

Die Umfrage ist keineswegs als repräsentativ anzusehen, da im Fall der AMS-Leser ein auto-affines Publikum und beim Kongress Fachkundige aus der Automotivszene angesprochen wurden. Daher weichen die Ergebnisse allein zwischen diesen beiden Gruppen ab. Der Autor hat zur weiteren Verdichtung eine eigene Umfrage mit denselben Fragen und Antwortmöglichkeiten über die Projekt-Website www.Car-Forensics.de gestartet und hier Antworten einer dritten Gruppe hinzugefügt. Diese Gruppe darf als an Fragen der IT-Sicherheit und Forensik interessiert angesehen werden, ist aber aufgrund der geringen Zahl an Rückmeldungen mit 26 Antworten statistisch vorsichtig zu bewerten. Die Einschränkung, dass nur eine Antwort ausgewählt werden kann, stammt von den Machern der AMS und wurde aus Vergleichbarkeitsgründen vom Autor für seine Umfrage so übernommen.

Als Ergebnis dieser Umfragen (gewichtete Mittelwerte) ist festzuhalten, dass nur etwa 23% der Befragten nicht daran glauben, dass sich autonomes bzw. automatisiertes Fahren durchsetzen wird. 88% sehen den Einsatz auf der Autobahn bzw. im Stau. Als Treiber für die Einführung des autonomen Fahrens wird mit 38% die Autoindustrie, dicht gefolgt mit 25% von den Technologiekonzernen und mit 19% der Gruppe der Autozulieferer angesehen. Mehr als zwei Drittel der Befragten äußern sich besorgt bzw. sehr besorgt, dass die Daten im Automotivumfeld missbraucht werden. Relativ deutlich fällt das Ergebnis auf die Frage aus, wer Zugriff auf die Daten im Automobil haben sollte. Im Mittel sind 57% der Meinung, dass die Daten ausschließlich dem Fahrzeughalter gehören, 30% sehen den PKW-Hersteller als zugriffsberechtigt an.

Befragt man eher Verbraucher, dann fällt das Ergebnis deutlicher in Richtung „ausschließlich Fahrzeughalter“ aus. Dem Staat (Polizei) oder gar Versicherungen steht die Mehrheit in diesem Aspekt sehr skeptisch gegenüber. Die Einführung des eCall-Systems wird gemessen am voraussichtlichen Sicherheitsgewinn überwiegend begrüßt (65%), aber auch hier gibt es Vorbehalte bzgl. Datensicherheit und Datenschutz.

Die Skepsis gegenüber der zunehmenden Vernetzung und Automatisierung der Fahrzeuge aber auch die unterschiedlichen – teils widersprüchlichen Einschätzungen und Anforderungen – spiegeln sich auch in der Presseberichterstattung in verschiedenen Medien wieder¹⁰. So forderte u.a. der Chef der Verbraucherzentrale Bundesverband Klaus Müller nach einer Meldung der AFP¹¹ vom 07.12.2016 gesetzliche Mindeststandards für das Fahren mit Autopilot. Nicht zuletzt bedarf es in diesem Zusammenhang auch einer ethischen Debatte, nämlich dann, wenn es darum geht, wie ein Automat zu entscheiden hat, wenn ein Unfall unausweichlich ist, jedoch verschiedene Optionen mit unterschiedlichen Schadensbildern zur Entscheidung stehen. Wird das Kind zugunsten des älteren Mitmenschen verschont oder steht der Schutz der eigenen Insassen an höchster Stelle? Eine spannende Diskussion, die sicherlich nicht im Rahmen dieser Forschungsarbeit beantwortet werden kann.

¹⁰ vgl. u.a. (All-Electronics, 2014); Birgit Priemer, „AMS Sonderheft: Autonomes fahren“, AMS Sonderheft Mobilität 2015, 2015.; AN, „Verbraucher wünschen sich kommunikative Autos“, AN 30062015.; (Schäfer, 2015)

¹¹ Quelle: (AFP-AN, 2016)

Update 05/2019: Die Bundesregierung hat hierzu im Herbst 2016 eine Ethikkommission eingesetzt, die diese grundsätzlichen Fragen klären und den Entwicklern Leitlinien an die Hand geben sollte, wie automatisiert agierende Systeme zukünftig auszulegen sind. Im August 2017 wurden folgende Ergebnisse veröffentlicht¹², die laut Bundesregierung nachfolgend in die Gesetzgebung einfließen sollen:

