio
	Navigationssystem
	Video-System
	Allgemeine Warnfunktionen
Zugriffsschutz	Schließsystem
	Diebstahlwarnanlage
	Wegfahrsperre
Karosserie	Lichtanlage
	Außenspiegel
	Verdeck
	Klimasteuerung

Tab. 1: Recherchierte Kfz-Komponenten als Ziel elektronischer Veränderungen

nenten ein erläuternder Text, der näher auf die Ziel-Komponente selbst sowie die recherchierten Motivationen für Veränderungen an ihnen bzw. die relevantesten technischen Ansätze hierzu eingeht.

Beginnend mit Veränderungen an der Motorsteuerung werden im Folgenden in dieser Reihenfolge wesentliche Veränderungen dokumentiert, die im Rahmen der Recherche ermittelt wurden.

Für jede behandelte Komponente wird dabei zunächst eine kurze Übersicht über relevante Funktionen gegeben, die diese typischerweise realisieren. Anschließend werden exemplarische Motivationen genannt, die Personen zu Veränderungen an diesen Systemen bewegen können. Aus der Recherche stammende Beispiele als praktische Belege für entsprechende Bestrebungen folgen dann jeweils am Ende der einzelnen Teilabschnitte.

Motorsteuerung

Funktionsübersicht

Die Motorregelung (Motormanagement) umfasst Komponenten (Sensoren, Aktoren, elektronische Steuergeräte) zur Regelung von Zünd- bzw. Einspritzzeitpunkt, Einspritzmenge, Luftmenge in Relation zur Kurbelwellenlage und steuert darüber hinaus weitere Aktoren, abhängig von der aktuellen Gaspedalstellung sowie externen Lastanforderungen.

Beispielhafte Motivationen

Für viele an der Motorsteuerung betriebene Veränderungen spielen finanzielle Motivationen eine Rolle. Viele Fahrer streben danach, das Verhältnis zwischen der Leistung des Fahrzeugs und den entstehenden Kosten (einmalige wie Anschaffung und Umrüstung sowie laufende wie Betrieb, Steuer und Versicherung) zu optimieren. Aus diesem Bestreben vorgenommene (mechanische wie elektronische) Eingriffe werden insbesondere im Motorbereich, aber auch in anderen Systemteilen meist als Tuning bezeichnet. Dies beinhaltet daher auch Bestrebungen, das Fahrzeug hinsichtlich eines geringeren Verbrauchs zu optimieren (was auch als ECO-Tuning bezeichnet wird), wodurch Kosten eingespart werden können.

Insbesondere im Bereich der Motorsteuerung gibt es seit der Einführung der elektronischen Einspritzanlagen immer wieder Versuche, mit Hilfe elektronischer Veränderung mehr Leistung aus dem Serien-Motor abzurufen. Dies reicht von dem so genannten „10 Cent Tuning“ für TDI-Motoren (bei dem ein serienmäßiger Kraftstofftemperaturfühler durch einen Festwiderstand ersetzt wird, welcher eine hohe Kraftstofftemperatur suggeriert) bis hin zu professionellen Tuningangeboten.

Im Rahmen der akademischen Veröffentlichung [R145] wurde zudem die hypothetische Motivation betrachtet, dass ein Angreifer über eingeschleusten Schadcode von Seiten des Fahrzeugbusses unsachgemäß in die Motorsteuerung eingreifen könnte, z. B. um das Fahrzeug zum Stillstand zu bringen – d. h. den Fahrzeugführer am (Weiter-)Fahren zu hindern.

Exemplarische Praxisbelege

Eine klassische Vorgehensweise besteht in der elektronischen Anpassung der Kennfelder im Motorsteuergerät, was i. d. R. über Diagnose Hard- und Software erfolgt (z. B. in der Tuning-Werkstatt oder wie angeboten in [R22] oder [R74]). Alternativ ist es teilweise auch üblich, die (aufgesteckten oder verlöteten) Speicherbausteine, auf denen die Kenn-

felder oder die verarbeitenden Algorithmen gespeichert sind, gegen veränderte Bausteine zu ersetzen, die z. B. im Internet käuflich zu erwerben sind (vgl. [R75]).

Einen weiteren Ansatz für Motortuning stellt der Einsatz zwischengeschalteter Steuergeräte dar, die von verschiedenen Anbietern (z. B. aus [R27, R28]) beziehbar sind. Der Einbau dieser Komponenten ist relativ simpel. Sie werden einfach in die vorhandene Motorregelung eingebunden und als Resultat wird dann per Knopfdruck das Kennfeld der Motorsteuerung verändert. Somit wird u. a. eine Leistungssteigerung erzielt. Entsprechende Einbauanleitungen werden von den Anbietern teils auch auf bekannten Video-Portalen im Internet verfügbar gemacht (vgl. [R27]). Somit erfordert diese Veränderung vom Anwender lediglich den Aufwand, sich die Hardware (teils aus dem Ausland, z. B. den USA) schicken zu lassen und diese dann per Videoanleitung zu montieren. Laut Hersteller-Angabe sind diese Zusatzkomponenten häufig auch unsichtbar gegenüber Herstellertestgeräten, wie sie im alltäglichen Gebrauch der Werkstatt zu finden sind. Entsprechende Zusatzgeräte bieten teilweise auch ein breites Spektrum von Funktionen. Das in [R123] beworbene Gerät erlaubt neben einem Modus zur Leistungssteigerung beispielsweise auch die Umstellung auf einen ECO-Modus sowie die Verwendung als Wegfahrsperre (siehe auch zugehöriges Kapitel unten).

Als unerwünschte Eingriffe in die Motorsteuerung von Seiten des Fahrzeugbusses wurden in der Veröffentlichung [R145] an einem Testfahrzeug verschiedene Umsetzungen praktisch demonstriert. Beginnend mit kleineren Eingriffen wie dem Ändern der Leerlaufdrehzahl wurde das Ziel, den Motor zum Stillstand zu bringen, über zwei verschiedene Wege erreicht: Den ersten stellt das gleichzeitige Deaktivieren aller Zylinder dar (durch Senden entsprechender Anweisungen über Bus-Nachrichten). Ebenfalls zum Ziel führt das Senden einer Busnachricht, über die die Motorsteuerung über das Auslösen von Airbags (d. h. über einen schweren Unfall) informiert wird. Teils bleibt die Nicht-Benutzbarkeit des Motors in den Tests aus [R145] auch über Neustarts hinweg bestehen.

Motorsteuerung: Abgasrückführung

Funktionsübersicht

Wie z. B. WALLENTOWITZ, 2006 zu entnehmen ist, wird bei vielen Motoren das Erreichen der Einhaltung der gesetzlich vorgeschriebenen NOx-Grenzwerte durch eine Abgasrückführung (AGR) realisiert. Mit der Rückführung von Abgas in den Ansaugtrakt lassen sich die NOx-Emissionen deutlich senken, weil dadurch sowohl die Brenngeschwindigkeit als auch die Verbrennungsspitzentemperatur gesenkt werden. Dabei wird die angesaugte Frischluft mit einem Teil der Abgase vermischt, um den Sauerstoffüberschuss im Brennraum zu verringern.

Beispielhafte Motivationen

Durch den enthaltenen Ruß soll die hierbei laut [R45] oft zu Verengungen und dadurch letztendlich zu Leistungsminderungen der Motoren führen. Eine in den Recherchen beobachtete Motivation ist daher, diesem Effekt vorzubeugen.

Exemplarische Praxisbelege

Bei einigen Fahrzeugen kann nach Anleitungen wie in [R45] die Rate der Abgasrückführung minimiert werden (z. B. über eine geeignete Ansteuerung des AGR-Ventils). Einige Personen versuchen so, den erwähnten Leistungsminderungen vorzubeugen.

Motorsteuerung: Geschwindigkeitsabregelung

Funktionsübersicht

Bei vielen Herstellern werden einzelne Modelle oft bei höheren Geschwindigkeiten abgeregelt. Nach der Quelle [R87] entstand dies aus einer vernunftbedingten Selbstverpflichtung deutscher Hersteller, die aber auch technisch bedingt war, da die Reifenqualität oft nicht ausreicht(e), um den extremen Bedingungen bei höheren Geschwindigkeiten standzuhalten. Heute hat diese Begrenzung auch oft Versicherungsrelevanz; eine Aufhebung ist i. d. R. meldepflichtig und kann zu einer Prämienerhöhung führen. In der Recherche fanden sich mehrere Quellen, die entsprechende Abregelungssperren, die teils auch als „vMax“ bezeichnet werden, diskutieren.

Beispielhafte Motivationen

Um mit dem Fahrzeug auch schnellere Geschwindigkeiten erreichen zu können, wird die Deaktivierung dieser Abregelungsfunktionen von einigen Besitzern angestrebt, wie z. B. die Quellen [R88] und [R89] belegen.

Exemplarische Praxisbelege

In [R93] werden Möglichkeiten diskutiert, ein bei 200 km/h abregelndes Fahrzeug zu entsperren. Hierzu soll es Anbieter geben, die auf geringere Erhöhungen der Leistung von z. B. 20 PS noch Garantie geben, aber auch größere Sprünge wie +40 oder +60 PS noch auf Eigenverantwortung des Fahrers vornehmen. Teils erfolgt dies über Einbau eines sog. V-max-Moduls, wie z. B. in [R89] als Möglichkeit angeführt wird. In [R92] wird alternativ auch das Vorgehen mit Diagnoselösungen beschrieben, um ein bei 250 km/h abregelndes Fahrzeug zu entsperren.

Motorsteuerung: Regelung für Autogas-Anlage

Funktionsübersicht

Mit einer Autogas-Anlage ist es möglich, Flüssiggas (eine Mischung aus Butan und Propan, das zum Beispiel bei der Erdgas- und Erdölförderung anfällt) zusätzlich als Treibstoff für den Pkw zu nutzen. Dies hat zum einen wirtschaftliche Vorteile, da Autogas steuerlich begünstigt wird, und zum anderen verbrennt es umweltfreundlicher als herkömmlicher Treibstoff. Da weiterhin dasselbe Triebwerk zum Einsatz kommt, muss eine Autogasanlage auch elektronische Aufgaben übernehmen: Das Motormanagement muss auf den andersartigen Kraftstoff umgestellt werden.

Bi-Fuel-Fahrzeugantriebe, die sowohl Ottokraftstoff als auch Gas (Erdgas, Compressed Natural Gas, CNG oder Flüssiggas, Liquified Petroleum Gas, LPG) verwenden, benötigen ein Betriebsartenmanagement, das die Umstellung von einer Kraftstoffart auf die andere auch zur Laufzeit koordiniert.

Beispielhafte Motivationen

Während es bereits Fahrzeuge gibt, die herstellerseitig mit einer Autogas-Anlage ausgerüstet werden, stellt auch das Nachrüsten einer solchen Anlage bei anderen Fahrzeugen eine oft angefragte Erweiterung dar. Beispielsweise wird in Rechercheergebnis [R135] eine entsprechende Erweiterung in einem themenbezogenen Forum nachgefragt.

Exemplarische Praxisbelege

In der Konsequenz muss bei entsprechenden Nachrüstungen entweder die Hard- und Software einer bestehenden Motorsteuerung komplett adaptiert werden oder es wird nach dem Prinzip einer Zweiteilung eine zusätzliche Motorsteuerung für den Gasmodus hinzugefügt (vgl. WALLENTOWITZ, 2006).

Dass die Nachrüstung von Autogas inkl. der notwendigen Regelungen auch in der Praxis betrieben wird, belegt beispielsweise die Recherchequelle [R134], bei der eine auf entsprechende Nachrüstungen spezialisierte Firma ihre Dienste anbietet.

Potenziell resultierende Gefahren insbesondere durch unzureichend qualifizierte Anbieter werden in Kapitel 5.2.1 diskutiert.

Getriebesteuerung

Funktionsübersicht

Elektronische Regelungssysteme finden sich derzeit sowohl in Automatikgetrieben als auch in automatisierten Schaltgetrieben.

Beim Automatikgetriebe werden auf Basis u. a. von Last-, Drehzahl- und Geschwindigkeitssignalen (z. B. unter Verwendung eines Drehmomentwandlers) Schaltvorgänge zur idealen Drehmoment- und Drehzahlanpassung durch ein elektronisches Steuergerät ausgelöst (vgl. WALLENTOWITZ, 2006).

Automatisierte Schaltgetriebe stammen initial aus dem Bereich des Motorsports, halten jedoch zunehmend auch Einzug in Serienfahrzeuge (insbesondere in der Kompaktklasse, vgl. WALLENTOWITZ, 2006, S. 30). Diese Getriebe, die auch als Automated Manual Transmission (AMT) bezeichnet werden, übernehmen teilautomatisiert Funktionen des Schaltvorgangs durch Kupplungsautomaten und schließen das Verschalten weitestgehend aus.

Beispielhafte Motivationen

Bezüglich Automatikgetrieben konnte in den Recherchen Anzeichen für die Motivation ermittelt werden, die Schaltpunkte zu verlegen (siehe [R133]), z. B. um eine sportlichere Fahrweise zu ermöglichen.

Als eine Motivation für Veränderungen an Schaltgetrieben wurde in den Recherchen die Umrüstung einer Standard-H-Schaltung in eine pseudo-automatisierte Schaltung ermittelt. Diese Motivation kann beispielsweise aus dem inhärenten Nachteil der konventionellen (nicht-elektronischen) H-Schaltung entstehen, dass hierbei ein potenzielles Verschalten auftreten kann. Dieses kann u. U. erhebliche Beschädigungen am Antriebsstrang des Fahr-

zeugs und ein abruptes Abbremsen zur Folge haben, welches ggf. zusätzlich nicht durch die Bremsleuchten optisch dem Nachfolgeverkehr signalisiert wird.

Exemplarische Praxisbelege

Bezüglich des Verlegens von Schaltpunkten am Automatikgetriebe findet sich in Quelle [R61] eine Anleitung, wie dies mit Hilfe von Schaltpunktveränderungen am Getriebesteuergerät realisiert werden kann. Laut [R61] genügt für die Änderung am dort besprochenen Fahrzeugtyp gängige Diagnosesoftware.

Angebote zur nachträglichen Umrüstung auf eine pseudo-automatisierte Schaltung finden sich beispielsweise in den Quellen [R60] und [R138]. Bei diesen Modulen, die auch zum Selbst-Einbau verfügbar sind, wird an das Getriebe eine kleine Mechanikbox mit integrierter Steuerungslogik montiert, die auf Tippeingaben eigenständig die Gänge hoch- und runter-schaltet.

Startsteuerung (Start-Knopf)

Funktionsübersicht

Die Startsteuerung regelt das Starten des Motors über den Anlasser und verhindert gleichzeitig ein versehentliches (Wieder-)Einleiten des Startvorgangs (insbesondere bei bereits laufendem Motor). Der konventionell über das Zündschloss eingeleitete Startvorgang wird aus Komfortgründen zunehmend auch über einen Start/Stopp-Knopf realisiert (siehe Glossar unter „Keyless Entry and Go“)

Beispielhafte Motivationen

Im Rahmen der Recherche wurde auch eine Diskussion ermittelt, der die Absicht eines Fahrzeugbesitzers entnommen werden kann, einen Startknopf nachzurüsten (in einem Fahrzeug, in dem die Zündung standardmäßig ausschließlich über den Schlüssel erfolgt). Die zugrunde liegende Motivation ist hierbei, dieses vergleichsweise moderne Funktionsmerkmal auch in einem älteren Fahrzeug verfügbar zu haben.

Exemplarische Praxisbelege

Bei der in [R40] beschriebenen Veränderung soll ein zusätzlicher Druckschalter vor das Kabel zum Anlasser geschaltet und z. B. in einer Leerblende positioniert werden. Nach Einstecken des Schlüssels, Entriegeln der Lenkradsperre und Drehen auf Zündungsstellung ermöglicht dies, den Anlasser alternativ zum Weiterdrehen des Schlüssels auch (wie in vielen modernen Fahrzeugen) per Startknopf zu betätigen. Eine entsprechend durch fachlich unzureichend qualifizierte Personen durchgeführte Veränderung kann unter Umständen auch ungewollte Nebeneffekte und Gefahren bergen, die in Kapitel 5.1.2 thematisiert werden.

Servolenkung

Funktionsübersicht

Unter einer Servolenkung versteht man im Allgemeinen ein Aggregat zur Lenkkraftunterstützung. Im Zuge des Einsatzes von elektronischen Regelsystemen wurden geschwindigkeitsabhängige Lenkkraftunterstützungen möglich. Diese verstärken die Lenkkraft umso mehr, je geringere Geschwindigkeiten gefahren werden. Servolenkungen, die rein elektrisch funktionieren, werden auch elektrische Hilfskraftlenkungen genannt (vgl. auch WALLENTOWITZ, 2006).

Beispielhafte Motivationen

Motivationen für Eingriffe in die Lenkunterstützung, d. h. die so genannte Servolenkung, beziehen sich meist auf eine angestrebte Änderung der Lenkunterstützung oder des Lenkspiels. Eine beispielhafte Motivation ist eine härtere Einstellung der Lenkung, wie sie beispielsweise in Recherchequelle [R139] in einem Forum diskutiert wird.

Teils wird auch die Nachrüstung von elektro-hydraulischen Servolenkungen angestrebt, teils als Ersetzung einer vorhandenen riemengetriebenen Servolenkung durch eine elektrisch angetriebene. In [R69] wird hierzu als Hauptargument beworben, dass der Motor mehr Leistung für das Fahren umsetzen kann (vgl. hierzu auch WALLENTOWITZ, 2006, S. 134).

Exemplarische Praxisbelege

Die o. g. Änderungen an der Servolenkung waren in der Vergangenheit meist mechanische Eingriffe am Lenkgetriebe (vgl. [R62]), die für die verfolgte Zielstellung nicht zentral von Interesse sind. Dies trifft eher auf elektrohydraulische Anlagen zu, bei

denen das Lenkunterstützungsverhalten je nach Ausführung über die Veränderung der Lenkgetriebesoftware beeinflusst werden kann. Beispielsweise wurde in Recherchequelle [R139] eine Forendiskussion ermittelt, in der eine Anleitung für eine härtere Einstellung der Servolenkung per Software diskutiert und erprobt wird. Für die Realisierung bei dem betreffenden Fahrzeugtyp genügt ebenfalls das Einsetzen eines gängigen, frei erhältlichen Diagnoseproduktes.

Bezüglich der Nachrüstung als Ersetzung einer vorhandenen riemengetriebenen Servolenkung durch eine elektrisch angesteuerte wird beispielsweise in [R69] ein Nachrüst-Kit beworben. Durch Einbringen einer elektrischen Servopumpe und zugehöriger Elektronik entfällt der zuvor vorhandene Riemen-Antrieb. In [R69] wird hierbei auch darauf hingewiesen, dass für diese Erweiterung keine Allgemeine Betriebserlaubnis erhältlich ist.

Das Nachrüsten elektrischer angesteuerter Lenkunterstützungen, die sich ebenfalls adaptiv zur gefahrenen Geschwindigkeit verhalten, wird auch im Falle von Oldtimern angeboten (vgl. [R70]). Da diese Nachrüstungen Oldtimer (also Liebhaberfahrzeuge) betreffen und typischerweise deren Besitzer eine besondere Bindung zu ihrem Fahrzeug haben, ist davon auszugehen, dass zumindest die Wahl des Anbieters und der Einbau fachmännisch erfolgen.

Adaptive Niveauregulierung

Funktionsübersicht

Besonders Fahrzeuge der Oberklasse sowie Sport Utility Vehicles (SUV) bieten seit einigen Jahren oft das Leistungsmerkmal eines adaptiven Luftfederungs-Fahrwerkes, bei dm sich über die Niveauregulierung Parameter wie Federung und Dämpfung einstellen lassen. Um das Aus- und Einsteigen komfortabler zu gestalten, kann die Karosserie abgesenkt werden. Dies wird vom System in der Regel nur im Stand oder bis zu einer geringen Geschwindigkeit zugelassen (i. d. R: Schrittgeschwindigkeit).

Beispielhafte Motivationen

Mit dem Ziel, bei der normalen Fahrt im Straßenverkehr eine bessere Straßenlage zu erzielen, verfolgen Veränderungen an diesem System zunehmend das Ziel, ein „elektronisches Tieferlegen“ zu realisieren.

Exemplarische Praxisbelege

Nach Quellen wie z. B. [R45] sind bei entsprechenden Fahrzeugen rein elektronisch Tieferlegungen z. B. um bis zu 40 mm möglich. Laut [R45] ist dies häufig über gängige Diagnose-Produkte möglich. Entsprechende Eingriffe werden beispielsweise auch von vielen Tunern angeboten (z. B. [R01]).

Fahrdynamikregelsysteme

Funktionsübersicht

Systeme wie das Elektronische Stabilitätsprogramm (ESP) sowie das häufig als Teilfunktion realisierte Antiblockiersystem (ABS) und die Antischlupfregelung (ASR) dienen grundsätzlich zur Sicherung der Fahrstabilität und somit der Sicherheit der Insassen und des Verkehrs (vgl. auch HEIßING, 2008). Unter anderem sind sie zur Erfüllung ihrer Aufgabe dazu in der Lage, einzelne Räder gezielt abzubremsen.

Beispielhafte Motivationen

Anzeichen auf praktische Veränderungen an diesen Systemen fanden sich in der Recherche nur bzgl. der kompletten Deaktivierung dieser Systeme. Dies kann einerseits konstruktive Hintergründe haben, z. B. um bei Fahrtrainings den Nutzen der Systeme zu veranschaulichen, indem das System vor einer simulierten Ausnahmesituation abgeschaltet wird (vgl. [R115]). Andererseits wurden in der Mehrzahl der Fälle anderweitige Motivationen recherchiert. In Quelle [R116] werden beispielsweise „Spaß“ bzw. das „Quietschen“-lassen durchdrehender Reifen, in [R118] „richtig im Schnee driften“ als Motivation angeführt.

Die Kopplung des Bremssystems an elektronische Systeme könnte zudem Dritte zur destruktiven Motivation verleiten, unsachgemäß in die Fahrzeugsteuerung einzugreifen, z. B. durch das Einleiten unerwünschter oder das Verhindern gewünschter Bremsvorgänge, wie der akademischen Veröffentlichung [R145] entnommen werden kann.

Exemplarische Praxisbelege

Die Realisierung der Deaktivierung dieser Funktionen ist z. B. nach [R115] bei einzelnen Herstellern, z. B. über verbaute Schalter, standardmäßig möglich. Teilweise werden durch diese „ESP-Off“-Funktionen jedoch nur Teilsysteme (z. B. lediglich ASR,

siehe [R118]) deaktiviert oder ein solcher Schalter ist gar nicht vorhanden. Um auch in diesen Fällen eine Abschaltung dieser Systeme zu erreichen, findet sich eine Vielzahl von Quellen, in denen sich Nutzer gegenseitig Hilfestellungen zur Deaktivierung gegeben. In Quelle [R116] wird beispielsweise auf Anleitungen verwiesen, welche Sicherungen zu entfernen sind [R117] oder wie ein entsprechender Knopf auch in solchen Fahrzeugen nachgerüstet werden kann. Auch in Quelle [R118] werden ähnliche Ansätze diskutiert. Ein Deaktivieren der ESP-Funktion über digitale Bussignale wird zudem in Quelle [R137] diskutiert.

In Veröffentlichung [R145] wird anhand eines Testfahrzeugs praktisch demonstriert, wie durch CAN-Bus-Nachrichten (die z. B. durch eingedrungenen Schadcode generiert werden) die elektronische Steuerung über die Bremsen übernommen werden kann. Dies beinhaltet sowohl den Fall des Einleitens eines durch den Fahrer ungewollten Bremsvorgangs (was auch selektiv auf einzelnen Rädern möglich ist) als auch das Aufheben eines durch den Fahrer eingeleiteten Bremsvorgangs. In letzterem Fall hat bei dem getesteten Fahrzeug dann selbst kräftiges Betätigen des Bremspedals keinen Einfluss auf die Bremswirkung mehr.

Airbag-System/Gurtstraffer

Funktionsübersicht

Das Airbag-System ist wie die meisten Sicherheits-Systeme im „normalen Fahrbetrieb“ vom Fahrer und den weiteren Insassen i. d. R. kaum wahrnehmbar. Nur in Ausnahmefällen, d. h. bei schweren Unfällen, soll es durch geeignete Koordination der pyrotechnischen Airbag-Zündung und Gurtstraffer-Betätigung die Schwere möglicher Personenschäden reduzieren. Obwohl diese Systeme daher während der normalen Fahrzeugnutzung für die Nutzer keinen aktiven Zugewinn darstellen, stehen sie dennoch zunehmend im Fokus elektronischer Veränderungen.

Beispielhafte Motivationen

Airbags müssen häufig nach Unfallereignissen (insbesondere wenn diese mit einer Auslösung einhergingen) oder bei altersbedingten Fehlfunktionen gegen neue Exemplare ausgetauscht werden. Motivationen für Veränderungen an Airbag-Systemen können sich insbesondere daraus ergeben, dass Reparaturen speziell an diesen Systemen für den Kunden sehr teuer werden, da hier i. d. R. kein Weg an dem Kauf von Neuware vorbei führt – auch wenn das fragliche Fahrzeug bereits älterer Generation ist. Neben der Tatsache, dass der Kauf von Gebraucht- oder günstigeren Alternativprodukten bei einem sicherheitskritischen System wie dem Airbag riskant wäre, unterliegen diese auch aufgrund des enthaltenen Sprengstoffes strengen Regularien. Recherchierten Quellen wie [R49], [R50] oder [R51] kann entnommen werden, dass zunehmend Airbags aus Gebraucht- [R52] und häufig sogar Neuwagen in Autohäusern [R50] entwendet werden. Diese werden auch laut Versicherungsberichten [R53] meist nach Osteuropa verschifft und dort z. B. zur Wertsteigerung in reparierte Unfallfahrzeuge verbaut – teils nicht funktionsfähig, wie die Polizei warnt [R52].

Exemplarische Praxisbelege

Zwei mögliche Ziele von unautorisierten Veränderungen an Airbag-Systemen sollen daher an dieser Stelle näher erläutert werden.

Praktische Hinweise auf den Schwarzhandel von Airbags (insbesondere mit gestohlenen Gebrauchtgeräten) finden sich z. B. in den recherchierten Quellen [R52] und [R53]. Dass sich diese in der Folge in weiteren, potenziell typfremden Fahrzeugen wieder korrekt in Betrieb nehmen lassen, ist dagegen nicht gesichert. Insbesondere kann laut [R52] ein Problem darstellen, dass der Airbag nicht mit der Ansteuerungs-Elektronik (d. h. dem Airbag-Steuergerät) im Zielfahrzeug kompatibel ist. Ggf. könnten die einbauenden Personen mit Kenntnissen zu geeigneten elektronischen Veränderungen hier improvisierte Notlösungen umsetzen. Häufig liegt das notwendige Fachwissen beim Einbau jedoch nicht vor oder entsprechende Anpassungen wären zu teuer, sodass der korrekte Betrieb nach entsprechenden unfachmännischen Reparaturen nicht gesichert ist. Airbags, die durch entsprechende Quellen wieder „instand gesetzt“ wurden, werden laut Rechercheergebnis [R52] daher als „Mogelpackung“ bezeichnet; sie könnten ggf. nicht angemessen, gar nicht oder sogar zu Unrecht auslösen.

Ein zweites riskantes Ziel ist das Verbergen der Nicht-Funktionalität eines Airbagsystems oder einzelner seiner Komponenten. Beispielsweise könnte ein krimineller Gebrauchtwagenhändler seinen Gewinn zu steigern beabsichtigen, indem er Unfall-

fahrzeuge mit defekten oder unpassenden gestohlenen Airbag-Systemen nur äußerlich wieder instand setzt. Da gerade im Falle des Airbags die tatsächliche Funktionalität des Systems für den Käufer (bzw. die späteren Fahrzeugnutzer generell) nur in Extremsituationen zweifelsfrei feststellbar ist, wäre das Risiko einer zeitigen Erkennung aus seiner Perspektive gering. Dagegen könnten die Nutzer im schlimmsten Fall dabei auch zu ernsthaften Personenschäden kommen. Da Fahrzeuge Fehlfunktionen des Airbagsystems aus diesem Grund i. d. R. aktiv signalisieren (meist z. B. über Warnleuchten im Kombiinstrument, s. u.), erfordern auch derartige Aktionen zusätzlich elektronische Veränderungen. In der wissenschaftlichen Veröffentlichung [R54] wurde anhand eines Laborversuches demonstriert, dass sich derartige Eingriffe an heutiger Technik mit vergleichsweise geringem Aufwand realisieren lassen. Dort wird gezeigt, wie das Versuchssystem derartig verändert werden kann, dass trotz entnommenen Airbagsystems sowohl die Airbag-Warnleuchte erlischt als auch dem Werkstattpersonal bei Routineuntersuchungen mit Diagnosetestern ein fehlerfreies Airbag-System vorgetäuscht wird.

Dass vergleichbare Veränderungen auch in der Praxis betrieben werden, zeigen zum Beispiel Quellen wie [R112]: Im Kontext des Einbaus von Sportsitzen oder Tuninglenkrädern werden mit den serienmäßig vorhandenen Komponenten zunehmend auch darin enthaltene Airbags aus dem System entfernt. Um die resultierenden Fehlermeldungen zu unterdrücken, werden die entsprechenden Airbags wenn möglich softwareseitig stillgelegt oder deren korrekte Funktion durch eingelötete Überbrückungselektronik simuliert (Angebote hierzu werden in [R112] ebenfalls referenziert). [R112] zeigt jedoch auch, dass einzelne Bastler sich hierbei durch den Hersteller eine Unbedenklichkeitsbescheinigung ausstellen lassen und eine Eintragung des Umbaus vornehmen lassen, was jedoch nicht den Standardfall darstellen dürfte. Auch unabhängig vom Tuning-Kontext wird die praktische Relevanz entfernter Airbagsysteme durch Berichte wie [R97] bestätigt, wo es im Kontext der Hauptuntersuchung zum Bereich der passiven Insassensicherheit heißt: „Am häufigsten signalisierte die Kontrollleuchte des Airbags eine Fehlfunktion. Die Prüfingenieure der KÜS staunten nicht wenig, als sie bei einigen Fahrzeugen nach genauer Prüfung keinen Airbag mehr vorfanden – er war komplett demontiert.“ Weitere Hinweise für praktische Veränderungen am Airbagsystem gibt es bezüglich des Falls, dass leuchtende Warnanzeigen (vgl. auch Kapitel „Allgemeine Warnfunktionen“), die auf einen Fehler des Systems hindeuten, vorsätzlich manipuliert (z. B. abgeklemmt) werden, um teure Reparaturkosten am Airbagsystem zu sparen. Dies wird in einem weiteren Bericht im Kontext der elektronischen Hauptuntersuchung von Gutachtern berichtet (vgl. [R111]).

Längsführung

Funktionsübersicht

Die in diesem und dem folgenden Teilabschnitt behandelten Systeme zur Längs- und Querführung sind hinsichtlich potenzieller Folgen von unautorisierten Eingriffen besonders kritisch, da diese aktiv in das Fahrverhalten eingreifen können.

Das klassische Beispiel zur Längsführung ist die Geschwindigkeitsregelanlage (GRA, teils auch als Tempomat oder Cruise Control/CC bezeichnet), bei der das Fahrzeug über eine geeignete Regelung der Kraftstoffzufuhr versucht, eine durch den Fahrer vorgegebene Geschwindigkeit automatisch beizubehalten. Modernere Systeme wie insbesondere adaptive Geschwindigkeitsregelanlagen (engl. Adaptive Cruise Control/ACC) erweitern dies um die zusätzliche Berücksichtigung des Abstandes zu vorausfahrenden Fahrzeugen, sodass die Geschwindigkeit bei Bedarf automatisch reduziert bzw. das Fahrzeug abgebremst wird.

Beispielhafte Motivationen

Elektronische Eingriffe in diese Systeme werden ebenfalls zu verschiedenen Zwecken betrieben. Bezüglich einfacher Tempomaten wird teils eine Nachrüstung in Fahrzeugen angestrebt, die diese Funktion ursprünglich nicht aufweisen.

Aufgrund der komplexen Gestaltung und des hohen Integrationsgrades sind die nachgerüsteten Tempomaten vornehmlich deterministischer Natur, eine nachträglich eingebaute adaptive Regelung ist nicht bekannt. Bei ACC-Systemen versuchen viele Anwender dagegen auch häufig, diese in ihrer eigentlichen Funktion anzupassen. Insbesondere erscheint vielen Nutzern der vom ACC-System eingehaltene Mindestabstand zu vorausfahrenden Fahrzeugen als zu groß und es wird versucht, diesen zu reduzieren, Quellen, die dies belegen, finden sich in [R77], [R83] und [R84].

Exemplarische Praxisbelege

Das Nachrüsten eines einfachen Tempomaten wird, wie z. B. Quelle [R85] belegt, häufig in der Praxis betrieben. Insbesondere bei Fahrzeugen, die über ein elektronisch angebundenes Gaspedal verfügen, halten die relevanten Steuergeräte die für den Tempomaten benötigte Funktionalität teils auch bei solchen Fahrzeugen bereit, die der Hersteller ohne dieses System ausliefert. Wie [R85] hierzu schreibt, muss bei einigen Modellen lediglich der Blinkerhebel gegen die um die Tempomatbedienung erweiterte Version getauscht und diese per Software angelernt werden.

Neben den bestehenden Hinweisen zu Änderungen an ACC-Systemen in den Quellen [R77] und [R84] werden hierzu insbesondere in [R83] konkrete Anleitungen und Erfahrungen diskutiert. Dies erfolgt zumeist über entsprechendes softwareseitiges Umkonfigurieren der Software. Indem die entsprechenden Funktionen bzw. Optionen zur Mindestabstandsregelung rekonfiguriert werden, wird erreicht, dass ein geringerer Abstand zum Vordermann gehalten wird. Eine ausführliche Darstellung der Motivation und möglicher Gefahren folgt in den Kapiteln 5 und 5.2.

Querführung

Funktionsübersicht

Ein Beispiel für Querführungssysteme sind Spurhalteassistenten, die unbeabsichtigtes Überfahren von Spurbegrenzungen (Fahrbahnmarkierungen sowie natürliche Begrenzungen wie Bordsteinkanten) zu vermeiden helfen. Im Anschluss an eine Detektion kann dies sowohl über eine Warnung an den Fahrer erfolgen (Lane- Departure-Warning-System) oder ebenfalls zusätzlich anhand (leichter) Eingriffe in die Lenkung realisiert sein (Lane-Keeping-Assist-System).

Beispielhafte Motivationen

Da diese Systeme serienmäßig derzeit eher gering verbreitet sind (hauptsächlich in Oberklassenfahrzeugen verbaut), gab es in den Recherchen keine konkreten Hinweise auf Veränderungen an bestehenden Systemen.

Eine, wenn auch selten, beobachtbare Motivation ist hingegen, Querführungsassistenten bei Fahrzeugen nachzurüsten, die zuvor nicht mit einem solchen System ausgestattet sind. Ein exemplarischer Hintergrund für derartige Nachrüstungen kann z. B. die Übergabe von Fahraufgaben an ein automatisiertes System sein.

Exemplarische Praxisbelege

Ein Querführungsassistent kann mit überschaubarem Aufwand sowohl als Erweiterung einer bestehenden Längsführung als auch als eigenständiges System nachgerüstet werden. Er kann entweder als warnendes System, als regelndes System oder als kombiniertes System ausgelegt sein. Dazu wird z. B. im Innenraum unter dem Rückspiegel (vgl. [R78]) oder im vorderen Stoßfängerbereich eine Kamera angebracht. Über eine Bildverarbeitungssoftware wird das Überfahren der Fahrbahnbegrenzungsmarkierung festgestellt. Beim unbeabsichtigten Überfahren (Blinkerkonnektivität vorausgesetzt) wird eine Warnung erzeugt oder ein Eingriff in die Lenkung des Fahrzeuges vorgenommen. Der Lenkeingriff erfolgt dabei entweder aktiv durch das Aufbringen eines Lenkmoments, was entsprechende Aktoren (Stellmotoren) voraussetzt, oder passiv durch Wegnahme der Lenkunterstützung. Auch die passive Regelung kann richtungsspezifisch ausgestaltet sein, also die Wegnahme der Lenkunterstützung z. B. nur für eine Richtung (die der Begrenzungslinienüberfahrung) erfolgen.

Instrumentenkombination

Funktionsübersicht

Visuelle Anzeigen fahrrelevanter Informationen werden typischerweise in einem zentralen Anzeigeinstrument gebündelt, das gemeinhin als Instrumentenkombination oder auch Kombiinstrument bezeichnet wird. Zu den (teils über Analogzeiger) angezeigten Informationen gehören u. a. der aktuelle Stand des Wegstreckenzählers („Kilometerstand“), die aktuell gefahrene Geschwindigkeit oder anstehende Servicetermine. Zudem werden auch Warnsymbole häufig im Kombiinstrument angezeigt. Diese wurden jedoch als separate Funktion behandelt (siehe Kapitel „Allgemeine Warnfunktionen“).

Beispielhafte Motivationen

Recherchierte Motivationen für elektronische Veränderungen an der Instrumentenkombination beziehen sich auf den Wegstreckenzähler, die

Serviceintervallanzeige und das Fahrerinformationssystem (FIS).

Änderung des Wegstreckenzählers (des Kilometerstandes), dessen Inhalt zumeist in der Instrumentenkombination angezeigt wird, zählen zu den klassischsten und am weitesten verbreiteten (siehe Kapitel 4.2.1) Veränderungen an Kraftfahrzeugen. Meist wird der Kilometerstand reduziert, z. B. um den Wiederverkaufswert zu erhöhen oder Kosten bei Versicherungs- oder Leasinggesellschaften zu reduzieren. Doch auch eine Erhöhung kann als Veränderung eine Rolle spielen z. B. um bei Anrechenbarkeit von Kilometerpauschalen gegenüber dem Arbeitgeber oder der Steuer einen finanziellen Vorteil zu erzielen (vgl. [R07] und [R131]). Seit 2005 ist die Tachomanipulation/Tachojustierung nach § 22b StVG in Deutschland generell verboten bzw. strafbar und wird daher auch von Tuningbetrieben nicht mehr offiziell angeboten (vgl. auch [R110]).

Ein ebenfalls häufiger elektronischer Eingriff ist das unautorisierte Zurücksetzen der Serviceintervallanzeige in der Instrumentenkombination. Dies kann beispielsweise im Zuge eines Weiterverkaufs durch den Verkäufer erfolgen, um negative Eindrücke der Kunden (z. B. bei der Testfahrt) zu vermeiden, oder auch seitens des Besitzers selbst motiviert sein, wenn er aus verschiedenen Gründen den Servicetermin nicht wahrnehmen kann oder möchte, sich aber von der Erinnerung an den Servicetermin gestört fühlt.

Eine weitere Motivation für elektronische Veränderungen an der Instrumentenkombination bezieht sich z. B. auf das Fahrerinformationssystem (FIS). Dieses zeigt während der Fahrt verschiedene textuelle oder grafische Informationen wie z. B. den Namen des aktuell eingestellten Radiosenders. Einige Fahrzeugnutzer versuchen, das FIS z. B. mit selbst konstruierter Elektronik anzusteuern und diese so an das Fahrzeug als Ausgabemedium anzubinden (vgl. z. B. Forendiskussionen in [R02] oder [R04]). In [R145] wird zudem das Anzeigen von Falschinformationen als potenzielle destruktive Motivation genannt (z. B. Kraftstoff- und Geschwindigkeitsanzeige sowie in Form beliebiger textueller Nachrichten).

Exemplarische Praxisbelege

Bzgl. Änderungen am Wegstreckenzähler gibt es trotz des Verbotes (s. o.) dennoch Hinweise, dass dies weiterhin betrieben wird. Im weiteren Verlauf dieses Dokumentes folgende Einschätzungen eines Tuningbetriebs sowie von Gutachtern (siehe jeweils Kapitel 4.2.1) bestätigen diesen Sachverhalt zumindest teilweise. Auch im Ausland finden sich entsprechende Angebote, wie z. B. Quelle [R126] zeigt.

Die Vorgehensweise hierbei hängt ebenfalls stark von der Implementierung des Systems ab. Bei klassischen Bauweisen in älteren Fahrzeuggenerationen waren die Kilometerzähler ausschließlich mechanisch realisiert, sodass Veränderungen nicht elektronisch vorgenommen wurden (sondern z. B. durch das Vorwärtsdrehen über die Null-Stellung mit einer Bohrmaschine). Seit mehreren Jahren wird der Kilometerstand bei nahezu allen Herstellern elektronisch hinterlegt und angezeigt. Entsprechend erfordern Veränderungen daran seitdem elektronische Eingriffe.

Typischerweise werden hierzu teils frei erhältliche Diagnoseprodukte eingesetzt (z. B. [R47]). Da es für das Verstellen des Kilometerstandes auch zulässige und legale Anwendungsfälle gibt (z. B. der Austausch eines defekten bzw. beschädigten Kombiinstrumentes), wird dieser Vorgang prinzipiell unterstützt und kann deshalb, teils mangels wirksamer Schutzfunktionen, auch von unautorisierten Personen vorgenommen werden. Aus Sicherheitsgründen ist hier aber häufig nur das Anlernen von neuen Kombiinstrumenten vorgesehen, die z. B. eine Laufleistung von nicht mehr als 100 km vorweisen (vgl. [R47]). Dennoch werden am Markt auch Produkte beworben, die derartige Beschränkungen der Hersteller angeblich umgehen (z. B. [R46]). Eine weitere softwaretechnische Möglichkeit zur mittel- bis langfristigen Reduktion des Kilometerstandes ist eine Änderung der sog. K-Zahl (vgl. [R122]). Im Wesentlichen durch den Reifendurchmesser bestimmt, wird der Messeinrichtung über diesen Wert mitgeteilt, wie die eingehenden Impulse in die zurückgelegte Wegstrecke umgerechnet werden. Indem diese z. B. über eine Diagnosesoftware angepasst wird, kann diese z. B. so eingestellt werden, dass sie einen kleineren Reifendurchmesser angibt und damit die Impulse einer geringeren Wegstrecke entsprechen.

Zur Rücksetzung der Serviceintervallanzeige wird meist auf die Diagnosesoftware zurückgegriffen, was z. B. in [R45] und [R48] beschrieben ist. Bei vielen Fahrzeugen ist dies aber auch über eine definierte Tastenkombination (z. B. am Lenkstockhe-

bel) möglich, die teils auch in den Handbüchern dokumentiert ist. Dies kann beispielsweise einem der Kommentare zu Beitrag [R45] entnommen werden.

Bzgl. der Ansteuerung des Fahrerinformationssystems (FIS) wurden bei der Recherche beispielsweise einige Quellen gefunden (z. B. [R2] und [R4]), bei denen diskutiert bzw. beschrieben wird, wie durch Eingriffe in die Buskommunikation eigene Nachrichten an das FIS zur Anzeige gesendet werden können. Dies wird beispielsweise genutzt, um ein selbst gebautes MP3-Abspielgerät an das Fahrzeugnetzwerk anzuschließen und Titelinformationen direkt in der Instrumentenkombination anzeigen zu lassen. Entsprechende Eingriffe erfordern teilweise, dass andere Meldungen (z. B. von der Navigations-/Radioeinheit) unterdrückt werden, da sich diese (durch ungewollte zeitliche Überlappung der jeweiligen Anzeigetexte) gegenseitig stören würden. Da die notwendigen Informationen zu den zum Beschreiben des FIS eingesetzten Protokollen (insbesondere digitaler Art über die fahrzeuginternen Bussysteme) i. d. R. nicht öffentlich sind, müssen diese zuvor von den agierenden Personen z. T. manuell analysiert werden. Dies erfolgt oft interaktiv in den entsprechenden Communities bzw. Foren, in denen Zwischenergebnisse und Anleitungen aktiv ausgetauscht werden (vgl. Recherchequelle [R137]).

Von Seiten der Bussysteme kann auch das Anzeigen von Falschinformationen auf der Instrumentenkombination realisiert werden, z. B. durch eingedrungenen Schadcode. Dies wurde in [R145] praktisch an einem Testfahrzeug demonstriert. Am Testfahrzeug konnten so u. a. falsche Werte an die Kraftstoff- und Geschwindigkeitsanzeige übergeben sowie beliebige textuelle Nachrichten angezeigt werden.

Radio

Funktionsübersicht

Das Radio dient gleichermaßen der Unterhaltung (z. B. in Form von Musik) wie der Information (z. B. Nachrichten, Verkehrsfunk). In aktuellen Fahrzeugreihen ist es häufig in übergeordnete Einheiten wie z. B. das Navigationssystem integriert.

Beispielhafte Motivationen

In der akademischen Veröffentlichung [R145] wird darauf hingewiesen, dass nachgekaufte Radiogeräte durch den häufig vorhandenen Anschluss an die internen Bussysteme des Fahrzeugs potenziell zur Einschleusung von Schadcode genutzt werden könnten. Auch die potenzielle Motivation, für die Insassen, unerwünschte Einstellungen vorzunehmen, wird in [R145] diskutiert.

Exemplarische Praxisbelege

Praxistests, die im Rahmen der Veröffentlichung [R145] an einem Testfahrzeug vorgenommen wurden, beinhalten z. B. das Anzeigen beliebiger Nachrichten (z. B. Falschmeldungen) auf dem Display des Radios. Auch wurde demonstriert, dass eingedrungener Schadcode das Radio zum Einspielen von Signaltönen verwenden könnte. Durch das Anheben der Lautstärke auf den Maximalwert könnte der Fahrer insbesondere erschreckt und erheblich abgelenkt werden. Dem konnte im Versuch in [R145] auch durch manuelle Bedienung nicht entgegengesteuert werden.

Navigationssystem

Funktionsübersicht

Die primär zur Standortermittlung und Routenführung bestimmten Navigationssysteme haben sich in den vergangenen Jahren stark verbreitet und sind als (in das Fahrzeug) integrierte Systeme oder als tragbare Geräte auf dem Markt verfügbar.

Kernfunktionen sind die derzeit i. d. R. über GPS-Technologie (siehe Glossar) realisierte Positionsbestimmung in Verbindung mit digitalen Straßenkarten sowie Algorithmen zur Routenberechnung.

Derzeit bieten sie häufig auch eine Vielzahl weiterer, ergänzender Funktionen. Beispielsweise können unter der Bezeichnung „Points of Interest“ (POI, siehe Glossar) auch die Positionen vieler, für den Nutzer potenziell interessanter Objekte in der digitalen Karte eingeblendet werden. Hierzu können z. B. die Standorte gastronomischer Betriebe oder auch touristische Sehenswürdigkeiten zählen.

Als eine weitere Funktion, die im Folgenden relevant ist, haben einige Navigationssysteme eine sog. Fahrschulfunktion implementiert, bei der Informationen wie z. B. die aktuelle Geschwindigkeit und ggf. Blinkrichtung zusätzlich über das geräteeigene Display angezeigt werden (z. B. damit Fahrlehrer und ggf. Prüfer diese Anzeigen besser einsehen können).

Beispielhafte Motivationen

Gerade bezüglich dieser heute immer weiter verbreiteten Systeme wurde bereits ein breites Spektrum häufiger Motivationen zu ihrer Veränderung ermittelt.

Ein naheliegendes, vielfach anzutreffendes Beispiel ist das Nachinstallieren von Kartendaten. Da für das Nachinstallieren weiterer Länderkarten sowie auch für die Aktualisierung bereits in einer alten Version erworbener Länderkarten finanzielle Kosten entstehen, liegt hier die Motivation vieler Fahrzeugbesitzer nahe, diese Erweiterungen und Aktualisierungen kostenlos zu bekommen.

Jedoch sind für viele Fahrer nicht nur gastronomische oder touristische Informationen als POI von Interesse. Zunehmend werden auch Erweiterungen nachgefragt, die zur rechtzeitigen Warnung auch die Standorte stationärer Messeinrichtungen anzeigen, die der Verfolgung von Geschwindigkeits- und Abstandsverstößen dienen (vgl. auch „Geschwindigkeitsmesseinrichtungen", Kapitel 2.1.2).