- *Das automatisierte und vernetzte Fahren ist ethisch geboten, wenn die Systeme weniger Unfälle verursachen als menschliche Fahrer.*
- *Sachschaden geht vor Personenschaden: In Gefahrensituationen hat der Schutz menschlichen Lebens immer höchste Priorität.*
- *In unausweichlichen Unfallsituationen ist jede Qualifizierung von Menschen nach persönlichen Merkmalen unzulässig.*
- *In jeder Fahrsituation muss klar geregelt und erkennbar sein, wer für die Fahraufgabe zuständig ist: Mensch oder Computer.*
- *Es ist zu dokumentieren und speichern, welche Person fährt - unter anderem zur Klärung möglicher Haftungsfragen.*
- *Der Fahrer oder die Fahrerin muss grundsätzlich selbst über Weitergabe und Verwendung seiner/ihrer Fahrzeugdaten entscheiden können.*

Für den Autor ist hierbei der erste Punkt hinsichtlich der möglichen Auslegung interessant. Man könnte dies so interpretieren, dass das manuelle Fahren in Zukunft aus ethischen Gründen verboten wird, wenn automatisiert fahrende Fahrzeuge nachweislich weniger Unfälle verursachen. Ob das jedem Bürger und Verbraucher dann tatsächlich gefallen wird, ist eine gesellschaftspolitisch spannende Frage und löst weitere Diskussionen aus, u.a. was mit Old- und Youngtimern passiert und wie sich generell die Automobilindustrie und die Wertschöpfungsketten in Industrieländern wie Deutschland verändern werden.

2.4 Level automatisierten Fahrens

Für die weitere Diskussion ist es hilfreich, auf eine einheitliche und anerkannte Klassifizierung für die Stufen automatisierten Fahrens zurückzugreifen. Die amerikanische National Highway Traffic Safety Administration (NHTSA) definierte am 30.05.2013 fünf Automationsgrade für das pilotierte Autofahren¹³:

0. No-Automation (Level 0): Der Fahrer hat die volle Kontrolle und Steuerungsaufgabe für das gesamte Fahrzeug. Es gibt keine Fahrerassistenzsysteme (auch kein ESP, ABS etc.).
1. Function-specific Automation / assistiert (Level 1): Der Fahrer hat die volle Kontrolle und Steuerungsaufgabe für das gesamte Fahrzeug. Es gibt einzelne Fahrerassistenzsysteme wie ESP, ABS usw., die den Fahrer in betriebskritischen Situationen bei der Steuerung unterstützen und vor einem Unfall bewahren sollen.

¹² Quelle: <https://www.bundesregierung.de/breg-de/aktuelles/klare-ethik-regeln-fuer-fahrcomputer-389346>

¹³ Quelle: NHTSA (NHTSA, 2013)

2. Combined Function Automation / teilautomatisiert (Partial Automated Driving – PAD) / (Level 2): Der Fahrer kann einzelne Steuerungsaufgaben an Assistenzsysteme übergeben und wird von der Steuerungs-, nicht aber von der Kontrollaufgabe entbunden. Er ist also immer noch „im Loop“ (Beispiel: Adaptiv Cruise Control in Kombination mit einem Spurhalteassistenten).
3. Limited Self-Driving Automation (Highly Automated Driving – HAD) / hochautomatisiert (Level 3): Der Fahrer kann in bestimmten Umgebungen (z.B. Autobahn) von der Fahr- und Kontrollaufgabe vollständig entbunden werden und kann dann auch sogenannte Sidetasks ausführen (sofern rechtlich zulässig). Das Fahrzeug übergibt die Steuerung in einem definierten Prozess in einem Zeitfenster von typisch 10 Sekunden zurück an den Fahrer, z.B. wenn das Fahrzeug sich einem Abschnitt nähert, in dem autonomes Fahren nicht möglich ist, bis hin zum sogenannten „Safe Harbour Modus“, wenn der Fahrer die Kontrolle nicht mehr übernimmt.
4. Full Self-Driving Automation (Fully Automated Driving – FAD) / vollautomatisiert bzw. fahrerlos (Level 4): Das Fahrzeug ist in der Lage, eine komplette Fahrt vollständig automatisiert und eigenständig durchzuführen. Der „Fahrer“ gibt lediglich das Navigationsziel ein (ggf. auch von extern) und braucht während der Fahrt nicht zwingend an Bord zu sein.