Während sich der bestimmungsgemäße Zweck der o. g. Fahrschulfunktion, wie der Name sagt, auf Fahrzeuge von Fahrschulen bezieht, fanden sich in den Recherchen Anzeichen dafür, dass vereinzelt auch normale Fahrzeugnutzer eine Aktivierung dieser Funktion anstreben (z. B. damit die Anzeigen auch für die Mitfahrer besser einsehbar sind).

Auch bzgl. weiterer, allgemeiner Änderungen und Erweiterungen an Navigationssystemen gibt es insbesondere im Internet Projekte, die sich damit befassen, entsprechende eigene Änderungen an den im System gespeicherten Betriebsdaten vorzunehmen. Eine recherchierte Motivation kann beispielsweise darstellen, die beim Systemstart angezeigte Herstellergrafik durch ein beliebiges eigenes Bild zu ersetzen (vgl. z. B. [R31]).

Weitere relevante Motivationen für elektronische Veränderungen, die sich auch auf das Navigationssystem beziehen, wurden in der vorliegenden Studie aus Gründen der passenderen Zuordnung anderen Komponenten zugeordnet: Die häufig im Navigationssystem implementierten TV-Systeme werden im Text zum Video-System behandelt (im vorliegenden Kapitel 2.1.1) und das Einspielen ver-/oder gefälschter Verkehrsmeldungen über das RDS/TMC-Protokoll (siehe Glossar) in Kapitel 2.1.2 unter „Funkschnittstellen“ vorgestellt.

Exemplarische Praxisbelege

Bezüglich des Nachinstallierens von Kartendaten werden in vielen Foren wie z. B. [R105], [R106] und [R124] Fragen und Anleitungen zum Kopieren von Navigations-CDs und DVDs gegeben, die seitens vieler Hersteller seit einigen Jahren mit Kopierschutzverfahren gesichert sind.

Obwohl der Einsatz von POI-Erweiterungen mit Standorten von Geschwindigkeitsmesseinrichtungen in Deutschland illegal ist, was teils auch in Foren wie [R104] angemerkt wird, werden diese bei den Anwendern vielfach nachgefragt und von einigen renommierten Herstellern insbesondere portabler Navigationsgeräte explizit unterstützt und beworben (beispielsweise bietet in [R130] ein Hersteller auf seiner Homepage einen entsprechenden Dienst an). Zudem bieten Portale wie [R107] umfangreiche Datenbanken mit Informationen zu stationären sowie mobilen Geschwindigkeitsmesseinrichtungen sowie vorgefertigt als POI-Liste für viele verbreitete Navigationsgeräte zum Download an. Dadurch, dass lediglich der Einsatz im Fahrzeug (siehe § 23 1b StVO sowie Kapitel 2.1.2), nicht jedoch der Vertrieb dieser Systeme verboten ist, ist anzunehmen, dass deren praktischer Einsatz erheblich gefördert wird, zumal sich viele Nutzer des Verbotes entsprechenden POI-Materials nicht bewusst sind (wie z. B. in der Diskussion in [R104] deutlich wird).

Die Aktivierung einer teils im Navigationssystem implementierten Fahrschulfunktion kann i. d. R. über gängige Diagnosesoftware erfolgen. Hinweise darauf, dass auch Nutzer außerhalb des Fahrschulumfelds von dieser Möglichkeit Gebrauch machen, finden sich beispielsweise in den Kommentaren der Quelle [R45], bei denen ein Nutzer diese Möglichkeit beschreibt.

Anleitungen bzw. freie Software und Diskussionsforen zu Änderungen an den Betriebsdaten verschiedener Navigationssysteme werden z. B. auf Internetseiten wie [R8] und [R31] angeboten. Hierbei werden in der Regel die Daten eines originalen Software-Updates des Herstellers (welches nach dem Brennen und Einlegen einer entsprechenden Update-CD/DVD eingespielt werden kann) gezielt bearbeitet, um die gewünschten Änderungen zu erzielen. In den genannten Quellen beschränken sich die Akteure dabei noch auf vergleichsweise ungefährliche, optische Veränderungen wie insbesondere das Ändern des Bootlogos, welches bei System-

start eingeblendet wird. Prinzipiell wären durch vergleichbare Eingriffe jedoch auch Änderungen im Programmablauf denkbar, welche die eigentliche Funktion des Gerätes oder gar sein Verhalten im automotiven Gesamtsystem betreffen können. Im Rahmen der systembedingt zulässigen bzw. möglichen Buszugriffe könnten hierdurch auch weiterreichende Risiken für die Verkehrssicherheit entstehen. Zwar ist das Navigationssystem heute i. d. R. noch ausschließlich Konsument fahrkritischer Daten wie z. B. der aktuellen Geschwindigkeit (die zur Korrelation mit den GPS-Positionsdaten einbezogen werden) und kann diese nicht aktiv beeinflussen[1]. Wie aktuelle Entwicklungen z. B. des Herstellers Nissan zeigen [R91], sind jedoch auch bereits aktive Eingriffe des Navigationssystems in die Motor- und Getriebesteuerung als zulässige Interaktionen möglich, wie z. B. das frühzeitige Abbremsen per Motorbremse vor scharfen Kurven. Für derartige zulässige Interaktionen muss jedoch die herkömmliche (typischerweise durch ein Gateway-Steuergerät implementierte) Trennung zwischen dem Infotainment und dem Antriebsstrangnetzwerk reduziert werden. Dies könnte bei entsprechenden Softwareveränderungen im Infotainmentbereich gezielt für aktive Eingriffe in die Fahrfunktionen missbraucht werden. Auch wenn entsprechende Systeme in Deutschland (noch) nicht zugelassen sind, könnte sich diese Problematik z. B. durch einreisende ausländische Fahrzeuge auch im deutschen Straßenverkehr auswirken.

In den letzten Jahren sind Hersteller integrierter Navigationssysteme dazu übergegangen, die Integrität von Karten-Medien und Softwareupdates über Kopierschutzmaßnahmen und wirksamere integritäts- und authentizitätssichernde Maßnahmen gegen illegale Vervielfältigung und Manipulationen abzusichern (vgl. CLAUSING et al., 2009) Wie durch die zuvor genannte Quelle in Erfahrung gebracht wurde, hat dies als ein wesentlicher Faktor dazu beigetragen, dass die Aktivität der o. g. Projekte seitdem zurückgegangen ist und einzelne auch eingestellt wurden.

[1] Entsprechende Bus-Nachrichten werden in den Busnetzwerken vieler Fahrzeuge daher derzeit nur aus dem Antriebsstrang-Subnetz (z. B. von Motor-, Getriebe- oder ABS/ESP-Steuergerät) in das Infotainment-Subnetz (zum Navigationssystem) weitergeleitet und nicht umgekehrt.

Video-System (TV, Car-PCs etc.)

Funktionsübersicht

Für viele moderne Fahrzeuge bieten die Hersteller ein Video-System als Ausstattung an, das z. B. häufig als Teilfunktion in die integrierten Navigationssysteme implementiert ist. Es bietet typischerweise Schnittstellen zu Unterhaltungsmedien wie DVD-Playern oder TV-Systemen. Über teils dazu vorhandene Video-Eingänge können zudem weitere Signalquellen angeschlossen werden wie z. B. PC-Technik (z. B. Car-PCs, vgl. [R03] oder [R09]).

Beispielhafte Motivationen

Der Betrieb von Unterhaltungsfunktionen über entsprechende Video-Systeme ist derzeit jedoch meist nur unter Restriktionen möglich: In der Regel wird der Betrieb dieser Systeme (z. B. der Video-/Fernsehmodus oder das Anzeigen von Videotext, vgl. [R30]) während der Fahrt für den Fahrer nicht zugelassen. Dies ist offensichtlich Sicherheitsgründen geschuldet – hauptsächlich, damit der Fahrer nicht abgelenkt wird. Derzeit ist in Deutschland das Schauen von TV nach vorliegendem Kenntnisstand nicht verboten (vgl. z. B. § 23 StVO). Da eine übermäßige Ablenkung des Fahrers jedoch auch hier nicht unrealistisch ist, sind viele (insbesondere europäische) Hersteller aus Vernunftgründen eine freiwillige Selbstverpflichtung eingegangen, die sich nach den Empfehlungen der Europäischen Kommission zur sicheren Gestaltung der Mensch-Maschine-Schnittstelle richtet, dem so genannten European Statement of Principles on Human Machine Interaction (ESoP, siehe auch ESoP, 2007 im Literaturverzeichnis). Entsprechend werden stark ablenkende Unterhaltungsfunktionen, die insbesondere visueller Form sind, in den vertriebenen Fahrzeugen (auch in Deutschland) während der Fahrt unterbunden.

Aus diesem Grund ist das Ziel, das bei Veränderungen dieses Systems am häufigsten verfolgt wird, das Fernsehen auch während der Fahrt zu ermöglichen. Dieses Ziel von Eingriffen in die Fahrzeugelektronik wird oft auch als TV-in-Motion bzw. allgemein als Video-in-Motion (VIM) bezeichnet.

Exemplarische Praxisbelege

Aufgrund der genannten Motivationen ist daher auch das Video-System ein weiteres häufiges Ziel von unautorisierten elektronischen Veränderungen.

Wie dieser Eingriff erfolgt, hängt stark von der Implementierung des Video- bzw. TV-Systems ab. Oft ist dieses im Navigationssystem integriert (siehe auch gleichnamiger Abschnitt). Typische Vorgehensweisen der Hersteller sind das Prüfen der aktuellen Geschwindigkeit oder der angezogenen Handbremse. Wird die Handbremse zur Fahrt gelöst bzw. eine gewisse Grenzgeschwindigkeit (hier wird in aller Regel Schrittgeschwindigkeit angesetzt) überschritten, wird die (visuelle) TV-Ausgabe unterbrochen. Um an diese Informationen zu gelangen, werten die TV-Systeme in der Regel die entsprechenden Signale (Geschwindigkeit, Handbremskontakt) aus, die je nach Fahrzeuggeneration auf analogen Leitungen oder über digitale Bussysteme übertragen werden.

Praktisch kann ein Eingriff (je nach Implementierung) erfolgen, indem z. B. bei analogen Signalleitungen die entsprechenden Kabel durchtrennt oder auf Masse gelegt werden (vgl. [R36]). Für modernere Fahrzeuggenerationen, welche die Informationen digital über die Fahrzeug-Bussysteme beziehen, werden am Markt teils Filterboxen angeboten, die der Busleitung zwischengeschaltet werden und die relevanten Signale verändern (vgl. [R37]).

Recherchierte Quellen wie [R108] zeigen, dass es Länder gibt, in denen laut Gerichtsurteil das Fernsehen während der Fahrt auch für den Fahrer aktuell explizit gesetzlich zulässig ist und diese Funktion von den Kunden (in [R108] Taxifahrer) offensichtlich aktiv genutzt wird. Vermutlich auch aus diesem Grund sehen viele im Weltmarkt aktive Fahrzeughersteller (die auch in diesen Ländern Fahrzeuge verkaufen wollen) vor, dass diese Beschränkung (z. B. für solche Märkte) auch zulässigerweise aufgehoben werden kann. Dies kann insbesondere über die Diagnoseschnittstelle erfolgen oder teils bei älteren Fahrzeugen auch über gewisse Tastenkombinationen (z. B. am Navigationssystem). Entsprechend kodierte TV-Systeme können das Fernsehen bis zu höheren Geschwindigkeiten oder gänzlich uneingeschränkt zulassen. Nach öffentlich zugänglichen Anleitungen z. B. in [R41] und [R42] können derartige Kodierungen auch in Deutschland von unautorisierten Personen und ohne Berücksichtigung eventueller gesetzlicher Vorgaben vorgenommen und bei Bedarf wieder zurückgesetzt werden. Für entsprechend vorzunehmende Umkonfigurationen über die Diagnoseschnittstelle genügt dabei meist gängige Diagnosesoftware. Für die Fahrzeuge vieler Hersteller ist solches Zubehör über Dritthersteller (z. B. [R39]) frei erhältlich, da es auch für gängige Wartungszwecke, z. B. in freien Werkstätten, eingesetzt wird.

Eine weitere, nicht-technische Möglichkeit, auch beim Fahren dennoch TV schauen zu können, besteht selbstverständlich auch in dem Benutzen marktüblicher tragbarer Geräte.

Allgemeine Warnfunktionen

Funktionsübersicht

In modernen Fahrzeugen findet sich eine Vielzahl von Warnfunktionen, die z. B. auf Ausfall oder Fehlfunktionen von (sicherheitskritischen) Komponenten hinweisen sollen.

Ein Beispiel für eine derartige Warnfunktion wurde z. B. bereits im Kontext des Airbagsystems (s. o.) genannt, bei dem Fehler im Airbag-System bzw. an einzelnen Airbags über eine Warnleuchte im Kombiinstrument angezeigt werden.

Auch zunehmend integrierte Funktionen zur Reifendruckkontrolle (RDK) überprüfen regelmäßig den Reifendruck und zeigen dem Fahrer im Bedarfsfall eine Warnung bzgl. zu niedrigen (oder zu hohen) Reifendrucks an. Je nach Implementierung arbeiten diese Systeme z. B., indem sie den Radumfang dynamisch anhand der Räderdrehzahl und ABS/ESP-Sensoren berechnen und bei einer relevanten Änderung ein Warnsymbol im Kombiinstrument setzen (vgl. Kommentar in Quelle [R45]). Aber auch drahtlos angebundene Reifendrucksensoren werden zunehmend eingesetzt (vgl. Quelle [R146]).

Ein drittes relevantes Beispiel ist der Gurtwarner. Diese Funktion ist dafür bestimmt, als Erinnerung

Bild 4: Exemplarische Gurtwarnung (optischer Teil)

einen Warnton auszulösen, sofern eine im Fahrzeug sitzende Person ihren Sicherheitsgurt nicht angelegt hat und die Zündung eingeschaltet bzw. der Motor gestartet wird. Meistens wird gleichzeitig eine optische Warnung angezeigt, wie Bild 4 zeigt. Dazu werden entsprechende Sensoren abgefragt, die in der Regel (in Form einer integrierten Sitzbelegungsmatte) das Gewicht messen, das auf den Sitz einwirkt. Wird durch diese Sensoren ein – als belegt erscheinender – Sitz erkannt, bei dem der Gurt nicht eingesteckt ist, erfolgt eine Warnung, die i. d. R. optisch und akustisch ausgegeben wird.

Beispielhafte Motivationen

Ein wichtiger Faktor für die Effektivität dieser Funktionen ist, dass sie von dem Fahrer auch wahrgenommen und sachgemäß beachtet werden. Gerade dies ist jedoch häufig nicht der Fall. Wie in [R97] aus Erfahrungen bei Hauptuntersuchungen berichtet wird, ignorieren einige Autofahrer Warn- und Fehlermeldungen, die in der Armaturentafel auf Mängel hinweisen. Insbesondere akustische Signale, die gerade auf besonders dringliche Fehler hinweisen sollen, werden darüber hinaus häufig als störend empfunden, sodass es über das simple Ignorieren der Meldungen hinaus häufig Bestrebungen der Fahrer gibt, diese gänzlich zu deaktivieren.

Gerade auch bzgl. des oben vorgestellten Gurtwarners wird als häufiges Eingriffsziel das Deaktivieren dieser Funktion angestrebt. Häufiger Grund für diese Motivation ist laut der Quelle [R45], dass viele Fahrer das Warnsignal als lästig empfinden, da die Sitzbelegungserkennung häufig schon beim Transport schwerer Reisetaschen ein Tonsignal aussendet oder der (Bei~)Fahrer z. B. berufsbedingt oft ein- und aussteigen muss.

Aber auch das Aktivieren einer implementierten Warnfunktion kann eine beobachtbare Motivation von Fahrzeugnutzern sein, sofern diese Funktion im Fahrzeug serienmäßig nicht aktiviert ist. Dies wurde in den Recherchen z. B. bzgl. der Reifendruckkontrolle ermittelt (siehe Kommentar in Quelle [R45]).

In der akademischen Quelle [R146] wird zudem die potenzielle Motivation betrachtet, dass ein externer Angreifer einen Fahrer zum Anhalten verleiten möchte (ggf. als Vorbereitung krimineller Aktivitäten), indem er eine zu Unrecht ausgelöste Reifendruckwarnung provoziert.

Exemplarische Praxisbelege

Anleitungen zur Deaktivierung dieser Funktion finden sich z. B. in der recherchierten Quelle [R45] oder können von Tuningwerkstätten vorgenommen werden [R01], [R109]. Da sich manche Werkstätten mit Verweis auf die gesetzlichen Vorschriften jedoch weigern, diese Funktion zu deaktivieren, wird diese Veränderung laut [R45] häufig von den Besitzern mit der entsprechenden Ausstattung frei verfügbarer Diagnosesoftware (z. B. [R39]) selbst vorgenommen. Hierdurch kann jedoch indirekt auch die Insassensicherheit gefährdet werden (insbesondere bei unfachmännischem Vorgehen durch das Abtrennen bzw. Verändern/Manipulieren der Warnelemente (Aktoren) oder gar der Sensoren wie der Sitzbelegungsmatten, vor dem in [R81] gewarnt wird), worauf in Kapitel 5.1.3 noch vertieft eingegangen wird.

Ein recherchiertes Beispiel zum Freischalten einer serienmäßig nicht aktivierten Funktion ist das Einkodieren der Reifendruckkontrolle, was laut [R45] bei einigen Fahrzeugen möglich ist und in der Praxis betrieben wird. Laut der Quelle kann dies bei entsprechenden Fahrzeugen realisiert werden, indem Taster und ein Kabelsatz nachträglich eingesetzt werden und über gängige Diagnose-Software eine Freischaltung der Funktion im ABS-Steuergerät vorgenommen wird.

In der akademischen Quelle [R146] wird in einem Praxistest ein Angriff auf ein modernes Fahrzeug demonstriert, welches drahtlos angebundene Reifendrucksensoren besitzt. Es wird gezeigt, dass sich durch das Fälschen von Funksignalen von außen unzutreffende Reifendruckwerte an das Fahrzeug übermitteln lassen, wodurch eine Reifendruckwarnung provoziert werden kann.

Schließsystem

Funktionsübersicht

Das Schließsystem dient der Zugangskontrolle zum Fahrzeug. Primärer Zweck des Systems ist der Einbruchschutz, d. h., es soll das ungehinderte Eindringen in den Innenraum unterbinden bzw. so weit erschweren, dass der potenzielle Dieb nach einer gewissen Zeitspanne den Versuch abbricht, sich unautorisierten Zugang zum Fahrzeug zu verschaffen. Hiermit richtet sich das System explizit gegen absichtliche Eingriffe und Manipulationen und stellt damit ein Sicherheitssystem im Sinne der Security dar.

Ausgehend von klassischen mechanischen Schlüsselsystemen bieten aktuelle Schließsysteme dem Fahrer zumeist auch eine (z. B. in den Schlüssel integrierte) Fernbedienung, mit der er das Fahrzeug aus der Entfernung auf- und zuschließen kann – was durch das Fahrzeug meist über ein Aufleuchten der Blinker bestätigt wird. Ein Beispiel für eine in der Folge relevante Teilfunktion des Schließsystems ist die teils implementierte Autolock-Funktion. Diese Funktion verriegelt das Fahrzeug automatisch bei Erreichen einer Geschwindigkeit von z. B. 15 km/h und öffnet es dann z. B. erst bei Abziehen des Zündschlüssels wieder. Diese Funktion wird von den Herstellern teilweise für den Weltmarkt als Schutz gegen Car-Jacking (siehe Glossar) angeboten.

Beispielhafte Motivationen

Für Veränderungen an diesem System, die durch den Besitzer selbst erfolgen, sind vergleichsweise wenige Nachweise zu finden. Ein Beispiel ist das softwareseitige Aktivieren der o. g. Autolock-Funktion, das z. B. laut einem Nutzer in den Kommentaren zu Quelle [R45] eine beliebte Änderungsoption ist, z. B. da sie von einigen Kunden teils auch als geeignete Kindersicherung angesehen wird.

Der Großteil der bekannten Veränderungen am Schließsystem wird allerdings seit jeher hauptsächlich aus Diebstahls-Motivationen heraus betrieben. Hauptsächliche Motivation hierzu ist daher das unberechtigte Eindringen in den Fahrzeuginnenraum, z. B. um Wertgegenstände oder in der Folge das gesamte Fahrzeug zu entwenden.

In [R145] wurde als weitere potenzielle destruktive Motivation das Einsperren der Fahrzeuginsassen betrachtet, welches z. B. durch eingeschleusten Schadcode erfolgen kann, der die Kontrolle über das Schließsystem übernimmt.

Exemplarische Praxisbelege

Bzgl. der nachträglichen Aktivierung der Autolock-Funktion finden sich in Quelle [R45] Hinweise. Sofern diese bereits implementiert, jedoch seriemäßig nicht aktiviert ist, genügen hierzu wie in [R45] besprochen i. d. R. gängiges Diagnosezubehör und entsprechende Anleitungen.

Der Rest dieses Teilabschnittes zeigt das Spektrum recherchierter Möglichkeiten zum unautorisierten Eindringen in das Fahrzeug (s. o.) an einigen exemplarischen Beispielen auf.

Bereits klassische Schließsysteme, die rein mechanisch arbeiten, sind das primäre Ziel von Einbrechern gewesen. Für viele entsprechende Systeme ist es bereits auf mechanische Art und Weise möglich, relativ unkompliziert in das Innere des Fahrzeugs einzudringen (vgl. [R05]) und dort entweder Gegenstände zu entwenden oder mögliche weitere Manipulationen vorzunehmen. Dies erfolgt oft mittels vorgefertigter Generalschlüssel – im Jargon auch „Polenschlüssel“ genannt (z. B. [R33] oder weitere Spezialwerkzeuge wie z. B. in Quelle [R34] vertrieben). Während diese mechanischen Eingriffe nicht im Fokus stehen, spielen sie teilweise jedoch auch bei weiteren elektronischen Eingriffen eine Rolle (vgl. folgender Teilabschnitt „Diebstahlwarnanlage“).

Moderne Schließsysteme in heutigen Automobilen sind fast ausschließlich elektronisch gesteuert und funktionieren zumeist (auch) kontaktlos, d. h. über Funktechnologien[2]. Die leichte Überwindbarkeit rein mechanischer Schließsysteme in der Vergangenheit ist mit ein Grund dafür, warum heute von den Fahrzeugherstellern insbesondere in diesem Bereich (zusammen mit der Wegfahrsperre, s. u.) bereits vergleichsweise starke elektronische Sicherheitsmaßnahmen getroffen werden, die i. d. R. auf Kryptografie basieren. Doch auch für modernere elektronische Sicherungen in diesem Anwendungsbereich gibt es Möglichkeiten für Veränderungen, die dann ebenfalls elektronischer Natur sind.

Frühe elektronische Systeme (teils infrarotbasiert), bei denen die Fernbedienung eine für ein gegebenes Fahrzeug feststehende Codesequenz sendet, konnten in einigen Fällen durch einfache Replay-Angriffe ausgehebelt werden. Hierzu wurde ein normaler Vorgang der Fahrzeugöffnung mittels der Fernbedienung über geeignete Sensoren (z. B. Photosensoren bzw. Funkantennen) aufgezeichnet (z. B. durch eine in der Nähe des Fahrzeuges versteckte Person) und zu einem späteren Zeitpunkt über eigene Sende-Hardware wieder abgespielt (vgl. z. B. [R76]).

2 Aufgrund der über Funk erfolgenden Kommunikation zum Fahrzeugschlüssel, der sich beim Anwendungsfall der Fahrzeugöffnung in der Peripherie des Fahrzeugs befindet, könnte man dies auch als Kommunikation mit der Infrastruktur betrachten. Durch den starken Bezug zum Fahrzeug selbst soll diese Funktion hier jedoch als Kfz-System gewertet und daher nicht als drahtlose Kommunikation mit Infrastrukturkomponenten in Kapitel 2 behandelt werden.

Bei heutigen Systemen ändern sich die von den Fernbedienungen gesendeten Codes daher i. d. R. bei jedem Zugriff, z. B. auf Basis von sog. Rolling Codes oder Challenge-Response-Verfahren (vgl. WOLF, 2009, S. 50-52). Dadurch kann die erneute Wiedergabe eines aufgezeichneten Telegramms zu einem späteren Zeitpunkt vom Fahrzeug erkannt und abgelehnt werden. Dennoch sind, zumindest aus akademischer Sicht, bereits Angriffe auf diese Systeme bekannt. Je nach Implementierung können Challenge-Response-Verfahren beispielsweise durch den so genannten Mafia-Angriff (vgl. WOLF, 2009, S. 51) umgangen werden. Diese Systeme senden eine stets wechselnde Aufgabe an den Schlüssel, die nur dieser mit der Kenntnis eines gemeinsamen Geheimnisses korrekt beantwortet werden kann. Bei dem Mafia-Angriff wird diese Aufgabe durch den falschen Schlüssel über eine geeignete Kommunikationsverbindung an einen Komplizen geschickt, der sich in der Nähe des echten Fahrers und seines Schlüssels befindet, an den diese Aufgabe gefunkt wird. Die korrekte Antwort wird anschließend an den Angreifer zurück übermittelt, der die Aufgabe dem Fahrzeug gegenüber ebenfalls korrekt beantwortet. Zudem wurde kürzlich in der Forschung ein hardwarenaher Angriff auf ein kommerzielles Schließsystem demonstriert (vgl. [R71], [R72]). Den Forschern gelang es, durch eine sog. differentielle Stromanalyse (Differential Power Analysis/DPA) und eine differentielle elektromagnetische Analyse (Differential Electro-Magnetic Analysis/DEMA) einen herstellerweit gültigen Generalschlüssel zu ermitteln. Während dieser Teil des Angriffs derzeit noch mit einem erheblichen Aufwand für den Angreifer verbunden ist, genügt anschließend das Mitlesen zweier Nachrichten zwischen Sender und Empfänger (also z. B. Funkfernbedienung und Fahrzeug), um für ein konkretes System eine geklonte Fälschung des Schlüssels herzustellen.

Ein weiterer genereller Angriff auf Drahtlosprotokolle des Schließsystems besteht im so genannten Jamming (siehe Glossar), d. h. dem gezielten Stören der Kommunikation bei einem üblichen Vorgang (insbesondere beim Verschließen des Fahrzeuges). Nähere Details zur technischen Realisierung finden sich unter „Funkschnittstellen“ in Kapitel 2.1.2. Merkt der Fahrer nicht, dass z. B. das Verschließen des Fahrzeuges über die Fernbedienung nicht erfolgt ist (z. B. indem ihm nicht auffällt, dass das als Bestätigung dienende Blinken des Fahrzeuges ausbleibt), hat der Angreifer fortan freien Zugang zum nicht verriegelten Fahrzeug [R05].

In der akademischen Veröffentlichung [R145] wurde in praktischen Versuchen an einem Testfahrzeug demonstriert, dass die Fahrzeugnutzer durch die elektronische Ansteuerung der Türschlösser ein- bzw. ausgesperrt werden könnten. Im Beispiel aus [R145] erfolgte dies von Seiten des Busnetzwerks aus und könnte von einem Angreifer z. B. in Form eingeschleusten Schadcodes eingesetzt werden.

Diebstahlwarnanlage

Funktionsübersicht

Eine Diebstahlwarnanlage (DWA) dient dazu, Einbruchsversuche in das Fahrzeug zu erkennen. In diesem Fall werden üblicherweise über Aktoren wie Hupe oder Blinker Warnsignale generiert, die Personen im Umfeld auf das Ereignis aufmerksam machen sollen. Prinzipiell kann auch über Drahtlosschnittstellen (siehe Kapitel 2.1.2) wie verbaute Mobilfunkkomponenten ein Notruf abgesetzt werden. Zur Erkennung von Einbruchsversuchen können vorhandene Sensoren genutzt werden, um das Öffnen von Türen oder z. B. Erschütterungen zu detektieren.

Beispielhafte Motivationen

Die potenziell häufigste Motivation für elektronische Veränderungen an der DWA ist vermutlich das Ziel, die DWA zu deaktivieren bzw. zu umgehen. Unberechtigte Personen können dies anstreben, um unauffälliger Diebstähle vornehmen zu können. Eine Deaktivierung kann in Einzelfällen jedoch auch von berechtigten Personen angestrebt werden: In Recherchequelle [R141] führt beispielsweise ein Diskussionsteilnehmer an, seine DWA aufgrund einer Fehlfunktion bis zur Beseitigung der Ursache deaktivieren zu wollen (ggf. um die Belästigung für die Nachbarschaft zu reduzieren und die Batterie zu schonen).

Als ebenfalls beobachtbare Motivation mit eher konstruktivem Hintergrund kann die Absicht eingestuft werden, eine Diebstahlwarnanlage zum Schutz eines Fahrzeugs nachzurüsten, d. h. als neu hinzukommender oder ergänzender Schutzmechanismus.

Ein drittes Beispiel für eine Motivation mit Bezug zur Diebstahlwarnanlage wurde als Folge der Tatsache beobachtet, dass sich bei Einbruchsversuche am Schließsystem unter Verwendung der im

zugehörigen Kapitel vorgestellten „Polenschlüssel“ durch die Betätigung des Schließzylinders bei einzelnen Fahrzeugen auch die Diebstahlwarnanlage automatisch abschaltet (wie sie es auch beim Öffnen mit dem Originalschlüssel tut). Laut Quelle [R44] kann aus dieser Tatsache teils die Motivation resultieren, dieses Problem zu beheben, damit die Diebstahlwarnanlage bei Einsatz dieser „Polenschlüssel“ sich nicht abschaltet, sondern den Eingriff erkennt und einen Alarm auslöst.

Exemplarische Praxisbelege

Für eine Deaktivierung bzw. Umgehung der DWA werden in Quelle [R141] verschiedene Ansätze diskutiert. Beginnend mit eher physischen Eingriffen wie dem Entfernen von Sicherungen (für DWA oder Hupe und Blinker) oder dem elektrischen Abtrennen der betreffenden Elemente werden auch softwarebasierte Lösungen, insbesondere über frei verfügbare Diagnoseausstattung, diskutiert.

Mit Blick auf die erwähnte Motivation, eine DWA nachzurüsten, werden auf dem Markt Nachrüst-Kits angeboten, mit denen eine WFS-Funktion nachträglich eingebaut werden kann. Beispielsweise wird in Recherchequelle [R132] ein Nachrüstsatz vertrieben, der als ausschließlich lesender Busteilnehmer an bestehende CAN-Busse angeschlossen wird und nach Aktivierung die fahrzeuginterne Kommunikation auf Einbruchsanzeichen wie die oben genannten beobachtet.

Bezüglich der – bei einigen Fahrzeugen auftretenden – automatischen Deaktivierung der Wegfahrsperre beim Einsatz von „Polenschlüsseln“ wurden im Rahmen der Recherche auch Anleitungen ermittelt, die dieser Tatsache entgegenwirken. Nach Quelle [R44] ist es bei einigen der betroffenen Fahrzeuge per Software möglich, die Funktion des automatischen Entschärfens bei Betätigung des Schließzylinders zu deaktivieren. Nach der Vornahme dieser auch „Anti-Polenschlüssel“ genannten Kodierung (vgl. [R44]) wird fortan auch ein Einsatz dieser Einbruchswerkzeuge als Alarm wahrgenommen. Obwohl der Fahrer dann die Diebstahlwarnanlage zunächst manuell deaktivieren muss, bevor er das Fahrzeug mit dem echten Schlüssel öffnet, wird diese Änderung zugunsten des Diebstahlschutzes auch in der Praxis betrieben.

Wegfahrsperre

Funktionsübersicht

Die Wegfahrsperre (WFS) soll in modernen Fahrzeugen unautorisierte Personen daran hindern, das Kfz zu nutzen.

Beispielhafte Motivationen

Elektronische Eingriffe in und um dieses System erfolgen hauptsächlich zu dessen Umgehung bzw. Deaktivierung. Diese Motivation ist hauptsächlich in kriminellen Kreisen einzuordnen, z. B. zur initialen Entwendung eines Fahrzeugs oder um gestohlene Fahrzeuge auch langfristig wieder fahrbereit zu machen.

Als weitere, eher konstruktiv begründete Motivation konnte auch das Bestreben recherchiert werden, eine Wegfahrsperre an Fahrzeugen nachzurüsten, die eine solche serienmäßig nicht aufweisen (z. B. um Versicherungsanforderungen zu erfüllen).

Exemplarische Praxisbelege

Eine Quelle [R38] zeigt, wie eine WFS in einem Mittelklasse-Fahrzeug überwunden wird und das Fahrzeug dann zur unautorisierten Benutzung bereitsteht. Dabei ist aber davon auszugehen, dass sich die betreffende Person auf die WFS dieses Fahrzeugtyps spezialisiert hat. Auch in Quellen wie [R127] wird diese Thematik diskutiert.

Wie oben erwähnt werden Wegfahrsperren teilweise auch nachgerüstet, wozu es auf dem Markt verschiedene Angebote für Nachrüst-Kits gibt. Als Beispiel sei auf die Wegfahrsperrenfunktion der bereits im Kapitel zur Motorsteuerung aufgeführten Tuningbox aus [R123] verwiesen.

Lichtanlage (Steuerprogramme und Frontscheinwerfer)

Funktionsübersicht

Die Lichtanlage realisiert alle Funktionen, die das Beleuchtungssystem betreffen, d. h., sie koordiniert die Steuerung von Frontscheinwerfern, Rücklichtern, Richtungswechselanzeigen und sämtlicher weiterer Lichtelemente (z. B. Begrenzungsleuchten). Per Elektronik kann die Lichtsteuerung zunehmend durch Steuerprogramme automatisiert werden. Hierzu gehören z. B. die so genannten

Coming-Home/Leaving-Home-Funktionen, die nach dem Verlassen/vor dem Einsteigen Lichtelemente des Fahrzeuges für einen bestimmten Zeitraum aktivieren. Ein anderes Beispiel ist das so genannte Abbiege- oder Kurvenlicht: Im Niedriggeschwindigkeitsbereich wird je nach Lenkeinschlag ein Nebelscheinwerfer zugeschaltet (siehe [R64, R65]).

Beispielhafte Motivationen

In der Recherche wurden verschiedene Motivationen für Veränderungen an der Lichtanlage ermittelt. Eine ist die Umrüstung von Beleuchtungskomponenten gegen alternative Ausführungen (z. B. die Umrüstung auf Xenon-Licht). Hier stellt wohl das häufigste Motiv eine Verbesserung der Sicht des Fahrers dar. Jedoch sind sowohl Einschätzung der Leuchtdichte und Verteilung subjektiv geprägt – ebenso wie die Entscheidung, welche Komponente nachgerüstet oder ausgetauscht wird. Auch kann die Aktivierung bzw. Deaktivierung von Steuerprogrammen zur Komforterhöhung als ein verfolgtes Ziel von Veränderungen beobachtet werden.

Exemplarische Praxisbelege

Das Nachrüsten oder der Austausch verbauter Beleuchtungskomponenten bezieht sich vornehmlich auf den Bereich der Frontscheinwerfer. Eine bekannte Ausprägung in diesem Kontext ist der nachträgliche Einbau von so genannten Xenon-Leuchten (Hochvoltgasentladungslampen), i. d. R. im Austausch gegen die bestehenden (meist H4- oder H7-)Frontscheinwerfer [R19, R20]. Neben dem gewünschten Effekt des veränderten Lichtspektrums und der damit verbundenen visuellen Wahrnehmung stellen Xenon-Scheinwerferanlagen besondere Anforderungen bezüglich der Interaktion mit anderen Verkehrsteilnehmern. Da das Xenonlicht sehr hochenergetisch ist und spektral so liegt, dass die Stäbchen der Retina sehr sensitiv reagieren, kommt es zu einer stärkeren Blendung des (Gegen-)Verkehrs. Aus diesem Grund sind sowohl eine automatische Frontscheinwerfer-Höhenregulation (AFS) inklusive deren regelmäßige Funktionsprüfung sowie eine Streuscheibenreinigungsanlage vorgeschrieben. Teilweise werden aber die Scheinwerfer durch Personen mit unzureichender fachlicher Qualifikation verbaut und auf die Einstellung oder gar den Verbau der Regulierung verzichtet.

Neben diesem „Scheinwerfertausch“ werden auch oben genannte Funktionen wie „Coming Home“ oder „Leaving Home“ nachgerüstet, wie z. B. in [R63] und [R45] diskutiert wird. Ist ein entsprechendes Steuergerät schon vorhanden, können sie entweder direkt über eine kompatible Diagnosesoftware (vgl. [R45]) aktiviert werden oder es muss dazu zusätzlich eine Sicherheitssperre umgangen werden, da die Funktion häufig Bestandteil eines aufpreispflichtigen Extras und somit durch den Fahrzeughersteller vor Zugriffen geschützt ist. Eine Veränderung, die – wahrscheinlich aufgrund der Neuartigkeit der Funktionalität – bis dato selten vorkommt, ist das Zuschalten von Scheinwerfern während der Fahrt. Konkret beobachtet werden kann dies beim oben erwähnten Abbiege- oder Kurvenlicht (siehe [R64, R65]).

Die „amerikanische Blinkerschaltung“ bezeichnet Veränderungen an der hinteren Beleuchtungsanlage. Dabei werden die Blinkleuchten so mit den Rückleuchten verbunden, dass sie normal mitleuchten (auch in roter Farbe). Wenn der Blinker betätigt wird, blinken sowohl Rücklicht als auch Blinkleuchte der entsprechenden Seite. Der Blinker übernimmt also einen Teil der Rücklichtfunktion und das Rücklicht die des Blinkers [R68]. Problematisch für die umliegenden Verkehrsteilnehmer ist dabei die fehlende farblich-räumliche Trennung dieser beiden Funktionen.

Ein weiterer derzeitiger Trend ist das Anbringen von LEDs (Light Emitting Diode, siehe Glossar), vorzugsweise in der Farbe Blau. Diese wurde abgelöst durch weiße LED-Bänder, die im Stoßfänger als Tagfahrlicht oder an Karosserieteilen (als Begrenzungsleuchten) angebracht werden [R66, R67].

Außenspiegel

Funktionsübersicht

Verschiedene Fahrzeughersteller bieten elektrisch anklappbare Außenspiegel als Zusatzausstattung an.

Beispielhafte Motivationen

In den Recherchen wurden z. B. in Quelle [R140] Belege gefunden, dass einige Fahrer an Lösungen interessiert sind, wie das Anklappen auch während der Fahrt ermöglicht werden kann (in [R140] wird z. B. über 50 km/h als Ziel genannt). Eine dort erwähnte denkbare Motivation ist eine Verbesserung

der Aerodynamik. Zudem wurden Quellen gefunden, aus denen das Nachrüsten einer entsprechenden Funktion auch bei weiteren Fahrzeugtypen als Motivation hervorgeht (vgl. [R29]).

Exemplarische Praxisbelege

Eine Anleitung zum Nachrüsten elektrisch anklappbarer Außenspiegel findet sich in Recherchequelle [R29]. Neben der Auflistung des benötigten Materials wird dort auch ein Schaltplan als Anleitung angeboten

Laut eines im Rahmen der Recherche geschilderten Erfahrungsberichtes gehört das elektrische Anklappen bei einigen Neufahrzeugen bereits zur Serienausstattung, wobei das Anklappen zumindest bei einigen Modellen auch während der Fahrt möglich ist, d. h. vom Hersteller noch nicht eingeschränkt wird. Wie die Recherchequelle [R140] zeigt, werden entsprechende Schutzfunktionen jedoch auch seitens einiger Hersteller bereits implementiert und Wege zur Umgehung dieser Funktion durch einige Nutzer bereits in Webforen diskutiert.

Verdeck

Funktionsübersicht

Unter Verdeck versteht man allgemein das bei Cabrio-Fahrzeugen vorhandene Dach, welches sich öffnen und schließen lässt. Im vorliegenden Kontext wird unter dieser Bezeichnung das gesamte integrierte System verstanden, das insbesondere die Ansteuerung der Verstellelektronik realisiert.

Wie bereits zu den TV-Systemen (s. o.) diskutiert, gehört auch die Verstellelektronik des Verdecks bei Cabrio-Fahrzeugen zu denjenigen Systemen, für die viele Hersteller aus Sicherheitsgründen keine Betätigung während der Fahrt vorsehen. Bei vielen Herstellern ist dem Fahrer das Öffnen bzw. Schließen des Verdecks daher entweder nur im Stand oder bei sehr langsamer Fahrt (i. d. R: bis Schrittgeschwindigkeit) möglich.

Beispielhafte Motivationen

Entsprechend stellt die fehlende Möglichkeit des Verdecköffnens und -schließens bei vielen Anwendern einen nicht zufrieden stellenden Zustand dar, sodass Motivationen gegeben sind, diese Funktion über elektronische Veränderungen zu realisieren.

Exemplarische Praxisbelege

Im Rahmen der Recherchen wurden hierzu einerseits detaillierte Anleitungen gefunden (z. B. [R32]). Bei älteren Fahrzeuggenerationen hilft (äquivalent zu der geschilderten Vorgehensweise bei TV-In-Motion) das Durchtrennen oder „Auf-Masse-Legen“ einzelner analoger Signalleitungen. Je nach Implementierung der Verdecksteuerung soll hierdurch i. d. R. erreicht werden, dass das ausgewertete Geschwindigkeitssignal den Wert 0 annimmt, d. h. das Fahrzeug als stehend angesehen wird. Für neuere Fahrzeuge, bei denen die zugrunde gelegten Informationen digital über die Fahrzeugnetzwerke bezogen werden, gibt es von kommerziellen Anbietern ebenfalls Filter-Boxen käuflich zu erwerben (z. B. [R35]), die z. B. das digitale Geschwindigkeitssignal auf den Nullwert ändern.

Klimasteuerung

Funktionsübersicht

Durch eine Klimasteuerung kann ein gleichmäßiges Fahrzeuginnenraumklima beibehalten werden, was je nach Umgebungsbedingungen u. a. durch Heizung bzw. Kühlung erreicht werden kann.

Beispielhafte Motivationen

Im Rahmen der Recherche wurden keine Praxisbelege für Manipulationen gefunden, die aus einer subjektiven Verbesserung motiviert waren. Hingegen wird in der akademischen Veröffentlichung [R145] eine potenzielle destruktive Motivation diskutiert. Diese könnte z. B. auf eine Verringerung des Komforts für die Insassen abzielen, die bis hin zu körperlich belastenden Klimaeinstellungen reichen könnte.

Exemplarische Praxisbelege

In Quelle [R145] wird hierzu beschrieben, dass im Praxisversuch über spezielle CAN-Bus-Telegramme (z. B. von Seiten der Diagnoseschnittstelle) die Kontrolle über die Klimasteuerung des Testfahrzeugs übernommen werden kann. Dies ermöglicht u. a. das An-/Abstellen der Ventilatoren sowie der Kühl- und der Heizfunktion, teils ohne eine Möglichkeit der Übersteuerung durch die Fahrzeuginsassen.

2.1.2 Infrastruktursysteme als Ziel elektronischer Veränderungen

Nachdem in Kapitel 2.1.1 recherchierte Kfz-Systeme als Ziel von Veränderungen vorgestellt wurden, erfolgt in diesem Kapitel die Dokumentation der Rechercheergebnisse bezüglich elektronischer Veränderungen mit infrastrukturellem Schwerpunkt. Dies beinhaltet einerseits recherchierbare Hinweise und Motivationen für elektronische Veränderungen an Infrastrukturkomponenten als auch andererseits entsprechende Veränderungen, die durch im Fahrzeug befindliche Systeme realisiert werden, aber Systeme in der Infrastruktur adressieren.

Tabelle 2 zeigt die recherchierten Systeme, zu denen im weiteren Verlauf dieses Kapitels jeweils eine ausführlichere Dokumentation der Rechercheergebnisse erfolgt.

Komponentenklasse	Komponente
Infrastruktur-komponenten	Funkschnittstellen
	Verkehrstelematik
	Geschwindigkeits-messeinrichtungen

Tab. 2: Recherchierte Infrastrukturkomponenten als Ziel elektronischer Veränderungen

Funkschnittstellen (an den Beispielen Fahrzeugortung, Maut und Verkehrsinformationen)

Bereits heute findet sich eine Vielzahl von Funkschnittstellen, mit denen ein modernes Fahrzeug Daten aus der Peripherie erhalten oder teils mit ihr austauschen (senden) kann. Zu den unidirektionalen Funktechnologien gehört z. B. der Radioempfang, bei dem über Protokolle wie RDS (Radio Data System, siehe Glossar) auch digitale Daten übertragen werden können. Auch der Bestimmung der aktuellen Positionsdaten anhand von GPS (Global Positioning System, siehe Glossar) liegt die Auswertung unidirektionaler Signale der entsprechenden GPS-Satelliten zugrunde. Als Beispiele für bidirektionale Funkverbindungen im automotiven Einsatz sind heute im Wesentlichen folgende zu nennen, die meist aus dem Bereich der Mobilfunknetze stammen. Heute weit verbreitet ist die Technologie GSM (Global System for Mobile Communications, siehe Glossar). Über GSM kann durch speziell optimierte Protokolle wie EDGE (Enhanced Data Rates for GSM Evolution, siehe Glossar) auch Internet im Fahrzeug bereitgestellt werden. Zunehmend hält auch die modernere UMTS-Technologie (Universal Mobile Telecommunications System, siehe Glossar) im automotiven Einsatz Einzug. Wie unten noch beispielhaft erläutert wird, nutzen auch verschiedene Mautsysteme (s. u.) drahtlose Kommunikationstechnologien wie die vorab genannten. WLAN (Wireless Local Area Network, siehe Glossar) und Bluetooth (siehe Glossar) spielen zur Infrastrukturseite hin derzeit noch eine untergeordnete Rolle. Zunehmend werden diese aber auch dazu eingesetzt, um z. B. eine Fahrzeugdiagnose auch drahtlos, also auch von außerhalb des Fahrzeugs durchzuführen (entsprechende Produkte werden z. B. in [R98] angeboten).

Basierend auf der – aus dem WLAN-Bereich stammenden – Protokollfamilie IEEE 802.11 soll in Zukunft über die Variante 802.11p auch Car-to-Car (C2C) sowie Car-to-Infrastructure (C2I)-Kommunikation (allgemein: C2X) realisiert werden (siehe z. B. ZIMMERMANN, 2008, S. 387 ff). Hierdurch soll die Straßenverkehrssicherheit weiter erhöht werden, z. B. indem sich verschiedene Fahrzeuge gegenseitig vor schwierigen Verkehrsbedingungen warnen können. Auch sollen im Zusammenwirken mit der Infrastruktur die Verkehrsflüsse optimiert werden. Weitere Anwendungsbeispiele für C2X sowie ein Ausblick auf mögliche Gefahren und eine Übersicht über themenbezogene Forschungsprojekte finden sich in Kapitel 6. Das heißt, das vorliegende Kapitel konzentriert sich auf Technologien, die heute bereits verfügbar sind, und fasst Hinweise auf Bestrebungen für Veränderungen und entsprechende Aktivitäten zusammen, die diesbezüglich recherchiert werden konnten.

Eine wesentliche und vergleichsweise einfach zu realisierende Art der Veränderung bestehender Funkschnittstellen besteht im vollständigen Unterdrücken der Funkkommunikation. Je nach Art der eingesetzten Technik sowie der eingesetzten Funktechnologien und Protokolle kann dies entweder auf ein- bzw. ausgehende Funkverbindungen separat oder in beide Richtungen gleichzeitig wirken. Realisieren lässt sich dies konzeptuell auf verschiedene Weisen. Ein effektiver Weg ist das Entfernen, Abtrennen oder Blockieren der Sende- und/oder Empfangseinheiten wie insbesondere der zugehörigen Antennen. Teilweise kann es jedoch sein, dass deren Verbauorte nicht bekannt oder schwer zugänglich sind oder die Veränderung möglichst unauffällig gestaltet werden soll. Alternativ lässt sch das Unterbinden von Funkkommunikation daher auch realisieren, indem der Funkkanal durch Störsignale blockiert wird. Einige praktische Bei-

spiele und Nachweise aus der Recherche werden im Folgenden diskutiert.

Das Unterbinden von Datenaustausch (unter anderem durch Jamming, siehe Glossar) kann insbesondere die Ortbarkeit bzw. Positionsverfolgung (Tracking, siehe Glossar) von Fahrzeugen adressieren, die zu verschiedenen Zwecken betrieben werden kann. Trackingsysteme (z. B. als Kombination von GPS- und GSM-Technologie) zum Erkennen und Aufklären von Fahrzeugdiebstahl werden teils auch im Privatbereich eingesetzt. Dies kann z. B. dem Bericht in [R100] sowie kommerziellen Angebote wie in Quelle [R102] entnommen werden. Insbesondere in Amerika setzen nach Quelle [R101] auch Mietwagenfirmen vergleichbare Systeme zur Kontrolle ihrer Wagenflotten ein, teils auch, um Missbrauch vorzubeugen und verlorene Fahrzeuge zu orten. Nach der letztgenannten Quelle wird dies auch von deutschen Anbietern zunehmend erwogen. Wie in [R99] berichtet wird, planen die Niederlande die Einführung eines als Trackingkomponente konzipierten Mautsystems zur Ablösung der bisherigen pauschalen Kfz-Steuer durch eine fahrtstreckenabhängige. In allen drei genannten Szenarien könnten z. B. die Fahrer entsprechender Fahrzeuge die Motivation haben, das Tracking zu blockieren: Der Dieb eines gesicherten privaten oder eines Mietfahrzeuges möchte nicht gefasst werden, während ein Bürger mit seinem eigenen Fahrzeug reisen will, ohne dafür kilometerbezogene Steuern berechnet zu bekommen, oder seine Privatsphäre gesichert sehen möchte. Hinweise, dass diese und weitere Motivationen realistisch sind, liefert zudem auch die Quelle [R99], wonach im Fall des niederländischen Mautsystems erhebliche Strafen drohen sollen: Je nach Vorliegen eines nicht gemeldeten Defekts oder vorsätzlicher Manipulationen sind Strafgelder von 18.500 bis 74.000 EUR in Diskussion. Aber auch in deutschsprachigen Diskussionsforen wie [R103] finden sich reale Anfragen und Ratschläge, wie derartige Trackingsysteme, z. B. in Fahrzeugflotten größerer Konzerne, gezielt gestört werden können. Bezüglich der in Deutschland für Lkw relevanten Autobahnmaut (vgl. auch [R119]) sind hinsichtlich ähnlicher Manipulationen auch Medienberichte wie [R120] zu beachten, die das funkbasier, aktive Stören (Jamming) von GPS als einen prinzipiellen Ansatzpunkt zur Mautstörung nennen.

Um die Ortung von Fahrzeugen zu verhindern, kann z. B. die GSM-Schnittstelle im Fahrzeug, über welche die Positionsdaten des Fahrzeuges gesendet werden, gestört werden, sodass auch keine passive Ortung (über Triangulation des GSM-Signals) möglich ist. Zu diesem Zweck werden so genannte „Jammer“ eingesetzt, welche über diverse Onlineshops (z. B. [R56], [R57]) für ca. 100 bis 400 € erworben werden können. Die Störsender funktionieren batteriebetrieben, über den Zigarettenanzünder (12V) oder mittels Netzteils am 230 V Netz. Mit den Störsendern können je nach Einsatzziel der GSM-Empfang (der Jammer simuliert eine Empfangsstation), der GPS Empfang (Senden von Störsignalen im GPS Frequenzband), der WIFI-Empfang (siehe Glossar) und das Auslesen von RFID-Transpondern (im Fahrzeug insbesondere in der Wegfahrsperre eingesetzt) ganz oder teilweise gestört werden. Die Störung kann dabei jeglichen Empfang und das Senden unterbinden, kann aber auch gezielt falsche Signale und Daten an den Empfänger im Fahrzeug übermitteln. So ist es laut einem Medienbericht in Quelle [R144] möglich, gezielt falsche Ortsdaten über das GPS-Empfangssystem zu induzieren. Damit könnten Trackingdaten auch gefälscht werden, z. B. indem Fahrtenbücher so manipuliert werden, dass eine andere, als die gefahrene Strecke aufgezeichnet wird.

Vom Grundprinzip her ähnlich funktionierende Veränderungen werden auch zum Stören der Erfassung durch Geschwindigkeitsmesseinrichtungen betrieben, die jedoch i. d. R. nicht auf Funktechnologien basieren und daher unten in einem separaten Punkt behandelt werden.

Darüber hinaus lassen sich auch Hinweise auf komplexere Veränderungen von Funkschnittstellen finden, die nicht allein auf dem Stören bzw. Blockieren einer Funkverbindung basieren. Bezüglich der ebenfalls über eine Funkschnittstelle übermittelten Verkehrsmeldungen (die wie oben erwähnt im RDS/TMC-Protokoll über die UKW-Schnittstelle übertragen werden) wurde im Rahmen einer akademischen Veröffentlichung in [R11] die Machbarkeit des Sendens gefälschter Verkehrsmeldungen an ein Navigationssystem (vgl. auch Kapitel 2.1.1) nachgewiesen. Dies erfolgt drahtlos von extern, indem mittels einer UKW-Sendeeinheit gefälschte Informationen über das RDS/TMC-Protokoll gesendet werden. Dadurch könnten Verkehrsflüsse in der Praxis durch Dritte gezielt beeinflusst werden, z. B. indem diese unzutreffende Staumeldungen verbreiten und so einen großen Teil der Verkehrsteilnehmer zur Wahl einer Ausweichstrecke veranlassen.

Mit Blick auf elektronische Veränderungen an Funkschnittstellen kann als weiterer Bereich die Nachrüstung solcher Systeme angesehen werden. Diese können Teil einer Komponente sein, die nachgerüstet wird, wie Standheizung oder Zentralverriegelung, oder als Komponente direkt (Auslesen von CAN-Daten oder Speichern von Musikdaten o. Ä.) nachgerüstet werden. Auch hierfür gibt es bereits kommerzielle Angebote von Anbietern wie in [R129], die z. B. über Mobiltelefone Suche, Zugang und Startberechtigung bei Mietfahrzeugen ermöglichen. Viele dieser nachträglich verbauten Funkschnittstellen, z. B. auch zu drahtlos durchführbarer Fahrzeugdiagnose wie aus [R98], sind nicht durch den Fahrzeughersteller für die entsprechende Baureihe vorgesehen. Daher kann potenziell einerseits die reibungslose Zusammenarbeit mit dem Restsystem nicht garantiert werden[3]. Andererseits wird hierbei in den meisten Fällen auch keine elektromagnetische Verträglichkeitsprüfung (EMV) durchgeführt, weshalb es zu kurzfristigen Ausfällen von elektronischen Komponenten und langfristig zu deren potenzieller Zerstörung oder Beschädigung kommen könnte.

Verkehrstelematik

Der Straßenverkehr insgesamt wird nicht allein durch die an ihm teilnehmenden Fahrzeuge geprägt. Als ein weiteres potenzielles Eingriffsziel kommen zudem verschiedenste Arten von Infrastrukturkomponenten hinzu. Wesentliche Vertreter dieser sind verkehrstelematische Einrichtungen.

In den Vereinigten Staaten von Amerika wurde im Januar 2009 im Bundesstaat Texas eine autarke, mobile, elektronische Verkehrstafel manipuliert, um verschiedene Falschmeldungen anzuzeigen (z. B. „Caution! Zombies! Ahead!!!“). Laut den recherchierten Quellen [R19] und [R20], die auch Fotos der Falschmeldungen auf der manipulierten Verkehrstafel zeigen, wurde dazu das bekannte Standard-Passwort für Anlagen dieses Typs verwendet und anschließend geändert. Bei der Analyse des Vorfalls zeigte sich schnell, dass die notwendigen Informationen für den Eingriff für jedermann leicht im Internet recherchierbar waren.

Für eine Einschätzung, ob entsprechende Veränderungen an elektronischen Verkehrstafeln auch in Deutschland realistisch sind, ist die Betrachtung folgender Dimensionen sinnvoll: Zunächst kann die Art der Ansteuerung betrachtet werden. Dies kann einerseits lokal (d. h. manuell am Gerät selbst) als auch ferngesteuert (d. h. elektronisch aus der Entfernung) erfolgen. Im Fall der elektronischen Ansteuerung ist zudem von Interesse, ob dies über eine drahtgebundene oder drahtlose (d. h. Funk~) Schnittstelle erfolgt. Entscheidend ist letztendlich jedoch jeweils die Stärke der vorgesehenen Schutzvorkehrungen gegen unberechtigten Zugriff.

Im geschilderten Fall aus den USA lag ein mobiles System vor, bei welchem die Eingabe lokal erfolgte. Der über eine Zahlenkombination realisierte Schutzmechanismus war aufgrund des falschen Einsatzes (das Standardpasswort wurde verwendet) faktisch unwirksam.

Eine Veränderung aus der Entfernung wäre für einen Angreifer jedoch die attraktivere Variante, weil die Entdeckungsgefahr geringer ist, da er die Verkehrstafel nicht vor Ort manipulieren muss. Aufgrund der dadurch erhöhten Angriffswahrscheinlichkeit weisen ferngesteuerte Systeme einen deutlich höheren Schutzbedarf auf, insbesondere wenn die Ansteuerung drahtlos realisiert ist.

Mobile Verkehrstafeln sind z. B. auf Baustellen auch in Deutschland im Einsatz. Bild 5 zeigt ein entsprechendes Modell an einer Stadtautobahn. Wie die Tafel aus dem obigen Beispiel ist sie für Fußgänger frei zugänglich. Eine äquivalent durchgeführte Veränderung über manuellen Zugriff ist bei diesem exemplarisch gewählten System allerdings unwahrscheinlich, da es sich bei dem fotografierten System um eine ferngesteuerte Anzeige handelt. Die Ansteuerung erfolgt drahtlos über das GSM-Protokoll (worauf eine entsprechend beschriftete Sende-/Empfangseinheit auf der Rückseite hinweist).

Bezüglich der standardmäßigen Schutzmechanismen von GSM wurden in 2009 mehrere Schwachstellen aufgedeckt (siehe NOHL, 2009), die potenziell auch die Sicherheit von Verkehrstelematik-Systemen, die über GSM-Technologie gesteuert werden, gefährden könnten. Ob bei der zuvor betrachteten Verkehrstafel sowie entsprechenden weiteren GSM-Systemen über die GSM-Standard-

---

[3] Im Fall des Bluetooth-Diagnoseadapters aus [R98] zeigten eigene praktische Tests, dass auch jede dritte Person mit der Kenntnis des im Handbuch abgedruckten Zugangscodes „1234“ (der sich allem Anschein nach auch nicht umkonfigurieren lässt) über Bluetooth eine Diagnoseverbindung zu den Fahrzeugen aufbauen kann, in denen das Produkt aktuell an der Diagnosebuchse angeschlossen ist.

Bild 5: Eine mobile elektronische Verkehrstafel in Deutschland

Schutzmechanismen hinaus weitere Vorkehrungen gegen Missbrauch getroffen wurden, ist den Autoren nicht bekannt. Generell unterliegen Verkehrstelematiksysteme in Deutschland jedoch strengen Regularien. Sofern der ihrem ferngesteuerten Betrieb angemessene Schutzbedarf in Design, Implementierung und Konfiguration sorgfältig berücksichtigt wurde, sind äquivalente gezielte Veränderungen an diesen Systemen eher nicht zu erwarten.

Zumindest eine potenzielle Umsetzung von Denial-of-Service-Angriffen über GSM-Jammer (siehe Glossar sowie obiges Kapitel zu Funkschnittstellen) dürfte jedoch realisierbar sein. Potenziell könnten damit auch Manipulationen betrieben werden, die die Anbindung der Verkehrstafel stören und somit den Empfang aktualisierter anzuzeigender Informationen unterdrücken.

Geschwindigkeitsmesseinrichtungen

Ein weiteres Beispiel für Komponenten der Infrastruktur sind Einrichtungen für Geschwindigkeitsmessungen (wie Radar- und Lichtschranken- oder Lasermesssysteme), die durch Einrichtungen wie Ordnungsamt, Polizei etc. betrieben werden, um die Übertretung von Geschwindigkeitsbegrenzungen nachzuweisen und ahnden zu können. Wie auch z. B. das zuvor behandelte elektronische Verkehrsschild sind diese Geräte zu Infrastruktursystemen zu zählen. Allerdings sind Veränderungen, die direkt am Zielsystem selbst erfolgen, hier von geringerer praktischer Bedeutung. Beispielhafte Gründe hierfür sind, dass Veränderungen an einzelnen Geräten nur einem eingeschränkten Personenkreis nutzen und ein physischer Zugriff auf stationäre (aufgrund physischer Absicherung) bzw. mobile (aufgrund der Anwesenheit von Betriebspersonal) Messeinrichtungen zudem problematisch ist.

Um der Erfassung durch diese Geräte zu entgehen und sich daher potenziellen Strafen zu entziehen, versuchen viele Fahrzeugführer in diesem Fall, die Erfassung entweder durch Störsender zu verhindern oder sie durch Detektoren zumindest rechtzeitig zu erkennen und sich warnen zu lassen.

Die Benutzung derartiger Geräte ist in Deutschland verboten (vgl. § 23 1b StVO), dennoch werden am Markt verschiedene Geräte zur Warnung vor Geschwindigkeitsmessungen angeboten, die von entsprechenden Geräten emittierte Signale detektieren und signalisieren (z. B. Radar und Laserwarner, die durch Angebote wie z. B. seitens [R90] oder [R125] beworben oder in [R143] getestet werden). Der Fahrer verspricht sich von diesen Geräten üblicherweise das großteilige Übertreten von Geschwindigkeitsbegrenzungen, sodass er lediglich bei angezeigten Kontrollmessungen abzubremsen braucht und dadurch einem großen Teil möglicher Strafen entgeht.

Die Störung optischer Systeme wie Laserpistole oder Dreilichtschrankenmessung ist mit einem hohen Aufwand verbunden, prinzipiell jedoch möglich. Auch zu deren Störung gibt es diverse Produkte wie Reflektoren, Laser-Blinder, Laser-Jammer oder Gegenblitzer (vgl. z. B. [R56], [R57]) zu kaufen. Die Wirkweise basiert bei diesen Geräten auf dem Überlagerungsprinzip. Die vom Fahrzeug reflektierten Lichtwellen bzw. das Durchfahren der Lichtschranke sollen gestört werden, funkbasierte Systeme wie Radarmessgeräte sollen ebenfalls durch überlagerte Signale im entsprechenden Frequenzspektrum gestört werden.

2.2 Systematisierung: Aufbereitung der Rechercheergebnisse nach Komponentenklassen

In diesem Abschnitt werden die in Kapitel 2.1 komponentenweise vorgestellten Rechercheergebnisse

systematisiert aufbereitet und vorbereitend für die Abschätzung der Bedrohungslage diskutiert.

Eine allgemeine Übersicht über die Arten der Quellen, aus denen die insgesamt 129 Rechercheergebnisse aufgenommen wurden, zeigt Tabelle 3. Den Schwerpunkt bildete wie eingangs erwähnt eine Internetrecherche.

Neben der Anzahl der jeweiligen Recherchequellen ist bei den aus dem Internet stammenden Inhalten zudem die Anzahl der verschiedenen Domains angetragen.

Teils konnten aus einzelnen Webangeboten (z. B. Foren) verschiedene Inhalte zu unterschiedlichen Themen aufgenommen werden, sodass die Zahl der Domains einer Kategorie auch unter der Quellenanzahl dieser Kategorie liegen kann.

Als Ausgangspunkt der weiteren Diskussion wurden die im Kontext der Recherche identifizierten Komponenten aus den Bereichen Kfz- und Infrastruktursysteme (vgl. Kapitel 2.1) den in Kapitel 1.4.3 vorgestellten Komponentenklassen zugeordnet. Diese Zuordnung ist bereits auch in Tabelle 1 kenntlich gemacht. Sie wurde vorgenommen, da die Schwerpunkte für Motivationen in den genannten Domänen häufig unterschiedlich sind. Das heißt, in den verschiedenen Domänen werden oft verschiedene Ziele verfolgt.

Art der Quelle	Ergebnisse
Projekte	18
Publikationen	5
WWW: Medienberichte	22 (13 Domains)
WWW: Foren	63 (39 Domains)
WWW: kommerzielle Angebote	31 (30 Domains)
WWW: restliche Inhalte	25 (19 Domains)

Tab. 3: Übersicht über die Rechercheergebnisse nach Art der Quelle und Zahl der recherchierten Ergebnisse

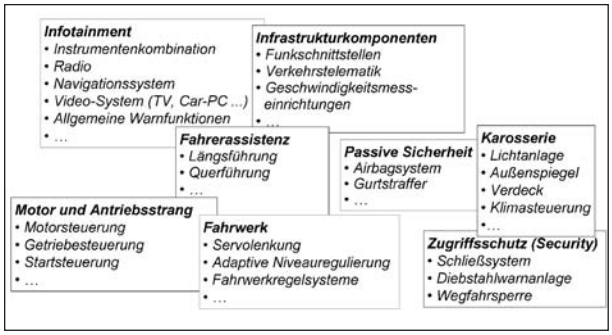


Bild 6: Visualisierung wesentlicher recherchierter Beispiele angegriffener Komponenten nach Komponentenklassen

Bild 6 zeigt eine grafische Unterteilung nach den gewählten Komponentenklassen, denen die in Kapitel 2.1 identifizierten Komponenten zugeordnet wurden. Die Überlappungen in Bild 6 deuten dabei an, dass sich diese (in Kapitel 1.4.3 vorgestellten) funktionalen Komponentenklassen in einigen Aspekten teilweise überschneiden.

Zur strukturierten Aufarbeitung nach den adressierten Komponenten zeigt Tabelle 4 die Zuordnung der Rechercheergebnisse zu den gewählten Komponentenklassen, unter welche die jeweiligen konkreten Eingriffsziele (vgl. Kapitel 2.1) fallen.

Komponentenklasse	Quellenauflistung	Summe
Motor und Antriebsstrang	[R01], [R06], [R07], [R10], [R22], [R23], [R24], [R27], [R28], [R40], [R45], [R60], [R61], [R73], [R74], [R75], [R79], [R82], [R85], [R87], [R88], [R89], [R91], [R92], [R93], [R98], [R122], [R123], [R127], [R128], [R133], [R134], [R135], [R138], [R145]	35
Fahrwerk	[R01], [R07], [R10], [R45], [R62], [R69], [R70], [R115], [R116], [R117], [R118], [R137], [R139], [R145], [R146]	15
Passive Sicherheit	[R01], [R45], [R49], [R50], [R51], [R52], [R53], [R54], [R81], [R109], [R111], [R112], [R145]	13
Fahrer-assistenz	[R85], [R77], [R78], [R83], [R84], [R94], [R145]	7
Infotainment	[R01], [R02], [R03], [R04], [R07], [R08], [R09], [R11], [R13], [R14], [R15], [R16], [R21], [R30], [R31], [R36], [R37], [R41], [R42], [R43], [R45], [R46], [R47], [R48], [R81], [R85], [R86], [R91], [R105], [R106], [R107], [R108], [R109], [R110], [R112], [R113], [R114], [R121], [R124], [R126], [R130], [R131], [R136], [R145], [R146]	45
Zugriffsschutz (Security)	[R05], [R07], [R33], [R34], [R38], [R44], [R71], [R72], [R76], [R100], [R101], [R102], [R103], [R123], [R127], [R129], [R132], [R141], [R145]	19
Karosserie	[R10], [R12], [R17], [R18], [R25], [R26], [R29], [R32], [R35], [R63], [R64], [R65], [R66], [R67], [R68], [R140], [R145]	17
Infrastruktur-komponenten	[R07], [R11], [R19], [R20], [R56], [R57], [R58], [R59], [R90], [R99], [R100], [R101], [R102], [R103], [R104], [R107], [R119], [R120], [R125], [R130], [R142], [R143], [R144]	23

Tab. 4: Aufbereitung der recherchierten Quellen (teils autorisierte sowie unautorisierte Eingriffe) nach den behandelten Komponentenklassen

Bereits in dieser Aufstellung zeichnet sich ab, dass insbesondere der Antriebsstrang (klassisches Leistungs- und zunehmendes ECO-Tuning) sowie der Infotainmentbereich verstärkt diskutierte Themengebiete sind, in denen insbesondere auch elektronische Veränderungen eine Rolle spielen. Dennoch sollte diese Auflistung nicht als alleinige repräsentative Basis zugrunde gelegt werden. Teilweise dürften die Ergebnisse noch durch verschiedene Effekte von der realen Lage abweichen. Beispielsweise wird insbesondere im Bereich Zugriffsschutz ein größerer als hier sichtbarer Anteil vermutet: Einerseits sind bei den Veränderungen aus dem Bereich des Fahrzeugdiebstahls weniger Folgen für die Safety (bis hin zur Straßenverkehrssicherheit) zu erwarten, sodass sich die Recherche durch den begrenzten Zeitrahmen eher auf das restliche Spektrum konzentrierte. Andererseits ist gerade im Bereich der Fahrzeugkriminalität eine hohe Dunkelziffer (vgl. Kapitel 4.2.1) zu erwarten, die sich in öffentlich zugänglichen Quellen nur bedingt darstellt.

2.3 Abschließende Abschätzung zur Bedrohungslage

Nach der Vorstellung der Rechercheergebnisse zu Veränderungen in Kapitel 2.1 und basierend auf der ersten Aufbereitung dieser Ergebnisse in Kapitel 2.2 erfolgt nun die Abschätzung zur Bedrohungslage.

Hierzu flossen einige weitere Informationen ein, die begleitend zur Recherche erhoben worden sind. Nach der Vorstellung dieser Betrachtungen in Kapitel 2.3.1 folgt das Ergebnis der Abschätzung anschließend in Kapitel 2.3.2.

2.3.1 Berücksichtigte Kenngrößen

Um eine möglichst zutreffende Abschätzung der Auftretenswahrscheinlichkeit erzielen zu können, wurde eine heterogene Mischung verschiedener Kenngrößen angestrebt, da jede der Kenngrößen mit einer gewissen Varianz verbunden ist. Da die einbezogenen Kenngrößen allerdings über einen begrenzten Recherchezeitraum erfasst wurden, stellen sie nur eine erste Tendenz dar. Nachfolgend werden die gewählten Kenngrößen beschrieben.

Nutzer- und Zugriffszahlen

Da der Fokus der Recherche auf neuen Medien liegt (vgl. Tabelle 3), sind ein Großteil der Rechercheguellen Internetseiten und -foren. Insbesondere Web-Foren liefern neben qualitativen Inhalten oft auch quantitative Informationen und Zugriffsstatistiken. Zur Abschätzung der Auftrittswahrscheinlichkeit sind insbesondere zwei Größen betrachtet worden:

- aktive Beteiligung (schreibende Teilnahme, Informationsbereitstellung),
- passive Beteiligung (lesende Teilnahme, Informationskonsum).

Abschätzungen für diese Werte lassen sich aus verschiedenen Statistiken ableiten, die von vielen verbreiteten Webforen-Systemen in unterschiedlich detaillierter Form angegeben werden. Diese können keine Vollständigkeit bieten, aber erste Tendenzen bezüglich der Verbreitung liefern:

- Angemeldete Nutzer: Die meisten Forensysteme liefern eine Angabe über die aktuelle Zahl angemeldeter Nutzer. Eine aktive Beteiligung (d. h. das Schreiben eigener Beiträge) ist in den meisten Foren nur angemeldeten Nutzern erlaubt. Teilweise ist auch das Lesen im Forum oder einzelner seiner Teilbereiche nur angemeldeten Nutzern erlaubt. Sofern das Schreiben bzw. Lesen entsprechend auf angemeldete Nutzer beschränkt ist, kann die Zahl registrierter Benutzer daher als erste Abschätzung der Obergrenze aktiver bzw. passiver Nutzer gewertet werden. Insbesondere wenn ein Forum primär auf eine abgeschlossene Thematik ausgerichtet ist (z. B. Motortuning), kann diese Zahl als ein erstes Maß für die praktische Verbreitung entsprechender Aktivitäten gewertet werden.
- Aktive Diskussionsbeteiligung: Insbesondere bei einzelnen Forenthemen (Diskussionsfäden bzw. engl. Threads) ist die Zahl der an der Diskussion aktiv beteiligten schreibenden Nutzer ein Maß für die aktive Beteiligung an der besprochenen Thematik und damit für das Interesse und die praktischen Verbreitung.
- Passive Diskussionsbeteiligung: In Einzelfällen kann auch die Zahl der passiven, d. h. lesenden Nutzer mit ermittelt werden. Dies ist relativ genau möglich, sofern die Zugriffszahlen auf die entsprechenden Threads von der Forensoftware erfasst und öffentlich in der Themenübersicht aufgelistet werden – was jedoch nur selten anzutreffen ist. Andernfalls kann zumindest die Zahl der angemeldeten Nutzer (s. o.) als Ober-

grenze angesetzt werden, sofern der lesende Zugriff nicht öffentlich möglich ist.

Derartige Zahlen (im Bearbeitungszeitraum von 6 Monaten) wurden insbesondere zu Webforen mit erhoben und bei der Abschätzung der Bedrohungslage berücksichtigt. Das Ergebnis dieser Abschätzung wird in Kapitel 2.3.2 in tabellarischer Form vorgestellt.

Kategoriebezogene Forenaktivität

Als ein weiterer Faktor bzgl. einer Abschätzung, die die praktische Situation möglichst zutreffend widerspiegelt, wurde auch die Frequentierung und inhaltliche Ausrichtung mit berücksichtigt. In SCHMIDT 2009 wurden hierzu zunächst die 10-13 namhaftesten deutschen Diskussionsforen mit Automobilschwerpunkt auf ihre generelle Aktivität hin untersucht. Am Beispiel motor-talk.de, das demnach mit ca. 200.000 Besuchern pro Tag am höchsten frequentiert ist und zudem insgesamt mehr Beiträge aufweist als alle anderen betrachteten Foren zusammen, wurde eine Übersicht über inhaltliche Kategorien geschaffen, auf die sich die Diskussionen in diesem Forum unterschiedlich stark konzentrieren. Zwar sollte man sich bei der Deutung bewusst sein, dass sich ein großer Teil der Beiträge nicht gezielt auf Änderungen an Fahrzeugen und ihrer Komponenten bezieht. Auch Fragen zu serienmäßigen Funktionen und gegenseitige Hilfe bei Problemen werden behandelt. Dennoch werden die Interessen der Forenteilnehmer hieraus deutlich, die sich auch auf ihre Motivationen nach subjektiver Optimierung und somit Veränderung automotiver Systeme übertragen lassen sollten.

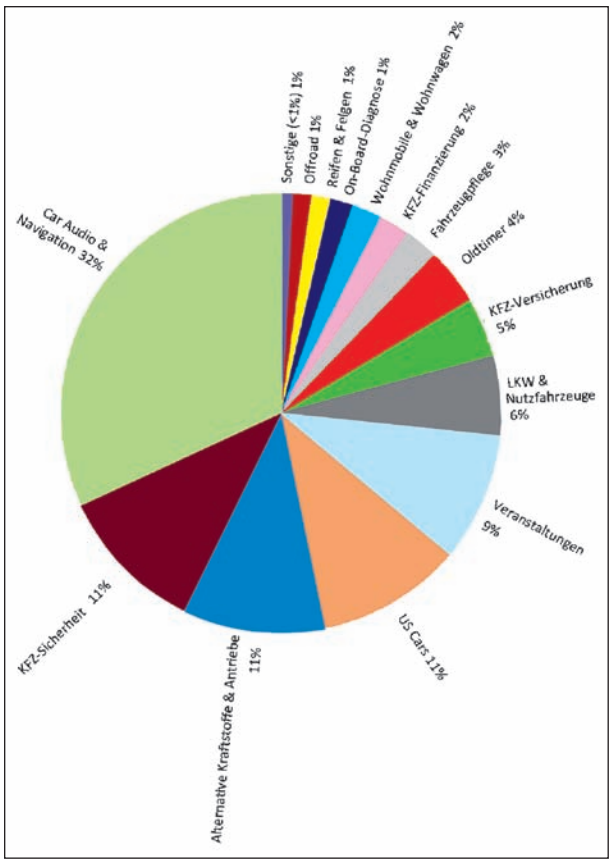


Bild 7: Verteilung inhaltlicher Themenschwerpunkte im großen deutschen Automobilforum motor-talk.de (Auswertung zum Stand von Oktober 2009)

Bild 7 zeigt die Auswertung der ermittelten Anteile als Kreisdiagramm. Aus dieser Darstellung wird ersichtlich, dass ein Großteil der Beiträge im Bereich Infotainment (Car-Audio und Navigation) sowie im Antriebsbereich und im Kfz-Sicherheitsbereich liegt. Zumindest für den Zeitraum der Erhebung lässt sich hieraus schlussfolgern, dass in diesen Bereichen für Fahrzeugbesitzer, die in entsprechenden Communities aktiv sind, das größte Interesse liegt.

2.3.2 Ergebnis der Abschätzung

Unter Einbeziehung der zuvor vorgestellten Faktoren wurden zur Abschätzung der Bedrohungslage insbesondere folgende zwei exemplarische Kriterien betrachtet:

Ein wesentlicher Faktor für die Relevanz der Bedrohungslage bezüglich einer gegebenen Veränderung ist die Verbreitung der zugehörigen Komponente am Markt.

Auch ist für die Abschätzung entscheidend, ob und wie umfangreich Informationen über die betrachtete Veränderung verfügbar sind. Im Kontext der Recherchen wurden hierzu sowohl Quellen gewertet, bei denen Anleitungen zu Veränderungen gegeben als auch angefordert wurden.

Die Abschätzung beruht dabei auf dem Verhältnis dieser beider Faktoren. Beispielsweise genügt nicht, dass ein System weit verbreitet ist, wenn kein Hinweis recherchiert werden kann, dass Veränderungen an dieser Komponente diskutiert werden. Umgekehrt sind auch intensiv diskutierte Veränderungen bedingt praxisrelevant, wenn die betroffenen Komponenten nur sehr gering am Markt vorkommen.

Tabelle 5 zeigt jeweils pro Komponente und Motivation zu einer Veränderung die vorgenommenen Abschätzungen für Markt- und Informationsverbrei-

			Abschätzung Bedrohungslage		
Art der Komponente (Teilfunktion)		**Potenzielle Motivation für die Veränderung**	**Geschätzte generelle Verbreitung der Komponente bzw. Teilfunktion**	**Geschätzte Verbreitung von Informationen über/Angebote von Veränderungs-möglichkeiten**	**Abschätzung Bedrohungs-lage**
Motor und Antriebsstrang	Motorsteuerung	Leistungssteigerung	hoch	mittel - hoch	mittel - hoch
		Verbrauchsreduktion	hoch	niedrig - mittel	mittel
		Nachrüstung von Regelungsfunktionen für Autogasanlage (Senkung Betriebskosten)	hoch	mittel	mittel - hoch
		Motor bzw. Fahrzeug zum Stillstand bringen (destruktive Motivation)	hoch	niedrig	mittel
	Motorsteuerung (Abgasrückführung)	Deaktivieren	niedrig	niedrig	niedrig
	Motorsteuerung (Geschwindigkeits-Abregelung)	Deaktivieren	niedrig	hoch	mittel
	Getriebesteuerung (Automatikgetrie-be, elektronische Schaltpunktsteue-rung)	Schaltpunkte verändern	niedrig - mittel	niedrig	niedrig
	Getriebesteuerung (pseudo-automati-sierte Schaltung)	Nachrüstung	mittel - hoch (für klassische H-Schaltun-gen als Ausgangsbasis)	sehr niedrig	niedrig - mittel
	Startsteuerung	Motorstart auf Knopfdruck (Startknopf nachrüsten)	hoch	sehr niedrig	niedrig
Fahrwerksysteme	Servolenkung	Härtere Einstellung	mittel für elektrische Servolenkungen	mittel	mittel
		Mehr Fahrleistung (Ersetzen durch eine elektro-nisch gesteuerte und elektrisch angetriebene Servolenkung, adaptive Regelung)	mittel für die Verbreitung riemen-getriebener Systeme	sehr niedrig	niedrig
	Adaptive Niveauregelung	Elektronisches Tieferlegen	niedrig - mittel	hoch	niedrig - mittel
	Fahrdynamikkregelsysteme	Deaktivieren einzelner Funktionen (z. B. ABS oder ESP)	mittel - hoch	mittel	mittel
		Einleiten unerwünschter/Verhindern gewünschter Bremsvorgänge (destruktive Motivation)	mittel - hoch	niedrig	niedrig - mittel
Passive Sicherheit	Airbagsystem/Gurtstraffer	Verbergen der Nichtfunktionalität	mittel - hoch	niedrig - mittel	mittel
Fahrerassistenz-systeme	Längsführung (Tempomat)	Nachrüstung nicht vorhandener Funktion	mittel (nicht vorhandenes System)	niedrig	niedrig - mittel
		Freischaltung nicht aktiver Funktion	mittel (vorhandenes System)	hoch	mittel - hoch
	Längsführung (ACC)	Mindestabstand verringern	niedrig	mittel - hoch	mittel
	Querführung	Aktiven Assistenten nachrüsten	mittel - hoch für das nicht vorhandene System	niedrig - mittel	mittel
Infotainment	Instrumentenkombination (Wegstreckenzähler)	Kilometerstand ändern	hoch	hoch	hoch
	Instrumentenkombination (Serviceintervallanzeige)	Zurücksetzen	mittel - hoch	mittel - hoch	mittel - hoch
	Instrumentenkombination (Fahrerinformationssystem)	Beschreiben mit eigenen Inhalten (es wurden konstruktive wie destruktive Motivationen ermit-telt)	mittel - hoch	niedrig - mittel	mittel
	Radio	Anheben der Lautstärke auf Maximum (destruk-tive Motivation)	hoch	niedrig	mittel
	Navigationssystem	Kostenloses Nachinstallieren von Kartenmaterial	mittel	hoch	mittel - hoch
		Installieren von POI („Blitzer"-Positionen etc.)	mittel	hoch	mittel - hoch
		Eigene Änderungen an Betriebssoftware und -daten	mittel	niedrig	niedrig - mittel
	Navigationssystem (Fahrschulfunktion)	Aktivierung	niedrig	niedrig	niedrig
	Video-System	TV In Motion	niedrig	hoch	mittel
	Allgemeine Warnfunktionen	Deaktivieren (z. B. Gurtwarner)	mittel - hoch	hoch	mittel - hoch
		Provozieren von Warnungen (z. B. Reifendruck-kontrolle) durch Dritte, um Fahrer zum Anhalten zu verleiten (destruktive Motivation)	mittel	niedrig	niedrig - mittel

Tab. 5: Abschätzung der Bedrohungslage (erste Teilergebnistabelle)

tung sowie die vorgenommene resultierende Abschätzung der Bedrohungslage. Entspricht die Motivation einer (unsachgemäß durchgeführten) Nachrüstung (vgl. Kapitel 1.4.1), so wurde die Verbreitung invertiert, da die entsprechende Komponente in diesen Fällen initial nicht vorhanden ist. Beispielsweise befindet sich unter den derzeit zugelassenen Fahrzeugen nur ein niedriger Anteil mit

			Abschätzung Bedrohungslage		
Art der Komponente (Teilfunktion)		Potenzielle Motivation für die Veränderung	Geschätzte generelle Verbreitung der Komponente bzw. Teilfunktion	Geschätzte Verbreitung von Informationen über/Angebote von Veränderungs-möglichkeiten	Abschätzung Bedrohungs-lage
Zugriffsschutz (Security)	Schließsystem (Zugang durch Funköffner)	Unberechtigtes Öffnen	hoch	niedrig	mittel
		Verhindern des Verschließens durch Jamming	hoch	mittel	mittel - hoch
	Schließsystem (Autolock-Funktion)	Nachrüsten/Aktivieren	hoch für Systeme ohne verbautes/aktiviertes Autolock	niedrig - mittel	mittel
	Schließsystem	Ein-/Aussperren der Fahrzeugnutzer (destruktive Motivation)	hoch	niedrig	mittel
	Diebstahlwarnanlage	Unberechtigte Deaktivierung	mittel - hoch	mittel	mittel
		Einbindung eines Nachrüst-Kits	niedrig - mittel für nicht vorhandene Systeme	niedrig - mittel	niedrig - mittel
		Setzen der „Anti-Polenschlüssel"-Kodierung	mittel	niedrig	niedrig - mittel
	Wegfahrsperre	Unberechtigte Deaktivierung	mittel - hoch	mittel	mittel
		Einbindung eines Nachrüst-Kits	niedrig - mittel für nicht vorhandene Systeme	niedrig - mittel	niedrig - mittel
Karosserie	Lichtanlage (Frontscheinwerfer)	Nachrüsten Xenon-Licht	hoch für normale Schein-werfer	mittel	mittel - hoch
	Lichtanlage (Steuerprogramme)	Aktivieren/Entfernen diverser Schaltoptionen	mittel - hoch	mittel	mittel
	Außenspiegel (elektr. Anklappfunkti-on)	Nachrüstung zur Komforterhöhung	hoch für nicht elektr. anklappbare Spiegel	niedrig	mittel
		Betätigung während der Fahrt	niedrig	niedrig	niedrig
	Verdeck	Betätigung während der Fahrt	niedrig	mittel	niedrig - mittel
	Klimasteuerung	Verringern des Komforts durch Dritte (destruktive Motivation)	mittel	niedrig	niedrig - mittel
Infrastrukturkomponenten	Funkschnittstellen (Ortungssysteme)	Unterdrückung (Jamming) gegen Tracking, Maut, Steuer, Überwachung	niedrig	niedrig - mittel	niedrig - mittel
	Funkschnittstellen (Verkehrsinforma-tionen)	Senden gefälschter Verkehrs-Meldungen z. B. zum eigenem Vorteil	mittel - hoch	niedrig	niedrig - mittel
	Funkschnittstellen (Fernbedienfunk-tionen)	Nachrüsten von Fernbedienfunktionen (z. B. für Standheizung, Zentralverriegelung)	mittel - hoch für nicht vorhandene Systeme/Funktion	niedrig	mittel
	Verkehrstelematik (autarke elektron. Verkehrstafel)	Unberechtigtes Anzeigen eigener Inhalte	niedrig	niedrig	niedrig
	Geschwindigkeits-Messeinrichtungen	Warnung vor Messungen	mittel	mittel - hoch	mittel - hoch
		Störung von Messungen	mittel	niedrig	niedrig - mittel

Tab. 5: Fortsetzung

serienmäßig verbautem Xenon-Licht. Eine Veränderung, die die Nachrüstung eines solchen vorsieht, ist daher für eine hohe Anzahl (= invertierter Schätzwert der Verbreitung) von Fahrzeugen potenziell interessant.

Anhand der gewählten Kriterien wurde die Höchstbewertung „hoch" ein einziges Mal bzgl. der Bedrohungslage zu Manipulationen am Kilometerstand vergeben. Die Teilfunktion des Wegstreckenzählers ist in allen aktuellen Fahrzeugen vorhanden (Verbreitung der Komponenten „hoch") und die Verbreitung von Informationen zur Veränderung aus der Recherche wurde gleichfalls als „hoch" eingeschätzt. Darüber hinaus gibt es mehrere Beispiele für Veränderungen, für die die Bedrohungslage als „mittel - hoch" eingeschätzt wurde. In diesen Fällen sind z. B. die betreffenden Systeme nur in einem geringeren Anteil der Fahrzeuge vorhanden oder die Verbreitung von Informationen zu ihrer Veränderung wurde nicht ebenfalls als hoch abgeschätzt.

3 Abschätzung ausgenutzter Schwachstellen unter Einbeziehung des Angreiferspektrums

Im vorigen Kapitel wurden verschiedenste Arten von Veränderungen an elektronischen Fahrzeug- und Infrastruktursystemen vorgestellt, die im Rahmen der Recherche ermittelt wurden. In vielen Fällen werden dadurch Vorgaben der Hersteller sowie des Gesetzgebers umgangen. Dass diese Veränderungen dennoch möglich sind, liegt an verschiedenen generellen Schwachstellen.

Als wesentliche Ursachen, die Veränderungen wie die zuvor genannten möglich machen, werden in Kapitel 3.1 fünf Schwachstellenkategorien definiert.

Anschließend wird in Kapitel 3.2 (ausgehend von den Erkenntnissen aus den Recherchen) auch das Angreiferspektrum näher untersucht, indem aus

Betrachtungen zu generellen Arten von Angriffen und Angreifern drei im Automobilkontext relevante Angreiferklassen gebildet werden.

Nach einer Aufarbeitung der Rechercheergebnisse bezüglich des erforderlichen Angreiferwissens in Kapitel 3.3 schließt dieses Kapitel mit das Abschätzung der Schwachstellen in Kapitel 3.4.

3.1 Definition exemplarischer Schwachstellenkategorien

Fünf wesentliche Kategorien von Schwachstellen, die in der Praxis betriebene elektronische Veränderungen insbesondere an Fahrzeugsystemen ermöglichen, sind:

- S1: Möglichkeit des Zugriffs auf herstellerseitig vorgesehene Optionen, die zu Testzwecken oder zur Verwendung in anderen Ländern bestimmt sind. Diese Möglichkeiten werden nach Bekanntwerden in den entsprechenden Interessentenkreisen (z. B. in Internetforen) aktiv kommuniziert und genutzt. Dabei handelt es sich oft um (über die Diagnosesoftware vorzunehmende) Kodierungen oder um versteckte Menüeinträge (die z. B. über geheime Tastenkombinationen aufrufbar sind).

- S2: Möglichkeit des Zugriffs auf analoge Kommunikationskanäle. Zum Beispiel werden diese durch Durchtrennen oder Kurzschließen auf einen fixen Zustand gesetzt, um einzelne Ein- bzw. Ausgaben dauerhaft zu verfälschen. Auch unzureichend gesicherte analoge, drahtlose Verbindungen zählen zu dieser Kategorie.

- S3: Möglichkeit des Zugriffs auf digitale Kommunikationskanäle. Mit geeigneten elektronischen Hilfsmitteln ist auch ein direkter Zugriff auf die digitalen, fahrzeuginternen Kommunikationsnetze (i. d. R. Feldbussysteme wie CAN, MOST oder FlexRay) möglich, der selektiv bis pauschal das Mitlesen, Einfügen, Löschen oder Modifizieren übertragener Nachrichten ermöglicht. Hinzu kommt die durch das modulare Systemkonzept und einzelne Busprotokolle unterstützte Erweiterbarkeit des IT-Verbunds: Das zusätzliche Einfügen – auch nicht autorisierter – Komponenten (insbesondere den Fahrzeugbussen zusätzlich hinzugefügte Steuergeräte wie spezielle Filterboxen) ist häufig problemlos möglich und wird durch die restliche Fahrzeugelektronik i. d. R. nicht unterbunden bzw. erkannt. Auch unzureichend gesicherte digitale drahtlose Verbindungen zählen zu dieser Kategorie.

- S4: Unzureichende Absicherung der Betriebssoftware und Konfigurationsdaten. Auch direkte Veränderungen der Betriebssoftware sowie ihrer wesentlichen Konfigurationsdaten (z. B. Kennfelder) in elektronischen Steuergeräten werden teilweise vorgenommen. Schnittstellen hierzu sind i. d. R. bereits für vorgesehene Softwareupdates seitens der Hersteller vorhanden. Oft genügt hier frei verfügbare (Diagnose~)Ausstattung. Diese Schwachstelle für unautorisierte Veränderungen der Software wird seitens der Hersteller zunehmend versucht zu schließen, z. B. indem Flash-Updates auf Integrität und Authentizität hin überprüft werden (wie z. B. seitens der Herstellerinitiative Software spezifiziert wurde, vgl. Quelle HIS, 2009).

- S5: Fehlende bzw. unzureichende Erschwerung des physischen Zugriffs auf sensible Fahrzeugteile. Dazu können freiliegende bzw. leicht zugängliche Busleitungen gehören (z. B. in die Außenspiegel). Im Internet finden sich zudem Anleitungen, wo Busleitungen an verschiedenen Fahrzeugtypen zugreifbar sind (z. B. [R73]). Zudem wird durch mangelnde Verplombung sicherheitskritischer Steuergeräte einerseits einem Angreifer der Hardware-Zugriff auf das Innenleben unnötig erleichtert (z. B. um selektiv relevante Elektronikbausteine zu ersetzen). Andererseits kann eine solche Veränderung an einem nicht verplombten Steuergerät im Nachhinein schwerer nachgewiesen werden. Neben unautorisierten Zugriffen auf Busleitungen und Steuergeräte fallen in diese Kategorie als dritter Unterpunkt auch nachträglich angebrachte Sensorik/Aktorik-Komponenten.

Dass diese Schwachstellen heute aktiv ausgenutzt werden, liegt im Allgemeinen entweder darin begründet, dass zum Zeitpunkt der Entwicklung der betroffenen System...

- …keine Schutzmaßnahmen bekannt waren, um die jeweils eingesetzte missbräuchliche Nutzung der entsprechenden Schwachstelle zu verhindern,

oder

- …Schutzmaßnahmen bekannt waren, diese aber entweder…

- …als unwirtschaftlich eingestuft und daher nicht verbaut wurden,
- …verbaut wurden, aber nicht (mehr) wirksam sind, d. h. (inzwischen) umgangen werden können, oder
- …verbaut wurden und noch wirksam, aber nicht in allen Ausführungen vorhanden sind.

Die soeben eingeführten Schwachstellenkategorien werden im weiteren Verlauf folgendermaßen aufgegriffen: In Kapitel 3.4 werden sie für die Abschätzung der den Rechercheergebnissen zugrunde liegenden Schwachstellen hinzugezogen. In Kapitel 5.1.3 werden sie zudem genutzt, um pauschal die typischen Größenordnungen von Gefährdungen abzuschätzen, die mit ihrer Ausnutzung im Allgemeinen einhergehen können.

3.2 Untersuchung des Angreiferspektrums

In diesem Kapitel steht die Analyse des Angreiferspektrums im Fokus der Untersuchungen, d. h., welche generellen Arten von Angriffen und Angreifern allgemein sowie im automotiven Kontext zu betrachten sind. Dazu werden mit den sog. Basis-Angriffen zunächst grundlegende Angriffs-Strategien vorgestellt (Kapitel 3.2.1) und anschließend das allgemeine Spektrum von Angriffen und Angreifern anhand der aus der Desktop-IT stammenden CERT-Taxonomie aufgezeigt (Kapitel 3.2.2). Abschließend werden in Kapitel 3.2.3 mit konkretem Bezug auf das vorliegende Anwendungsfeld drei Angreiferklassen bzgl. Veränderungen an Fahrzeug- und Infrastruktursystemen definiert, die im weiteren Verlauf verwendet werden.

3.2.1 Basis-Angriffe und ihre Kombinationen

Unabhängig von der konkret vorliegenden Schwachstelle lassen sich typische Vorgehensweisen bei den Veränderungen allgemein durch fünf generelle Arten von Basis-Angriffen beschreiben (vgl. Bild 8).

Abweichend vom normalen Datenfluss, der direkt von der Original-Quelle zum beabsichtigten Ziel gerichtet ist, kann ein Angreifer auf fünf generelle Arten (und deren Kombination) in diese Kommunikation eingreifen:

- Lesen. Als Beispiel sei hier das Mitlesen eines Schlüsselcodes bei alten Infrarotsystemen genannt (vgl. Absatz „Schließsystem“ in Kapitel 2.1.1)
- Modifizieren. Um z. B. das Fernsehen beim Fahren freizuschalten (Absatz „TV-System“ in Kapitel 2.1.1), wird z. B. häufig eine Filterbox vor dem betreffenden Steuergerät im Datenbus platziert, die das tatsächliche Geschwindigkeitssignal auf 0 km/h reduziert.
- Unterbrechen. Z. B. zum Öffnen des Verdecks während der Fahrt (vgl. Absatz „Verdeck“ in Kapitel 2.1.1) sehen einige Anleitung das Durchtrennen einer analogen Signalleitung vor. Dies kann als ein Beispiel für das Unterbrechen eines Informationsflusses angesehen werden.
- Erzeugen/Spoofen. Ergänzend zum ersten Beispiel kann der Angreifer z. B. die mitgelesene Codesequenz zu einem späteren Zeitpunkt wieder einspielen, um das Fahrzeug unautorisiert zu öffnen.
- Stehlen/Löschen. Z. B. um das Fahrerinformationssystem mit eigenen Nachrichten beschreiben zu können (vgl. Absatz „Instrumentenkombination“ in Kapitel 2.1.1), muss teilweise durch in den Fahrzeugbus geschaltete Filterboxen dafür gesorgt werden, dass vorgesehene eingehende Textnachrichten abgefangen werden und das Ziel nicht erreichen.

Die (soeben als Beispiel erwähnte) Kombination der Basisangriffe „Lesen“ und „Erzeugen/Spoofen“ wird gemeinhin auch als Replay-Angriff bezeichnet. Dies verdeutlicht, dass sich in der Regel auch komplexere Angriffe als eine Kombination dieser vorgestellten Basisangriffe darstellen lassen. Durch den gezielten Einsatz von Sicherheitsmaßnahmen, welche die Basisangriffe auf sicherheitsrelevante Daten(-flüsse) erschweren, könnten die Hersteller zukünftig auch größer angelegte Veränderungen erschweren oder sogar verhindern und somit einige der identifizierten Schwachstellen schließen. In der

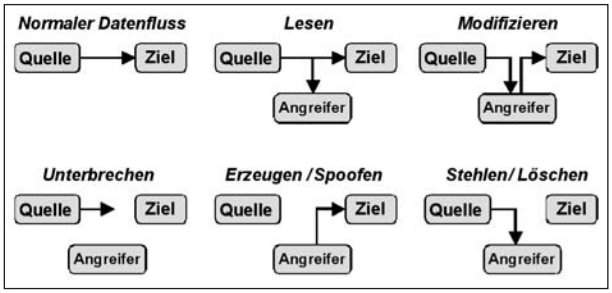


Bild 8: Die fünf generellen Basis-Angriffe

Praxis sind hierbei durch den hohen Kostendruck in der Automobilindustrie jedoch Kosten-/Nutzen-Abwägungen zu erwarten. Sind mit der Einführung einer Sicherheitsmaßnahme Kosten verbunden, kann z. B. die Schwere potenzieller Folgen (voraussichtlich insbesondere bzgl. potenzieller Safety-Auswirkungen) als ein Kriterium entscheidend sein.

3.2.2 Angreiferspektrum nach CERT

Die Systematisierung des Angreiferspektrums (insbesondere wesentlicher Aspekte wie z. B. relevante Klassen von Angreifern und ihres Kenntnisstandes und verfolgen Motivationen) soll für den automotiven Kontext entlang der sog. CERT-Taxonomie nach John D. Howard und Thomas A. Longstaff (vgl. HOWARD, 1998) erfolgen. Diese stammt aus dem Bereich der Computer Emergency Response Teams (CERT) und somit aus der Aufklärung von (IT~)Sicherheitsvorfällen, vornehmlich im Desktop-IT-Bereich (d. h., sie ist ursprünglich für größere Netzwerke von Server- und Desktopsystemen entwickelt worden). Mit dem Ziel, eine gemeinsame Sprache für in diesem Kontext relevante Zusammenhänge zu schaffen, hat sich die CERT-Taxonomie bereits in der Praxis für ganzheitliche Sicherheitsbetrachtungen bei der Evaluierung von Sicherheitsvorfällen in IT-Systemen bewährt und stellt eine Beschreibung zur strukturierten Analyse und Klassifikation von Sicherheitsvorfällen dar.

Die CERT-Taxonomie (vgl. Bild 9) unterscheidet dabei 7 wesentliche Elemente eines Sicherheitsvorfalls:

- Angreifer (attacker). Generell sind verschiedene Arten von Angreifern zu berücksichtigen. Die originale Taxonomie nennt hier z. B. Hacker, Spione oder unzufriedene Angestellte. Im automotiven Kontext sind weitere Klassen wie z. B. Tuner denkbar. Der von der CERT-Taxonomie ebenfalls abgedeckte Vandalismus wird im Bereich von Verkehrs- und Infrastruktursystemen derzeit hauptsächlich auf physische Art und Weise betrieben (z. B. das Zerkratzen von Autolack) und steht damit nicht im Fokus. Werden entsprechenden motivierten Angreifern zukünftig Werkzeuge zugänglich, Vandalismus auch auf elektronischer Ebene zu betreiben, könnte in diesem Bereich auch diese Angreiferklasse an Bedeutung gewinnen.
- Werkzeug (tool). Der Angreifer verwendet zum Einleiten seines Angriffs ein Werkzeug. Dies können beispielsweise Schadprogramme sein. Im Falle eines Fahrzeugs können auch physische Angriffe, z. B. das Hinzufügen spezieller Schaltungen oder Filterboxen, als Werkzeuge genutzt werden.
- Schwachstelle (vulnerability). Die eingesetzten Werkzeuge nutzen in der Regel eine Schwachstelle aus, um effektiv eingesetzt werden zu können. Diese kann bei jeder Art von IT-System, also auch im Automobile in einer der drei Phasen Design, Implementierung oder Konfiguration entstanden sein.
- Aktion (action). Während des Angriffs führt der Angreifer verschiedene elementare Aktionen aus. Die in Kapitel 3.2.1 vorgestellten Basisangriffe sind ein Beispiel für entsprechende Aktionen.
- Ziel (target). Die Aktionen beziehen sich dabei auf einzelne Ziele. Dies können einzelne Daten, Nutzeraccounts oder Prozesse sein, aber z. B. auch ganze (Fahrzeug~)Komponenten des Gesamtsystems.
- Unautorisiertes Resultat (unauthorized result). Der Angriff selbst führt schließlich zu einem erzielten Resultat, z. B. dem Erlangen von erhöhten Zugriffsrechte oder dem Auslesen bzw. Verändern geschützter Daten.
- Motivation (objectives). Letztendlich übt der Angreifer einen Angriff immer aus einer gewissen Motivation heraus aus. Dies kann z. B. einfach aus Nervenkitzel heraus geschehen, politisch oder finanziell motiviert sein.

Wie Bild 9 ebenfalls veranschaulicht, wird der gesamte Sicherheitsvorfall dabei in 3 ineinandergeschachtelte Phasen unterteilt:

- Vorfall (incident). Bei der Analyse des gesamten Vorfalls stehen neben dem Angriff zunächst im Wesentlichen der Angreifer und seine Absicht (Motivation) im Vordergrund.
- Angriff (attack). Bei der näheren Analyse des Angriffs werden die genutzten Werkzeuge und die

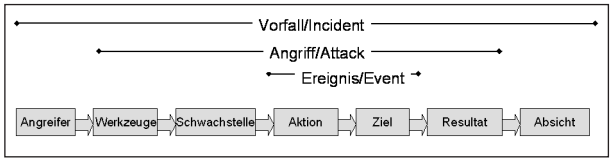


Bild 9: CERT-Taxonomie (Struktur), nachempfunden nach HOWARD, 1998

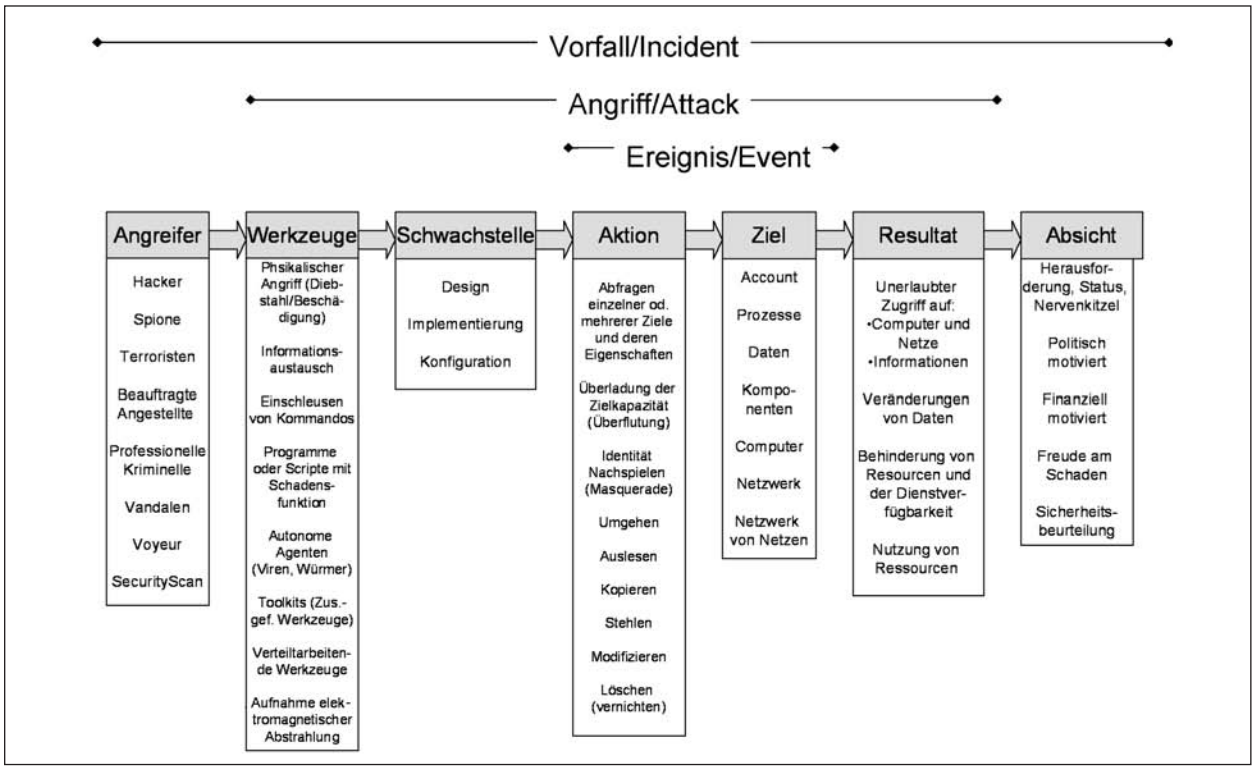


Bild 10: CERT-Taxonomie nach HOWARD, 1998 (mit Beispielen)

ausgenutzten Schwachstellen betrachtet, sowie das Resultat der durchgeführten Ereignisse.

- Ereignis (event). Als elementarer Angriffsschritt wird das Ereignis weiter in die einzelnen Aktionen und ihre jeweiligen Ziele unterteilt.

In Bild 10 ist die CERT-Taxonomie mit Beispielelementen für die einzelnen Phasen abgebildet.

Mit Blick auf die grundlegende Problematik elektronischer Veränderungen an Fahrzeug- und Infrastruktursystemen liegt der Fokus der Recherchen hauptsächlich auf der äußeren Schicht des Modells. Dies bedeutet, dass bei der Recherche im Wesentlichen zentrale Elemente der Ebene Vorfall betrachtet werden, also welche Arten von Angreifern mit welchen Motivationen agieren. Teilweise werden mit benutzten Werkzeugen und verantwortlichen Schwachstellen sowie der Nennung einzelner Resultate auch konkrete Elemente der Ebene Angriff dokumentiert. Diese stehen aufgrund des begrenzten Zeitrahmens jedoch nicht im Fokus.

3.2.3 Wesentliche Angreiferklassen elektronischer Veränderungen an Fahrzeug- und Infrastruktursystemen

Nach Sichtung der Rechercheergebnisse lässt sich das Angreiferspektrum am ehesten funktionell systematisieren: Welche Rolle nimmt eine Person im Verlauf der Veränderung ein? Damit wird der Begriff des „Angreifers“ erweitert. Der Bereich der Fahrzeugkriminalität wird anschließend gesondert betrachtet.

Der Großteil aller Motivationen zu Veränderungen findet seinen Ursprung in der „normalen“ Fahrzeugnutzung: Fahrer und Mitfahrer haben Erwartungen an verfügbare Funktionen. Dazu zählen sowohl der Verbau (z. B. Videosystemkomponenten) als auch dessen Funktionsweise (DVD, DVB-T, getrennte Bildschirme etc.). Ist eine der Funktionen nicht erwartungskonform, kann daraus das Bedürfnis erwachsen, diese Funktion nachträglich verfügbar zu machen oder entsprechend den Bedürfnissen zu optimieren. In diesem Kontext kann auch das Anpassen von Funktionen älterer Automobile an aktuelle Standards relevant sein. Diese Einschätzung kann aus der Dissonanztheorie (vgl. FESTINGER in ZIMBARDO, 2003) abgeleitet werden. Kommt es zu einem Konflikt zwischen Einstellung (hier: Erwartung an eine Funktion) und der Handlung (in diesem Fall die konkrete Nutzung einer Funktion), entsteht Dissonanz. Diese wird als unangenehm empfunden. In deren Folge kann die Person entweder die Einstellung ändern (z. B. „TV beim Fahren ist mir doch nicht so wichtig“) oder sie ist bestrebt, den Konflikt (als Ursache der Dissonanz) zu been-

den. Diese Bestrebungen bilden die Basis der Motivation zur Veränderung und in deren Folge Planung und Umsetzung der Veränderungen, bis der Konflikt gelöst wurde. An dieser Stelle sei erwähnt, dass die Erwartungen keineswegs fix sind – sich also im Laufe der Zeit ändern können. Als Einflussquellen gelten Aussagen von Freunden, Familienmitgliedern, Bekannten, Zeitschriften oder Fernsehsendungen (wie „Pimp my Ride“). Diese Quellen haben ebenfalls einen Einfluss auf die Lösung des Erwartungskonfliktes, indem sie die Bereitschaft zur Veränderung unterstützen (vgl. ARONSON et al. in ZIMBARDO, 2003). Je nach prozeduralem deklarativen Wissensstand und handwerklichem Geschick wird die Person den Eingriff entweder selbst vornehmen oder vornehmen lassen („rational choice theory“ – einem psychologischen Ökonomiemodell der Entscheidungsfindung, vgl. TVERSKY & KAHNEMANN in ZIMBARDO, 2003). Ersteres erfordert häufig den Zugang zu einer Werkstatt und/oder Spezialwerkzeug. Zu Letzterem kommt in letzter Zeit auch immer häufiger so genanntes Insiderwissen hinzu, bedingt durch die Bestrebungen der Automobilindustrie, die Datensicherheit in Fahrzeugen zu erhöhen (vgl. HIS Initiative/HIS, 2009). Dazu zählen Zugriffscodes – auch PIN genannt, IDs und der Aufbau von CAN-Botschaften (z. B. undokumentierte Botschaften) oder die Struktur des Bussystems und der verbauten Steuergeräte. Dieses notwendige Wissen besitzen immer weniger Fahrzeugbesitzer selbst und tendieren zur Beauftragung eines Dritten, den Eingriff vorzunehmen. Daraus ergibt sich eine Situation, welche die Gefahren durch eine Fehlfunktion der veränderten Komponente verstärkt: Personen, die den Eingriff selbst vornehmen, besitzen typischerweise ein detailliertes Wissen über die Art des Eingriffes und die verbundenen Konsequenzen im Gegensatz zu Personen, die den Eingriff vornehmen lassen. Die erstere Personengruppe kann somit u. U. angemessenere Reaktionen auf etwaiges Fehlverhalten zeigen. Innerhalb der Gruppe der Personen, die den Eingriff tatsächlich ausführen, kann zwischen Wissen generierenden Personen und den Wissen anwendenden Personen differenziert werden. Erstere analysieren die Ausgangslage (Hardware und Software), erkennen die Potenziale und entwickeln (kreative) Lösungen. Diese werden dann – je nach Motivation – kommerziell oder kostenfrei anderen Anwendern zur Verfügung gestellt oder selbst als Dienstleistung angeboten. Im Kontext der CERT-Taxonomie (siehe HOWARD, 1998 sowie Kapitel 3.2.2) entspricht das am ehesten dem klassischen „Hacker“, wenn zu Beginn des Angriffs kein finanzielles Interesse im Vordergrund steht. Ist das der Fall, können Angreifer dem Spektrum der professionellen Kriminalität zugeordnet werden. Wie eingangs erwähnt, gibt es neben den Fällen, in denen Fahrzeugbesitzer an ihren eigenen Fahrzeugen Eingriffe vornehmen oder vornehmen lassen, die Fälle, in denen sich die Angriffe gegen fremdes Eigentum richten. Die Angreifer lassen sich in drei Motivbereiche aufteilen: finanziell, politisch und schädigend, wobei es zwischen diesen Gruppen durchaus Überschneidungen geben kann.

Finanziell motiviert sind beispielsweise „professionelle“ Akteure, die im Auftrag von Dritten die (unter Kapitel 2.1.1) beschriebenen Veränderungen durchführen, oder Fahrzeugdiebe, die sich durch Manipulationen Zugang zum Fahrzeug verschaffen, um dies zu stehlen. Aber auch das Deaktivieren von Trackingsystemen (vgl. Kapitel 2.1.2) fällt in diesen Bereich, so wie derzeit noch eher „exotische“ Fälle, in denen dubiose Werkstätten durch das absichtliche Herbeiführen von Fehlerzuständen den Kunden zu teuren Reparaturen verleiten wollen.

In den Bereich der destruktiv motivierten Personen (Politik oder Vandalismus) fallen am ehesten terroristische Ambitionen. Hier trennt sich das Feld in zwei „Lager“: zum einen die potenziellen Attentäter, die mit ihrem Fahrzeug einen möglichst großen Schaden an Mensch und Infrastruktur anstreben, und zum zweiten potenzielle Personen, die gezielt bestimmte Personen aus Wirtschaft und Politik schädigen. Letztere könnten sich dabei Techniken zur Veränderung bedienen, die entweder den Fahrer zum Anhalten verleiten (z. B. durch das Provozieren einer Reifendruckwarnung wie in [R146] praktisch demonstriert) oder gezielt Fehlverhalten des Fahrzeuges provozieren (z. B. indem der Abstand zum vorausfahrenden Fahrzeug im adaptiven Geschwindigkeitsregelsystem – engl. Adaptive Cruise Control, ACC – auf minus 50 Meter eingestellt wird. In Kombination mit einer falschen Abstandsanzeige und abgeschalteter Übernahmewarnung könnte dies mindestens zu einem mittelschweren Auffahrunfall führen). Auch das Abhören sensibler Daten – etwa unter Zuhilfenahme der Freisprechanlage im Fahrzeug (vgl. auch Kapitel 2.1.1) – fällt in den Bereich politischer Motivation, könnte jedoch auch im kommerziellen Feld bei Industriespionage Anwendung finden. Aber auch Privatpersonen und deren Daten können in den Fokus von Kriminellen geraten – beispielsweise um mit der Identität einer anderen Person Straftaten durch-

zuführen und zu verdecken (vgl. betrügerisches Erlangen) [R55]. Ferner könnten in zukünftigen Szenarien Formen von elektronischem Vandalismus eine Rolle spielen. Vorstellbar sind in diesem Kontext gezielte Angriffe auf die elektronischen Fahrzeugkomponenten mit dem Ziel deren Zerstörung.

Zusammenfassend stellen demnach technisch ambitionierte Privatpersonen, Dienstleister (professionelle Akteure) und Fahrzeugbesitzer (die diese Dienstleistung bezahlen, also den Markt schaffen) das Gros des Spektrums der beteiligten Personen dar.

Mit Blick auf die Konsequenzen, die sich aus unsachgemäß durchgeführten Veränderungen ergeben, muss jedoch das Spektrum auf alle Angreifertypen erweitert werden. Denn durch die Abhängigkeit von der Reaktion des Fahrers können selbst triviale Fehlfunktionen eine Kettenreaktion in Gang setzen, wenn beispielsweise Fahrer auf solche Fehlfunktionen unangemessen reagieren.

Bezüglich unterschiedlicher Ebenen von Angreiferwissen und -ressourcen können drei unterschiedliche allgemeine Angreiferklassen zusammengefasst werden:

- A1: Privatperson: Hierunter fallen in der Regel Bastler und Hobbyschrauber sowie „klassische Hacker“. Die ihnen typischerweise zur Verfügung stehende Werkzeugausrüstung beschränkt sich auf generische Werkzeuge und Messtechnik (u. a. Laptop, Oszilloskop, einfache Löttechnik usw.).
- A2: Profi: Professionell organisierte Akteure wie Tuning- und Zubehöranbieter und Werkstätten zählen im Allgemeinen zu dieser Klasse, die kommerziell oder als Freundschaftsdienste agieren können. Sie haben üblicherweise Zugriff auf umfangreiche Spezialausrüstung, die häufig markenübergreifende Test- und Diagnosetechnik einschließt. Diese ist üblicherweise in ihrer Funktionalität eingeschränkt verglichen mit dem Leistungsumfang von herstellerunterstützter Werkstattausrüstung. Auch der Großteil krimineller Akteure mit durchschnittlicher Erfahrung kann in diese Klasse eingeordnet werden.
- A3: Spezialist: Die dritte Klasse beinhaltet Spezialisten mit besonderem Fachwissen. Darunter zählen z. B. Innentäter (z. B. aus der Fahrzeugentwicklung) sowie besonders geschulte Angehörige der organisierten Kriminalität. Auch Forscher, die als „Proof of Concept“ Sicherheitslücken demonstrieren, können dieser Klasse zugeordnet werden. Diese haben üblicherweise Zugriff auf Ausrüstung, welche z. B. auch Händlerbetriebe und Werksniederlassungen sowie z. T. Zulieferer und Entwickler haben. Hier kann auch von einem Zugriff auf Software sowie deren Modifikation für eigene Zwecke ausgegangen werden.

Die oben eingeführten Angreiferklassen werden im weiteren Verlauf des vorliegenden Dokumentes verwendet. Unter anderem nach diesen Klassen werden im folgenden Kapitel 3.3 die Rechercheergebnisse aufbereitet und in Kapitel 5.1.3 potenzielle Gefährdungen aus elektronischen Veränderungen abgeschätzt.

3.3 Aufbereitung der Rechercheergebnisse nach Angreiferwissen

Eine Aufarbeitung der Rechercheergebnisse nach dem für die Veränderungen notwendigen Angreifer-

Angreiferklasse	Quellenauflistung	Summe
A1/ Privatperson (Amateur/ Laie)	[R02], [R03], [R04], [R08], [R09], [R10], [R12], [R13], [R14], [R15], [R16], [R17], [R18], [R21], [R24], [R25], [R26], [R27], [R28], [R29], [R30], [R31], [R32], [R33], [R34], [R35], [R36], [R37], [R39], [R40], [R41], [R42], [R44], [R45], [R46], [R47], [R48], [R59], [R61], [R63], [R64], [R65], [R66], [R67], [R68], [R69], [R73], [R76], [R77], [R78], [R81], [R82], [R83], [R84], [R85], [R86], [R89], [R92], [R93], [R94], [R103], [R104], [R105], [R106], [R107], [R111], [R112], [R115], [R116], [R117], [R118], [R120], [R121], [R122], [R123], [R124], [R125], [R126], [R128], [R130], [R131], [R132], [R133], [R135], [R136], [R137], [R139], [R140], [R141], [R142], [R143]	91
A2/Profi	[R01], [R22], [R28], [R33], [R34], [R35], [R39], [R41], [R42], [R43], [R44], [R46], [R47], [R48], [R49], [R50], [R51], [R52], [R53], [R55], [R56], [R57], [R59], [R60], [R62], [R70], [R73], [R74], [R75], [R76], [R77], [R80], [R85], [R87], [R88], [R89], [R90], [R92], [R93], [R98], [R100], [R101], [R102], [R103], [R109], [R110], [R111], [R112], [R113], [R122], [R123], [R125], [R126], [R127], [R128], [R133], [R134], [R135], [R138], [R143]	60
A3/ Spezialist	[R05], [R11], [R19], [R20], [R54], [R58], [R71], [R72], [R79], [R99], [R144], [R145], [R146]	13

Tab. 6: Aufbereitung der recherchierten Quellen nach Einschätzung des notwendigen Angreiferwissens

wissen und -ressourcen (vgl. Kapitel 3.2) wurde in Tabelle 6 vorgenommen. Hierbei wurden die Rechercheergebnisse denjenigen Angreiferklassen zugeordnet, die bezüglich der enthaltenen Anzeichen auf Veränderungen tendenziell zuzuordnen sind.

Dabei kann die Summe der bisher gefundenen Referenzen als ein erstes Maß zur Verbreitung bzw. praktischen Bedeutung von Veränderungen an den entsprechenden Komponentenklassen bzw. mit dem entsprechenden Angreiferwissen gesehen werden. Rechercheergebnisse, die sich an die Zielgruppe Amateure bzw. „Hobbyschrauber" richten (Angreiferklasse A1/Privatpersonen), wurden deutlich häufiger recherchiert. Das Involvieren von Fachpersonal (Angreiferklasse A2/Profis) ist auch vergleichsweise häufig Thema der Diskussionen, da höchstwahrscheinlich nicht jede Privatperson die nötige Ausstattung und Erfahrung hat. Diese beiden Mengen überschneiden sich teilweise, zumal in Artikeln wie [R45] die Anschaffung von Softwareausstattung, die generell eher in (freien) Werkstätten (A2) anzusiedeln ist, zunehmend auch für den ambitionierten Privatanwender (A1) als sinnvoll dargestellt wird.

3.4 Abschließende Abschätzung zur Relevanz der Schwachstellen

Entsprechend der zugrunde liegenden Vorgehensweise (siehe Kap. 1.2) wurden die vorgestellten Recherchefälle nach der Abschätzung der Bedrohungslage auch bezüglich der Relevanzen der jeweils zugrunde liegenden Schwachstellen eingeschätzt.

Die Relevanz wurde jeweils bestimmt aus dem Verhältnis aus „Kosten" und „Nutzen", die jeweils kategorial abgeschätzt wurden (niedrig, mittel, hoch). Konkret wurden bei dieser Abschätzung daher folgende drei wesentliche Faktoren berücksichtigt:

- Die Art der Schwachstellen:

  Bezüglich der recherchierten Veränderungen werden aus den in Kapitel 3.1 vorgestellten Schwachstellenkategorien diejenigen ausgewählt, die sich als besonders relevant für den jeweiligen Fall einschätzen lassen.

- Die Einfachheit der Veränderung:

  Für die „Kosten" wurde je nach Art der ausgenutzten Schwachstellen (vgl. Kapitel 3.1) die resultierende Einfachheit der Veränderung abgeschätzt, welche sich aus dem nötigen Angreiferwissen ergibt. Je leichter eine bestimmte Schwachstelle für Veränderungen nutzbar ist, desto höher ist entsprechend die Einfachheit und vice versa (vgl. Kapitel 3.2). In der Folge ist eine Schwachstelle praktisch von desto geringerer Relevanz, je höher der für ihre Ausnutzung verbundene Aufwand ist (d. h. je niedriger die Einfachheit der Realisierung ist).

- Der subjektive Zugewinn für den Nutzer:

  Die Abschätzung des „Nutzens" wurde auf Basis des subjektiven Zugewinns für den Nutzer bestimmt. Diese basiert auf der potenziellen Motivation (siehe Spalte 2 der Teilergebnistabellen). Die Kategorisierung des Nutzens basiert auf den Einschätzungen zweier Kfz-Mechaniker und eines Diplom-Psychologen. Dabei wurde der relative Zugewinn in Bezug auf eine Komponente vor und nach der Veränderung herangezogen. Es wurden dafür ausschließlich die erwünschten Effekte betrachtet, im Bericht bezeichnet als Nutzenfunktions- und Nutzenstrukturwirkung (vgl. Tabelle 14).

Dieses Vorgehen soll anhand eines Beispiels verdeutlicht werden: Die Komponente sei die Motorsteuerung, die Motivation sei Leistungssteigerung. Die Art der Schwachstelle sei das Remapping (siehe Glossar), welche relativ schwierig realisierbar, also mit mittlerem Aufwand und/oder Kosten verbunden ist. Dadurch sei eine Leistungssteigerung von ca. 20 % zu erreichen, was im Falle eines 100 PS starken Motors 20 PS entspricht. Der Zugewinn für den Nutzer lässt sich als hoch einschätzen, denn im Vergleich zu anderen leistungssteigernden Veränderungen sind 20 % relativ viel. Somit ergibt sich ein Verhältnis bzw. Relevanz der Schwachstelle aus „Kosten" und „Nutzen" im Bereich mittel bis hoch.

Die Ergebnisse der entsprechend dieser Faktoren vorgenommenen Abschätzung der Schwachstellen sind in Tabelle 7 zusammengestellt.

Beispielsweise wurden die – in Kapitel 2 bezüglich der Bedrohungslage als „hoch" eingeschätzten – Manipulationen am Kilometerstand mit Blick auf die Relevanz der Schwachstellen mit „mittel bis hoch" abgeschätzt: Während der subjektive Zugewinn für den Nutzer ebenfalls als „hoch" abzuschätzen ist (z. B. Steigerung Verkaufswert), wird der Aufwand der Veränderung jedoch durch zunehmend komplexe Schutzvorkehrungen erhöht. Je nach Alter

				Abschätzung Schwachstellen			
Art der Komponente (Teilfunktion)		**Potenzielle Motivation für die Veränderung**	**Abschätzung Bedrohungs-lage (Kap. 2)**	**Art der Schwachstelle (Art der Veränderung)**	**Geschätzte Einfachheit der Veränderung**	**Geschätzter subjektiver Zugewinn für den Nutzer**	**Abschätzung Relevanz der Schwachstelle**
Motor und Antriebsstrang	Motorsteuerung	Leistungssteigerung	mittel - hoch	S4, S5 (Remapping, Chiptausch, Sensorik/Aktorik)	niedrig - mittel	hoch	mittel - hoch
		Verbrauchsreduktion	mittel	S4 (Remapping)	niedrig	hoch	mittel
		Nachrüstung von Regelungsfunk-tionen für Autogasanlage (Senkung Betriebskosten)	mittel - hoch	S4, S5 (Remapping, nachträglich Einbringen/Austausch von Chips, Sensorik, Aktorik)	niedrig	hoch	mittel
		Motor bzw. Fahrzeug zum Stillstand bringen (destruktive Motivation)	mittel	S3 (Einspielen von Befehlen über CAN)	hoch	hoch	hoch
	Motorsteuerung (Abgasrückführung)	Deaktivieren	niedrig	S1 (Konfiguration über OBD)	hoch	mittel	hoch
	Motorsteuerung (Geschwin-digkeits-Abregelung)	Deaktivieren	mittel	S1 (Konfiguration über OBD) S3 (vMax-Modul), S4 (Remapping)	niedrig	hoch	mittel
	Getriebesteuerung (Auto-matikgetriebe, elektronische Schaltpunktsteuerung)	Schaltpunkte verändern	niedrig	S1 (Konfiguration über OBD). S5 (Remapping)	hoch	mittel	mittel - hoch
	Getriebesteuerung (pseudo-automatisierte Schaltung)	Nachrüstung	niedrig - mittel	S2/S3 (Abgreifen A/D-Signale), S5 (physischer Zugriff)	niedrig - mittel	mittel	niedrig - mittel
	Startsteuerung	Motorstart auf Knopfdruck (Startknopf nachrüsten)	niedrig	S2 (analoges Kabel), S5 (physischer Zugriff)	mittel	niedrig	niedrig - mittel
Fahrwerksysteme	Servolenkung	Härtere Einstellung	mittel	S1 (Konfiguration über OBD)	hoch	mittel	mittel - hoch
		Mehr Fahrleistung (Ersetzen durch eine elektronisch gesteuerte und elektrisch angetriebene Servo-lenkung, adaptive Regelung)	niedrig	S2/S3 (Abgreifen A/D-Signale), S5 (physischer Zugriff)	niedrig - mittel	mittel	niedrig - mittel
	Adaptive Niveauregelung	Elektronisches Tieferlegen	niedrig - mittel	S1 (Konfiguration über OBD)	hoch	mittel - hoch	mittel - hoch
	Fahrdynamikkregelsysteme	Deaktivieren einzelner Funktionen (z. B. ABS oder ESP)	mittel	S1 (Konfiguration), S5 (Stromtrennung)	hoch	hoch	hoch
		Einleiten unerwünschter/Verhindern gewünschter Bremsvorgänge (destruktive Motivation)	niedrig - mittel	S3 (Einspielen von Befehlen über CAN)	hoch	hoch	hoch
Passive Sicherheit	Airbagsystem/Gurtstraffer	Verbergen der Nichtfunktionalität	mittel	S1 (Konfiguration), S2/S3 (Fälschen A/D-Signale), S5 (physischer Zugriff)	mittel - hoch	hoch	mittel - hoch
Fahrerassistenz-systeme	Längsführung (Tempomat)	Nachrüstung nicht vorhandener Funktion	niedrig - mittel	S2/S3 (Abgreifen A/D-Signale), S5 (physischer Zugriff)	niedrig	hoch	mittel
		Freischaltung nicht aktiver Funktion	mittel - hoch	S1 (Konfiguration), S5 (Schaltertausch)	mittel - hoch	hoch	mittel - hoch
	Längsführung (ACC)	Mindestabstand verringern	mittel	S1 (Konfiguration)	hoch	hoch	hoch
	Querführung	Aktiven Assistenten nachrüsten	mittel	S2/S3 (Abgreifen A/D-Signale), S5 (physischer Zugriff)	niedrig - mittel	mittel	niedrig - mittel
Infotainment	Instrumentenkombination (Wegstreckenzähler)	Kilometerstand ändern	hoch	S1 (Konfiguration), S2 (analoge Signale), S3 (digitale Signale)	niedrig - mittel	hoch	mittel - hoch
	Instrumentenkombination (Serviceintervallanzeige)	Zurücksetzen	mittel - hoch	S1 (Konfiguration)	hoch	mittel	mittel - hoch
	Instrumentenkombination (Fahrerinformationssystem)	Beschreiben mit eigenen Inhalten (es wurden konstruktive wie destruktive Motivationen ermittelt)	mittel	S3 (digitale Signale)	mittel	mittel	mittel
	Radio	Anheben der Lautstärke auf Maximum (destruktive Motivation)	mittel	S3 (Einspielen von Befehlen über CAN)	hoch	niedrig	mittel
	Navigationssystem	Kostenloses Nachinstallieren von Kartenmaterial	mittel - hoch	kein bzw. unsicherer Kopierschutz der Medien	mittel - hoch	hoch	mittel - hoch
		Installieren von POI („Blitzer"-Positionen etc.)	mittel - hoch	S1 (Konfiguration)	hoch	hoch	hoch
		Eigene Änderungen an Betriebssoftware und -daten	niedrig - mittel	S1 (Konfiguration)	mittel	mittel	mittel
	Navigationssystem (Fahrschulfunktion)	Aktivierung	niedrig	S1 (Konfiguration)	hoch	mittel	mittel - hoch
	Video-System	TV In Motion	mittel	S1 (Konfiguration), S2 (analoge Signale), S3 (digitale Signale)	hoch	hoch	hoch
	Allgemeine Warnfunktionen	Deaktivieren (z. B. Gurtwarner)	mittel - hoch	S1 (Konfiguration), S2 (Trennung Sensor/Aktor), S3 (Fälschen digitale Eingabewerte)	hoch	mittel	mittel - hoch
		Provozieren von Warnungen (z. B. Reifendruckkontrolle) durch Dritte, um Fahrer zum Anhalten zu verleiten (destruktive Motivation)	niedrig - mittel	S3 (Möglichkeit für Spoofing gefälschter Werte per Funk)	mittel	mittel	mittel

Tab. 7: Abschätzung der Schwachstellen (zweite Teilergebnistabelle)

				Abschätzung Schwachstellen			
Art der Komponente (Teilfunktion)		Potenzielle Motivation für die Veränderung	Abschätzung Bedrohungs-lage (Kap. 2)	Art der Schwachstelle (Art der Veränderung)	Geschätzte Einfachheit der Veränderung	Geschätzter subjektiver Zugewinn für den Nutzer	Abschätzung Relevanz der Schwachstelle
Zugriffsschutz (Security)	Schließsystem (Zugang durch Funköffner)	Unberechtigtes Öffnen	mittel	S3 (Funk)	niedrig	mittel	niedrig - mittel
		Verhindern des Verschließens durch Jamming	mittel - hoch	S3 (Störbarkeit Funk)	hoch	mittel	mittel - hoch
	Schließsystem (Autolock-Funktion)	Nachrüsten/Aktivieren	mittel	S1 (Konfiguration)	hoch	mittel	mittel - hoch
	Schließsystem	Ein-/Aussperren der Fahrzeug-nutzer (destruktive Motivation)	mittel	S3 (Einspielen von Befehlen über CAN)	hoch	niedrig	mittel
	Diebstahlwarnanlage	Unberechtigte Deaktivierung	mittel	S2 (analoge Signale), S3 (digitale Signale)	niedrig	hoch	mittel - hoch
		Einbindung eines Nachrüst-Kits	niedrig - mittel	S2 (analoge Signale), S3 (digitale Signale), S5 (physischer Zugriff)	niedrig - mittel	hoch	mittel
		Setzen der „Anti-Polenschlüssel"-Kodierung	niedrig - mittel	S1 (Konfiguration)	hoch	mittel	mittel - hoch
	Wegfahrsperre	Unberechtigte Deaktivierung	mittel	S2 (analoge Signale), S3 (digitale Signale)	niedrig	hoch	mittel - hoch
		Einbindung eines Nachrüst-Kits	niedrig - mittel	S2 (analoge Signale), S3 (digitale Signale), S5 (physischer Zugriff)	niedrig - mittel	hoch	mittel
Karosserie	Lichtanlage (Frontscheinwerfer)	Nachrüsten Xenon-Licht	mittel - hoch	S2/S3 (analoge/digitale Signale lesen), S5 (physischer Zugriff)	niedrig - mittel	hoch	mittel - hoch
	Lichtanlage (Steuerprogramme)	Aktivieren/Entfernen diverser Schaltoptionen	mittel	S1 (Konfiguration)	hoch	mittel	mittel - hoch
	Außenspiegel (elektr. Anklappfunktion)	Nachrüstung zur Komforterhöhung	mittel	S2 (analoge Steuerung), S5 (physischer Zugriff)	mittel	mittel	mittel
		Betätigung während der Fahrt	niedrig	S1 (Konfiguration), S2 (analoge Signale), S3 (digitale Signale)	mittel - hoch	mittel	mittel
	Verdeck	Betätigung während der Fahrt	niedrig - mittel	S2/S3 (Fälschen A/D-Signale)	mittel - hoch	mittel - hoch	mittel - hoch
	Klimasteuerung	Verringern des Komforts durch Dritte (destruktive Motivation)	niedrig - mittel	S3 (Einspielen von Befehlen über CAN)	hoch	niedrig	mittel
Infrastrukturkomponenten	Funkschnittstellen (Ortungssysteme)	Unterdrückung (Jamming) gegen Tracking, Maut, Steuer, Überwachung	niedrig - mittel	S3 (Digital-Funk)	hoch	hoch	hoch
	Funkschnittstellen (Verkehrsinformationen)	Senden gefälschter Verkehrs-Meldungen z. B. eigenen Vorteil	niedrig - mittel	S3 (Digital-Funk)	niedrig	mittel	niedrig - mittel
	Funkschnittstellen (Fernbedienfunktionen)	Nachrüsten von Fernbedien-funktionen (z. B. für Standheizung, Zentralverriegelung)	mittel	S5 (physischer Zugriff)	niedrig	hoch	mittel
	Verkehrstelematik (autarke elektron. Verkehrstafel)	Unberechtigtes Anzeigen eigener Inhalte	niedrig	S1 (Konfiguration)	hoch	mittel	mittel - hoch
	Geschwindigkeits-Mess-einrichtungen	Warnung vor Messungen	mittel - hoch	S3 (Detektierbarkeit Funk)	hoch	hoch	hoch
		Störung von Messungen	niedrig - mittel	S3 (Störbarkeit Funk)	niedrig	hoch	mittel

Tab. 7: Fortsetzung

und Modell wurde daher die Einfachheit der Veränderung zwischen „niedrig" und „mittel" abgeschätzt.

Als Schwachstellen mit Relevanz „hoch" wurden unter anderem die Detektierbarkeit und Störbarkeit von Funkschnittstellen abgeschätzt. Ein Schutz gegen gezielte Störung (Denial of Service, siehe Glossar) lässt sich auf dieser Ebene physikalisch bedingt praktisch nicht verhindern. Insbesondere im Bereich der Infrastruktursysteme können funkbasierte Systeme z. B. zur Mauterfassung, Geschwindigkeitsmessung, Tracking etc. so gezielt zu stören versucht werden, sofern diese keine zusätzlichen ergänzenden Sicherheitsvorkehrungen vorsehen.

4 Abschätzung des potenziellen Risikos durch Bewertung der Auftrittswahrscheinlichkeit elektronischer Veränderungen

Der nächste Schritt nach der zugrunde gelegten Vorgehensweise ist die Abschätzung des Risikos. Ziel ist daher, die Auftrittswahrscheinlichkeit der in den Rechercheergebnissen ermittelten Beispiele einzuschätzen. Dies erfolgt gemäß der in Kapitel 1.2 vorgestellten Vorgehensweise unter Einbeziehung der in den beiden vorangegangenen Schritten getroffenen Abschätzungen für die Bedrohungslage und die Schwachstellen.

Das Ergebnisse dieser Auswertung werden in Kapitel 4.1 erneut in der tabellarischen Form vorgestellt.

Anschließend werden diese Ergebnisse validiert und durch weitere Aspekte ergänzt. Dies erfolgt im abschließenden Kapitel 4.2.

4.1 Bewertung der Auftrittswahrscheinlichkeit aus der Risikoanalyse als Kombination der Abschätzungen für Bedrohungslage und Schwachstellen

Die Abschätzung des Risikos folgt dem in dem Kapitel 1.2 vorgestellten Zusammenhang Bedrohungslage x Schwachstellen = Risiko (engl.: Threat x Vulnerability = Risk).

Dazu wurden für die in der Recherche ermittelten Veränderungsfälle die zuvor getroffenen Abschätzungen verknüpft und so die Abschätzung für die Größenordnung des vorliegenden Risikos vorgenommen. Die Ergebnisse dieser Risikoabschätzung sind in Tabelle 8 zusammengefasst.

Bei den Auswertungen zur Bedrohungslage und der Relevanz der Schwachstellen wurde für keine Veränderung gleichzeitig die Abschätzung „hoch“ vergeben. In Tabelle 8 wurde jedoch an zwei Stellen eine Kombination von „hoch“ und „mittel - hoch“ (bzw. umgekehrt) auf die Gesamteinschätzung „hoch“ für das vorliegende Risiko aufgerundet. Demnach wird die praktische Auftretenswahrscheinlichkeit insbesondere bei der Kilometerstandsmanipulation als auch dem Installieren von POI-Daten mit Standorten von Geschwindigkeitsmesseinrichtungen als besonders hoch abgeschätzt.

Mit Blick auf Veränderungen von Infrastruktursystemen ergibt sich als Risikoabschätzung maximal der Wert „mittel“. Lediglich eine Veränderung mit Bezug zu infrastrukturellen Systemen erreicht die Abschätzung „mittel - hoch“. Dies ist der Einsatz von Geräten zur Warnung vor Geschwindigkeitsmesseinrichtungen. Bzgl. Geräten zur gezielten Störung von Messungen ergibt sich aufgrund der geringeren Bedrohungslage (vergleichsweise geringere Verbreitung) und Schwachstellenrelevanz (aufwändigere Realisierung) nur eine Risikoabschätzung „mittel“.

					Potenzielles Risiko
Art der Komponente (Teilfunktion)		**Potenzielle Motivation für die Veränderung**	**Abschätzung Bedrohungslage (Kap. 2)**	**Abschätzung Schwachstellen (Kap. 3)**	**Bewertung nach Zusammenhang in [1]**
Motor und Antriebsstrang	Motorsteuerung	Leistungssteigerung	mittel - hoch	mittel - hoch	mittel - hoch
		Verbrauchsreduktion	mittel	mittel	mittel
		Nachrüstung von Regelungsfunktionen für Autogasanlage (Senkung Betriebskosten)	mittel - hoch	mittel	mittel - hoch
		Motor bzw. Fahrzeug zum Stillstand bringen (destruktive Motivation)	mittel	hoch	mittel - hoch
	Motorsteuerung (Abgasrückführung)	Deaktivieren	niedrig	hoch	mittel
	Motorsteuerung (Geschwindigkeits-Abregelung)	Deaktivieren	mittel	mittel	mittel
	Getriebesteuerung (Automatikgetriebe, elektronische Schaltpunktsteuerung)	Schaltpunkte verändern	niedrig	mittel - hoch	mittel
	Getriebesteuerung (pseudo-automatisierte Schaltung)	Nachrüstung	niedrig - mittel	niedrig - mittel	niedrig - mittel
	Startsteuerung	Motorstart auf Knopfdruck (Startknopf nachrüsten)	niedrig	niedrig - mittel	niedrig
Fahrwerksysteme	Servolenkung	Härtere Einstellung	mittel	mittel - hoch	mittel - hoch
		Mehr Fahrleistung (Ersetzen durch eine elektronisch gesteuerte und elektrisch angetriebene Servolenkung, adaptive Regelung)	niedrig	niedrig - mittel	niedrig
	Adaptive Niveauregelung	Elektronisches Tieferlegen	niedrig - mittel	mittel - hoch	mittel
	Fahrdynamikkregelsysteme	Deaktivieren einzelner Funktionen (z. B. ABS oder ESP)	mittel	hoch	mittel - hoch
		Einleiten unerwünschter/Verhindern gewünschter Bremsvorgänge (destruktive Motivation)	niedrig - mittel	hoch	mittel - hoch
Passive Sicherheit	Airbagsystem/Gurtstraffer	Verbergen der Nichtfunktionalität	mittel	mittel - hoch	mittel
Fahrerassistenzsysteme	Längsführung (Tempomat)	Nachrüstung nicht vorhandener Funktion	niedrig - mittel	mittel	niedrig - mittel
		Freischaltung nicht aktiver Funktion	mittel - hoch	mittel - hoch	mittel - hoch
	Längsführung (ACC)	Mindestabstand verringern	mittel	hoch	mittel - hoch
	Querführung	Aktiven Assistenten nachrüsten	mittel	niedrig - mittel	niedrig - mittel

[1] **Risiko = Bedrohungslage x Schwachstelle** mit
Bedrohungslage = Verbreitung der Komponente x Verbreitung der Informationen über Veränderungsmöglichkeiten
Schwachstelle = Einfachheit der Realisierung x Nutzen

Tab. 8: Bewertung des potenziellen Risikos nach: Bedrohungslage x Schwachstellen = Risiko (dritte Teilergebnistabelle)

					Potenzielles Risiko
Art der Komponente (Teilfunktion)		**Potenzielle Motivation für die Veränderung**	**Abschätzung Bedrohungslage (Kap. 2)**	**Abschätzung Schwachstellen (Kap. 3)**	**Bewertung nach Zusammenhang in [1]**
Infotainment	Instrumentenkombination (Wegstreckenzähler)	Kilometerstand ändern	hoch	mittel - hoch	hoch
	Instrumentenkombination (Serviceintervallanzeige)	Zurücksetzen	mittel - hoch	mittel - hoch	mittel - hoch
	Instrumentenkombination (Fahrerinformationssystem)	Beschreiben mit eigenen Inhalten (es wurden konstruktive wie destruktive Motivationen ermittelt)	mittel	mittel	mittel
	Radio	Anheben der Lautstärke auf Maximum (destruktive Motivation)	mittel	mittel	mittel
	Navigationssystem	Kostenloses Nachinstallieren von Kartenmaterial	mittel - hoch	mittel - hoch	mittel - hoch
		Installieren von POI („Blitzer"-Positionen etc.)	mittel - hoch	hoch	hoch
		Eigene Änderungen an Betriebssoftware und -daten	niedrig - mittel	mittel	niedrig - mittel
	Navigationssystem (Fahrschulfunktion)	Aktivierung	niedrig	mittel - hoch	niedrig - mittel
	Video-System	TV In Motion	mittel	hoch	mittel - hoch
	Allgemeine Warnfunktionen	Deaktivieren (z. B. Gurtwarner)	mittel - hoch	mittel - hoch	mittel - hoch
		Provozieren von Warnungen (z. B. Reifendruck-kontrolle) durch Dritte, um Fahrer zum Anhalten zu verleiten (destruktive Motivation)	niedrig - mittel	mittel	niedrig - mittel
Zugriffsschutz (Security)	Schließsystem (Zugang durch Funköffner)	Unberechtigtes Öffnen	mittel	niedrig - mittel	niedrig - mittel
		Verhindern des Verschließens durch Jamming	mittel - hoch	mittel - hoch	mittel - hoch
	Schließsystem (Autolock-Funktion)	Nachrüsten/Aktivieren	mittel	mittel - hoch	mittel
	Schließsystem	Ein-/Aussperren der Fahrzeugnutzer (Destruktive Motivation)	mittel	mittel	mittel
	Diebstahlwarnanlage	Unberechtigte Deaktivierung	mittel	mittel - hoch	mittel
		Einbindung eines Nachrüst-Kits	niedrig - mittel	mittel	mittel
		Setzen der „Anti-Polenschlüssel"-Kodierung	niedrig - mittel	mittel - hoch	mittel
	Wegfahrsperre	Unberechtigte Deaktivierung	mittel	mittel - hoch	mittel
		Einbindung eines Nachrüst-Kits	niedrig - mittel	mittel	mittel
Karosserie	Lichtanlage (Frontscheinwerfer)	Nachrüsten Xenon-Licht	mittel - hoch	mittel - hoch	mittel - hoch
	Lichtanlage (Steuerprogramme)	Aktivieren/Entfernen diverser Schaltoptionen	mittel	mittel - hoch	mittel
	Außenspiegel (elektr. Anklappfunktion)	Nachrüstung zur Komforterhöhung	mittel	mittel	mittel
		Betätigung während der Fahrt	niedrig	mittel	niedrig - mittel
	Verdeck	Betätigung während der Fahrt	niedrig - mittel	mittel - hoch	mittel
	Klimasteuerung	Verringern des Komforts durch Dritte (destruktive Motivation)	niedrig - mittel	mittel	niedrig - mittel
Infrastrukturkomponenten	Funkschnittstellen (Ortungssysteme)	Unterdrückung (Jamming) gegen Tracking, Maut, Steuer, Überwachung	niedrig - mittel	hoch	mittel
	Funkschnittstellen (Verkehrsinformationen)	Senden gefälschter Verkehrs-Meldungen z. B. eigenen Vorteil	niedrig - mittel	niedrig - mittel	niedrig - mittel
	Funkschnittstellen (Fernbedienfunktionen)	Nachrüsten von Fernbedienfunktionen (z. B. für Standheizung, Zentralverriegelung)	mittel	mittel	mittel
	Verkehrstelematik (autarke elektron. Verkehrs-tafel)	Unberechtigtes Anzeigen eigener Inhalte	niedrig	mittel - hoch	niedrig - mittel
	Geschwindigkeits-Messeinrichtungen	Warnung vor Messungen	mittel - hoch	hoch	mittel - hoch
		Störung von Messungen	niedrig - mittel	mittel	mittel

[1] **Risiko = Bedrohungslage x Schwachstelle** mit
Bedrohungslage = Verbreitung der Komponente x Verbreitung der Informationen über Veränderungsmöglichkeiten
Schwachstelle = Einfachheit der Realisierung x Nutzen

Tab. 8: Fortsetzung

4.2 Verifikation und Ergänzung der tabellarischen Risikobewertung

Ergänzend zu der in Kapitel 4.1 vorgenommenen Bewertung des Risikos, die auf Basis von Bedrohungslage und Schwachstellen vorgenommen wurde, werden in diesem Kapitel weitere Faktoren einbezogen. Ziel ist es, die Bewertungen zu verifizieren und ggf. zu ergänzen.

4.2.1 Informationen von Experten

Ein begrenzender Faktor der bis hierher verfolgten Vorgehensweise, hauptsächlich Informationen aus öffentlich zugänglichen Quellen einzubeziehen, ist die Berücksichtigung der Dunkelziffer zu Aktivitäten insbesondere im rechtlich kritischen Bereich. Aus Bedenken bezüglich einer eventuellen Strafverfolgung werden voraussichtlich einige Motivationen und Bestrebungen von den entsprechenden Personen nicht öffentlich kundgetan. Auch unterbinden

viele Foren Fragen nach rechtlich problematischen Themen in ihren Teilnahmebedingungen und kritische Diskussionen werden durch Moderatoren gesperrt bzw. gelöscht.

Daher wurden zusätzlich auch Aussagen von Fachkundigen mit einbezogen. Dennoch können auch diese nur eine weitere Ergänzung darstellen und wie die anderen Ansätze keinen Anspruch auf Vollständigkeit begründen.

Dem Ansatz folgend, dass gerade professionelle Tuner einen umfassenden Überblick der verschiedenen Arten von Veränderungen haben und die Verteilung ihres Auftretens in der Praxis abschätzen können, wurde versucht, einige ausgewählte Vertreter dieses Geschäftsfeldes ausfindig zu machen, und diese gebeten, in inoffiziellen Gesprächen eine Auskunft zu geben. Dieses Vorgehen stellte sich praktisch insofern schwierig dar, als dass sehr wenige Tuner zu einem Gespräch bereit waren. Jedoch konnte auf bereits bestehende Kontakte zurückgegriffen werden, die an dieser Stelle jedoch nicht namentlich genannt werden wollen. Die Aussage eines Anbieters teilt sich in zwei Kategorien: zum Einen in offizielle Aufträge und zum Zweiten so genannte inoffizielle Aufträge. Daraus ergaben sich grobe Kategorien der nachgefragten Änderungen sowie ungefähre Abschätzungen zu der relativen Häufigkeit entsprechender Aufträge. Diese sind für die offiziellen Aufträge in Tabelle 9 und für die inoffiziellen Aufträge in Tabelle 10 aufgeführt.

Ein weiterer Anbieter schätzte die Ausprägungen seiner Aufträge ähnlich ab, wie in Tabelle 11 ersichtlich ist.

Nach den Aussagen dieses zweiten Anbieters werden die „getuneten“ Kraftfahrzeuge in den meisten Fällen ohne aktualisierte Zulassung im Straßenverkehr weiter bewegt. Da sie damit meist nicht mehr den Vorschriften entsprechen, wollte auch dieser Anbieter anonym bleiben.

Generell wurde von den angesprochenen Tuninganbietern zurückgemeldet, dass das Auftragsvolumen gerade im elektronischen Bereich kontinuierlich zugenommen hat, während die Aufträge für nicht-elektronische Maßnahmen eher rückläufig sind.

Ergänzend werden Einschätzungen von fachkundigen Gutachtern einbezogen. Zwar konnten bei eigenen Versuchen der Kontaktaufnahme keine konkreten Aussagen bzgl. bekannter Vorfälle, die aus

Rang	Art des offiziellen Tuning-Auftrags	Häufigkeit (Schätzung)
1	Motortuning (Steuergerät): mehrheitlich Leistungssteigerung, aber auch zunehmend ECO Tuning	50 % (der offiziellen Aufträge)
2	Funktionsaktivierung (z. B. Coming-Home-Licht und TV)	30 % (der offiziellen Aufträge)
3	Weiteres (z. B. Freischalten von Sitzmemory und gewechselten Steuergeräten, Anlernen von Schlüsseln bei älteren Fahrzeugen)	20 % (der offiziellen Aufträge)

Tab. 9: Schätzung aus Gesprächen mit einem Tuninganbieter zu offiziellen Aufträgen

Rang	Art des inoffiziellen Tuning-Auftrags	Häufigkeit (Schätzung)
1	Tachojustierung	50 % (der inoffiziellen Aufträge)
2	Freischalten von Steuergeräten (Wegfahrsperre und Airbag – vor allem nach Tausch, ohne dass der Hersteller involviert werden muss)	30 % (der inoffiziellen Aufträge)
3	Gesperrte Geräte aktivieren (z. B. Radio oder Navigationssysteme nach falschen Codeeingaben)	20 % (der inoffiziellen Aufträge)

Tab. 10: Schätzung aus Gesprächen mit einem Tuninganbieter zu inoffiziellen Aufträgen

Rang	Art des Tuning-Auftrags	Häufigkeit (Schätzung)
1	Chiptuning (Steuergerät wird eingeschickt und modifiziert)	30 % (aller Aufträge)
2	Motorverändernde Maßnahmen (inkl. Austausch des Steuergerätes mit alternativer Hard- und/oder Software	40 % (aller Aufträge)
3	Nicht-elektronische Eingriffe/ Tuning wie z. B. Luftfilter	30 % (aller Aufträge)

Tab. 11: Schätzung aus Gesprächen mit einem weiteren Tuninganbieter zu bearbeiteten Aufträgen

vorsätzlichen, insbesondere elektronischen Veränderungen resultieren, erhalten werden. Allerdings findet sich in der recherchierten Quelle [R114] in einem Medienbericht eine diesbezügliche Aussage. Dort schätzte ein Vertreter der Dekra, dass der Kilometerstand in ca. ein Drittel der Gebrauchtfahrzeuge mit elektronischem Zähler manipuliert sei. Da dieser Artikel im Jahr 2002 erschien, ist fraglich, ob diese angegebene Größenordnung derzeit noch zutrifft. Zwar wurden seitens der Hersteller seitdem verstärkte Bemühungen zum Manipulationsschutz

des Kilometerstands betrieben; die Erfahrung zeigt aber, dass bis zu der Umgehung eines neuen Systems nur einige Monate bis wenige Jahre vergehen. Daher könnte davon auszugehen sein, dass die bereits in Kapitel 4.2.1 erfolgte Abschätzung der Fahrzeugtuner zutrifft und das Manipulieren von Kilometerständen weiterhin den häufigsten Eingriff (zumindest bzgl. inoffiziell durchgeführter Aufträge) mit hoher Dunkelziffer darstellen dürfte.

Das demnach ebenfalls häufig (offiziell) beauftragte Motortuning ist insbesondere auch im professionellen Einsatz als weit verbreitet anzusehen. Änderungen im Infotainmentbereich, die laut des Tunerberichtes in Kapitel 4.2.1 nur einen geringen Teil der Aufträge ausmachen, scheinen dagegen am stärksten im Privatbereich verbreitet zu sein (vgl. in Kapitel 2.3.1, „Kategoriebezogene Forenaktivität“). Das Kopieren von Kartenmaterial oder Beschaffen von „Blitzerinformationen“ als POI-Material scheint den Recherchen nach im Wesentlichen eigenständig durch die Endnutzer vorgenommen zu werden. Die Dienste von professionellen Anbietern werden im Infotainmentbereich demnach potenziell eher in Ausnahmefällen in Anspruch genommen, z. B. wenn Geräte nach der Eingabe falscher Zugriffscodes entsperrt werden müssen, wozu Kenntnisse und Ausstattung im Privatbereich offensichtlich meist nicht ausreichen bzw. in öffentlich zugänglichen Quellen auch nicht recherchiert wurden.

Als Fazit kann bezüglich der Häufigkeit und Verteilung von Veränderungen (d. h. der Abschätzung ihrer Auftrittswahrscheinlichkeit) vom Angebot-Nachfrage-Modell ausgegangen werden. Betrachtet man den Nachfragesektor – also das Bedürfnis von Fahrern, den (Serien~)Zustand ihres Fahrzeuges zu verbessern oder anzupassen –, wurden TV-in-motion, Leistungssteigerung, Abschalten von Gurtwarnungen und Tachomanipulation als besonders häufige Beispiele entsprechender Motive (z. B. in Internetforen) ermittelt (vgl. Kapitel 2). Dies konnte in der Begutachtung des Angebotes kommerzieller Tuninganbieter größtenteils bestätigt werden. Einschränkend muss an dieser Stelle hinzugefügt werden, dass die Nachfrage stark von der Serienausstattung abhängt. Bieten Fahrzeughersteller entsprechende Funktionalitäten ohne störend empfundene Einschränkungen an, brauchen diese nicht nachgerüstet werden. Dabei sind allerdings auch Fahrzeughersteller an Richtlinien und Gesetze gebunden, die ihrerseits einem zeitlichen Wandel unterlegen sind. Im Umkehrschluss kann dies auch zu Änderungen im Nachfrageverhalten der Fahrer führen.

5 Abschätzung potenzieller Gefahren aus elektronischen Veränderungen

Im vorliegenden Kapitel 5 wird (ergänzend zum in Kapitel 4 analysierten Risiko des Auftretens von Veränderungen) untersucht, inwieweit sich durch die vorgenommenen Eingriffe potenziell konkrete Gefährdungen für das einzelne Fahrzeug bis hin zum gesamten Straßenverkehr ergeben können.

Dazu werden einleitend im Kapitel 5.1 zunächst Vorbetrachtungen diskutiert, die für das Spektrum potenzieller Gefahren genereller Art im Automobilbereich sensibilisieren, und anhand theoretischer Grundlagen und praktischer Beispiele verdeutlicht.

Die Abschätzung praktischer Gefährdungen, auch und insbesondere in Bezug auf den Straßenverkehr, erfolgt anhand praktischer Beispiele aus den Recherchen (und unter Bezugnahme auf die Grundlagen aus Kapitel 5.1) im anschließenden Kapitel 5.2.

5.1 Vorbetrachtungen zur Gefahrenanalyse

Als Vorbetrachtungen zur Gefahrenanalyse werden zunächst in Kapitel 5.1.1 mit Komfort, Security und Safety drei Gebiete diskutiert, auf die sich Gefahren aus elektronischen Veränderungen auswirken können. Anschließend werden in Kapitel 5.1.2 die Ursachen für resultierende Gefahren konkretisiert, indem in Funktions- und Strukturwirkung von vorgenommenen Veränderungen differenziert wird. Kapitel 5.1.3 behandelt das generelle Spektrum von Gefahren näher, die sich im Kontext von Fahrzeug- und Infrastruktursystemen ergeben können.

5.1.1 Berücksichtigung von Einbußen in Komfort, Security und Safety

Hierzu werden in diesem Kapitel zunächst drei Bereiche betrachtet, auf die sich Veränderungen an Fahrzeug- und Infrastruktursystemen grundsätzlich auswirken können:

- Safety,
- Security und
- Komfort,

die sich in einigen Fällen auch gegenseitig bedingen können.

Seitens der Safety (vgl. Kapitel 1.4.2) liegt der Fokus in dieser Studie auf Auswirkungen auf die Verkehrssicherheit, d. h. auf Gefährdungen des Straßenverkehrs als Risiko für Leib und Leben der Verkehrsteilnehmer. Aspekte der funktionalen Sicherheit werden ebenfalls berührt, jedoch nicht vertieft betrachtet. Mit Blick auf diese Ausrichtung stehen entsprechende Safety-Auswirkungen (die aus vorsätzlichen Eingriffen, d. h. Security-Vorfällen, entstehen können) im Vordergrund der Recherchen und folgenden Betrachtungen.

Auswirkungen auf die Security können z. B. Einflüsse auf den Zugriffschutz des Fahrzeuges sein. Dies umfasst sowohl physischen Zugang z. B. hinsichtlich des Innenraumes als auch logische Zugriffe hinsichtlich der Nutzbarkeit von Fahrfunktionen bis hin auf einzelne durch die Fahrzeug-IT verarbeitete Daten. Gefahren, die durch elektronische Veränderungen für die Security entstehen, können daher einerseits das Umgehen bzw. eine Steigerung/Reduzierung von Zugriffsschutzvorkehrungen sein, die beispielsweise die Diebstahlszahlen und Versicherungsaspekte betreffen. Andererseits können auch Einschränkungen/Verletzungen des Datenschutzes bzw. der Privatsphäre (Privacy) auftreten, wenn personenbezogene oder -beziehbare Daten, die im Fahrzeug gespeichert und verarbeitet werden, unautorisiert ausgelesen und -gewertet werden. Derartige Folgen sind jedoch mit Blick auf die Verkehrssicherheit nur bedingt relevant. Resultierende Gefahren von Veränderungen, die primär der Security zuzuordnen sind, sind daher nicht vertieft untersucht worden.

Einige elektronische Veränderungen führen primär zu Folgen, die den Komfort betreffen. In der Regel haben Änderungen am Bedienkomfort keinen nennenswerten Einfluss auf die Verkehrssicherheit, sodass auch dieser Bereich potenzieller Gefahren nicht vertieft in der Recherche berücksichtigt wird. Auch hier sind identifizierte Sonderfälle jedoch teils dokumentiert, wenn z. B. durch die Auswirkung einer Veränderung auf den Komfortbereich die Aufmerksamkeit des Fahrers beeinträchtigt wird und dadurch auch Auswirkungen auf die Straßenverkehrssicherheit denkbar werden.

Um die funktionale Sicherheit (d. h. Sicherheit im Sinne der Safety, vgl. Kapitel 1.4.2) eines Systems abzuschätzen und nachprüfbare Kriterien zu schaffen, hat sich in der Industrie die Einführung so genannter Sicherheits-Integritäts-Level (engl.: Safety Integrity Levels/SILs) etabliert, die ein zentrales Hilfsmittel des Standards IEC/EN 61508 sind. Hierbei handelt es sich um vier diskrete Stufen, die jeweils einem Bereich für die zulässige Ausfallwahrscheinlichkeit einer Sicherheitsfunktion einer betrachteten Komponente bzw. Teilsystems entsprechen und nach denen sich Anforderungen für diese ableiten lassen. Diese erwähnte Deutung nach Ausfallwahrscheinlichkeiten, die beispielsweise in INNOTEC, 2009 erläutert wird, gibt für High-Demand-Systeme[4] numerische Werte für zulässige Ausfallwahrscheinlichkeiten an, die in Tabelle 12 aufgeführt ist. Dies bedeutet mit anderen Worten, dass die Ausfallwahrscheinlichkeit eines Systems (bzw. einer Teilfunktion), welches den Anforderungen von SIL2 genügen soll, im Mittel zwischen 1/1 Mio. und 1/10 Mio. liegen sollte.

In der Literatur finden sich auch weitere Dimensionen, über die SILs gedeutet bzw. zugewiesen werden können, z. B. welche Arten von Vorfällen zu vermeiden sind (siehe z. B. HSL, 2004) oder wie sich ein Versagen der betrachteten Komponente auf die Kontrollierbarkeit des Fahrzeuges auswirken würde (siehe z. B. MISRA, 2001).

Inzwischen wird in Anlehnung an den sehr breit angelegten Industriestandard IEC 61508 (s. o.) speziell für den Einsatz in der Automobilindustrie ein Standard namens ISO 26262 entwickelt, in dem speziell auf die Anwendung in der Automobilindustrie zugeschnittene Automotive Safety Integrity Levels (ASILs) spezifiziert werden. Während auch hier 4 generelle Stufen definiert wurden, werden diese mit den Buchstaben A-D bezeichnet und es

Safety Integrity Level	Ausfallwahrscheinlichkeit pro Stunde
SIL1	$\geq 10^{-6}$ bis $<10^{-5}$
SIL2	$\geq 10^{-7}$ bis $<10^{-6}$
SIL3	$\geq 10^{-8}$ bis $<10^{-7}$
SIL4	$\geq 10^{-9}$ bis $<10^{-8}$

Tab. 12: Zulässige Wahrscheinlichkeit eines Gefahr bringenden Ausfalls pro Stunde nach INNOTEC, 2009

4 Unter High-Demand-Systemen versteht man sicherheitsrelevante Systeme bzw. Funktionen, die durchgehend bereitstehen müssen, d. h., die ihre Aufgabe im Gegensatz zu sog. Low-Demand-Systemen nicht nur sporadisch auf Anfrage zu erfüllen haben.

SIL	ASIL
SIL 1	ASIL A
SIL 2	ASIL B/ASIL C
SIL 3	ASIL C/ASIL D
SIL 4	(keine Entsprechung)

Tab. 13: Gegenüberstellung SILs und ASILS nach SCHEIBEL, 2009, S. 3

liegt auch keine direkte Abbildung auf die SILs 1-4 vor (vgl. Tabelle 13)

Besonders in der wahrscheinlichkeitsorientierten Deutung aus Tabelle 12 zeigt sich jedoch deutlich, dass sich diese in der Safety bewährten Konzepte nicht unmittelbar auch auf Safety-Probleme anwenden lassen, deren Ursprung in der Security liegt: Für Unfälle, die direkt oder indirekt aus elektronischen Veränderungen entstanden sind, sind statistische Zahlen zu Komponentenversagen meist kein geeignetes Mittel. Dies liegt darin begründet, dass der Auslöser hier in der Regel kein Komponentenversagen ist, sondern sich als Folge eines absichtlichen Eingreifens ergibt (das ein indirekt resultierendes Komponentenversagen allerdings zusätzlich fördern kann). Um auch die Security mit abzudecken, müsste sich daher auch die Wahrscheinlichkeit des Auftretens von absichtlichen Eingriffen verschiedenster Art hinreichend sicher bestimmen lassen. Diese lässt sich jedoch aktuell nur sehr schwer in Zahlen ausdrücken. Auch das diesbezüglich interessante Ziel, den Trend elektronischer Veränderungen an Fahrzeug- und Infrastruktursystemen aus den Ergebnissen der Recherchen abzuleiten, kann maximal einen ersten Schritt in diese Richtung darstellen.

5.1.2 Unterscheidung von direkten Auswirkungen und potenziellen Nebeneffekten

Mit Blick auf die eingangs vorgestellte Zielstellung stehen insbesondere solche Folgen elektronischer Veränderungen an Fahrzeug- und Infrastruktursystemen im Fokus, die potenziell Auswirkungen auf die Straßenverkehrssicherheit haben können. Hierbei steht also die Safety im Sinne von der Vermeidung von Folgen für Leib und Leben des Menschen im Vordergrund.

Selbst wenn die Verringerung der Verkehrssicherheit kein beabsichtigtes Ziel der agierenden Personen ist (vgl. Absicht in der CERT-Taxonomie, Bild 10), können solche Gefahren auch durch das ihnen häufig fehlende Verständnis der komplexen Zusammenhänge automotiver Technik entstehen. Dass die wenigsten Hersteller technische Dokumentationen zu ihrer Technik öffentlich bereitstellen und höchstens in eingeschränktem Umfang den Werkstätten zugänglich machen, trägt ebenfalls zu dieser Tatsache bei.

Insbesondere kann zwischen zwei generellen Arten möglicher Folgen bzw. Wirkung elektronischer Veränderungen unterschieden werden:

- Funktionswirkung: Hierunter sind die direkten Folgen zu verstehen, welche die Veränderung auf die Funktion der Ziel-Komponente hat. Üblicherweise fällt das erwünschte Ergebnis des Eingriffs unter die Funktionswirkungen. Es können jedoch auch ungewünschte Funktionswirkungen auftreten. Gewünschte (beabsichtigte) sowie unerwünschte (unbeabsichtigte) Funktionswirkungen werden in der Folge auch mit „Nutzen-Funktionswirkung“ bzw. „Gefahren-Funktionswirkung“ bezeichnet.
- Strukturwirkung: Indirekte Folgen, welche die Veränderung (oder ihre direkten Folgen) auf die Funktion des Gesamtsystems und seine Umgebung haben kann, werden als Strukturwirkung bezeichnet. Hieraus resultierende Gefahren sind deswegen besonders kritisch, da sich die agierenden Personen Strukturwirkungen typischerweise weniger bewusst sind. Strukturwirkungen können daher von der eigentlichen Absicht abweichen und unerwünscht bzw. sogar gefährlich sein. Alternativ kann sich der Angreifer einzelnen Nebenwirkungen seiner Veränderung bewusst sein und sie fahrlässig hinnehmen. In Einzelfällen können Strukturwirkungen auch als nützlich erachtet werden und mit beabsichtigt sein. Äquivalent werden in der Folge unerwünschte (unbeabsichtigte) Strukturwirkungen sowie gewünschte (beabsichtigte) Strukturwirkungen auch als Gefahren-Strukturwirkungen bzw. Nutzen-Strukturwirkungen bezeichnet.

Tabelle 14 veranschaulicht diesen Zusammenhang.

Die praktische Relevanz dieser Problematik steht im Mittelpunkt des im weiteren Verlauf folgenden Kapitels 5.2. Dort werden in den Recherchen gefundene praktische Beispiele für potenzielle (ungewollte) Nebenwirkungen dokumentiert und diskutiert.

Zuvor sollen jedoch noch einige ausgewählte resultierende Aspekte der Nutzung veränderter Fahrzeugfunktionen diskutiert werden. Bild 11 liefert

hierüber einen Überblick, der ähnlich zu Bild 3 in Kapitel 2.1.1 strukturiert ist. Ausgehend von der Tatsache, dass eine Veränderung stattgefunden hat, resultiert daraus für den Fahrer die Phase der Nutzung einer (oder mehrerer) veränderter Funktionen. Auch an dieser Stelle spielen Entscheidungen des Fahrers eine zentrale Rolle, vor allem dann, wenn dieser eine Funktionsbeeinträchtigung (oder Ausfall) feststellt und darauf reagiert (oder nicht). Da diese Entscheidungen die Wahrscheinlichkeiten für eine bestimmte Gefährdung (~sursache) beeinflussen, eignen sie sich im Umkehrschluss entsprechend für gezielte Interventionen auf technischer

Konsequenz / Wirkung	Funktion	Struktur
Nutzen	„Nutzen-Funktions-Wirkung“	„Nutzen-Struktur-Wirkung“
Gefahr	„Gefahren-Funktions-Wirkung“	„Gefahren-Struktur-Wirkung“

Tab. 14: Übersicht über Funktions- und Strukturwirkungen

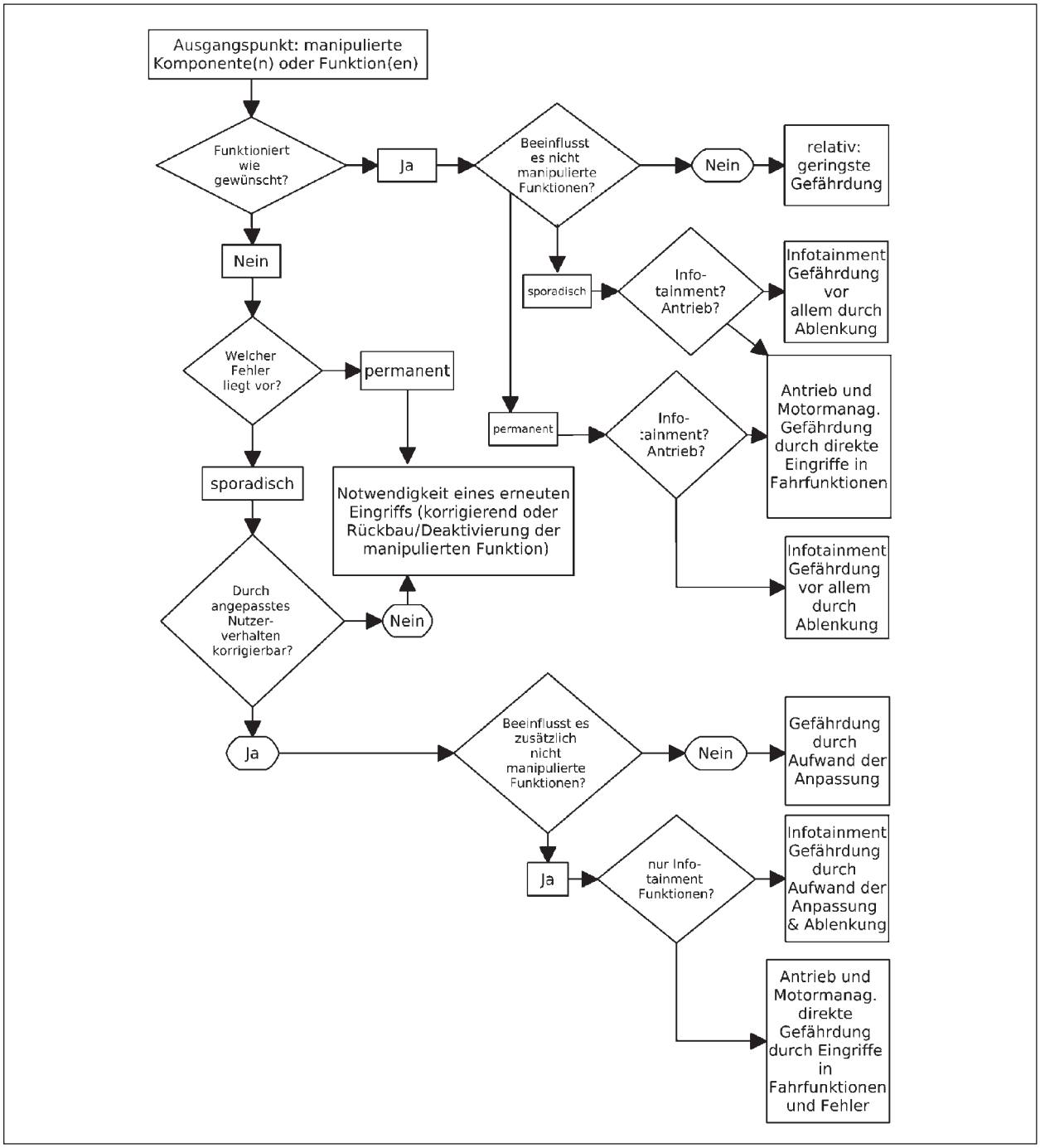


Bild 11: Exemplarisches Entscheidungsdiagramm zur Nutzung veränderter Fahrzeugfunktionen

und/oder juristischer Ebene. Das Entscheidungsdiagramm in Bild 11 illustriert diese Prozesse exemplarisch.

5.1.3 Das allgemeine Spektrum von Gefahren im Automobilbereich

Als abschließender Teil der Vorbetrachtungen zur Gefährdungsabschätzung zeigt dieses Kapitel das Spektrum von Gefährdungen auf. Ziel ist es, für die mögliche Reichweite insbesondere solcher Gefährdungen zu sensibilisieren, die durch elektronische Veränderung an Fahrzeug- und Infrastruktursystemen entstehen können. Dabei wird insbesondere auch die potenzielle Skalierung ihrer Wirkungen auf das betroffene Fahrzeug bis hin zum gesamten Straßenverkehr betrachtet.

Als Ausgangspunkt für die weiteren Betrachtungen soll zunächst für die Spannbreite potenzieller praxisrelevanter Gefährdungen im und um das Fahrzeug im Allgemeinen sensibilisiert werden. Dazu werden im ersten Unterabschnitt zunächst einige recherchierte Beispiele für praktische Mängel und Gefährdungen behandelt, die im Kontext von Fahrzeuguntersuchungen festgestellt wurden. Die dort diskutierten Safety-relevanten Gefahren können durchaus auch ohne Vorliegen einer unautorisierten Veränderung eintreten, jedoch auch für die Einschätzung dieser Fälle eine Hilfe sein. Dies wird im zweiten Unterabschnitt durch recherchierte Berichte zu weiteren Gefährdungen ergänzt, in denen lokale Störungen bis auf Gefährdungen für den Straßenverkehr skalieren können.

Der dritte Unterabschnitt untersucht dagegen anhand der zuvor eingeführten Systematisierungen der Schwachstellenkategorien und Angreiferklassen explizit das theoretische Gefahrenspektrum von Veränderungen an Fahrzeug- und Infrastruktursystemen.

Verbreitete Mängel und ihre Gefährdungen aus dem Kontext von Fahrzeuguntersuchungen

Zu allgemeinen Arten sicherheitsgefährdender Mängel (im Sinne von Safety) konnten insbesondere aus Mängelstatistiken, die im Kontext der Hauptuntersuchung von Fahrzeugen bei den dazu berechtigten Institutionen erfasst werden, erste Informationen zusammengetragen werden. In gezielten Nachfragen bei Vertretern entsprechender Einrichtungen (z. B. TÜV Süd, TÜV Nord, KÜS) zeichnete sich das allgemeine Bild ab, dass bei der Erfassung festgestellter Mängel derzeit anscheinend leider nicht detailliert nach der Ursache des Mangels unterschieden wird. So schreibt beispielsweise ein Vertreter des TÜV Nord: „Eine generelle statistische Auswertung zu Mängeln bei Hauptuntersuchungen aufgrund technischer Fahrzeugveränderungen führen wir nicht.“ Insbesondere eine Unterscheidung zwischen absichtlichen Veränderungen (inkl. unsachgemäß durchgeführter Veränderungen) sowie unabsichtlichen Schäden/Verschleißerscheinung wäre für die vorliegende Zielstellung hilfreich gewesen. Entsprechende Daten zu derjenigen Teilmenge der bemängelten Gefährdungsfaktoren, die explizit aus absichtlichen Eingriffen hervorgingen, lagen laut Kenntnis der Ansprechpartner jedoch entweder nicht vor bzw. es konnten keine entsprechenden Daten bereitgestellt werden.

Doch die vorhandenen Mängelstatistiken können auch ohne diese Unterscheidung als ein erster Anhaltspunkt einbezogen werden, um die betrachteten Gefährdungen durch Veränderungen abzuschätzen. Sofern Veränderungen betrieben werden, die zu erkennbaren Gefährdungen für die Straßenverkehrssicherheit führen könnten, wären diese als ein Teil der erkannten Mängel in den bestehenden Statistiken enthalten. Die Mängelstatistiken und -berichte können also als eine Obergrenze für erkennbare Mängel aus Veränderungen angesehen werden. Während ein häufig beobachteter Mangel nicht zwangsläufig auf intensiv betriebene Veränderungen hindeutet, so zeugt ein selten beobachteter Mangel davon, dass ggf. betriebene Veränderungen die zugehörige Gefährdung nicht erkennbar mit sich bringen.

In der recherchierten Quelle [R95] wird seitens der Gesellschaft für Technische Überwachung (GTÜ) – entsprechend ohne nähere Unterscheidung nach zugrunde liegenden Ursachen – von mehreren Beispielen für verbreitete Fahrzeugmängel aus dem Jahr 2008 berichtet, die in der Folge exemplarisch diskutiert werden. Während 54 % der überprüften Fahrzeuge Mängel aufwiesen, habe die Zahl festgestellter erheblicher Mängel im beschriebenen Zeitraum im Vergleich zu den Vorjahren weiter zugenommen, sodass von insgesamt 42 Millionen Pkw nach Schätzung der Gutachter mehr als 7 Millionen Fahrzeuge mit gravierenden Mängeln am Straßenverkehr teilnehmen, wodurch sich das Unfallrisiko durch diese Fahrzeuge wiederum erheblich erhöhen würde.

Nach [R85] stellte in 2008 die häufigste Kategorie festgestellter Mängel mit 23,5 % die Beleuchtung und Elektrik dar. Wie groß hierbei insbesondere der Anteil von unsachgemäß durchgeführtem Umbau von Lichtanlagen (vgl. Kapitel 2.1.1) ist, kann der Quelle leider nicht entnommen werden. Die Relevanz bzw. potenzielle Gefährdung des Straßenverkehrs durch den unangemessenen Zustand von Lichtanlagen wird hierdurch jedoch erneut bestätigt. Auf den beiden nächsten Plätzen folgen Mängel an Bremsanlagen (17,7 %) und Achsen/Rädern/Reifen (17,5 %), bei denen zu einem Teil auch unautorisierte Leistungssteigerungen zu einem erhöhten Verschleiß beigetragen haben könnten. Letzteres kann sich auch in erhöhter Umweltbelastung (16,7 %), insbesondere durch erhöhte Abgaswerte oder Lärmentwicklung, negativ auswirken. Bild 12 zeigt eine grafische Darstellung der häufigsten Mängelkategorien bei Fahrzeuguntersuchungen in 2008, die der Statistik des Kraftfahrt-Bundesamtes [R96] entnommen ist.

Gerade der Untersuchung elektronischer Komponenten kommt eine zunehmende Bedeutung zu. Nachdem die Untersuchung elektronischer Komponenten bereits seit 2006 für ausgewählte Fahrzeuge (z. B. Taxen und Mietwagen) durchgeführt wird (vgl. Bericht der KÜS [R97] zu 2006), ist diese auch laut der bereits referenzierten GTÜ-Statistik [R95] seit 2009 zudem bei weiteren Fahrzeugen im Visier der Gutachter. Insbesondere die Sicherheitselektronik werde laut [R95] verstärkt mit auf Mängel kontrolliert (darunter z. B. ABS, ESP, Airbags, Rückhalteeinrichtungen, Geschwindigkeitsbegrenzer und Bremsassistenten). Wie bereits in Kapitel 2.1.1 im Teil zu Veränderungen an Airbagsystemen angeführt, konnten laut [R97] in 2006 insbesondere

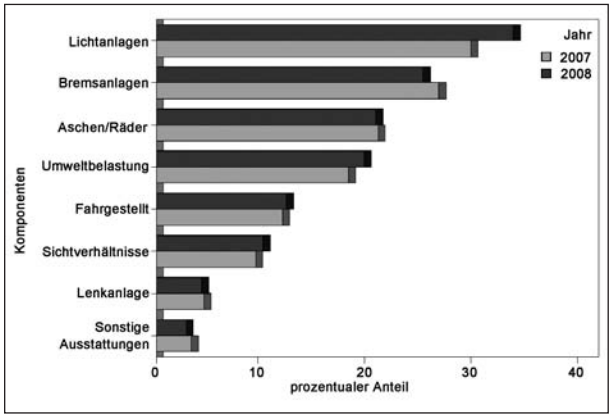


Bild 12: Häufigste Mängel bei Hauptuntersuchungen an Pkw nach Mängelarten in 2007 und 2008 nach [R96] (als Obergrenze erkennbarer Mängel durch Veränderungen)

Mängel an Systemen der passiven Insassensicherheit (z. B. Airbag, Gurtstraffer) festgestellt werden, bei denen ein Teil auch laut [R97] explizit nicht aus Defekten entstanden ist, sondern aus absichtlichen Eingriffen: In mehreren Fällen sollen Airbagsysteme nach [R97] bei der Ursachensuche als komplett entfernt vorgefunden worden sein. Auch die Gefahr der Blendung des Gegenverkehrs durch Mängel an Xenon-Scheinwerfern (vgl. zugehöriger Absatz in Kapitel 2.1.1) wird in [R97] explizit betont. Darüber hinaus werden vermehrt Mängel an der Fahrdynamikregelung (insbesondere ESP) beobachtet, wie nicht oder falsch verbundene Steckkontakte oder falsch behandelte Pulsringe im Fall von ABS. Dieses soll laut Einschätzung aus [R97] häufig aus Nachlässigkeit, d. h. Fehlern bei Wartung und Reparaturen, entstehen.

Weitere Berichte zu praktischen Gefährdungen durch Fahrzeug-IT und ihre potenzielle Skalierung

Auch unabhängig von Prüfberichten ließen sich einige weitere markante Beispiele recherchieren, die das mögliche Ausmaß praktischer Gefährdungen erahnen lassen, die (teils ebenfalls ohne absichtliche Eingriffe, sondern auch aus Fehlfunktionen heraus) aus der Fahrzeugelektronik heraus entstehen können:

In der recherchierten Quelle [R94] berichtet ein Nutzer in einem großen Automobilforum, dass sein ACC-System (vgl. zugehöriger Teil in Kapitel 2.1.1) sporadisch fehlerhaft agiert und dabei teils unangemessen in die Fahrzeugsteuerung eingreift. Er berichtet von Fehlerkennungen insbesondere auf der Autobahn, bei denen z. B. ein zunächst erkanntes, vorausfahrendes Fahrzeug wieder verloren wird und das ACC zu Unrecht wieder beschleunigt oder bei denen umgekehrt Fahrzeuge auf den rechten Spuren als vorausfahrend erkannt werden und zu Unrecht ein Bremsvorgang eingeleitet wird.

Als ein weiterer Erfahrungsbericht wurde im Rahmen eines persönlichen Gespräches mit einem ehemaligen Kfz-Servicetechniker eines namhaften deutschen Automobilherstellers von einem ähnlichen Fall berichtet, in dem eine Fehlfunktion eines komfortzentrierten Steuergerätes offensichtlich beinahe zu schwerwiegenden Folgen für die Straßenverkehrssicherheit geführt hätte. Dabei handelte es sich um das Steuergerät für die elektronische Sitzverstellung, die häufig mit einem Memory-System kombiniert ist. Im berichteten Fall gab ein sichtlich

geschockter Fahrer dem Werkstattpersonal zu verstehen, dass während der Fahrt auf der Autobahn bei zügiger Fahrweise plötzlich der Sitz ohne Zutun des Fahrers weit zurück fuhr (d. h. den Abstand des Fahrers zu Lenkrad und Bremspedal erhöhte) und zusätzlich in Liegeposition schaltete. Solange sich eine derartige Fehlfunktion des Steuergerätes, als die sich dies Vorkommnis im Nachhinein herausstellte, im Stand ereignet (d. h. eine eingespeicherte bzw. manuell gesteuerte Sitzposition nicht angefahren oder eine ungewünschte eingestellt wird), so besteht im Wesentlichen nur eine Beeinträchtigung des Komforts. Während der Fahrt kann ein Nichterfolgen einer gewünschten Positionsänderung des Sitzes oder, schlimmer noch, eine unbeauftragte Umstellung des Fahrersitzes in ungewünschte Positionen jedoch erhebliche Auswirkungen auf die Verkehrssicherheit haben. Somit kann eine deutliche Gefährdung des Straßenverkehrs im Einzelfall auch aus üblicherweise als nicht sonderlich Safetyrelevant betrachteten Bereichen des Komforts entstehen.

Folgendes Beispiel aus dem Bereich der Infrastruktursysteme (vgl. Kapitel 2.1.2) illustriert zudem gut, dass technische Systeme auch bei korrekter Funktion Mitverursacher für das Entstehen praktischer Gefährdungen im Straßenverkehr sein können. Meist spielt hier insbesondere der komplexe Faktor Mensch die entscheidende Rolle, der bei der Entwicklung von automotiven Systemen grundsätzlich mit einbezogen werden sollte. Der Quelle [R119] ist diesbezüglich zu entnehmen, dass ein zur Kontrolle von On-Board-Units des deutschen Mautsystems entworfenes System eine große Ähnlichkeit mit bekannten Systemen zur Geschwindigkeitsüberwachung (vgl. Kapitel 2.1.2) aufweist. Durch die rein optische Ähnlichkeit soll es nach [R119] bei einem Test mit diesen Systemen im Jahr 2002 auf der Autobahn A 3 zu vier schweren Auffahrunfällen gekommen sein: Indem diese Anlagen von vielen Fahrern für Geschwindigkeitsmesseinrichtungen gehalten wurden, veranlasste dieser Eindruck die Fahrer anschließend in vielen Fällen zu einer drastischen Reduzierung ihrer Geschwindigkeit, die in mehreren Fällen zu schweren Auffahrunfällen führte.

Das Gefährdungspotenzial elektronischer Veränderungen nach Schwachstellenkategorien und Angreiferklassen

In diesem Kapitel erfolgt eine Abschätzung zu erwartender Größenordnungen von Gefährdungen, die potenziell aus elektronischen Veränderungen resultieren können. Dies erfolgt basierend auf den in Kapitel 3.1 vorgestellten Schwachstellenkategorien, die bei elektronischen Veränderungen insbesondere an Kfz-Systemen ausgenutzt werden. Die Betrachtungen in diesem Kapitel sind zunächst theoretischer Natur und unabhängig von der praktischen Auftretenswahrscheinlichkeit entsprechender Vorkommnisse (d. h. sie beziehen die in den Kapiteln 2, 3 und 4 erfolgten Abschätzungen zum praktischen Risiko noch nicht ein). Eine anhand ausgewählter praktischer Beispiele aus der Recherche substantiierte Dokumentation beispielhafter Gefährdungen wird in Kapitel 5.2 geliefert.

Ausgehend von den Schwachstellenkategorien S1 bis S5 (siehe Kapitel 3.1), die bei elektronischen Veränderungen insbesondere an Kfz-Systemen ausgenutzt werden können, wird folgende Abschätzung zu den zu erwartenden Größenordnungen potenziell resultierender Gefährdungen vorgenommen:

Bzgl. Schwachstellenkategorie S1

Veränderungen, die über herstellerseitig vorgesehene Optionen vorgenommen werden (Kategorie S1 nach Kapitel 3.1), dürften hinsichtlich potenzieller Nebenwirkungen und daraus resultierender Gefährdungen im Schnitt vergleichsweise unkritisch sein. Auch wenn die zugrunde liegenden Funktionen teilweise nur zu Testzwecken oder für Benutzung in anderen Ländern vorgesehen sind, sind diese in der Regel von den Entwicklern des Zielsystems entwickelt worden, die sich der Systemeigenschaften und Wechselwirkungen mit dem Gesamtsystem generell eher bewusst sind. Da sich die missbräuchliche Benutzung durch unautorisierte Personen (z. B. nach Forenanleitungen) in diesem Fall oft auf das bloße (De~)Aktivieren von Funktionalitäten oder auf die Wahl von Konfigurationswerten aus einer vorgegebenen Optionsmenge beschränkt, sind potenzielle Nebenwirkungen hier erwartungsgemäß begrenzt. Dennoch können ungeeignete Kodierungen auch an vorgesehenen Konfigurationsdaten selbstverständlich im Einzelfall unangebracht sein bzw. zu Gefahren führen. Als allgemeine Abschätzung der Gefährdung von Veränderungen, die diese Kategorie von Schwachstellen ausnutzen, wird daher niedrig bis mittleres Gefährdungspotenzial veranschlagt (vgl. Tabelle 15).

Bzgl. Schwachstellenkategorien S2 und S3

Dagegen sind Veränderungen, die über direkte Zugriffe bzw. Veränderungen an analogen oder sogar digitalen Signalen umgesetzt werden (Kategorie S2 und S3 nach Kapitel 3.1), typischerweise nicht durch den Hersteller vorgesehen (das heißt: nicht einmal zu Testzwecken). Nach Einschätzung basierend auf den Rechercheergebnissen werden auf diese Art vorgenommene Veränderungen zumeist von nicht ausreichend fachkundigen Personen durchgeführt, die insbesondere in die Angreiferklasse A1/Privatperson nach Kapitel 3.2.3 fallen. Es ist anzunehmen, dass sich gerade dieser Personenkreis der potenziellen Nebenwirkungen entsprechender Eingriffe oft nicht bewusst ist, da ihnen die entwicklerseitigen Spezifikationen des Systems sowie seine Wechselwirkungen mit dem Gesamtsystem in der Regel nicht bekannt sind. Allerdings weisen viele automotive Regelsysteme aus Safety-Gründen Notlaufeigenschaften auf bzw. verwenden Ersatzwerte, falls wichtige Eingabedaten fehlen (z. B. durch einen Kabelschaden) oder zu stark von zulässigen Werten abweichen. Als allgemeine Abschätzung der Gefährdung von Veränderungen, die diese Kategorie von Schwachstellen ausnutzen, wird daher ein mittleres Gefährdungspotenzial veranschlagt (vgl. Tabelle 15).

Bzgl. Schwachstellenkategorien S4 und S5

Eingriffe in die gesamte Betriebssoftware sowie in Konfigurationsdaten von Steuergeräten, insbesondere auch mit physischem, invasivem Zugriff auf die Steuergeräte (teils z. B. mit dem Austausch von Elektronikbausteinen) bieten verhältnismäßig deutlich umfangreichere Interaktionsmöglichkeiten mit zentralen Fahrzeugfunktionen. Oftmals können hierdurch verstärkt auch fahrsicherheitsrelevante Folgen entstehen. Dadurch erfordern die hierbei anzuwendenden Techniken vergleichsweise viel Erfahrung. Die ist insbesondere auf die Angreiferklasse A2/Profi nach Kapitel 3.2.3 zutreffend. Einerseits ist daher zu hoffen, dass dieser Personenkreis (z. B. professionelle Tuning-Anbieter) sich seiner Verantwortung für potenzielle Folgen der Veränderung bewusst ist. Andererseits liegen auch Akteuren der Angreiferklasse A2/Profi i. d. R. nicht sämtliche Spezifikations- und Entwicklungsdokumente der betroffenen Systeme vor: Dokumente mit z. B. als geheim eingestuften Informationen werden teils auch Vertragswerkstätten nicht zugänglich gemacht. Sind Angehörigen der Angreiferklasse A2 relevante Wechselwirkungen nicht bekannt, können auch trotz ihrer Erfahrung Fehleinschätzungen und potenzielle Gefährdungen durch die Eingriffe nicht gänzlich ausgeschlossen werden. Auch können andere Motivationen für entsprechende Eingriffe vorliegen: In besonders bedrohlichen Fällen könnten durch soft- und hardwareinvasive Angriffe bewusst destruktive Veränderungen an fremden Fahrzeugen durch Profis genutzt werden, um fremden Personen gezielt Schaden zuzufügen. In diesem Kontext sei insbesondere auf solche Vorfälle nach der CERT-Taxonomie in Kapitel 3.2.2 verwiesen, z. B. die politisch bzw. finanziell motiviert sind oder aus Freude am Schaden betrieben werden. Aufgrund des umfassenden Interaktionspotenzials mit den betroffenen Fahrzeugfunktionen wird als allgemeine Abschätzung der Gefährdung von Veränderungen, die diese Kategorie von Schwachstellen ausnutzen, kann daher ein hohes Gefährdungspotenzial veranschlagt werden (vgl. Tabelle 15).

Aufarbeitung nach Schwachstellenkategorien und Angreiferklassen

In Tabelle 15 werden die soeben getroffenen Abschätzungen zusammengefasst. Dabei werden die in Kapitel 3 herausgearbeiteten Schwachstellenkategorien mit der ungefähren Größenordung ihrer potenziell (als beabsichtigte Funktions- wie auch unbeabsichtigte Strukturwirkungen) resultierenden Gefahren gegenübergestellt.

Analog zu den vorangegangenen Ausführungen fasst Tabelle 16 die erfolgten Abschätzungen zusammen, welche Schwachstellenkategorien aus Kapitel 3 typischerweise von welchen Akteuren (nach den Angreiferklassen aus Kapitel 3.2.3) ausgenutzt werden bzw. werden können. Zusammen mit dem Bewusstsein dieser Personengruppen für potenzielle Folgen der Veränderungen soll diese Tabelle insbesondere mit Bezug auf Tabelle 15 für

Schwachstellenkategorie	Abschätzung potenziell resultierender Gefahren
S1 (Optionen)	Niedrig bis mittel
S2 (analoge Signale)	Mittel
S3 (digitale Signale)	Mittel
S4 (software/Konfiguration)	Hoch
S5 (physischer Eingriff)	Hoch

Tab. 15: Abschätzung der Größenordnung potenziell resultierender Gefahren nach Schwachstellenkategorie

Angreiferklasse:	A1 (Privatperson)	A2 (Profi)	A3 (Spezialist)
Systemkenntnisse	gering	mittel	hoch
Verfügbare Werkzeuge	einfaches/günstiges	kommerzielles	Spezialwerkzeug
Typischerweise ausgenutzte Schwachstellenkategorien (vgl. Gefahren nach Tabelle 15)	S1, S2, teils S3	S1,S4, S5	S3, S4
Vermutetes Bewusstsein für potenzielle Folgen	niedrig	mittel	hoch

Tab. 16: Abschätzung der Relevanz ausgenutzter Schwachstellenkategorien durch Akteure der Angreiferklassen und potenziell resultierender Gefahren

die potenziell dadurch entstehenden Gefahren sensibilisieren.

Bewertung des allgemeinen Gefährdungsspektrums

Bevor die Relevanz für die reale Gefährdung in der Praxis, d. h. für den Straßenverkehr, im folgenden Kapitel konkret anhand verschiedener Praxisbeispiele erfolgt, kann an dieser Stelle abschließend folgende Abschätzung zu potenziell entstehenden Gefahren getroffen werden:

Mit Blick auf die zuvor diskutierten Klassifizierungen gibt es zwei Kombinationen, aus denen besonders schwerwiegende potenzielle Gefahren entstehen können:

1. Unbewusste Herbeiführung von Gefahren durch mangelnde Systemkenntnisse und Risikobewusstsein. Hierunter fällt hauptsächlich die Angreiferklasse A1. Privatpersonen versuchen oft mit einfachen Mitteln und Werkzeugen, aber begrenzten Systemkenntnissen und Risikobewusstsein, subjektiv empfundene Optimierungen an ihren Fahrzeugen vorzunehmen. Hierbei werden oft Wechselwirkungen übersehen, aus denen teils gefährliche Gefahren resultieren können. Auf professionelle Anbieter (A2) trifft dies nur in abgeschwächter Form zu, da diese (zumindest aus Erfahrung) meist größere Systemkenntnisse und Risikobewusstsein haben und ihnen i. d. R. auch professionellere Werkzeuge zur Verfügung stehen, über die sich das Ziel eleganter erreichen lässt als über die teils amateurhaften Eingriffe im Privatbereich.

2. Bewusste Herbeiführung von Gefahren mit Hilfe umfangreicher Systemkenntnisse und Werkzeuge. Das generell höhere Risikobewusstsein bei den Profis (A2) und insbesondere Experten (A3) ist irrelevant, sofern a) die Bedrohungslage besteht, dass vorsätzlich versucht wird, Gefahren gezielt herbeizuführen, und b) Schwachstellen bestehen, die dies ermöglichen und gezielt ausgenutzt werden. Spielen Freude am Schaden oder politische Motivationen eine Rolle (vgl. CERT-Taxonomie in Bild 10), könnte das erhöhte Risikobewusstsein daher sogar als ein verstärkender Faktor wirken. In Kombination mit den zur Verfügung stehenden professionellen Werkzeugen und Systemkenntnissen wären hier potenziell erhebliche Gefahren vorstellbar, die sich aus entsprechenden absichtlichen Veränderungen bzw. Manipulationen/Sabotagen ergeben. Dass solche praktischen Gefahren durchaus nicht unrealistisch sind, wird insbesondere durch das in Kapitel 2.1.1 („Fahrdynamikregelsysteme“) vorgestellte akademische Praxisbeispiel aus [R145] untermauert, bei dem mittels gezielt generierter Busnachrichten bei laufender Fahrt die Bremsen deaktiviert wurden.

Neben den akademischen Quellen, die derartige Gefahren aus Sicht der Forschung untersuchen, sind die recherchierten Praxisbeispiele (die den überwiegenden Teil der Rechercheergebnisse darstellen) ausschließlich dem ersten Punkt zuzuordnen. Folglich sei als ein Ergebnis darauf hingewiesen, dass in den zugrunde gelegten öffentlichen Quellen keine konkreten Hinweise auf bewusst herbeigeführte Gefährdungen zu finden waren. Dadurch kann jedoch nicht auf deren Nicht-Existenz in der Praxis geschlossen werden. Die praktische Gefährdung für den Straßenverkehr wird in Kapitel 5.2 auf Basis der recherchierten Praxisbeispiele abschließend abgeschätzt.

5.2 Abschätzung der Gefährdung für den Straßenverkehr

Dieses Kapitel untersucht an konkreten Beispielen aus der Recherche mögliche Gefährdungen, die aus elektronischen Veränderungen an Fahrzeug- und Infrastruktursystemen entstehen könnten. Mit

Bezug auf die in Kapitel 2.1 recherchierten Veränderungen und auf Grundlage der durchgeführten Recherchen werden in Kapitel 5.2.1 ausgewählte Beispiele für Nebenwirkungen aufgeführt. Hierdurch wird die Tendenz für Gefährdungen aufgezeigt, die sich nach elektronischen Veränderungen an Fahrzeug- und Infrastruktursystemen potenziell ergeben können. Anschließend folgt in Kapitel 6 ein Ausblick auf zukünftig potenziell hinzukommende Gefährdungen im Kontext der Car-to-X-Kommunikation, der anhand eines simulierten Wurmausbruchs in Car-to-Car-Netzwerken gestaltet wird.

5.2.1 Recherche zu praktischen Vorkommnissen entsprechender Gefährdungssituationen bzw. Gefahren

Dazu werden im Folgenden 19 Beispiele für Nebenwirkungen aufgeführt, die zu einem großen Teil den Quellen der in Kapitel 2.1 recherchierten Veränderungen entnommen werden konnten. Hierbei sind insbesondere solche Strukturwirkungen aufgezeigt, die sich potenziell auf die Safety und damit auf die Straßenverkehrssicherheit auswirken können.

Motorsteuerung – Exemplarische Gefährdungen durch Leistungssteigerungen

Die in Kapitel 2.1.1 vorgestellten Veränderungen an Motorsteuerung zur Leistungssteigerung, in deren Kontext zusätzlich die Aufhebung einer Geschwindigkeitsabregelung zu sehen ist, bergen mehrere Gefahren, die aus der Art der Veränderung resultieren können. Durch die gesteigerte Leistung und Geschwindigkeiten können Verschleißerscheinungen beschleunigt auftreten bzw. sich auch darüber hinausgehende Materialschäden ergeben. Dies beschränkt sich nicht allein auf den Motor selbst, sondern kann auch Strukturwirkungen auf andere Komponenten nach sich ziehen. Beispielsweise können verschiedene Fahrzeugkomponenten nicht für die erhöhte Beanspruchung ausgelegt sein.

Erfolgt die Leistungssteigerung beispielsweise, indem das Kennfeld direkt verändert wird (vgl. Kapitel 2.1.1), können einerseits Motorschäden eine unmittelbare Folge sein (z. B. durch Überhitzung bei falschem Kraftstoff-Luft-Verhältnis). Werden die Sensorsignale verändert, die dem Motorsteuergerät als Basis für die Berechnung der Kraftstoffmenge dienen – z. B. das Drehzahlsignal –, können durch überhöhte Drehzahlen der Motor und Antriebsstrang beschädigt oder zerstört werden. Beide haben eine direkte negative Wirkung auf die Fahrdynamik – als Beispiel sei auf das Liegenbleiben eines Fahrzeuges in einer unübersichtlichen Verkehrssituation (Tunnel oder Kurve/Kuppe) verwiesen.

Ein praktisches Beispiel für einen entsprechenden Fall konnte im Gespräch mit einem Mitarbeiter in der Entwicklungsabteilung eines großen deutschen Automobilherstellers in Erfahrung gebracht werden. Hier wurde ein neu gekaufter deutscher Sportwagen in einer Tuningwerkstatt hinsichtlich aller angebotener Faktoren mit dem Ziel der Leistungssteigerung „optimiert“. Anschließend erfolgte ein Test auf deutschen Autobahnstrecken ohne Geschwindigkeitsbegrenzung (Richtgeschwindigkeit 130 km/h), bei dem der Fahrer die neuen Grenzen seines Fahrzeuges untersuchte. Nachdem bei einem spontanen Zwischenhalt auf einem Rastplatz ein hellrotes Glühen der Auspuffanlage festgestellt wurde, fing das Fahrzeug Feuer und brannte aus. Dass das Fahrzeug in kurzer Zeit von der hohen Betriebstemperatur ohne langsames Herunterkühlen zum Stand gebracht wurde, war dabei nur ein nebenläufiger Faktor zum Ausbruch des Brandes. Hauptsächliches Problem war, dass die vorhandene Auspuffanlage nicht für die vorgenommene Leistungssteigerung ausgelegt bzw. geeignet war bzw. deren Leistungsreserven deutlich überstieg. Nach Einschätzung des Entwicklers kann dies auch auf andere Komponenten zutreffen, wie insbesondere Motor und Getriebe sowie auch Bremsscheiben. Dies relativiert sich teilweise, sofern der Hersteller innerhalb einer Modellreihe aus logistischen Gründen auch für verschiedene verkaufte Motorleistungen identische Bremsscheiben, Getriebe und teils sogar Motoren verbaut (die dann z. T. softwareseitig auf die bezahlte Leistung begrenzt werden): Zumindest für Leistungssteigerungen der günstigen Ausstattungen dürften die Reserven der beteiligten Systemkomponenten dann ausreichen. Allerdings könnten vermutlich auch bei derartigen Modellen Leistungssteigerungen an den bereits nominal mit der vollen Leistung verkauften Fahrzeugen zu ähnlichen Gefährdungen führen.

Weitere indirekte Effekte der Leistungssteigerung können sich auch in Wechselwirkung mit dem Faktor Mensch ergeben, der am Steuer sitzt: Wenn insbesondere junge Fahrer die hinzugewonnene Leistung konsequent ausnutzen, können im Zusammenhang mit Leichtsinn und Selbstüberschätzung Unfälle begünstigt werden, die mit der ursprüngli-

chen Motorisierung des Fahrzeuges möglicherweise nicht eingetreten oder weniger kritisch verlaufen wären. Da gerade in Unfällen bei hohen Geschwindigkeiten auch der Straßenverkehr in der unmittelbaren Umgebung verstärkt mit betroffen sein kann, können sich hier demnach auch für unbeteiligte Personen Gefährdungen ergeben.

Weitere Folgen einer unfachmännisch vorgenommenen Leistungssteigerung können sich in Form rechtlicher Konflikte ergeben. Einerseits können seitens der Versicherung Zusatzansprüche anfallen, die beispielsweise durch das Erreichen einer höheren Leistungsklasse entstehen (bei vielen Versicherungen stellt die Motorleistung ein Hauptkriterium bei der Bemessung der Versicherungsprämie dar). Andererseits könnten auch die Schadstoffemissionen bei einer nicht eingetragenen Leistungssteigerung die zulässigen Grenzwerte übersteigen, was bei dem Nachweis einer fehlenden Genehmigung (d. h. keine gültige ABE) ebenfalls rechtliche Konsequenzen für den Besitzer nach sich ziehen könnte.

Motorsteuerung: Abgasrückführung – Exemplarische Gefährdungen bei einer Deaktivierung

Wie auch den Kommentaren in [R45] zu entnehmen ist, sind Änderungen an der Abgasrückführung abgasrelevant (d. h. können die Schadstoffemissionen negativ beeinflussen) und können rechtlich zum Erlöschen der Betriebserlaubnis führen. Im Falle eines Unfalls könnten daher aufgrund der faktisch fehlenden Betriebserlaubnis insbesondere Versicherungen eine Kostenübernahme verweigern und dadurch erhöhte Regressansprüche an den Fahrzeugbesitzer gestellt werden.

Motorsteuerung: Regelung für Autogas-Anlage – Exemplarische Gefährdungen bei unsachgemäßer Nachrüstung

Die steuer- und regelungstechnische Herausforderung beim Nachrüsten von Autogasanlagen liegt darin, dass der Erdgasbetrieb Veränderungen praktisch aller gasspezifischen Motorsteuerungsfunktionen bedingt. Hieraus können sich bei unsachgemäßer Durchführung potenzielle Gefährdungen ergeben.

Laut [R128] berichten Prüfingenieure der KÜS von nachgerüsteten Gasanlagen (vgl. Kapitel 2.1.1), bei denen die Nachrüstung unfachmännisch vorgenommen wurde und dadurch Gefährdungen eröffnet. Teilweise sei die Gasleitung am Auspuff vorbei gelegt und noch dazu an den beweglichen Stabilisatoren befestigt worden. In einem anderen Fall sei ein Tankstutzen im Kofferraum angebracht gewesen. Ein weiterer Fall berichtet von einer Montage, wo die mitgelieferten Befestigungsbänder offenbar zu kurz waren. Hier seien zwei Schrauben an die zu kurzen Bänder angeschweißt worden. Im Fall eines Unfallereignisses wäre die Gefahr demnach groß gewesen, dass die Konstruktion gerissen wäre. Der Gastank hätte sich vermutlich losgerissen, was zu fatalen Folgen hätte führen können. Die festgestellten Mängel kann man auch auf die Tatsache zurückführen, dass Gutachter-Zertifikate zu entsprechenden Nachrüstungen auf Grund einer Überprüfung an einem Referenzfahrzeug erstellt werden und nicht auf alle Anlagen gleicher Bauart übertragbar sind.

Getriebesteuerung – Exemplarische Gefährdungen durch unsachgemäße Nachrüstung einer pseudo-automatisierten Schaltung

Bezüglich der Nachrüstung einer pseudo-automatisierten Schaltung übernimmt, wie in Kapitel 2.1.1 erläutert, nicht mehr ausschließlich der Fahrer das Schalten der Gänge, sondern zu einem gewissen Teil die Steuerungslogik (vgl. auch [R60] und [R138]). Ausfälle der Steuerungslogik werden dabei ggf. nicht aufgefangen und können zu unvorhersehbaren, potenziell Safety-kritischen, Konsequenzen führen. Fällt also die Zusatzkomponente (z. B. auf Grund eines Verlustes der Stromversorgung) aus, könnte der Fahrer dadurch die Kontrolle über die Schaltung und somit ggf. auch über das Fahrzeug verlieren.

Startsteuerung – Exemplarische Gefährdungen durch unsachgemäße Nachrüstung eines Start-Knopfes

Im Rahmen der Diskussion zur Nachrüstung eines Start-Knopfes ([R40]) werden mehrere mögliche Nebenwirkungen diskutiert. Von einigen Teilnehmern geäußerte Befürchtungen, man könne dadurch auch ohne eingesteckten Schlüssel fahren (d. h. diesen z. B. während der Fahrt herausziehen) und dann u. U. das Lenkradschloss einrasten, sind angesichts der dortigen technischen Beschreibung des Eingriffs anscheinend zwar nicht zutreffend. Allerdings scheint es möglich zu sein, den Anlasser auch während der Fahrt erneut zu betätigen (da

z. B. ein mechanischer Schutz am Zündschloss durch die Veränderung umgangen wird). Durch das Einspuren in die Schwungmasse des laufenden Motors (das durch ein absichtliches oder versehentliches Betätigen erfolgen kann) können unter Umständen Schäden an Motor und Anlasser entstehen und so der Verkehr ebenfalls gefährdet werden.

Adaptive Niveauregulierung – Exemplarische Gefährdungen durch elektronisches Tieferlegen

Wenn Systeme zur elektronischen Tieferlegung, die z. T. eigentlich nur für den Stand vorhergesehen sind (vgl. Kapitel 2.1.1), durch Beseitigung entsprechender Schutzvorkehrungen zur Benutzung auch während der Fahrt freigeschaltet werden, können ebenfalls sicherheitskritische Nebeneffekte auftreten. Durch Faktoren wie zu geringe Bodenfreiheit sowie für die Fahrt nicht ausreichendem Federweg der Stoßdämpfer könnten sich beispielsweise bei Bodenwellen Beschädigungen ergeben oder in schlimmeren Fällen das Fahrzeug außer Kontrolle geraten sowie der nachfolgende Verkehr durch abgefallene Teile gefährdet werden.

Fahrdynamikregelsysteme – Exemplarische Gefährdungen beim Deaktivieren einzelner Funktionen

Auch das Deaktivieren von Stabilitätsfunktionen wie ESP, ABS oder ASR kann bei unsachgemäßer Durchführung ungewünschte Nebeneffekte mit sich bringen. Insbesondere beim Entfernen von Sicherungen z. B. zum Deaktivieren einzelner dieser Funktionen wird in Quellen wie [R117] berichtet, dass hierdurch teils auch die anderen von den betroffenen Steuergeräten realisierte Funktionen nicht mehr zur Verfügung stehen und eine Vielzahl von Fehlercodes generiert wird (z. B. fallen bei der Technik zur Deaktivierung von ABS, die in [R117] diskutiert wird, auch ESP und weitere Funktionen aus).

Airbagsysteme – Exemplarische Gefährdungen durch Verschleierung von Eingriffen in das Airbagsystem

Wie in Kapitel 2.1.1 beschrieben, wird bei Airbagsystemen teils auch die korrekte Funktion einzelner Airbags oder des gesamten Airbagsystems vorgetäuscht. Vergleichsweise harmlos ist dies noch, wenn es im Zuge der Nachrüstung von Sportsitzen oder Sportlenkrädern erfolgt, damit die mit den alten Komponenten entfernten Airbags nicht als Fehlerereignis gewertet werden. Hier sollte jedoch durch eine Eintragung die Unbedenklichkeit der Änderung sichergestellt sein, auch damit fremde Personen, die das Fahrzeug später nutzen oder ggf. erwerben, Kenntnis davon haben, welche Airbags nicht mehr vorhanden sind. Kritischer wird es, wenn entsprechende Symptome unterdrückt werden, um Gutachter, Käufer oder (z. B. im Falle eines Airbagdiebstahls) den Besitzer selbst zu täuschen. Sobald eine Abtrennung der Airbagwarnleuchte (siehe auch Kapitel zu Warnleuchten) oder das Vorhandensein eingebauter Simulatoren dem Fahrer oder sogar selbst dem (ggf. gewechselten) Besitzer eines Fahrzeuges nicht bekannt ist, können Fehlfunktionen unerkannt bleiben und notwendige Reparaturen völlig unbewusst ausbleiben. Im Falle eines Unfalls wäre dann mit erheblich größeren Personenschäden zu rechnen (vgl. auch [R97], [R111]).

Querführung – Exemplarische Gefährdungen durch eine unsachgemäße Nachrüstung

Insbesondere bezüglich potenzieller Risiken für die Straßenverkehrssicherheit kann die Abtretung von primären Fahraufgaben an ein automatisches System mit besonderen potenziellen Gefahren verbunden sein, vor allem vor dem Hintergrund nicht ausgereifter Sensoren, Aktoren und Algorithmen. So hängt die adäquate Regelung der Aktoren entscheidend von vollständigen Sensordaten und deren korrekter Fusion und Interpretation ab. Weitere potenzielle Gefahrenquellen ergeben sich aus der Notwendigkeit des Zugriffs auf die Fahrzeugbussysteme (z. B. Prüfen der Blinkerbetätigung sowie Reduktion der Lenkkraftverstärkung). Die Verlässlichkeit der Daten beider Richtungen wird dabei (zumindest im CAN-Bus) nicht geprüft.

Instrumentenkombination – Exemplarische Gefährdungen durch Veränderungen am Wegstreckenzähler und der Serviceintervallanzeige

Auch das Ändern des Kilometerstandes (vgl. Teil zur Instrumentenkombination in Kapitel 2.1.1) kann außer der eigentlichen Änderung des angezeigten Kilometerwerts (Funktionswirkung) noch zu Nebenwirkungen (Strukturwirkungen) führen. Ebenso wie das explizite Zurücksetzen der Serviceintervallanzeige (siehe ebenfalls Kapitel 2.1.1) kann das He-

rabsetzen des Kilometerstands dazu führen, dass der Käufer eigentlich ratsame Serviceinspektionen versäumt. Auch ist zu erwarten, dass der Verschleiß z. B. an Bremsscheiben und Reifen im Vergleich zu einem tatsächlich weniger gefahrenen Fahrzeug erhöht ist. Vermutlich hätten die Ursachen einiger Unfälle, die durch verschleißbedingtes Komponentenversagen entstanden sind, andernfalls rechtzeitig entdeckt und behoben werden können. Auch können Verschleißeffekte weniger kritischer Natur auch konstruktiv als Indiz für das Vorliegen eines entsprechenden Eingriffs einbezogen werden. Die recherchierten Quellen [R114] und [R113] listen hierzu z. B. die verstärkte Abnutzung von Sitzpolstern, der Türverkleidung, Abrieb an Gummipads auf den Pedalen oder des Bodenbelags. Auch Auffälligkeiten im Scheckheft sowie signifikante Abweichungen der angezeigten Laufleistung zu Erwartungswerten wie (Alter * Durchschnittsverbrauch), vergessene Aufkleber/Etiketten im Motorraum, bei der vorige Laufleistungen z. B. bei Ölwechseln vermerkt wurden, sowie Auffälligkeiten an mechanischen Zählwerken werden als mögliche Indizien bzw. Nebeneffekte der Veränderung erwähnt.

Erfolgt die Manipulation des Kilometerzählers über die Einstellung einer unzutreffenden K-Zahl (vgl. Kapitel 2.1.1), wird i. d. R. als zusätzliche Nebenwirkung auch der Tachometer während der Fahrt eine zu niedrige Geschwindigkeit anzeigen. Ist sich der Fahrer dieser Tatsache nicht permanent bewusst, könnte dies das Fahren mit zu hoher Geschwindigkeit fördern und so auch zu einer Gefährdung für den Straßenverkehr führen.

Video-System – Exemplarische Gefährdungen durch Veränderungen für „Video-in-Motion“

Bei Veränderungen zur Freischaltung von Video-in-Motion (vgl. entsprechender Abschnitt in Kapitel 2.1.1) ist eine generell relevante Nebenwirkung, die auch bei nicht-invasiven Realisierungen wie der Verwendung tragbarer Geräte relevant ist, die Ablenkung des Fahrers. Insbesondere sofern technische Veränderungen vorgenommen werden, um aus einem bereits verbauten System die entsprechende Beschränkung zu entfernen, können auch weitere technische Nebenwirkungen als Strukturwirkung dieses Eingriffs auftreten. Wie in Kapitel 2.1.1 beschrieben, werden hierzu in vielen Fällen zentrale Betriebsdaten wie z. B. Geschwindigkeits- oder Handbremssignal verändert, um entsprechend implementierte Sicherheitsüberprüfungen seitens des Systems zu umgehen. Je nachdem, wie dies erfolgt, können die verfälschten Betriebsdaten auch andere (Teil~)Systeme im adressierten Gerät oder sogar Busnetzwerk erreichen und von diesen verarbeitet werden. Dies kann prinzipiell zu Nebenwirkungen sowohl seitens der Zielkomponenten (meist integriert im Navigationssystem) als auch des Gesamtfahrzeuges haben. Ein auf 0 gesetztes Geschwindigkeitssignal kann beispielsweise auch die geschwindigkeitsabhängige Lautstärken-Anpassung (GALA) beeinflussen. Indem das System von einem stehenden Fahrzeug ausgeht, ist es effektiv deaktiviert, eine geschwindigkeitsabhängige Lautstärkeerhöhung oder -verringerung findet nicht mehr statt. Dies entspricht einer Reduzierung des Komforts als Strukturwirkung. Durch das Entfernen des Geschwindigkeitssignals wird auch oft die Genauigkeit der Navigation beeinflusst (wie der recherchierten Quelle [R43] zu entnehmen ist), die auf die Einbeziehung dieser Information ausgelegt ist und ausschließlich über GPS-Daten nicht angemessen arbeitet. Dies kann während der Fahrt bis zu Abbrüchen und Abstürzen der Zielführung führen. Da der Fahrer dadurch beim Fahren teils Korrekturen an den Einstellungen bzw. Neustarts einstellen muss, kann dies zu einer erhöhten Ablenkung des Fahrers führen, die zu einer Gefahr für die Verkehrssicherheit werden kann.

Ein noch drastischeres Beispiel hierzu konnte im Gespräch mit dem Mitarbeiter der Entwicklungsabteilung eines großen deutschen Automobilherstellers ermittelt werden. In diesem Fall hatte ein Kunde sein Oberklassefahrzeug zu einem Tuning-Anbieter gegeben, der im Auftrag das Freischalten der TV-Funktion beim Fahren vornehmen sollte. Mangels einer exakt für dieses Model bestimmten Lösung verwendete der besagte Tuninganbieter hierzu eine CAN-Filterbox, die für ein Mittelklassefahrzeug des besagten Herstellers bestimmt ist. Deren Funktion ist wie in Kapitel 2.1.1 beschrieben, das Geschwindigkeitssignal auf dem CAN-Bus für das entsprechende Steuergerät herauszufiltern bzw. auf null zu setzen, sodass das Gerät auch ein fahrendes Fahrzeug als stehend interpretiert. Prinzipiell ist die Wahl einer Filterbox für ein abweichendes Modell desselben Herstellers meist ebenso möglich, da dieser die Nachrichtensyntax (auch laut Aussage des Mitarbeiters) in der Regel modellübergreifend konstant hält. Allerdings konnte der Tuning-Anbieter die Filterbox nicht, wie für das Mittelklassefahrzeug vorgesehen, direkt vor dem

verantwortlichen Steuergerät platzieren, da dieses im vorliegenden Oberklassemodell an einen MOST-Bus angeschlossen ist. Dieser beruht auf einer Glasfaserverkabelung, für die bis heute kaum entsprechende (vergleichsweise deutlich teurere) Ausrüstung für elektronische Eingriffe verfügbar ist. Daher platzierte der Tuner die Filterbox zwischen dem über CAN realisierten Antriebsstrang-Netzwerk und dem zentralen Gateway, der Nachrichten zwischen den Teilnetzwerken des Fahrzeuges verteilt. Auch an dieser Stelle verbaut, war die Freischaltung des TV-Systems erfolgreich. Einige Zeit später bemerkte der Besitzer bei Autobahnfahrten, dass die adaptive Lenkung insbesondere bei schneller Fahrt viel zu leichtgängig wurde und das Fahrzeug nur schwer zu kontrollieren war. Da die Vertragswerkstatt auch mit der elektronischen Fahrzeugdiagnose keine Fehlerursache finden konnte, wurde das Fahrzeug ausgetauscht und durch Experten des Herstellers untersucht. Hierbei fiel schließlich die vor den Gateway geschaltete Filterbox auf, deren Effekt (d. h. das Setzen des Geschwindigkeitssignals auf null) anschließend ermittelt wurde. Indem die Filterbox in diesem Fall zwischen Antriebsstrang und Gateway platziert wurde, war die aktuelle Geschwindigkeit in sämtlichen anderen Teilnetzwerken (d. h. nicht nur am TV-System im Infotainment-Subnetz) nur noch mit dem Wert 0 sichtbar. Dies konnte als Ursache dafür festgestellt werden, dass auch die adaptive Lenkung bei hohen Geschwindigkeiten viel zu leichtgängig war, da das System auch in diesen Fällen eine Geschwindigkeit von null als Eingabe bekam. Wie die Analysen anschließend feststellten, hätten noch weitaus kritischere Folgen auftreten können: In dem Fahrzeug war auch ein System zum schlüssellosen Zugang verbaut (Keyless Entry and Go, siehe Glossar), bei dem auch die Zündung ohne Schlüssel mit Hilfe eines Start/Stopp-Knopfes betätigt werden kann. Dadurch ist das Lenkradschloss bei diesem Fahrzeug nicht konventionell mechanisch mit dem Zündschloss gekoppelt, sondern wird elektronisch angesteuert. Da auch dieses System durch den Eingriff während der Fahrt eine Geschwindigkeit von 0 als Eingabewert bekam, hätte der Stopp-Knopf prinzipiell auch während der Fahrt betätigt werden können. Bei einer versehentlichen Betätigung wäre aus Sicht der Experten auch das Lenkradschloss eingerastet, was als weitere Strukturwirkung des Eingriffs insbesondere bei schneller Fahrt weitaus schwerwiegende Gefahren für die Fahrzeuginsassen und den weiteren Straßenverkehr hätte bedeuten können.

Allgemeine Warnfunktionen – Exemplarische Gefährdungen durch (De~)Aktivierung

Bezüglich der verschiedenen Warnfunktionen im Fahrzeug (vgl. auch Vorstellung in Kapitel 2.1.1) lassen sich diese teils auch mit Diagnosemitteln aktivieren bzw. deaktivieren. Beides kann jedoch neben den erwünschten Effekten auch unerwünschte Nebeneffekte mit sich bringen, die generell abzuwägen sind.

Die nach den Rechercheergebnissen sehr verbreitete Veränderung der Gurtwarner-Deaktivierung führt zwar dazu, dass bei der Ablage schwererer Gegenstände auf dem Beifahrersitz eine oft als störend empfundene Warnung unterbleibt (Funktionswirkung). Gleichzeitig kann durch die Veränderung jedoch als Strukturwirkung auch das Vergessen des Gurt-Anlegens durch Personen auf dem Beifahrersitz begünstigt werden. Dies kann im harmlosen Falle zu Bußgeldern bei Kontrollen führen (siehe Bußgeldkatalog des BMVBS/BKatV, 2009). Im ernsteren Falle eines Unfalls sind dadurch hauptsächlich Leib und Leben der nicht angeschnallten Insassen durch die fehlende Schutzfunktion gefährdet. Problematisch kann auch im Falle eines Weiterverkaufs sein, wenn der Käufer nicht auf die Deaktivierung des Warntons hingewiesen wird. Häufig wird die Deaktivierung der Warnfunktion unfachmännisch vorgenommen, sodass auch noch weiterreichende Auswirkungen auftreten können. Wird zum Deaktivieren des Beifahrer-Gurtwarners beispielsweise der Kontakt der Sitzmatte im Beifahrersitz getrennt, wovor in [R81] gewarnt wird, können als Strukturwirkung dieser Veränderung auch weitere Systeme betroffen sein: Beispielsweise können mit den Beifahrerairbags und Gurtstraffern sogar Systeme zur passiven Insassensicherheit erheblich gestört sein, da diese nun auch nicht mehr erkennen können, ob auf dem Beifahrersitz tatsächlich eine Person sitzt. Je nach Art der Veränderung können durch nicht auslösende Airbags auf belegten Plätzen (fehlender Aufprallschutz) sowie auch durch auslösende Airbags auf unbelegten Plätzen (z. B. erhöhter Schallpegel durch unnötige Auslösungen) erhebliche Schäden für Körper und Gehör auftreten. Potenziellen Folgen wie diesen sind sich die Akteure bei Veränderungen mit vergleichsweise harmlosen Funktionswirkungen wie der Warntondeaktivierung oft nicht bewusst. Die Risiken einer Deaktivierung des Gurtwarners werden in den Kommentaren aus [R45] auch durch die Einschätzung des Vertreibers einer entsprechenden Diagnoselösung bestätigt, der

schreibt: „Nur sind die genannten Änderungen an Gurtwarner oder Abgasrückführung doch nur in bestimmten seltenen Einzelfällen sinnvoll und keineswegs als 'Standardmodifikation' im öffentlichen Straßenverkehr anzuraten! Mit 'Tuning' hat so etwas meiner Meinung nach nichts zu tun“ (siehe [R45]).

Nach dem Bericht eines Autohausangestellten soll es im Falle eines französischen Herstellers bei den Fahrzeugen ein Sprachausgabesystem geben, über das neben allgemeinen Ausgaben (z. B. eine Begrüßung des Fahrers beim Einstieg) auch Warnungen wie insbesondere Fehlervorkommnisse kommuniziert werden. So kann beispielsweise vor einer nicht gelösten Handbremse oder einer defekten Glühbirne gewarnt werden. Da sich viele Fahrer von der häufigen Einspielung einzelner Nachrichtentypen gestört fühlen, lassen sich einige die Kommunikation dieser Meldungen in der Werkstatt selektiv abschalten. Dies bedeutet, dass über die Diagnosesoftware eine Markierung (Flag) gesetzt wird, dass diese Nachricht nicht mehr ausgegeben werden soll. Laut dem Mitarbeiter soll dies aber automatisch nicht nur die Ausgabe per Sprachausgabe betreffen, sondern sich z. B. auch auf die visuellen Ausgaben wie insbesondere im Kombiinstrument auswirken.

Generell können sich durch das Deaktivieren von Warnfunktionen Probleme ergeben, dass die Warnungen überhaupt nicht mehr wahrgenommen werden. Insbesondere wenn diese Einstellungen nach einem Verkauf des Fahrzeugs nicht wieder auf die Standardeinstellungen zurückgestellt werden, ist es wahrscheinlich, dass der Käufer von der bewussten Ausblendung einzelner Informationen keine Kenntnis hat.

Andere Warnfunktionen sind standardmäßig (d. h. im Auslieferungszustand vieler Fahrzeuge, z. B. länderabhängig) nicht aktiv, können aber per Diagnosesoftware aktiviert werden. Ein Beispiel hierfür ist die durch einen Nutzerkommentar zu [R45] genannte Aktivierung der Reifendruckkontrolle. Generell birgt das Vorhandensein von Warnfunktionen allerdings die Gefahr, dass der Fahrer sich auf deren korrekte Funktion verlässt und das durch die Warnfunktion abgedeckte Funktionsspektrum des Fahrzeuges nicht mehr aktiv kontrolliert. So könnte ein Fahrer beispielsweise nach der Aktivierung der Reifendruckkontrolle nachlässig in der aktiven eigenen Kontrolle des Reifendrucks werden. Sollte einer der beteiligten Sensoren oder die gesamte Warnfunktion eine Fehlfunktion haben, könnte z. B. ein zu niedriger Reifendruck durch den Fahrer länger unbemerkt bleiben, als dies ohne die durch ihn vorgenommene Aktivierung der Warnfunktion der Fall gewesen wäre.

Lichtanlage: Frontscheinwerfer – Exemplarische Gefährdungen durch unsachgemäße Nachrüstung von Xenon-Licht

Das Nachrüsten von Xenon-Licht erfolgt in vielen Fällen unsachgemäß (vgl. [R17]), d. h. ohne die notwendigen Vorkehrungen, an die eine Zulassungsfähigkeit gebunden ist (z. B. Streuscheibenreinigungsanlage, automatische Leuchtweitenregulierung). Dies erhöht die Gefahr, dass z. B. der Gegenverkehr geblendet wird, was ebenfalls die Straßenverkehrssicherheit gefährden kann. So heißt es beispielsweise in [R97] im Kontext einer Berichterstattung zu Erfahrungen aus der Hauptuntersuchung: „Ein stark blendendes, mit Xenonlicht bestücktes Fahrzeug wird auf der Straße schnell zu einer massiven Gefahr für den Gegenverkehr.“

Außenspiegel – Exemplarische Gefährdungen durch Veränderungen zum Anklappen während der Fahrt

Sollten zunehmend Fahrer, wie sich z. B. in Recherchequelle [R140] andeutet, die Außenspiegel während der Fahrt anklappen (z. B. aus Gründen der Aerodynamik), dann könnten sich durch derartige Veränderungen durchaus Gefährdungen für die Straßenverkehrssicherheit ergeben. Allein durch den Innenrückspiegel kann keine ausreichende Sicht (seitlicher und rückwärtiger Bereich) ermöglicht werden. Aktuell scheinen zu einem solchen Trend jedoch keine Anzeichen zu bestehen.

Verdeck – Exemplarische Gefährdungen durch Veränderungen zur Betätigung während der Fahrt

Wie in Kapitel 2.1.1 ebenfalls dokumentiert wurde, werden auch elektronische Veränderungen betrieben, um bei Cabrios ein Öffnen des Verdecks während der Fahrt zu ermöglichen. Da dies sehr offensichtlich die Kontrollierbarkeit des Fahrzeugs gefährden kann, begrenzen einige Anbieter von Hardware für entsprechende Veränderungen die Anwendbarkeit ihrer Lösung selbst auf z. B. (modellabhängig) 40 oder 60 km/h [R35]. Andere Anlei-

tungen wie insbesondere [R32] sind jedoch komplett geschwindigkeitsunabhängig und appellieren lediglich an die Vernunft der Endanwender. Neben Strukturwirkungen, die das Fahrzeug selbst gefährden, könnten durch abgerissene Teile auch weitere Teilnehmer des Straßenverkehrs gefährdet werden.

Infrastruktursysteme: Verkehrstelematik – Exemplarische Gefährdungen durch Falschanzeigen

Unautorisierte Eingriffe in Infrastruktursysteme bieten potenziell ebenfalls ein erhebliches Gefahrenpotenzial. Zwar sind entsprechende Einheiten in der Regel stationär, interagieren aber mit einer Vielzahl vorbeifahrender Fahrzeuge. Das in Kapitel 2.1.2 vorgestellte Beispiel des manipulierten elektronischen Verkehrsschilds macht deutlich, dass sich eine Vielzahl von Fahrern von Falschmeldungen beeinflussen lassen dürfte. Neben dem Wegfall der ursprünglich angezeigten Meldung können die Verkehrsteilnehmer durch die neu hinzugefügten Nachrichten gezielt beeinflusst werden, insbesondere wenn diese weniger offensichtlich als gefälscht zu erkennen sind, als dies im obigen Beispiel der Fall war. Beispielsweise könnte eine Meldung wie „Straße gesperrt, bitte hier auf Freigabe warten“ vermutlich eher geeignet sein, den Verkehr stark zu beeinflussen. Dies gilt prinzipiell genauso für das ebenfalls in Kapitel 2.1.2 genannte Beispiel der gefälschten Verkehrsmeldungen, welches jedoch bisher nur anhand akademischer Quellen belegt ist und nach vorliegendem Kenntnisstand in der Praxis glücklicherweise noch nicht missbräuchlich eingesetzt und beobachtet wurde.

Infrastruktursysteme: Funkschnittstellen – Exemplarische Gefährdungen bei Einsatz von Ortungssystemen

Mit Blick auf Quellen wie [R101] werden auch weitere potenzielle Gefährdungen deutlich. Dort wird zu den Ortungssystemen, die als Diebstahlsschutz eingesetzt werden, berichtet, dass es möglich ist, ein gestohlenes Fahrzeug aus der Zentrale stillzulegen, indem die Wegfahrsperre und die Warnblinkanlage aktiviert werden. Erfolgt dies im falschen Zeitpunkt, könnte durch das plötzliche Stehenbleiben des Fahrzeugs der gesamte Straßenverkehr gefährdet werden. Selbst im Fall zunehmender Diebstahlsfälle könnte dies daher ein unangemessenes Mittel sein, dessen rechtliche Zulässigkeit in dieser Form fraglich ist. Sollte die Implementierung dieses oft als nachrüstbare Komponente von Drittherstellern realisierten Systems Sicherheitslücken aufweisen, könnte es möglicherweise auch gezielt von Dritten missbraucht werden, um auch nicht gestohlene Fahrzeuge, die dieses System aufweisen, außer Betrieb zu setzen. Dies wäre dann ebenfalls ein weiterer gefährlicher potenzieller Nebeneffekt der Installation eines solchen Systems.

Infrastruktursysteme: Geschwindigkeitsmesseinrichtungen – Exemplarische Gefährdungen beim Einsatz von Systemen zur Warnung vor Geschwindigkeitsmessungen

In Recherchequelle [R143] wurde im Rahmen praktischer Tests verschiedener Geräte zur Geschwindigkeitswarnung ermittelt, dass in vielen Fällen nach der Warnung vor einer Messung nur noch ein unverzügliches Einleiten des Bremsvorgangs hilft, um einer Ahndung zu entgehen. In diesem Kontext wird explizit die Gefahr eines Auffahrunfalls genannt. Auch wenn der nachfolgende Fahrer einen zu geringen Abstand einhält, trägt bei unbegründetem unvorhersehbarem Bremsen nach [R143] der Vorausfahrende die Schuld. Das aus der Reaktion auf die Warnung erfolgende scharfe Bremsen wird dort explizit als Verkehrsgefährdung eingestuft.

Weitere recherchierte Gefährdungen als resultierende Nebenwirkungen nach sonstigen Änderungen am Fahrzeug

Im Folgenden sind Nebenwirkungen einer weiteren Veränderung genannt, die in den Recherchen zusätzlich ermittelt werden konnten.

Nachrüstung Multifunktionslenkrad

In [R13] wird nach der Nachrüstung eines Multifunktionslenkrades berichtet, dass sich das Navigationssystem alle zwei Minuten oder während starken Beschleunigens abschaltet (vgl. oben zu Video-in-Motion genannte Nebenwirkung durch Ablenken) sowie der Ton unterbricht und das Fahrerinformationssystem erlischt. Als Ursache wurde das durch eine unvollständige Verkabelung hervorgerufene Senden eines Signals identifiziert, das eine abgeschaltete Zündung kommuniziert. Prinzipiell könnte diese Fehlinformation auch weitere Steuergeräte negativ beeinflussen, was neben der Aufmerksamkeit des Fahrers im ungünstigsten Fall auch die Steuerbarkeit des Fahrzeuges gefährden könnte.

5.3 Abschließende Abschätzungen zu Gefährdungen aus elektronischen Veränderungen

Die Interpretation der Gefährdungen für den Straßenverkehr basiert hauptsächlich auf der Betrachtung der unbeabsichtigten und strukturellen Wirkungen von häufig veränderten Komponenten. Anhand verschiedener praktischer Beispiele wurde das Spektrum dieser unbeabsichtigten Wirkungen in Kapitel 5.2.1 aufgezeigt. Es ist auch möglich, diese in verschiedene Kategorien zu systematisieren, die direkte von indirekten, aktive von passiven sowie technische (physisch/physikalisch) von psychologischen Wirkungen unterscheiden. So kann sich die Gefährdung durch TV-in-Motion i. Allg. indirekt auf der psychologischen Ebene durch eine erhöhte Ablenkung des Fahrers (passiv) ausprägen, während das Abschalten von Gurtwarnungen vermutlich eine direkte Gefährdung des Fahrers nach sich ziehen kann, wenn dieser nicht angeschnallt in eine Kollision verwickelt wird und dabei physischen Schaden nimmt. Die Leistungssteigerung führt direkt zu einer Gefährdung auf technischer Ebene z. B. durch erhöhten Verschleiß und Erreichen von Geschwindigkeiten, für die Fahrzeugkontrollsysteme wie Lenkung oder Bremsen nicht ausgelegt sind (aktiv).

Die sich aus den Recherchen ergebenden Beispiele für potenzielle Gefahren aus Veränderungen wurden in Tabelle 17 zusammengestellt.

Über die im Verlauf von Kapitel 5.2.1 konkret behandelten Gefahrenbeispiele hinaus wurden auch für die weiteren Komponenten, zu denen im vorderen Teil dieses Dokumentes Anzeichen für Veränderungen recherchiert werden konnten, potenziell resultierende Gefahren ergänzt. Ein abschließender zusammenfassender Überblick über potenzielle Gefährdungen, die als besonders relevant für den Straßenverkehr abgeschätzt wurden, findet sich im Rahmen der abschließenden Einschätzung der Ergebnisse in Kapitel 7.1.

				Potenzielle Gefahren (Funktions- und Strukturwirkungen)	
Art der Komponente (Teilfunktion)		**Potenzielle Motivation für die Veränderung**	**Potenzielles Risiko (Kap. 4)**	**bzgl. der veränderten Komponente bzw. Teilfunktion**	**bzgl. weiterer Komponenten bzw. Teilfunktionen**
Motor und Antriebsstrang	Motorsteuerung	Leistungssteigerung	mittel - hoch	Erhöhter Verschleiß, Motorschaden	Ausfälle weiterer Komponenten wie Bremskraftverstärker, Servolenkung; Regresse (Versicherung, Steuer), Rechtlich (Allgemeine Betriebserlaubnis, Schadstoffgrenzwerte), Unfälle durch Selbstüberschätzung des Fahrers
		Verbrauchsreduktion	mittel	Überhitzung, Motorschaden, erhöhte NOX-Werte	Ausfälle weiterer Komponenten wie Bremskraftverstärker, Servolenkung
		Nachrüstung von Regelungsfunktionen für Autogasanlage (Senkung Betriebskosten)	mittel - hoch	bei unsachgemäßer Durchführung: Ausfall Motorsteuerung, Motorschaden, Gasentzündung, unzulässige Abgaswerte	Ausfälle weiterer Komponenten wie Bremskraftverstärker, Servolenkung
		Motor bzw. Fahrzeug zum Stillstand bringen (destruktive Motivation)	mittel - hoch	-	Kontrollverlust über das Fahrzeug, ggf. Verkehrsgefährdung. Bei Senden von Airbag-Auslöse-Benachrichtigung je nach Systemeigenschaften ggf. Strukturwirkungen weiterer Systeme (z. B. automatische Türöffnung)
	Motorsteuerung (Abgasrückführung)	Deaktivieren	mittel	Überschreitung Schadstoffgrenzwerte	Überschreiten Schadstoffgrenzwerte, Erlöschen Allgemeine Betriebserlaubnis, bei Unfällen Weigerung der Kostenübernahme durch Versicherung
	Motorsteuerung (Geschwindigkeits-Abregelung)	Deaktivieren	mittel	(i. d. R. nicht relevant, wenn das Fahrzeug für höhere Geschwindigkeiten konzipiert wurde)	Unpassende Reifen, längerer Bremsweg, Fehleinschätzung Geschwindigkeit, …
	Getriebesteuerung (Automatikgetriebe, elektronische Schaltpunktsteuerung)	Schaltpunkte verändern	mittel	Getriebeschaden, Verschleiß	Erhöhter Kraftstoffverbrauch bei Verlagerung der Schaltpunkte in höhere Drehzahlbereiche
	Getriebesteuerung (pseudo-automatisierte Schaltung)	Nachrüstung	niedrig - mittel		Kontrollverlust bei Fehlfunktion, ggf. Schäden an Motor und Kupplung, abrupter Bremsvorgang ohne Aufleuchten der Bremslichter
	Startsteuerung	Motorstart auf Knopfdruck (Startknopf nachrüsten)	niedrig	Schaden am Anlasser (versehentliches Betätigen des Startknopfes bei laufendem Motor)	Motorschaden (als Folge von Anlasserschaden), ggf. Gefährdung des Verkehrs als Folgeerscheinung

Tab. 17: Übersicht über potenzielle Gefahren (vierte Teilergebnistabelle)

				Potenzielle Gefahren (Funktions- und Strukturwirkungen)	
Art der Komponente (Teilfunktion)		**Potenzielle Motivation für die Veränderung**	**Potenzielles Risiko (Kap. 4)**	**bzgl. der veränderten Komponente bzw. Teilfunktion**	**bzgl. weiterer Komponenten bzw. Teilfunktionen**
Fahrwerksysteme	Servolenkung	Härtere Einstellung	mittel - hoch	-	Ggf. Kontrollverlust über das Fahrzeug, ggf. Verkehrsgefährdung
		Mehr Fahrleistung (Ersetzen durch eine elektronisch gesteuerte und elektrisch angetriebene Servolenkung, adaptive Regelung)	niedrig	-	Kontrollverlust, unerwartetes/unangemessenes Lenkverhalten
	Adaptive Niveauregelung	Elektronisches Tieferlegen	mittel	Dämpferschäden	Beschädigungen am Unterboden und befestigten Teilen bei Bodenwellen durch zu tief konfigurierte Fahrzeuglage
	Fahrdynamikkregelsysteme	Deaktivieren einzelner Funktionen (z. B. ABS oder ESP)	mittel - hoch	(Fehlercodeeinträge nach Stromverlust)	Gleichzeitiges Wegfallen weiterer Funktionen, die auf dem deaktivierten Gerät implementiert sind
		Einleiten unerwünschter/Verhindern gewünschter Bremsvorgänge (destruktive Motivation)	mittel - hoch	Temporäte Nichtverfügbarkeit der Fahrdynamikregelsysteme	Kontrollverlust über das Fahrzeug, erhebliche Verkehrsgefährdung
Passive Sicherheit	Airbagsystem/Gurtstraffer	Verbergen der Nichtfunktionalität	mittel	Nichtfunktionalität bzw. eingeschränkte Funktion	Unkenntnis über Missstand bei Käufern. Schwerere Verletzungen bei Unfällen.
Fahrerassistenzsysteme	Längsführung (Tempomat)	Nachrüstung nicht vorhandener Funktion	niedrig - mittel	-	Kontrollverlust bei unsachgemäßer Nachrüstung
		Freischaltung nicht aktiver Funktion	mittel - hoch	-	-
	Längsführung (ACC)	Mindestabstand verringern	mittel - hoch	-	Erhöhter Bremsverschleiß und -belastung, höheres Risiko für Auffahrunfälle
	Querführung	Aktiven Assistenten nachrüsten	niedrig - mittel	-	Kontrollverlust bei unsachgemäßer Implementierung/Systemversagen (durch Einbringen von Lenkmoment)
Infotainment	Instrumentenkombination (Wegstreckenzähler)	Kilometerstand ändern	hoch	Falsch angezeigte Geschwindigkeit (bei k-Zahl Änderung)	Erhöhter Verschleiß durch Wartungsversäumnisse. Bei k-Zahl-Änderung: Unfälle durch unbewusst falsche Geschwindigkeitsanzeige. Falsches Schalterverhalten bei elektronischen Getriebesteuerungen
	Instrumentenkombination (Serviceintervallanzeige)	Zurücksetzen	mittel - hoch	Fehlender Hinweis auf notwendige Wartungsarbeiten	Erhöhter Verschleiß – hin zu Schäden an wartungsbedürftigen Komponenten (z. B. Motor), Garantieverlust
	Instrumentenkombination (Fahrerinformationssystem)	Beschreiben mit eigenen Inhalten (es wurden konstruktive wie destruktive Motivationen ermittelt)	mittel	Verlust regulär angezeigter Nachrichten	Folgeerscheinungen aufgrund der Nicht-Wahrnehmung überschriebener Nachrichten. Beeinträchtigung des Fahrers durch angezeigte Falschwerte bzw. -meldungen
	Radio	Anheben der Lautstärke auf Maximum (Destruktive Motivation)	mittel	-	Beeinträchtigung des Fahrers durch zu laute Audioausgabe (z. B. durch eingedrungenen Schadcode vorgenommen)
	Navigationssystem	Kostenloses Nachinstallieren von Kartenmaterial	mittel - hoch	ggf. Leseschwierigkeiten selbst erstellter Kopien, Navigationsprobleme durch ungeeignete Kartendaten, Programmmodule, Firmware aus nicht vertrauenswürdiger Quelle	Ablenkung des Fahrers durch ggf. auftretende Fehlfunktionen
		Installieren von POI („Blitzer"-Positionen etc.)	hoch	-	Fahrer bremst abrupt, ggf. Verkehrsbeeinflussung
		Eigene Änderungen an Betriebssoftware und -daten	niedrig - mittel	ggf. Fehlfunktionen veränderter/erweiterter Teilfunktionen des Navigationssystems	Ablenkung des Fahrers durch ggf. auftretende Fehlfunktionen
	Navigationssystem (Fahrschulfunktion)	Aktivierung	niedrig - mittel	-	-
	Video-System	TV In Motion	mittel - hoch	-	Ablenkung bei der Nutzung des Systems durch den Fahrer. Durch Signalveränderungen: Wegfall Lautstärkeanpassung, Ungenaue Navigation, unangemessene adaptive Lenkung, Einrasten Lenkradschloss während der Fahrt.
	Allgemeine Warnfunktionen	Deaktivieren (z. B. Gurtwarner)	mittel - hoch	-	Begünstigtes Vergessen der Ursache. Fehlende Kenntnis nach Weiterverkauf. z. B.: Gurtanlegung: Bußgelder; erhöhtes Verletzungsrisiko bei Unfällen; Herausschleudern unangeschnallter Personen in den Straßenverkehr. Gestörte Airbagauslösung
		Provozieren von Warnungen (z. B. Reifendruckkontrolle) durch Dritte, um Fahrer zum Anhalten zu verleiten (destruktive Motivation)	niedrig - mittel	ggf. Nichtverfügbarkeit der korrekten Reifendruckwerte für die Dauer des Angriffs	Ggf. Wechselwirkungen mit weiteren Fahrzeugfunktionen, die den Reifendruck mit in die Berechnungen einbeziehen

Tab. 17: Fortsetzung

				Potenzielle Gefahren (Funktions- und Strukturwirkungen)	
Art der Komponente (Teilfunktion)		Potenzielle Motivation für die Veränderung	Potenzielles Risiko (Kap. 4)	bzgl. der veränderten Komponente bzw. Teilfunktion	bzgl. weiterer Komponenten bzw. Teilfunktionen
Zugriffsschutz (Security)	Schließsystem (Zugang durch Funköffner)	Unberechtigtes Öffnen	niedrig - mittel	-	Verlust/Diebstahl von Gegenständen aus dem Fahrzeug
		Verhindern des Verschließens durch Jamming	mittel - hoch	temporärer Ausfall/Einschränkung der Verfügbarkeit	Verlust/Diebstahl von Gegenständen aus dem Fahrzeug, Versicherungsschutz erlischt wegen Nichtverriegelung
	Schließsystem (Autolock-Funktion)	Nachrüsten/Aktivieren	mittel	(gering, da meist regulär vorhandene Funktion, die lediglich aktiviert wird)	Ggf. fehlende Unfallnotentriegelung (je nach Implementierung).
	Schließsystem	Ein-/Aussperren der Fahrzeugnutzer (destruktive Motivation)	mittel	temporärer Ausfall/Einschränkung der Verfügbarkeit des Schließsystems	Stresssituation für die Fahrzeugnutzer, ggf. Verkehrsbehinderung bei ungünstiger Position eines nicht zugänglichen Fahrzeugs im Straßenverkehr
	Diebstahlwarnanlage	Unberechtigte Deaktivierung	mittel	Nichtfunktion Diebstahlwarnanlage	
		Einbindung eines Nachrüst-Kits	mittel	-	
		Setzen der „Anti-Polenschlüssel"-Kodierung	mittel	(gering, da meist regulär vorhandene Funktion, die lediglich aktiviert wird)	-
	Wegfahrsperre	Unberechtigte Deaktivierung	mittel	Nichtfunktion Wegfahrsperre	Ggf. Liegenbleiben des veränderten Fahrzeuges, falls System wieder aktiv wird.
		Einbindung eines Nachrüst-Kits	mittel	-	Ggf. Liegenbleiben des veränderten Fahrzeuges bei Fehler in der Umsetzung des Nachrüstsystems.
Karosserie	Lichtanlage (Frontscheinwerfer)	Nachrüsten Xenon-Licht	mittel - hoch	-	Blendung des Gegenverkehrs bei fehlender/ nicht angemessener Leuchtweitenregulierung
	Lichtanlage (Steuerprogramme)	Aktivieren/Entfernen diverser Schaltoptionen	mittel	(geringe Gefahren, da durch Hersteller implementiert und nur nachträglich aktiviert)	Ggf. rechtlich, wenn Betrieb der Option im Inland unzulässig
	Außenspiegel (elektrische Anklappfunktion)	Nachrüstung zur Komforterhöhung	mittel	-	Ungewolltes Anklappen während der Fahrt bei unsachgemäßer Nachrüstung
		Betätigung während der Fahrt	niedrig - mittel		Unfälle durch unzureichende Sicht
	Verdeck	Betätigung während der Fahrt	mittel	Beschädigung des Verdecks durch Ein-/Abreißen	Kontrollverlust über das Fahrzeug, Gefährdung des Verkehrs durch abgerissene Teile
	Klimasteuerung	Verringern des Komforts durch Dritte (destruktive Motivation)	niedrig - mittel	-	Beeinträchtigung des Fahrers durch ungünstige Klimatisierung (z. B. Aktivierung der Heizung im Hochsommer durch eingedrungenen Schadcode)
Infrastrukturkomponenten	Funkschnittstellen (Ortungssysteme)	Unterdrückung (Jamming) gegen Tracking, Maut, Steuer, Überwachung	mittel	Nichtfunktionalität des Systems selbst	Störung weiterer Funkbasierter (Teil-)Systeme (z. B. Mobiltelefone) ggf. auch anderer Verkehrsteilnehmer
	Funkschnittstellen (Verkehrsinformationen)	Senden gefälschter Verkehrs-Meldungen z. B. eigenen Vorteil	niedrig - mittel	-	Beeinflussung einer Vielzahl von Verkehrsteilnehmern durch die gefälschten Verkehrsmeldungen.
	Funkschnittstellen (Fernbedienfunktionen)	Nachrüsten von Fernbedienfunktionen (z. B. für Standheizung, Zentralverriegelung)	mittel	Falschauslösung bei unzureichender Implementierung/Einbau	Ggf. Batterieentleerung durch erhöhten Stromverbrauch im Ruhezustand
	Verkehrstelematik (autarke elektron. Verkehrstafel)	Unberechtigtes Anzeigen eigener Inhalte	niedrig - mittel	ggf. Zugriffsverlust für berechtigtes Personal nach Passwortänderung	Beeinflussung einer Vielzahl von Verkehrsteilnehmern durch die neue sowie den Verlust der alten Meldung
	Geschwindigkeits-Messeinrichtungen	Warnung vor Messungen	mittel - hoch	-	Fahrer bremst abrupt, ggf. Verkehrsbeeinflussung
		Störung von Messungen	mittel	Störung des Messvorgangs (evtl. des Messgerätes)	-

Tab. 17: Fortsetzung

6 Potenzielle Entwicklungen in naher Zukunft

Wie bereits in einer kurzen Abhandlung in Kapitel 2.1.2 (unter: Funkschnittstellen) erwähnt, bieten zukünftige Funkschnittstellen wie insbesondere Car-to-Car (C2C) und Car-to-Infrastructure (C2I) nicht zuletzt aufgrund ihres geplanten komplexen-Anwendungsspektrums vielfältige Anreize für potenzielle elektronische Veränderungen. Allerdings handelt es sich bei dieser verallgemeinernd auch als Car-to-X (C2X) Kommunikation bezeichneten Technologie trotz einer Vielzahl aktueller und abgeschlossener Forschungsprojekte noch um ein Zukunftsthema. Aus diesem Grund erfolgt die Behandlung dieses Themas im vorliegenden separaten Kapitel 6. Bis zu einer praktischen Einführung dieser Systeme sind Veränderungs- und Miss-

brauchsszenarien eher hypothetischer bzw. akademischer Natur. Entsprechende Quellen, in denen konkrete praktische Hinweise auf Veränderungen zu recherchieren sind, gibt es hierzu daher (insbesondere in den neuen Medien wie Internetforen) nach aktuellem Kenntnisstand noch nicht.

Dennoch befassen sich verschiedene Forschungsprojekte neben Anwendungen für C2X gleichzeitig zum Teil auch bereits mit der Identifikation denkbarer Missbrauchs-Szenarien, für die geeignete Schutzvorkehrungen vorzusehen sind. Eine Auswahl aktuell diskutierter Anwendungen aus dem Gebiet der C2X-Kommunikation und eine Übersicht über exemplarische themenbezogene Forschungsprojekte werden in Kapitel 6.1 aufgeführt, um die Tendenzen in der Forschung aufzuzeigen. Anschließend werden in Kapitel 6.2 die Ergebnisse einer Simulation vorgestellt, die die mögliche Reichweite von (noch hypothetischen) elektronischen Veränderungen in diesem Bereich veranschaulicht.

6.1 Übersicht über exemplarisch ausgewählte Forschungsprojekte zu C2X

Zu verschiedenen Zwecken wie insbesondere Erhöhung der Straßenverkehrssicherheit und Optimierung des Verkehrsflusses werden aktuell verschiedenste Anwendungen diskutiert, die zukünftig auf der Basis C2X-Kommunikation realisiert werden könnten (Tabelle 18). Diese Auflistung (die auch Teil der Veröffentlichung von BIßMEYER, 2009, Folie 4 ist) wurde im Projekt SIM-TD zusammengestellt, in dem aktuell in Deutschland in breiten Praxistests die Realisierbarkeit verschiedener solcher Anwendungen untersucht wird.

Daneben gibt es auch eine Vielzahl weiterer Forschungsprojekte zum Themengebiet der Car-to-X-Kommunikation. Tabelle 19 liefert eine Übersicht über ausgewählte beendete sowie aktuelle Projekte mit einer kurzen Beschreibung.

Mehrere dieser Projekte nehmen sich neben angestrebten Anwendungen auch Fragen der Absicherung dieses Funktionsspektrums gegen Missbrauch, d. h. der Informationssicherheit, an. So werden beispielsweise Verfahren für Authentizitätsprüfungen untersucht, um insbesondere das Spoofing von Nachrichten zu verhindern (vgl. gleichnamiger Basisangriff Kapitel 3), d. h. die Herkunft

Verkehr:
Erfassung der Verkehrslage und ergänzender Informationen/Basisdienste (Infrastruktur- und fahrzeugseitige Datenerfassung, Ermittlung der Verkehrslage und Verkehrswetterlage, Identifikation von Verkehrsereignissen)
Verkehrs(-fluss-)Information und Navigation (Straßenvorausschau, Baustelleninformationssystem, erweiterte Navigation)
Verkehrs(-fluss-)Steuerung (Umleitungsmanagement, Lichtsignalanlagen Netzsteuerung, lokale verkehrsabhängige Lichtsignalanlagensteuerung)
Fahren und Sicherheit:
Lokale Gefahrenwarnung (Hindernis-, Stauende-, Straßenwetter- und Einsatzfahrzeugwarnung)
Fahrerassistenz (Verkehrszeichen- und Ampelphasen-Assistent/-Warnung, Längsführungs-, Kreuzungs- und Querverkehrsassistent)
Ergänzende Dienste:
Internetzugang und lokale Informationsdienste (Internetbasierte Dienstnutzung, Standortinformationsdienste)

Tab. 18: Exemplarische Beispielanwendungen Car-to-X nach BIßMEYER, 2009, Folie 4

Projekttitel/URL	Kurzbeschreibung
CarNet (http://www.sichere-identitaet.de/zukunftsthemen/kommunikation/carnet)	Sicherheit und Kommunikation in Fahrzeugnetzen
CarTorrent	A Bit-Torrent System for Vehicular Ad-hoc networks
COMeSafety (http://www.comesafety.org/)	Communication for eSafety
COMO (http://omen.cs.uni-magdeburg.de/ auto motive/, http://www.ovgu.de/automotive/)	Competence in Mobility (Teilbereich B3: IT-Security Automotive)
Coopers (http://www.coopers-ip.eu)	CO-OPerative SystEms for Intelligent Road Safety
CVIS (http://www.cvisproject.org)	Cooperative vehicle-infrastructure systems
IntelliDrive (http://www.its.dot.gov/intellidrive/)	Active safety applications for preventing crashes
I-WAY (http://www.iway-project.eu)	Intelligent co-operative system in cars for road safety
MARTA	Technology Used To Improve Traffic Flow And Road Safety
PRECIOSA (http://www.preciosaproject.org/)	PRivacy Enabled Capability In Co-Operative Systems and Safety-Applications
Prevent (http://www.prevent-ip.org/)	Preventive and Active Safety
Safespot (http://www.safespot-eu.org/)	Cooperative vehicles and road infrastructure for road safety
SeVeCom (http://www.sevecom.org/)	Secure Vehicular Communication
SIM-TD (http://www.simtd.de/)	Sichere intelligente Mobilität – Testfeld Deutschland

Tab. 19: Übersicht exemplarischer Forschungsprojekte mit Bezug zum Themengebiet C2X-Kommunikation

einer Nachricht zweifelsfrei verifizieren zu können. Auch werden Ansätze zur Anonymisierung oder Pseudonymisierung der Nachrichten erforscht, um ein unautorisiertes Tracking von Fahrzeugen (siehe Kapitel 2.1.2 zu Funkschnittstellen) zu erschweren und somit die Privatsphäre der Nutzer zu schützen. Die Projekte adressieren dabei z. B. auch Herausforderungen, zunächst widersprüchlich erscheinende Teilkonzepte wie die beiden soeben genannten geeignet kombinieren zu können

6.2 Simulation eines hypothetischen Angriffsszenarios: Wurm-Epidemien in C2C-Netzen

Ein Wurmausbruch bezeichnet die massenhafte Verbreitung einer Schadsoftware über Netzwerkinfrastrukturen. Aus dem Bereich der Desktop-IT finden sich hierzu bereits etliche Praxisbeispiele. In diesem Kapitel soll für das automotive Umfeld exemplarisch am Beispiel einer Wurm-Epidemie aufgezeigt werden, welche Auswirkungen zukünftige Angriffe auf automotive Funkkommunikation haben könnten. Damit soll neben dem Potenzial entsprechender zukünftiger C2C- und C2I-Anwendungen auch für potenzielle gleichzeitig entstehende Risiken und Gefahren sensibilisiert werden.

Im Kontext der Netzwerksicherheit sind Wurmausbrüche als ein praxisrelevantes Angriffsszenario bekannt. Dahinter steht eine spezielle Ausprägung von Schadsoftware, welche die Eigenschaft aufweist, sich über Netzwerkverbindungen eigenständig auszubreiten (d. h. auf weitere Systeme zu replizieren). Insbesondere in der Desktop-IT war hierzu bereits eine Vielzahl entsprechender praktischer Ausbrüche zu beobachten. Dabei handelt es sich um keine Problematik, die ausschließlich drahtgebundene Netzwerke betrifft: Im Jahr 2008 zeigten bereits amerikanische Forscher mit Hilfe einer Simulation, dass sich ein geeignet programmierter Wurm auch in drahtlosen Netzwerken epidemieartig ausbreiten könnte (siehe HU, 2008). Hierbei wurde basierend auf realen Standortdaten von WLAN-Routern und unter Annahmen verschiedener Schutzstufen die Ausbreitung eines hypothetischen WIFI-Wurms unter den Stationären Routersystemen untersucht.

Speziell für den Anwendungsfall der Car-to-Car-Kommunikation wurden in 2009 Forschungsergebnisse der Universität Magdeburg veröffentlicht, die in einer daran angelehnten Simulation eine hypothetische Wurm-Epidemie in C2C-Netzen untersuchte. In BIERMANN, 2009 wurden hierzu zunächst relevante Gemeinsamkeiten und Unterschiede zwischen WLAN-Netzen aus der Desktop-IT und C2C-Netzen aus dem automotiven Anwendungsfeld gegenübergestellt. Auch wenn beide in Teilen technisch sehr ähnlich umgesetzt sind[5], zeichnen sich C2C-Netze demnach insbesondere durch die hohe Dynamik ihrer Teilnehmer (der Fahrzeuge) aus. Auch mit Blick auf Unterschiede in der kryptografischen Netzabsicherung sowie der begrenzten nutzerseitigen Administrierbarkeit von C2X-Onboard-Units wurde ausgehend von den Annahmen der Ausgangsarbeit (HU, 2008) das Angriffsszenario für den C2C-Fall angepasst.

In Anlehnung an das Simulationskonzept aus HU, 2008 wurden für das C2C-Szenario daher geeignete neue Annahmen für die Ausbreitung einer vergleichbaren Wurmepidemie gemacht. Grundannahme hierzu ist, dass potenzielle Angreifer in zukünftigen C2X-On-Board-Units (OBUs) potenzielle Sicherheitslücken finden, die sich in Form von Exploits zum Einschleusen beliebiger Programmcodes nutzen lassen. Software-Schwachstellen, die durch Anfälligkeiten für Fehler wie Puffer-, Heap- oder Ganzzahlüberläufe aktuell zunehmend im Bereich der Desktop-IT in verschiedensten Softwareprodukten gefunden und zur Verbreitung von Schadcode – insbesondere auch von Würmern – genutzt werden, könnten zukünftig potenziell auch in automotiven IT-Anwendungen gefunden werden. Angesichts verschiedener Faktoren ist zu befürchten, dass entsprechende Vorfälle auch in diesem Bereich zukünftig wahrscheinlicher werden. Hierzu zählen die zunehmende Komplexität des Programmcodes in automotiver IT sowie der steigende Anreiz für Angreifer aufgrund der zunehmenden Vernetzung, Leistungsfähigkeit und Anwendungsvielfalt moderner automotiver IT. Werden beispielsweise in einem Code zur Verarbeitung über C2C eingehender Verkehrsmeldungen keine oder unzureichende Prüfungen der Eingabedaten vorgenommen, könnte das Eintreffen nicht standardkonformer Daten unter Umständen in einer Absturz resultieren und sich durch Angreifer mittels entsprechend präparierter Verkehrsmeldungs-Nachrichten

[5] Auch die C2X-Kommunikation wird mit IEEE 802.11p auf einem Standard der 802.11-Protokollfamilie aufbauen, dem heute bereits die WLAN-Netze der Desktop-IT zugrunde liegen

potenziell auch zum Einschleusen beliebigen Schadcodes ausnutzen lassen.

Die begrenzte Heterogenität automotiver IT kann die Tragweite derartiger Angriffe zusätzlich begünstigen. Wenige große Automobilhersteller produzieren einen Großteil der im Verkehr vorkommenden Fahrzeuge und beziehen die verbauten Steuergeräte über einen begrenzten Kreis von (teils gemeinsamen) Zulieferern. Daher könnte eine bei der Analyse der OBU eines einzelnen Fahrzeugs entdeckte Sicherheitslücke in ungünstigen Fällen in identischer Form nicht nur in weiteren Fahrzeugen dieses Modells, sondern ggf. auch in anderen Modellen desselben Herstellers oder möglicherweise sogar in Fahrzeugen anderer Hersteller mit demselben Zulieferer enthalten und ausnutzbar sein. Umgekehrt können OBUs einzelner Hersteller natürlich auch besonders gründlich entwickelt oder durch zusätzliche Sicherheitsmechanismen geschützt sein und daher mangels bekannter Schwachstellen als potenzielles Ziel des Angreifers ausscheiden. Ein generelle Herausforderung bei der Absicherung von elektronischen IT-Systemen im Automobil sind z. B. Schnittstellen zur Aktualisierung von Soft- oder Hardwarekomponenten. In Kapitel 3 wurde diesbezüglich z. B. bereits die Prüfung von Flash-Updates auf Integrität und Authentizität erwähnt, die in der Quelle HIS, 2009 spezifiziert wurde. Auch die Alterung von Algorithmen, die zum Schutz eingesetzt werden, kann insbesondere bei langlebigen Produkten wie im Automobilbereich ein Problem darstellen. Beispielsweise kann dies eintreten, wenn durch Fortschritte in der Kryptanalyse Verfahren gefunden werden, mit denen zuvor nicht bekannte oder als zu aufwändig angenommene Angriffe auf eingesetzte kryptografische Verfahren möglich werden.

Parallel zu den in der Quelle HU, 2008 betrachteten Schutzstufen (die sich dort in der Sicherheit der Funkverschlüsselung und der Sicherheit des für die Administrator-Schnittstelle verwendeten Passworts widerspiegeln) werden in dem angepassten C2C-Szenario verschiedene Schutzstufen in Form unterschiedlicher Anfälligkeit der verschiedenen OBUs für die Ausnutzung von Sicherheitslücken zugewiesen. In dieser Adaption werden dadurch unterschiedlich sichere Implementierungen (individuelle Umsetzungen der relevanten C2C-Standards durch die Hersteller/Zulieferer) konkrete OBUs unterschiedlicher Hersteller/Zulieferer berücksichtigt, die in der Vielzahl der am Straßenverkehr teilnehmenden Fahrzeuge verbaut sind. Äquivalent zu heutigen Sicherheitslücken im PC-Bereich könnten in einer OBU von Hersteller A Sicherheitslücken existieren, die ein automotiver C2C-Wurm schnell ausnutzen kann, wogegen in OBUs von Hersteller B lediglich schwieriger auszunutzende (und damit zur Überwindung mehr Zeit erfordernde) oder gar keine Lücken bestehen.

Die eigentliche Simulation wurde anschließend mit der Verkehrsflusssimulationssoftware TRANSIMS Open-Source durchgeführt (siehe TRANSIMS, 2009), die dafür um die benötigten Berechnungen des Angriffsszenarios im C2C-Umfeld erweitert wurde. Dies beinhaltet insbesondere die Programmlogik zur dynamischen Berechnung der Übertragung der hypothetischen Epidemie, zu der während der Simulation folgende Voraussetzungen überprüft werden:

- In Funk-Reichweite des betrachteten nicht infizierten Fahrzeugs befindet sich aktuell zumindest ein weiteres infiziertes Fahrzeug.

- Falls das betrachtete Fahrzeug die niedrigste Schutzstufe besitzt (d. h. eine bekannte und sofort ausnutzbare Sicherheitslücke bekannt ist), wird die Infektion in jedem Fall übertragen. Besitzt das Fahrzeug die höchste Schutzstufe (d. h., es besitzt keine C2C-OBU oder die eines Typs, in dessen Implementierung keine Sicherheitslücke bekannt ist), bleibt es uninfiziert. Besitzt das Fahrzeug die mittlere Infektionsstufe (dies bedeutet, es sind Sicherheitslücken bekannt, die sich jedoch nur bedingt ausnutzen lassen), wird die Infektion nur bedingt (hier: bei einer von 1.000 Begegnungen mit infizierten Fahrzeugen) übertragen.

Im Rahmen der in BIERMANN, 2009 untersuchten praktischen Simulationen wurde das für C2C angepasste Angriffszenario in mehreren Szenarien untersucht. Folgendes Szenario betrachtet die Entwicklung der absoluten Infektionszahlen über den Simulationstag hinweg unter der Annahme, dass während der Einführungsphase von C2C-Technologie erst ca. 30 % der Fahrzeuge eine eigene OBU aufweisen. Neben den 70 % der Fahrzeuge ohne OBU werden weitere 15 % der Fahrzeuge als nicht infizierbar angenommen, in deren OBU keine ausnutzbare Sicherheitslücke bekannt ist. Für 10 % der Fahrzeuge wird als bekannt vorausgesetzt, dass deren OBUs sofort ausnutzbare Sicherheitslücken enthalten, während die OBUs von 5 % der Fahrzeuge Sicherheitslücken aufweisen, die nur bedingt

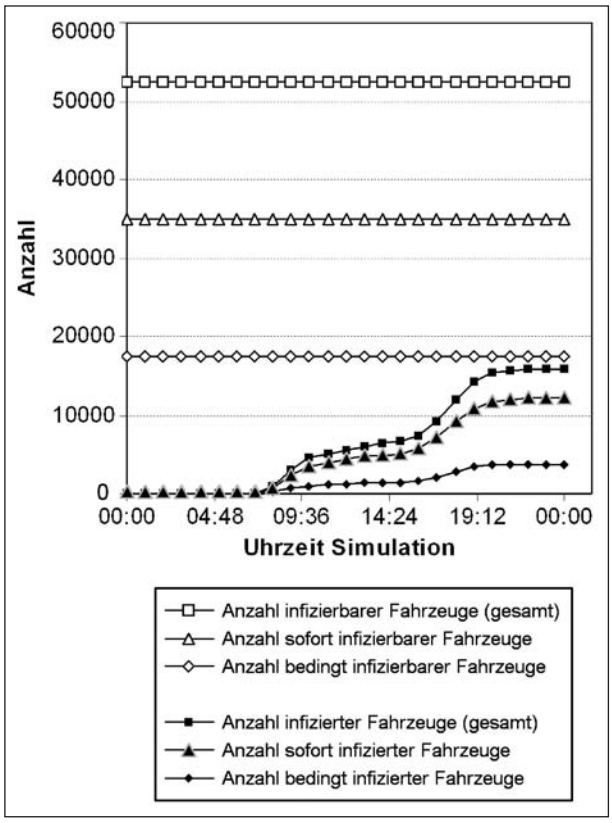


Bild 13: Ausbreitung unter insgesamt ca. 349.000 Fahrzeugen im Testset Alexandria (aus: BIERMANN, 2009)

ausgenutzt werden können (s. o.). Die Epidemie beginnt morgens um 7 Uhr, d. h. während der morgendlichen Rush-Hour, mit der ersten (initialen) Infektion.

Bild 13 veranschaulicht für eine Simulation, in der der Verkehrsfluss einer Stadt mit insgesamt knapp 350.000 beteiligten Fahrzeugen berechnet wird, die erfassten Zahlen zur Ausbreitung der Infektion unter den ca. 52.000 Fahrzeugen mit prinzipiell infizierbaren OBUs.

Auch trotz der vergleichsweise moderaten Annahmen (erst 30 % der Fahrzeuge besitzen eine C2X-OBU, s. o.) zeigt Bild 13 deutlich, dass sich die Infektion gerade zu den Zeiten des Berufsverkehrs verstärkt ausbreitet. Wie weitere im Kontext von BIERMANN, 2009 durchgeführte Simulationsdurchläufe zeigten, liegt gerade mit Blick auf den Zeitpunkt der initialen Infektion eine erhebliche Abhängigkeit von der Tageszeit vor: Das Setzen der initialen Infektion eines Fahrzeugs führt zu Beginn des Simulationstages (0 Uhr) häufig zu keinen oder nur vereinzelten weiteren Infektionen am Simulationstag. Die wenigen früh morgens startenden Fahrzeuge begegnen sich nur selten und sind nach Erreichen ihres Ziels im Simulationszeitraum teils nicht erneut unterwegs. Erfolgt die initiale Infektion dagegen bei höherer Verkehrsdichte, breitet sie sich noch am Simulationstag unaufhaltsam aus.

Bild 14 veranschaulicht grafisch die Ausbreitung einer Infektion, die in STENGEL, 2009 in einer erweiterten Implementierung und in einem ähnlichen Test-Setup ermittelt wurden:

- Graue Punkte: stehen für die Positionen prinzipiell infizierbarer Fahrzeuge, die noch nicht infiziert sind.
- Schwarze Punkte: bezeichnen die Positionen bereits infizierter Fahrzeuge.
- Die Positionen von Fahrzeugen, die nicht infizierbar sind (da sie entweder noch keine eigene C2X-OBU enthalten oder in dieser noch keine Sicherheitslücke bekannt ist, über welche die Infektion auf sie übergreifen könnte), sind als hellgraue, kleinere Punkte dargestellt, die sich aufgrund der Schwarzweißdarstellung in dieser Abbildung nicht deutlich aus dem Straßennetz hervorheben.

Wie die Tests zeigen, würde eine solche hypothetische Epidemie im C2C-Umfeld im Vergleich zu HU, 2008 (statische WLAN-Strukturen) in ihrer Ausbreitungsgeschwindigkeit deutlich durch die Mobilität der Fahrzeuge begünstigt, wodurch die Reichweite der erreichbaren Opfer erheblich zunimmt. Zusätzlich zur Ausbreitungsfunktion könnte der Angreifer die infizierten OBUs zu Denial-of-Service-(DoS-)Angriffen anweisen. Diese können sich einerseits gegen die infizierten Fahrzeuge selbst richten (bzw. einzelne ihrer internen vernetzten Komponenten). Da die Zahl der Infektionen am Ende des ersten Simulationstages bereits ca. 15 % der Fahrzeuge mit OBU erreicht (ca. 30 % der infizierbaren Fahrzeuge), könnten die infizierten OBUs andererseits durch unsachgemäßes Verhalten in den C2C-Netzen auch weitere Fahrzeuge (u. a. auch nicht anfällige) beeinflussen. Dazu könnten sie z. B. Multi Hop Connections unterbrechen oder die begrenzte Bandbreite durch Flooding unnötig belegen und so einen lokalen Ausfall der legitimen C2C-Kommunikation bewirken. In beiden Fällen könnten DoS-Attacken neben Komforteinbußen auch Auswirkungen auf den Verkehrsfluss sowie die Verkehrssicherheit haben, indem z. B. plötzliche Behinderungen durch Liegenbleiben von Fahrzeugen entstehen oder solche nicht mehr automatisiert kommuniziert werden können. Folglich begrenzen sich die Auswirkungen des betrachteten Angriffs im

Bild 14: Ausbreitung der Infektion (Testset Alexandria). Oben links: unmittelbar nach der initialen Infektion; oben rechts: Ausbreitung der Infektion nach 4 Minuten; unten links: Ausbreitung der Infektion nach weiteren 12 Minuten; unten rechts: Ausbreitung der Infektion nach weiteren 11 Minuten (nach STENGEL, 2009)

automotiven Umfeld nicht nur auf die infizierten Fahrzeuge selbst.

6.3 Diskussion im Kontext zukünftiger Fahrerassistenzsysteme

Da insbesondere auch zukünftige Fahrerassistenzsysteme (FAS) eine Anbindung an entsprechende C2X-Infrastrukturen voraussichtlich nutzen werden und vielfach gleichzeitig zulässige Eingriffe in die Fahrfunktionen vornehmen können, könnten angesichts potenzieller Sicherheitslücken dieser Drahtlosanbindungen auch weitere sicherheitskritische Folgen entstehen. Fahrerassistenzsysteme – auch in aktuellen Ausführungen wie teils zuvor vorgestellt – sollen den Fahrer in schwierigen Fahrsituationen unterstützen. Potenzielle Motivationen bezüglich dieser Systeme lassen sich bereits heute vermuten, auch wenn im Rahmen der Recherchen (z. B. in Kapitel 2.1) nur ansatzweise bereits bestehende Motivationen hierzu gefunden werden konnten. Häufig stellt aber bereits das temporäre Deaktivieren einzelner Funktionen (vgl. Fahrdynamikregelsysteme/Kapitel 2.1.1) oder Ändern gewisser existierender Betriebsparameter (z. B. Mindestabstand beim ACC, vgl. ebenfalls Kapitel 2.1.1) oder der Art ihrer Interaktion (vgl. Warnmeldungen in Kapitel 2.1.1) nachweisbare Motivationen dar. Auch bezüglich neuerer und zukünftiger FAS-Funktionen sind potenzielle Aspekte denkbar, die der Fahrer als Bevormundung ansieht und deaktivieren oder weniger restriktiv (oder im Gegenteil restriktiver) gestalten will. Aber angesichts der gerade durch die Drahtlosanbindung relevanter werdenden externen Akteure sind weitere Motivationen denkbar, die im schlimmsten Fall potenzielle Schäden der Insassen und des Straßenverkehrs in Kauf nehmen oder gar beabsichtigen.

7 Einschätzung der Ergebnisse

In den in Kapitel 2.1 dokumentierten Rechercheergebnissen wurden Eingriffe in 24 verschiedene Zielkomponenten (zuzüglich verschiedener Teilfunktionen) ermittelt, die 8 generellen Komponentenklassen zugeordnet werden konnten. Hierdurch ist eine erste Übersicht über aktuell verfolgte Ziele elektronischer Veränderungen von Fahrzeug- und

Infrastruktursystemen aufgezeigt worden, die auch potenzielle Tendenzen andeutet.

Die vier Teilergebnistabellen (Tabelle 5, Tabelle 7, Tabelle 8 und Tabelle 17) bilden zusammengefügt eine Gesamtergebnistabelle. Gemeinsam liefern sie so die Gesamtübersicht der vorgenommenen Abschätzungen über die Bedrohungslage, die ausgenutzen Schwachstellen, das Risiko des Auftretens der jeweiligen elektronischen Veränderung und potenziell resultierender Gefahren.

Nach den erfolgten Recherchen insbesondere auch in neuen Medien wie dem Internet kann folgendes erstes Fazit bezüglich des Bedrohungspotenzials elektronischer Veränderungen an Fahrzeug- und Infrastruktursystemen getroffen werden: In den zusammengetragenen öffentlichen Quellen ist eine Vielzahl von Hinweisen auf entsprechende Aktivitäten vorhanden. Der überwiegende Teil der Rechercheergebnisse bezieht sich dabei auf Veränderungen, die in der Adressierung eines (subjektiv angenommenen) verbesserungswürdigen Zustandes des eigenen Fahrzeugs begründet liegen. Das heißt, dass die entsprechend agierenden Personengruppen in der überwiegenden Zahl der Fälle berechtigte Nutzer (meist Besitzer) der Fahrzeuge sind und zum persönlichen Vorteil zu handeln glauben. Tendenziell konzentrieren sich solche Fälle auf Fahrzeuge der Kompakt- und Mittelklasse. Hinweise für entsprechende Bestrebungen zu Veränderungen an Fahrzeugen der Oberklasse gab es nur sehr vereinzelt, wahrscheinlich da die Kosten bei dieser Käuferklientel nur eine untergeordnete Rolle spielen und z. B. eine hohe Motorleistung oder weitere angestrebte Funktionen bereits von vornherein mit erworben werden. Ursachen für Motivationen zur Veränderung, die käufergruppenübergreifend sind, können jedoch auch zu Veränderungen an Fahrzeugen der Oberklasse auslösend sein. Dies zeigte beispielsweise der in Kapitel 5.2.1 (Teilabschnitt Video-System) berichtete Fall, bei dem eine Veränderung zur Aufhebung der TV-Beschränkungen an einem Oberklassefahrzeug zu erheblichen Nebenwirkungen führte.

Dass elektronische Manipulationen potenziell auch zu ernsthaften Gefährdungen für die Straßenverkehrssicherheit führen können, wurde in mehreren recherchierten akademischen Quellen festgestellt und durch die Forscher bereits mehrfach in Praxisversuchen nachgewiesen. Wie in dem gegen Ende des vorangegangenen Absatzes referenzierten Beispiel konnten auch in mehreren nicht-akademischen Quellen Hinweise auf potenzielle Nebenwirkungen gefunden werden, die auch und insbesondere die Verkehrssicherheit gefährden könnten. In vielen Quellen werden diese bewusst vor dem Hintergrund der Warnung und Mahnung genannt, sodass anzunehmen ist, dass sich zumindest ein Teil der Personen potenzieller Gefährdungen und der Verantwortung für das eigene Fahrzeug und den Straßenverkehr offensichtlich bewusst ist. Als Fazit zu praktischen Gefährdungen, die sich aus derartigen Nebenwirkungen für den Straßenverkehr ergeben können, werden in Kapitel 7.1 wesentliche ausgewählte Beispiele aus den Rechercheergebnissen noch einmal zusammenfassend diskutiert.

7.1 Fazit zum Gefährdungspotenzial: Subsumierung ausgewählter potenzieller Gefahren mit besonderer Relevanz für den Straßenverkehr

Aus der in Kapitel 5.3 vorgenommenen Abschätzung von Gefahren sollen an dieser Stelle einige ausgewählte Einträge abschließend als besonders relevante Beispiele genannt werden. Im Fokus stehen hier insbesondere potenzielle Gefahren für die Straßenverkehrssicherheit. Dazu wurden diejenigen Beispiele ausgewählt, bei denen entsprechende Folgen praktisch beobachtbarer Veränderungen hinreichend belastbar als realistische Gefahren resultieren können. Die zugehörigen Auszüge aus der Ergebnistabelle aus Kapitel 5.3 werden hier in einer abschließenden Diskussion mit dem besonderen Fokus auf potenzielle Gefahren für die Straßenverkehrssicherheit behandelt.

7.1.1 Exemplarische Gefahren nach Veränderungen zur Leistungssteigerung

Nach unsachgemäß vorgenommenen Eingriffen zur Leistungssteigerung (Tabelle 20) können sich ebenfalls Gefahrenwirkungen (vgl. Tabelle 14) ergeben. Für das veränderte Fahrzeug ist ein höherer Verschleiß der Motorteile sehr wahrscheinlich, für andere Verkehrsteilnehmer stellt ein „Pannenfahrzeug“ ebenfalls eine Gefahr dar. Einige konkrete Beispiele sollen diese Aussage illustrieren:

- Zylinderkopfdichtungsschaden: Wird beispielsweise der Ladedruck des Turboladers erhöht, versagt die Zylinderkopfdichtung durch den zu hohen Druck im Brennraum bei der Verdichtung

des Kraftstoff-Luftgemisches. Die Folge ist austretendes Motorenöl in die Umwelt – eventuell auf die Straße – oder in den Kühlwasserkreislauf. Bei ungenügender Schmierung des Motors kann dies zum kompletten Ausfall führen. Daraus resultiert neben dem klassischen „Liegenbleiben“ des Fahrzeuges der Ausfall von Komponenten, die vom laufenden Motor abhängig sind, wie z. B. der Bremskraftverstärker. Ohne Bremskraftverstärker verlängert sich der Bremsweg enorm und dies wiederum gefährdet sowohl Insassen als auch andere Verkehrsteilnehmer.

- Antriebswellenschaden: Alle Bauteile eines Fahrzeuges sind aufeinander abgestimmt. Erhöht man die Motorleistung über den Tolleranzbereich der verbunden Bauteile, können Schäden an diesen Bauteilen hervorgerufen werden. Eine Antriebswelle überträgt die Kraft vom Getriebe an die angetriebenen Räder. Ist die Kraftwirkung zu hoch, nehmen die Lager der Antriebswelle Schaden. Die Folge ist eine unzureichende Passung der Lager bis hin zum Abreißen der Antriebswellenlager. Passiert dies einseitig, werden die Räder des Fahrzeuges auf der intakten Seite weiter angetrieben und die Gefahr des Ausbrechens des Fahrzeuges ist hoch.
- Kupplungs- und Getriebeschaden: Wie im Beispiel der Antriebswelle unterliegen auch Kupplung und Getriebe durch einen stark leistungsgesteigerten Motor einem erhöhten Verschleiß. Im Falle der Kupplung kann evtl. nicht mehr die gesamte Kraft des Motors an das Getriebe übertragen werden und sie „rutscht durch“. Das erhöht sehr stark den Abrieb der Kupplungsbeläge (frühzeitiges Altern) oder die Oberfläche der Beläge „verglast“ durch die hohen Temperaturen, die beim Rutschen entstehen (keine Haftreibung mehr). Die letztliche Konsequenz ist, dass das Fahrzeug liegen bleibt und die Kupplung erneuert werden muss. Im Getriebe kann es z. B. zu Zahnrad- oder Lagerschäden führen. Im besten Fall ist das Getriebe defekt, im schlimmsten Fall blockiert es die Antriebsräder – was einer unerwarteten Vollbremsung gleichkommt. Dadurch wird vor allem der nachfolgende Verkehr stark gefährdet.

7.1.2 Exemplarische Gefahren nach Veränderungen an der Servolenkung

Die Lenkfähigkeit eines Fahrzeuges ist eine primäre und Safety-relevante Funktion. An eine adaptive, elektrisch unterstützte Lenkeinrichtung stellen die Fahrzeugbenutzer die Erwartung, dass ein der Fahrgeschwindigkeit angemessenes unterstützendes Lenkmoment dem Fahrer beim Lenken hilft. Potenzielle Gefährdungen durch elektronische Veränderungen an der Servolenkung (vgl. Tabelle 21) können daher kritische Auswirkungen haben. In einem nicht angemessenen Zustand könnte die Servounterstützung im Fall geringer Geschwindigkeiten (bspw. beim Ausparken) nicht angemessen (typischerweise zu schwergängig) erfolgen. Ungleich kritischer jedoch ist eine zu leichtgängige

			Potenzielle Gefahren (Funktions- und Strukturwirkungen)	
Art der Komponente (Teilfunktion)		Potenzielle Motivation für die Veränderung	bzgl. der veränderten Komponente bzw. Teilfunktion	bzgl. weiterer Komponenten bzw. Teilfunktionen
Motor und Antriebsstrang	Motorsteuerung	Leistungssteigerung	Erhöhter Verschleiß, Motorschaden	Ausfälle weiterer Komponenten wie Bremskraftverstärker, Servolenkung; Regresse (Versicherung, Steuer), rechtlich (ABE, Schadstoffgrenzwerte), Unfälle durch Selbstüberschätzung des Fahrers

Tab. 20: Exemplarische Gefahren nach Veränderungen zur Leistungssteigerung

			Potenzielle Gefahren (Funktions- und Strukturwirkungen)	
Art der Komponente (Teilfunktion)		Potenzielle Motivation für die Veränderung	bzgl. der veränderten Komponente bzw. Teilfunktion	bzgl. weiterer Komponenten bzw. Teilfunktionen
Fahrwerksysteme	Servolenkung	Härtere Einstellung	-	Ggf. Kontrollverlust über das Fahrzeug, Verkehrsgefährdung

Tab. 21: Exemplarische Gefahren nach Veränderungen an der Servolenkung

Lenkung durch zu starke Lenkmomentunterstützung bei hohen Geschwindigkeiten. Veränderungen u. a. an der Adaptivität beeinträchtigen hochwahrscheinlich die veränderte Komponente nicht. Jedoch kann ein Verreißen der Lenkung mit schwerwiegenden Folgen für das eigene Fahrzeug und andere Verkehrsteilnehmer auftreten.

7.1.3 Exemplarische Gefahren nach Veränderungen zum elektronischen Tieferlegen

Beim elektronischen Tieferlegen (vgl. Tabelle 22) resultiert die konkrete Gefahr aus dem Unterschreiten der Toleranzgrenze für die Bodenfreiheit eines Fahrzeuges. Alle öffentlichen Straßen sind auf dieses Maß mit den Fahrzeugherstellern abgestimmt. Unterschreitet ein Fahrzeug dieses Bodenfreiheitsmaß, kann es bei Unebenheiten (z. B. Wellen in der Fahrbahn – wie bei den so genannten „Bremshügeln“) zum Abriss von – am Unterboden befestigten – Fahrzeugteilen kommen. Dazu zählen exemplarisch: Auspuffanlage, Kraftstoff- und Bremsleitungen, Teile der Schaltung (zum Getriebe) oder die Motorölwanne. Abgesehen vom Schaden am eigenen Fahrzeug stellen diese Teile eine Gefahr für nachfolgende Fahrzeuge dar.

Darüber hinaus ist ein frühzeitiges Altern der Stoßdämpfer des Fahrzeuges wahrscheinlich, wenn diese nicht dem geänderten Federweg (durch das „Tieferlegen“) angepasst werden. Eine unzureichende Dämpfung wiederum verringert den Kontakt der Räder zur Fahrbahn und das Fahrzeug wird instabil, vor allem bei starken Lenkmanövern wie einem Ausweichvorgang.

7.1.4 Exemplarische Gefahren nach Veränderungen am Airbagsystem

Veränderungen an elektronischen Systemen zur passiven Sicherheit (u. a. Airbags und pyrotechnische Gurtstraffer, vgl. Tabelle 23) sollten durch die Eigenüberwachungsfunktion den Fahrer über erkannte Mängel informieren. Werden jedoch Sensoren und Aktoren dieses Systems bewusst derart verändert, dass die Eigenüberwachung getäuscht wird (z. B. um einen Komponentendefekt zum Bestehen der Hauptuntersuchung oder als Verkaufsargument zu vertuschen), so kann ein teilweiser oder vollständiger Ausfall der elektronisch gesteuerten Systeme zur passiven Sicherheit die Folge sein. Neben den Folgen für die betroffe Komponente hat das im Falle eines Unfalls auch schwere Folgen für Leib und Leben für die Insassen eines Fahrzeugs, da dieses in seinem Unfallverhalten nur für funktionierende derartige Systeme ausgelegt ist.

7.1.5 Exemplarische Gefahren nach Veränderungen am Wegstreckenzähler

Die zurückgelegte Gesamtwegstrecke ist ein wichtiges Datum für viele elektronische Systeme innerhalb eines Kraftfahrzeugs. Insbesondere im Verkaufsfall ist es zudem ein wichtiger wertbestimmender Faktor. Aus diesem Grund werden Zähler der Gesamtwegstrecke verändert, um eine niedrigere Gesamtfahrleistung vorzutäuschen (vgl. Tabelle 24). Dies kann auf unterschiedlichen Wegen erfolgen, z. B. über die Veränderung des Radumfangs, welches u. a. auch eine niedrigere angezeigte Geschwindigkeit und ggf. auch damit eine unzuverlässige Navigation zur Folge haben kann, wenn (typischerweise festinstallierte) Navigationssysteme diesen Wert in die Routenberechnung einbeziehen. Da die Geschwindigkeit auch ein wichtiger Faktor für das Schaltverhalten einer automatischen Getriebesteuerung ist, können sich auch Folgen ergeben. Durch die beschriebene Veränderung oder auch durch direktes Überschreiben des Wertes für die Gesamtwegstrecke mit geeigneter Hard- und Softwareausstattung wird ebenfalls eine ggf. im Fahrzeug befindliche Serviceintervallanzeige beeinflusst und damit eine ggf. notwendige Wartung Safety-relevanter Komponenten (u. a. im Lenkungs- und Bremssystem) nicht rechtzeitig durchgeführt, was sowohl den Fahrer des betroffenen Fahrzeugs als auch andere Verkehrsteilnehmer gefährden kann.

7.1.6 Exemplarische Gefahren nach Veränderungen zur Warnung vor Geschwindigkeitsmesseinrichtungen

Wie in Kapitel 5.2.1 beschrieben und auch anhand von Praxistests in einer Recherchequelle belegt wurde, kann der Straßenverkehr beim Einsatz von technischen Maßnahmen zur Warnung vor Geschwindigkeitsmesseinrichtungen (vgl. Tabelle 25) gefährdet werden. Abrupte eingeleitete Bremsmanöver, die für den nachfolgenden Verkehr oft nicht voraussehbar sind, können das Auftreten von Auffahrunfällen potenziell begünstigen. Prinzipiell ist es dabei unerheblich, welcher Art das eingesetzte Gerät ist. Neben Geräten zur Detektion der Messeinrichtungen (vgl. Kapitel 2.1.2/Geschwindigkeitsmesseinrichtungen) kann auch der Einsatz von POI-Erweiterungen mit entsprechenden Standorten stationärer und zunehmend auch mobiler Messeinrichtungen (vgl. Kapitel 2.1.1/Navigationssystem) diese

			Potenzielle Gefahren (Funktions- und Strukturwirkungen)	
Art der Komponente (Teilfunktion)		Potenzielle Motivation für die Veränderung	bzgl. der veränderten Komponente bzw. Teilfunktion	bzgl. weiterer Komponenten bzw. Teilfunktionen
Fahrwerksysteme	Adaptive Niveauregelung	Elektronisches Tieferlegen	Dämpferschäden	Beschädigungen am Unterboden und befestigten Teilen bei Bodenwellen durch zu tief konfigurierte Fahrzeuglage

Tab. 22: Exemplarische Gefahren nach Veränderungen zum elektronischen Tieferlegen

			Potenzielle Gefahren (Funktions- und Strukturwirkungen)	
Art der Komponente (Teilfunktion)		Potenzielle Motivation für die Veränderung	bzgl. der veränderten Komponente bzw. Teilfunktion	bzgl. weiterer Komponenten bzw. Teilfunktionen
Passive Sicherheit	Airbagsystem/ Gurtstraffer	Verbergen der Nichtfunktionalität	Nichtfunktionalität bzw. eingeschränkte Funktion	Unkenntnis über Missstand bei Käufern. Schwerere Verletzungen bei Unfällen

Tab. 23: Exemplarische Gefahren nach Veränderungen am Airbagsystem

			Potenzielle Gefahren (Funktions- und Strukturwirkungen)	
Art der Komponente (Teilfunktion)		Potenzielle Motivation für die Veränderung	bzgl. der veränderten Komponente bzw. Teilfunktion	bzgl. weiterer Komponenten bzw. Teilfunktionen
Infotainment	Instrumentenkombination (Wegstreckenzähler)	Kilometerstand ändern	Falsch angezeigte Geschwindigkeit (bei k-Zahl Änderung)	Erhöhter Verschleiß durch Wartungsversäumnisse. Bei k-Zahl-Änderung: Unfälle durch unbewusst falsche Geschwindigkeitsanzeige. Falsches Schalterverhalten bei elektronischen Getriebesteuerungen
	Instrumentenkombination (Service-Intervallanzeige)	Zurücksetzen	Fehlender Hinweis auf notwendige Wartungsarbeiten	Erhöhter Verschleiß bis hin zu Schäden an wartungsbedürftigen Komponenten (z. B. Motor), Garantieverlust

Tab. 24: Exemplarische Gefahren nach Veränderungen am Wegstreckenzähler (Kilometerstand)

			Potenzielle Gefahren (Funktions- und Strukturwirkungen)	
Art der Komponente (Teilfunktion)		Potenzielle Motivation für die Veränderung	bzgl. der veränderten Komponente bzw. Teilfunktion	bzgl. weiterer Komponenten bzw. Teilfunktionen
Infotainment	Navigationssystem	Installieren von POI („Blitzer"-Positionen etc.)	-	Fahrer bremst abrupt, ggf. Verkehrsbeeinflussung
Infrastruktur-komponenten	Geschwindigkeits-messeinrichtungen	Warnung vor Messungen	-	Fahrer bremst abrupt, ggf. Verkehrsbeeinflussung

Tab. 25: Exemplarische Gefahren nach Veränderungen zur Warnung vor Geschwindigkeitsmesseinrichtungen

Art potenzieller Gefahren für den Straßenverkehr mit sich bringen.

7.1.7 Exemplarische Gefahren nach Veränderungen für TV/Video in Motion

Konkrete Gefahren nach Veränderungen für Video-in-Motion, also das Fern- oder Videosehen während der Fahrt (vgl. Tabelle 26), können sich aus der Ablenkung des Fahrers ergeben. Fahren ist primär eine visuelle Nachführaufgabe mit dem Ziel, das Fahrzeug in definierten Grenzen (meist Fahrbahnränder oder Markierungen) so zu bewegen, dass Kollisionen mit anderen Verkehrsteilnehmern und anderen Hindernissen vermieden werden. Schaut der Fahrer auf ein Display (Video), kann er nicht gleichzeitig die Umgebung visuell wahrnehmen. Es wächst die Wahrscheinlichkeit, dass er die

			Potenzielle Gefahren (Funktions- und Strukturwirkungen)	
Art der Komponente (Teilfunktion)		Potenzielle Motivation für die Veränderung	bzgl. der veränderten Komponente bzw. Teilfunktion	bzgl. weiterer Komponenten bzw. Teilfunktionen
Infotainment	Video-System	TV In Motion	-	Ablenkung bei der Nutzung des Systems durch den Fahrer. Durch Signalveränderungen: Wegfall Lautstärkeanpassung, ungenaue Navigation, unangemessene adaptive Lenkung, Einrasten Lenkradschloss während der Fahrt

Tab. 26: Exemplarische Gefahren nach Veränderungen für TV/Video in Motion

			Potenzielle Gefahren (Funktions- und Strukturwirkungen)	
Art der Komponente (Teilfunktion)		Potenzielle Motivation für die Veränderung	bzgl. der veränderten Komponente bzw. Teilfunktion	bzgl. weiterer Komponenten bzw. Teilfunktionen
Karosserie	Lichtanlage (Frontscheinwerfer)	Nachrüsten Xenon-Licht	-	Blendung des Gegenverkehrs bei fehlender/nicht angemessener Leuchtweitenregulierung

Tab. 27: Exemplarische Gefahren nach unsachgemäßer Nachrüstung von Xenon-Scheinwerfern

Grenzen der Fahrbahn verlässt oder mit anderen Fahrzeugen, Personen oder Gegenständen kollidiert, weil er diese visuell nicht wahrgenommen hat. Tatsächlich stellt die Ablenkung, bzw. Unaufmerksamkeit mit 86 % aller tödlichen Verkehrsunfälle eine der häufigsten Unfallursachen dar (vgl. KUHN, 2005).

7.1.8 Exemplarische Gefahren nach unsachgemäßer Nachrüstung von Xenon-Scheinwerfern

Der nachträgliche Einbau von so genannten Xenon-Scheinwerfern (vgl. Tabelle 27) stellt insofern keine Gefährdung dar, wenn er sachgemäß vorgenommen wird. Dies schließt eine adaptive Leuchtweitenregulierung (Adaptive-Frontlightning-System – AFS) unbedingt ein und diese ist vom Gesetzgeber vorgeschrieben. Da Fahrzeuge, welche ab Werk ohne Xenon-Scheinwerfer ausgeliefert werden, dieses AFS nicht besitzen, muss es entsprechend nachgerüstet werden. Dazu wird der Verbau von Neigungssensoren – meist Federwegsensoren – notwendig, sowie eine entsprechende elektronische Regelung. Diese Regelung korrigiert die Höheneinstellung bzw. Leuchtweite der Scheinwerfer in Abhängigkeit der Neigung (z. B. durch Beladung) automatisch. Problematisch wird der nachträgliche Verbau von Xenon-Scheinwerfern, wenn das AFS nicht mit eingebaut wird (z. B. aus Kostengründen) oder nicht korrekt funktioniert (z. B. aufgrund von Fehlern in der AFS-Steuergerätprogrammierung). Dies kann zu einer sehr starken Blendung des Gegenverkehrs führen, denn die Leuchtdichte von Xenon-Scheinwerfer ist wesentlich höher als die der Halogenscheinwerfer (H4, H7).

7.2 Fazit und Folgerungen für die Zukunft

Wie im vorigen Kapitel nochmals anhand ausgewählter Beispiele zusammengefasst wurde, können sich durch elektronische Veränderungen an Fahrzeug- und Infrastruktursystemen Gefährdungen ergeben, die sich im kritischsten Fall auf die Sicherheit des Straßenverkehrs auswirken können. Vielfacher Grund ist, dass ein großer Teil der vorgenommenen Veränderungen unsachgemäß erfolgt. Insbesondere bei elektronischen Veränderungen, die immer tiefer in automotive IT-Systeme eingreifen, können ungewollte Strukturwirkungen auftreten, die sich bis auf die Straßenverkehrssicherheit auswirken können. Eine häufige Ursache kann beispielsweise sein, dass den agierenden Personen aufgrund fehlender Informationen zu dem Gesamtsystem (z. B. technische Spezifikationen) das Verständnis über potenzielle Wechselwirkungen in den zunehmend komplexen automotiven Systemen fehlt.

Als positiver Aspekt kann insgesamt festgestellt werden, dass keine Hinweise auf das gezielte prak-

tische Betreiben Safety-kritischer Veränderungen recherchiert werden konnten, die explizit aus bösartigen/destruktiven Motivationen resultieren, z. B. um dritten Personen gezielt Schaden zuzufügen. Sämtliche hierzu recherchierten Quellen sowie darin beschriebene Praxisversuche sind rein akademischer Natur. Dies kann aber auch dadurch begründet sein, dass Personengruppen mit entsprechenden Hintergründen dies nicht in öffentlichen Quellen aussprechen. Es kann daher nicht ausgeschlossen werden, dass auch böswillig motivierte Veränderungen in der Praxis durch entsprechende Tätergruppen betrieben werden.

Insgesamt zeichnet sich jedoch als beobachteter Trend eine Entwicklung zu technisch immer tiefer eingreifenden Veränderungen ab. Neben der Möglichkeit der weiteren Zunahme von Gefahren durch unbeabsichtigte Nebenwirkungen könnten sich zukünftig potenziell betriebene Veränderungen aber auch zunehmend für beabsichtigtes Herbeiführen von Gefährdungen einsetzen lassen. Insbesondere vor dem Hintergrund der aufkommenden modernen Technologien wie modernen Fahrerassistenzsystemen (siehe z. B. entsprechender Teil in Kapitel 2.1.1) und Car-to-X-Kommunikation (Kapitel 6) sollten entsprechende Fahrzeug- und Infrastruktursysteme daher zukünftig besonders kritisch unter dem Aspekt potenzieller Motivationen und Ansatzpunkte für elektronische Veränderungen reflektiert werden.

Um weitere Schritte abzuschätzen, wie diesem Trend in Zukunft begegnet werden kann, sollte der erarbeitete erste breite Überblick über die aktuelle Situation weiter konkretisiert werden.

Ein erster sinnvoller Schritt zu mehr Nachvollziehbarkeit hinsichtlich der Verbreitung praktisch betriebener Veränderungen wäre, bei den ohnehin betriebenen regelmäßigen Fahrzeuguntersuchungen gezielter nach den vermuteten Ursachen identifizierbarer Mängel zu unterscheiden. Insbesondere eine Unterscheidung nach unbeabsichtigten Ursachen (z. B. üblicher Verschleiß, zufälliges Komponentenversagen) und Mängeln aus vorsätzlich herbeigeführten Veränderungen sollte dabei mit mehr Nachdruck betrieben werden. Dadurch würde es möglich, den Anteil erkennbarer mängelbedingter Gefährdungen für die Straßenverkehrssicherheit konkreter zu benennen, der sich explizit aus Veränderungen ergibt.

Jedoch müssen viele unautorisierte Veränderungen (insbesondere wenn sie Hard- und Software elektronischer Regelsysteme betreffen) nicht zwangsläufig zu erkennbaren Mängeln führen und sind auch durch elektronische Untersuchungen, z. B. mit derzeitig eingesetzter Diagnosetechnik, nur schwierig nachzuweisen. Der Gesetzgeber, Fahrzeughersteller, Versicherungen und Flottenbetreiber haben ein gewichtiges Interesse, u. a. die zuvor beschriebenen Veränderungen zu verhindern bzw. nachweisen zu können. Zur Verhinderung von (unautorisierten) Veränderungen wird aktuell in verschiedenen Forschungsprojekten untersucht, wie automotive IT gegen unautorisierte Interaktionen wirksam abgesichert werden kann. Herausforderungen liegen hierbei in der Anpassung teils bereits bewährter Konzepte an die speziellen Anforderungen im Automobilbereich (z. B. geringe Ressourcen, hoher Kostendruck). Auch liegen die typischen Produktlebenszyklen von Automobilen (oft 10-20 Jahre) noch deutlich über denen kryptografischer Verfahren (teils deutlich unter 10 Jahre), die die Grundlage vieler in der Desktop-IT bewährter Schutzkonzepte bieten. Letzteres ist insbesondere den stetigen Fortschritten in der Kryptanalyse geschuldet. In der Konsequenz würde dies für die Fahrzeughersteller die Möglichkeit erforderlich machen, innerhalb des Lebenszyklus des Automobils inzwischen unsicher gewordene kryptografische Verfahren durch aktuelle ersetzen zu können. Die Herausforderung liegt hier beispielsweise darin, dass die Hardware von vornherein auf den Fall eines Updates der kryptografischen Verfahren ausgelegt sein müsste, z. B. um auch auf Verfahren mit unterschiedlichem Ressourcenbedarf wechseln zu können.

Ergänzend können daher auch Maßnahmen zum Nachweis von elektronischen Veränderungen sinnvoll sein. Dazu bietet sich auf technologischer Ebene in der automotiven Umgebung die Adaptierung bekannter geeigneter Verfahren aus der Desktop-IT an. Dazu zählen beispielsweise Verfahren zur Einbruchserkennung bzw. -verhinderung, engl. Intrusion Detection/Prevention System (vgl. HOPPE, 2009 sowie MÜTER, 2010) als auch Maßnahmen aus der IT-Forensik (vgl. KILTZ, 2009). Auch in diesen Fällen ist eine Adaption in der Desktop-IT bekannter und etablierter Techniken und Vorgehensweisen auf das automotive IT-Umfeld notwendig, da die dort eingesetzten elektronischen Regelsysteme typischerweise vergleichsweise ressourcenbeschränkt sind (u. a. Speicherkapazität und Rechenleistung) und sich vom Aufbau her als heterogene, verteilt arbeitende Systeme deutlich von gängiger Desktop-IT unterscheiden.

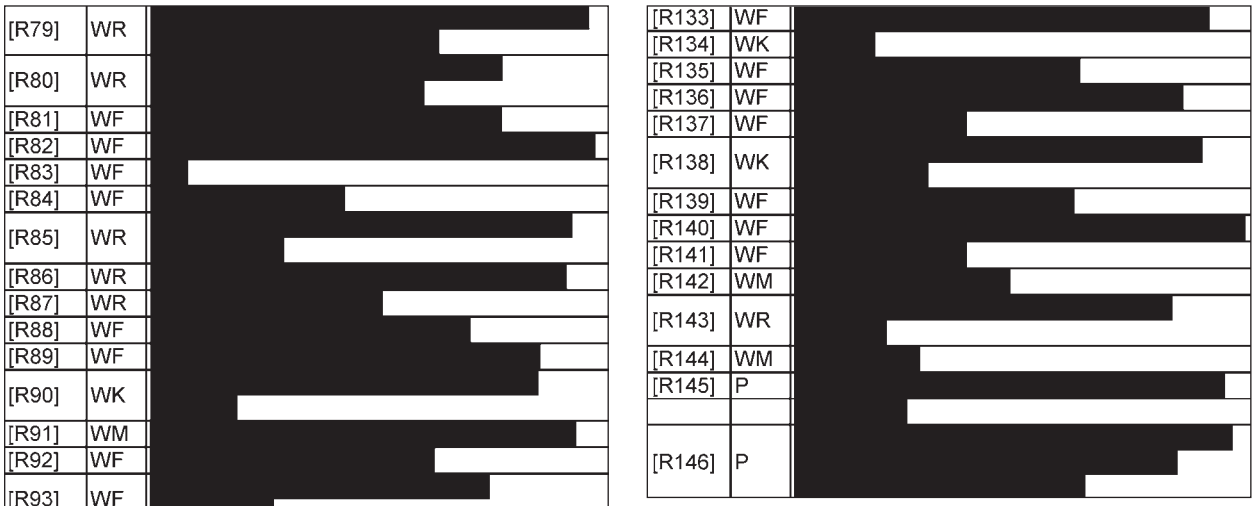
8 Kompaktübersicht Rechercheergebnisse

Aufgrund ihres Umfangs sind die Rechercheergebnisse selbst nicht als Teil dieses Dokumentes beigefügt. Sie können bei Interesse bei der Bundesanstalt für Straßenwesen (BASt) eingesehen werden.

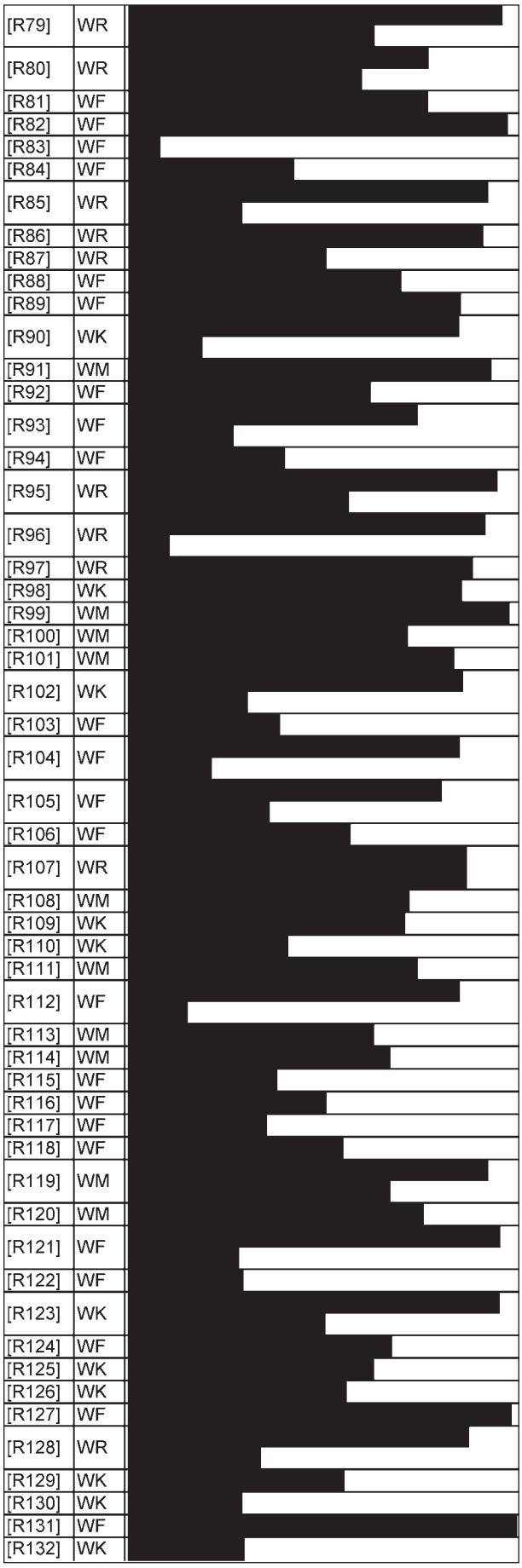
Die im Folgenden gelieferte tabellarische Aufstellung wurde aus Datenschutzgründen anonymisiert. Sie enthält daher keine vollwertigen Quellenverweise; für jede Recherchequelle ist ausschließlich ihr Titel (z. B. Überschrift, Webseiten-Titel etc.) angegeben. In Einzelfällen, in denen der jeweilige Quellentitel nicht mit der anonymisierten Zusammenstellung vereinbar war, sind stattdessen kurze textuelle Beschreibungen angegeben und durch Klammern und Kusivschreibung kenntlich gemacht.

Die enthaltenen Verweise sind dabei als exemplarisch zu betrachten. Da in vielen Fällen zu erwarten ist, dass sich ähnliche Belege an vielen weiteren Stellen finden, erhebt die Auflistung keinen Anspruch auf Vollständigkeit. Angesichts dessen wurde über die Nennung der Titel hinaus lediglich eine Zuordnung zu der Art der Recherchequelle vorgenommen (vgl. Tabelle 3). Dies erfolgt über die Angabe von Kategorie-Kürzeln für wissenschaftl. Veröffentlichungen (P), Medien-Berichte und Pressemitteilungen (WM), Diskussionsforenbeiträge (WF), kommerzielle Webseiten (WM) und restliche Web-Quellen (WR).

Ref.	Kat.	Fundstelle
[R01]	WK	
[R02]	WF	
[R03]	WF	
[R04]	WR	
[R05]	WM	
[R06]	WF	
[R07]	WM	
[R08]	WF	
[R09]	WF	
[R10]	WF	
[R11]	P	
[R12]	WF	
[R13]	WF	
[R14]	WF	
[R15]	WF	
[R16]	WF	
[R17]	WM	
[R18]	WF	
[R19]	WM	
[R20]	WR	
[R21]	WF	
[R22]	WK	
[R23]	WF	
[R24]	WF	
[R25]	WF	
[R26]	WF	
[R27]	WM	
[R28]	WK	
[R29]	WR	
[R30]	WR	
[R31]	WR	
[R32]	WR	
[R33]	WK	
[R34]	WK	
[R35]	WK	
[R36]	WF	
[R37]	WK	
[R38]	WM	
[R39]	WK	
[R40]	WF	
[R41]	WR	
[R42]	WF	
[R43]	WF	
[R44]	WR	
[R45]	WR	
[R46]	WK	
[R47]	WF	
[R48]	WR	
[R49]	WR	
[R50]	WM	
[R51]	WM	
[R52]	WM	
[R53]	WR	
[R54]	P	
[R55]	WR	
[R56]	WK	
[R57]	WK	
[R58]	WK	
[R59]	WK	
[R60]	WK	
[R61]	WF	
[R62]	WF	
[R63]	WF	
[R64]	WF	
[R65]	WF	
[R66]	WF	
[R67]	WF	
[R68]	WF	
[R69]	WK	
[R70]	WF	
[R71]	P	
[R72]	WM	
[R73]	WR	
[R74]	WK	
[R75]	WK	
[R76]	WF	
[R77]	WF	
[R78]	WK	



[R133]	WF
[R134]	WK
[R135]	WF
[R136]	WF
[R137]	WF
[R138]	WK
[R139]	WF
[R140]	WF
[R141]	WF
[R142]	WM
[R143]	WR
[R144]	WM
[R145]	P
[R146]	P



[R79]	WR
[R80]	WR
[R81]	WF
[R82]	WF
[R83]	WF
[R84]	WF
[R85]	WR
[R86]	WR
[R87]	WR
[R88]	WF
[R89]	WF
[R90]	WK
[R91]	WM
[R92]	WF
[R93]	WF
[R94]	WF
[R95]	WR
[R96]	WR
[R97]	WR
[R98]	WK
[R99]	WM
[R100]	WM
[R101]	WM
[R102]	WK
[R103]	WF
[R104]	WF
[R105]	WF
[R106]	WF
[R107]	WR
[R108]	WM
[R109]	WK
[R110]	WK
[R111]	WM
[R112]	WF
[R113]	WM
[R114]	WM
[R115]	WF
[R116]	WF
[R117]	WF
[R118]	WF
[R119]	WM
[R120]	WM
[R121]	WF
[R122]	WF
[R123]	WK
[R124]	WF
[R125]	WK
[R126]	WK
[R127]	WF
[R128]	WR
[R129]	WK
[R130]	WK
[R131]	WF
[R132]	WK

Literatur

AUGUST, R., WINKLER, S., DIEBLER, A.: Zukünftige Car-to-X-Kommunikation, Bericht zum Seminar „Sicherheit eingebetteter Systeme“ im Wintersemester 2009/2010, Okt./Nov. 2009, Universität Magdeburg

BIERMANN, M., HOPPE, T., DITTMANN, J., SCHULZE, S., SAAKE, G.: Adaption des Szenarios einer WiFi-Wurm-Epidemie auf den Automotive-Bereich zur Sensibilisierung und Aufklärung; in: Sichere Wege in der vernetzten Welt: Tagungsband zum 11. Deutschen IT-Sicherheitskongress; SecuMedia Verlag Ingelheim, ISBN 978-3-922746-97-3, 2009

BIßMEYER, N., STÜBING, H.: simTD Security Architecture: Deployment of a Security and Privacy Architecture in large scale Field Operational Tests. In: escar – Embedded Security in Cars, 7th Conference, 24.-25. November 2009, Düsseldorf

BKatV: Bußgeldkatalog-Verordnung der Bundesrepublik Deutschland (Verordnung über die Erteilung einer Verwarnung, Regelsätze für Geldbußen und die Anordnung eines Fahrverbots wegen Ordnungswidrigkeiten im Straßenverkehr), http://bundesrecht.juris.de/bkatv_2002/, 2009

BORGEEST, K.: Elektronik in der Fahrzeugtechnik – Hardware, Software, Systeme und Projektmanagement, 1. Auflage 2008, Verlag VIEWEG + TEUBNER, ISBN 978-3-8348-0207-1, 2008

BURG, H., MOSER, A. (Hrsg.): Handbuch Verkehrsunfallrekonstruktion – Unfallaufnahme, Fahrdynamik, Simulation, 2., aktualisierte Auflage 2009, Verlag VIEWEG + TEUBNER, ISBN 978-3-8348-0546-1, 2009

CLAUSING, R., HIELSCHER, T., BRAUN, W.: Benutzerseitiges Flashen von Navigationssystemen, Bericht zur Veranstaltung „IT-Security Project“ im Sommersemester 2009, Universität Magdeburg.

ECKERT, C.: IT-Sicherheit; Konzept – Verfahren – Protokolle, 3., überarbeitete und erweiterte Auflage, Oldenbourg Verlag München, Wien, ISBN 3-486-20000-3, 2004

ELLIMS, M.: „Is Security Necessary for Safety?”, Embedded Security in Cars (ESCAR’07) Berlin, 2006

ERNST, K., FINSTER, F., HULTSCH, A.: Spektrum von Fahrzeug- und Infrastruktursystemen als Ziel von Manipulation, Bericht zum Seminar „Sicherheit eingebetteter Systeme“ im Wintersemester 2009/2010, Okt./Nov. 2009, Universität Magdeburg

ESoP: European Statement of Principles (ESoP), Official Journal of the EU (2007/78/EC) vom 06.02.2007

HEIßING, B., ERSOY, M.: Fahrwerkhandbuch – Grundlagen, Fahrdynamik, Komponenten, Systeme, Mechatronik, Perspektiven. 2., verbesserte und aktualisierte Auflage 2008, Verlag VIEWEG + TEUBNER, ISBN 978-3-8348-0444-0, 2008

HIS: Herstellerinitiative Software, http://www.automotive-his.de/, 2009

HOLTHUSEN, S.: Bericht zum Praktikum an der AG Multimedia and Security, Bachelor-Praktikum im Wintersemester 2009/2019, Otto-von-Guericke-Universität Magdeburg, 2009

HOLZKNECHT, M., GARZ, R., RASSEK, F.: Häufigkeit von Manipulationen und entsprechender automotiver Systeme am Markt, Bericht zum Seminar „Sicherheit eingebetteter Systeme“ im Wintersemester 2009/2010, Okt./Nov. 2009, Universität Magdeburg

HOPPE, T., KILTZ, S., DITTMANN, J.: Applying Intrusion Detection to Automotive IT – Early Insights and Remaining Challenges; in: Journal of Information Assurance and Security (JIAS), ISSN: 1554-1010, Vol. 4, Issue 6, pp. 226-235, 2009

HOWARD, J. D., LONGSTAFF, T. A.: A Common Language for Computer Security Incidents (SAND98-8667)/Sandia National Laboratories, 1998 (ISBN 0-201-63346-9)

HSL: Innovation Electronics (UK) LTD, Health and Safety Laboratory (HSL): A methodology for the assignment of safety integrity levels (SILs) to safety-related control functions implemented by safety-related electrical, electronic and programmable electronic control systems of machines, 2004 – Forschungsbericht

HU, H., MYERS, S., COLIZZA, V., VESPIGNANI, A.: WiFi Epidemiology: Can Your Neighbors’ Router Make Yours Sick?, 2008

IEC61508: Functional safety of E/E/PE safety-related systems, Internationaler Standard der International Electrotechnical Commission (IEC)

INNOTEC: SIL – Safety Integrity Level, Webseite unter http://www.innotecsafety.de/beratungsleistungen/functional-safety-management/sil-safety-integrity-level, innotec, last access: November 2009

IO26262: Road vehicles – Functional safety, Standard der International Organization for Standardization (ISO)

KILTZ, S., HILDEBRANDT, M., DITTMANN, J.: Forensische Datenarten und -analysen in automotiven Systemen; In: PATRICK HORSTER (Ed.), DACH Security 2009; Bochum; 19./20. Mai 2009

KUHN, A.: Jahresbericht des statistischen Bundesamtes 2004 (1). Wiesbaden: Statistisches Bundesamt (2005)

MENZEL, W., WILLMANN, R., WULFÄNGER, M.: Nebenwirkungen automotiver Eingriffe und ihre Skalierung, Bericht zum Seminar „Sicherheit eingebetteter Systeme“ im Wintersemester 2009/2010, Okt./Nov. 2009, Universität Magdeburg

MÜTER, M., HOPPE, T., DITTMANN, J.: Decision Model for Automotive Intrusion Detection Systems; In: Automotive – Safety & Security 2010, Sicherheit und Zuverlässigkeit für auto-

mobile Informationstechnik; Ada Deutschland Tagung 22. und 23. Juni 2010, Stuttgart; ISBN 978-3-8322-9172-3, S. 103-116, Shaker Verlag, Aachen, 2010

MISRA: Development guidelines for vehicle based software/MISRA. 2001 (ISBN 0 9524156 0 7). Forschungsbericht

NOHL, K., PAGET, C.: GSM – SRSLY?, Vortrag auf dem 26. Chaos Communication Congress, 27.-30. Dezember 2009, Berliner Congress Center, Berlin, 2009

ROSENBLUTH, W., Adams, H. A.: Retrieval and Interpretation of Crash-Related Data from Nonresponsive Electronic Control Units in Land Vehicle Systems, Journal of Testing and Evaluation, JTEVA, Vol. 30, No. 4, July 2002, pp. 350-361

SCHEIBEL, M., WOLF, M.: Security Risk Analysis for Vehicular IT Systems – A Business Model for IT-Security Measures, In: escar – Embedded Security in Cars, 7th Conference, 24.-25. November 2009, Düsseldorf

SCHMIDT, F.: Bericht zum Praktikum an der AG Multimedia and Security, Bachelor-Praktikum im Wintersemester 2009/2010, Otto-von-Guericke-Universität Magdeburg, 2009

SCHUSTER, A., STEINDORF, D., FISCHER, F.: Überblick moderne Fahrerassistenzsysteme, Bericht zum Seminar „Sicherheit eingebetteter Systeme“ im Wintersemester 2009/2010, Okt./Nov. 2009, Universität Magdeburg

SCHWENKE, C.: Analyse zu Bedrohungslage und Manipulationsschutz eingebetteter Systeme in sicherheitskritischen Umgebungen am Beispiel Automotive, Technischer Bericht, 2009, Universität Magdeburg

STALLINGS, W.: Modern Operating Systems. Prentice Hall. ISBN 0-13-180977-6. 1995

STEIN, A., STROHMEYER, T., PARTSCH, C.: Sicherheitsrisiken für den Menschen im Fahrzeug und seinem Umfeld, Bericht zum Seminar „Sicherheit eingebetteter Systeme“ im Wintersemester 2009/2010, Okt./Nov. 2009, Universität Magdeburg

STENGEL, M., LIPACZEWSKI, M., WINTER, M.: Simulated worm attacks in car-2-car communication networks with TRAN-SIMS traffic simulation software, Ausarbeitung im Rahmen des Praktikums IT-Sicherheit, WS2008/09, Universität Magdeburg

StVO: Straßenverkehrs-Ordnung der Bundesrepublik Deutschland, http://bundesrecht.juris.de/stvo/index.html, 2009

StVZO: Straßenverkehrs-Zulassungs-Ordnung der Bundesrepublik Deutschland, http://bundesrecht.juris.de/stvzo/index.html, 2009

TRANSIMS – Transportation Analysis and Simulation, 2009, http://sourceforge.net/projects/tran sims/

TUCHSCHEERER, S.: Menschliche Faktoren bei der Bewertung von Fahrer-Fahrzeug-Interaktionen, Technischer Bericht, Projekt COmpetence in MObility (COMO), Universität Magdeburg, 2009

WALLENTOWITZ, H., REIF, K.: Handbuch Kraftfahrzeugelektronik – Grundlagen, Komponenten, Systeme, Anwendungen, 1. Auflage September 2006, vieweg Verlag, ISBN 978-3-528-03971-4, 2006

WINNER, H., HAKULI, S., WOLF, G. (Hrsg.): Handbuch Fahrerassistenzsysteme – Grundlagen, Komponenten und Systeme für aktive Sicherheit und Komfort, 1. Auflage 2009, Verlag VIEWEG + TEUBNER, ISBN 978-3-8348-0287-3, 2009

WOLF, M.: Security Engineering for Vehicular IT Systems – Improving the Trustworthiness and Dependability of Automotive IT Applications, 1. Auflage 2009, Verlag VIEWEG + TEUBNER, ISBN 978-3-8348-0795-3, 2009

WRIGHT, C. S.: A Taxonomy of Information Systems Audits, Assessments and Reviews, SANS Institute, 2007

ZIMBARDO, P. G., GERRIG, R. J.: Psychologie. Eine Einführung. Gebundene Ausgabe: Springer, Berlin, 7. A., 2003. ISBN 3-540-64633-7; TB-Ausgabe bei Verlag: Pearson Studium; 16. Auflage, 2004, 976 Seiten. ISBN 3-8273-7056-6, 2003

ZIMMERMANN, W., SCHMIDGALL, R.: Bussysteme in der Fahrzeugtechnik – Protokolle und Standards, 3., aktualisierte und erweiterte Auflage, Vieweg Verlag, ISBN 978-3834804471, 2008

Schriftenreihe

Berichte der Bundesanstalt für Straßenwesen

Unterreihe „Fahrzeugtechnik“

1997

F 22: **Schadstoffemissionen und Kraftstoffverbrauch bei kurzzeitiger Motorabschaltung**
Bugsel, Albus, Sievert € 10,50

F 23: **Unfalldatenschreiber als Informationsquelle für die Unfallforschung in der Pre-Crash-Phase**
Berg, Mayer € 19,50

1998

F 24: **Beurteilung der Sicherheitsaspekte eines neuartigen Zweiradkonzeptes**
Kalliske, Albus, Faerber € 12,00

F 25: **Sicherheit des Transportes von Kindern auf Fahrrädern und in Fahrradanhängern**
Kalliske, Wobben, Nee € 11,50

1999

F 26: **Entwicklung eines Testverfahrens für Antriebsschlupf-Regelsysteme**
Schweers € 11,50

F 27: **Betriebslasten an Fahrrädern**
Vötter, Groß, Esser, Born, Flamm, Rieck € 10,50

F 28: **Überprüfung elektronischer Systeme in Kraftfahrzeugen**
Kohlstruck, Wallentowitz € 13,00

2000

F 29: **Verkehrssicherheit runderneuerter Reifen**
Teil 1: Verkehrssicherheit runderneuerter PKW-Reifen
Glaeser
Teil 2: Verkehrssicherheit runderneuerter Lkw-Reifen
Aubel € 13,00

F 30: **Rechnerische Simulation des Fahrverhaltens von Lkw mit Breitreifen**
Faber € 12,50

F 31: **Passive Sicherheit von Pkw bei Verkehrsunfällen – Fahrzeugsicherheit '95 – Analyse aus Erhebungen am Unfallort**
Otte € 12,50

F 32: **Die Fahrzeugtechnische Versuchsanlage der BASt – Einweihung mit Verleihung des Verkehrssicherheitspreises 2000 am 4. und 5. Mai 2000 in Bergisch Gladbach** € 14,00

2001

F 33: **Sicherheitsbelange aktiver Fahrdynamikregelungen**
Gaupp, Wobben, Horn, Seemann € 17,00

F 34: **Ermittlung von Emissionen im Stationärbetrieb mit dem Emissions-Mess-Fahrzeug**
Sander, Bugsel, Sievert, Albus € 11,00

F 35: **Sicherheitsanalyse der Systeme zum Automatischen Fahren**
Wallentowitz, Ehmanns, Neunzig, Weilkes, Steinauer, Bölling, Richter, Gaupp € 19,00

F 36: **Anforderungen an Rückspiegel von Krafträdern**
van de Sand, Wallentowitz, Schrüllkamp € 14,00

F 37: **Abgasuntersuchung - Erfolgskontrolle: Ottomotor – G-Kat**
Afflerbach, Hassel, Schmidt, Sonnborn, Weber € 11,50

F 38: **Optimierte Fahrzeugfront hinsichtlich des Fußgängerschutzes**
Friesen, Wallentowitz, Philipps € 12,50

2002

F 39: **Optimierung des rückwärtigen Signalbildes zur Reduzierung von Auffahrunfällen bei Gefahrenbremsung**
Gail, Lorig, Gelau, Heuzeroth, Sievert € 19,50

F 40: **Entwicklung eines Prüfverfahrens für Spritzschutzsysteme an Kraftfahrzeugen**
Domsch, Sandkühler, Wallentowitz € 16,50

2003

F 41: **Abgasuntersuchung: Dieselfahrzeuge**
Afflerbach, Hassel, Mäurer, Schmidt, Weber € 14,00

F 42: **Schwachstellenanalyse zur Optimierung des Notausstiegsystems bei Reisebussen**
Krieg, Rüter, Weißgerber € 15,00

F 43: **Testverfahren zur Bewertung und Verbesserung von Kinderschutzsystemen beim Pkw-Seitenaufprall**
Nett € 16,50

F 44: **Aktive und passive Sicherheit gebrauchter Leichtkraftfahrzeuge**
Gail, Pastor, Spiering, Sander, Lorig € 12,00

2004

F 45: **Untersuchungen zur Abgasemission von Motorrädern im Rahmen der WMTC-Aktivitäten**
Steven € 12,50

F 46: **Anforderungen an zukünftige Kraftrad-Bremssysteme zur Steigerung der Fahrsicherheit**
Funke, Winner € 12,00

F 47: **Kompetenzerwerb im Umgang mit Fahrerinformationssystemen**
Jahn, Oehme, Rösler, Krems € 13,50

F 48: **Standgeräuschmessung an Motorrädern im Verkehr und bei der Hauptuntersuchung nach § 29 StVZO**
Pullwitt, Redmann € 13,50

F 49: **Prüfverfahren für die passive Sicherheit motorisierter Zweiräder**
Berg, Rücker, Bürkle, Mattern, Kallieris € 18,00

F 50: **Seitenairbag und Kinderrückhaltesysteme**
Gehre, Kramer, Schindler € 14,50

F 51: **Brandverhalten der Innenausstattung von Reisebussen**
Egelhaaf, Berg, Staubach, Lange € 16,50

F 52: **Intelligente Rückhaltesysteme**
Schindler, Kühn, Siegler € 16,00

F 53: **Unfallverletzungen in Fahrzeugen mit Airbag**
Klanner, Ambos, Paulus, Hummel, Langwieder, Köster € 15,00

F 54: **Gefährdung von Fußgängern und Radfahrern an Kreuzungen durch rechts abbiegende Lkw**
Niewöhner, Berg € 16,50

2005

F 55: **1st International Conference on ESAR „Expert Symposium on Accident Research“ – Reports on the ESAR-Conference on 3rd/4th September 2004 at Hannover Medical School** € 29,00

2006

F 56: **Untersuchung von Verkehrssicherheitsaspekten durch die Verwendung asphärischer Außenspiegel**
Bach, Rüter, Carstengerdes, Wender, Otte € 17,00

F 57: **Untersuchung von Reifen mit Notlaufeigenschaften**
Gail, Pullwitt, Sander, Lorig, Bartels € 15,00

F 58: **Bestimmung von Nutzfahrzeugemissionsfaktoren**
Steven, Kleinebrahm € 15,50

F 59: **Hochrechnung von Daten aus Erhebungen am Unfallort**
Hautzinger, Pfeiffer, Schmidt € 15,50

F 60: **Ableitung von Anforderungen an Fahrerassistenzsysteme aus Sicht der Verkehrssicherheit** Vollrath, Briest, Schießl, Drewes, Becker

€ 16,50

2007

F 61: **2nd International Conference on ESAR „Expert Symposium on Accident Research" – Reports on the ESAR-Conference on 1st/2nd September 2006 at Hannover Medical School** € 30,00

F 62: **Einfluss des Versicherungs-Einstufungstests auf die Belange der passiven Sicherheit**
Rüter, Zoppke, Bach, Carstengerdes € 16,50

F 63: **Nutzerseitiger Fehlgebrauch von Fahrerassistenzsystemen**
Marberger € 14,50

F 64: **Anforderungen an Helme für Motorradfahrer zur Motorradsicherheit**
Dieser Bericht liegt **nur** in digitaler Form vor und kann kostenpflichtig unter www.nw-verlag.de heruntergeladen werden.
Schüler, Adoplh, Steinmann, Ionescu € 22,00

F 65: **Entwicklung von Kriterien zur Bewertung der Fahrzeugbeleuchtung im Hinblick auf ein NCAP für aktive Fahrzeugsicherheit**
Manz, Kooß, Klinger, Schellinger € 17,50

2008

F 66: **Optimierung der Beleuchtung von Personenwagen und Nutzfahrzeugen**
Jebas, Schellinger, Klinger, Manz, Kooß € 15,50

F 67: **Optimierung von Kinderschutzsystemen im Pkw**
Weber € 20,00

F 68: **Cost-benefit analysis for ABS of motorcycles**
Baum, Westerkamp, Geißler € 20,00

F 69: **Fahrzeuggestützte Notrufsysteme (eCall) für die Verkehrssicherheit in Deutschland**
Auerbach, Issing, Karrer, Steffens € 18,00

F 70: **Einfluss verbesserter Fahrzeugsicherheit bei Pkw auf die Entwicklung von Landstraßenunfällen**
Gail, Pöppel-Decker, Lorig, Eggers, Lerner, Ellmers € 13,50

2009

F 71: **Erkennbarkeit von Motorrädern am Tag – Untersuchungen zum vorderen Signalbild**
Bartels, Sander € 13,50

F 72: **3rd International Conference on ESAR „Expert Symposium on Accident Research" – Reports on the ESAR-Conference on 5th/6th September 2008 at Hannover Medical School** € 29,50

F 73: **Objektive Erkennung kritischer Fahrsituationen von Motorrädern**
Seiniger, Winner € 16,50

2010

F 74: **Auswirkungen des Fahrens mit Tempomat und ACC auf das Fahrerverhalten**
Vollrath, Briest, Oeltze € 15,50

F 75: **Fehlgebrauch der Airbagabschaltung bei der Beförderung von Kindern in Kinderschutzsystemen**
Müller, Johannsen, Fastenmaier € 15,50

2011

F 76: **Schutz von Fußgängern beim Scheibenanprall II**
Dieser Bericht liegt **nur** in digitaler Form vor und kann kostenpflichtig unter www.nw-verlag.de heruntergeladen werden.
Bovenkerk, Gies, Urban € 19,50

F 77: **4th International Conference on ESAR „Expert Symposium on Accident Research"**
Dieser Bericht liegt **nur** in digitaler Form vor und kann kostenpflichtig unter www.nw-verlag.de heruntergeladen werden. € 29,50

F 78: **Elektronische Manipulation von Fahrzeug- und Infrastruktursystemen**
Dittmann, Hoppe, Kiltz, Tuchscheerer € 17,50

Alle Berichte sind zu beziehen beim:

Wirtschaftsverlag NW
Verlag für neue Wissenschaft GmbH
Postfach 10 11 10
D-27511 Bremerhaven
Telefon: (04 71) 9 45 44 - 0
Telefax: (04 71) 9 45 44 77
Email: vertrieb@nw-verlag.de
Internet: www.nw-verlag.de

Dort ist auch ein Komplettverzeichnis erhältlich.