Der VDA bzw. die Bundesanstalt für Straßenwesen (BAST) definieren die Stufen praktisch identisch¹⁴, unterscheiden jedoch Level 4 in „vollautomatisiert“ (Stufe 4) und „fahrerlos“ (Stufe 5). Einigkeit herrscht unter Fachleuten darüber, dass eine besondere Herausforderung im Sprung von Level 2 zu Level 3 zu sehen ist. Genau an diesem Übergang ist der heutige Stand der Technik (2016) zu sehen, denn es gibt bereits vereinzelt Serienfahrzeuge, die technisch in der Lage sind, die Fahraufgabe im Stau oder definierten Umgebungen (Automatic Highway Driving Assist) zu übernehmen. Ein weiterer wichtiger Fachbegriff, der vor allem Auswirkungen auf die rechtliche Betrachtung hat, ist, ob der Fahrer „im Loop“ ist oder nicht.

Mit „im Loop“ ist gemeint, dass der menschliche Fahrer integraler Bestandteil der als Schleife (Loop) ablaufenden Steuerungs- und Kontrollaufgaben für die Führung eines Fahrzeugs ist. Selbst wenn das Fahrzeug in Level 2 und vor allem in Level 3 die Fahraufgabe für einen längeren Zeit- und Streckenabschnitt vollautomatisch übernehmen kann, kommt dem Fahrer immer noch eine kontrollierende und überwachende Funktion zu. Auch wenn er gar nicht korrigierend eingreifen muss, hat er jedoch ständig das System und seine Entscheidungen dahingehend zu prüfen, dass kein Verkehrsverstoß begangen und kein Unfall verursacht wird. Gegenüber dem Fahrzeug bzw. dessen Steuerungseinheit muss er dies i.d.R. durch eine regelmäßige Bestätigung quittieren. Dies erfolgt z.B. dadurch, dass er eine Hand an Lenkrad lässt oder auf den Automatikwählhebel legt und durch die Berührung bzw. leichte Bewegungen dem System die generelle Aufmerksamkeit und Eingreifmöglichkeit signalisiert wird. Erfolgt längere Zeit keine solche Bewegung, so schaltet sich das System i.d.R. mit einer Warnmeldung ab.

¹⁴ Quelle: VDA/BAST, „VDA - Level Automatisiertes Fahren“, 2014
<<https://www.vda.de/de/themen/innovation-und-technik/automatisiertes-fahren.html>> [zugegriffen 30 Mai 2015].

2.5 Zielsetzungen der Forschungsarbeit

Aus dem breiten Spektrum der im vorangegangenen Kapitel skizzierten Aspekte rund um das automatisierte bzw. autonome Fahren und die Digitalisierung moderner Verkehrsmittel erwachsen für die Forschungsarbeit verschiedene Blickwinkel, die für die nachfolgenden Untersuchungen der einzelnen Systeme maßgebliche Motivation sind und dort – wo möglich – entsprechend diskutiert werden.

- Sicherheitssicht (Road-Safety)
- Sicherheitssicht (IT-Security)
- Datenschutzsicht
- Forensiksicht

Die Ergebnisse wiederum kann man unterschiedlich einsetzen:

- Zur Prävention
- Zur Analyse und Aufklärung

2.5.1 Sicherheitssicht (Safety)

Die Betriebssicherheit von Kraftfahrzeugen wird i.d.R. bzw. bisher allein unter dem Aspekt der Safety-Criticalness betrachtet. Alle Komponenten eines Fahrzeugs müssen so konzipiert sein, dass sie im Rahmen der regulären Betriebsparameter weder die Insassen noch andere Verkehrsteilnehmer gefährden und keine Sachen (andere Systeme, Umwelt etc.) beschädigen oder über Gebühr belasten.

Dem wird u.a. dadurch Rechnung getragen, dass ab dem 01.07.2015 bei einer Hauptuntersuchung auch die Funktionsfähigkeit von Fahrerassistenzsystemen (rudimentär) geprüft wird¹⁵.

Beispiel: Die Lenkradsperre muss so konzipiert sein, dass sie zu keinem Zeitpunkt beim Betrieb eines PKW durch eine Fehlbedienung oder den Ausfall eines anderen Systems während der Fahrt aktiviert wird. Solange das Fahrzeug rollt, darf also weder das Stoppen des Motors noch das Ausschalten der Zündung noch das versehentliche Abziehen des Zündschlüssels zu einem Einrasten der Lenkradsperre führen. Dass diese Anforderung nicht immer gewährleistet ist, zeigen durch defekte Zündschlösser verursachten Unfälle mit Todesfolge im Fall von General Motors¹⁶.

Die Integrität der Vehicle-Safety kann bisher nur durch einen Konstruktionsfehler, Verschleiß, physikalische Beschädigung oder direkte Manipulation erschüttert werden. Sie setzt bisher immer eine lokal und räumlich auf das Fahrzeug bezogene Interaktion voraus.

¹⁵ Quelle: u.a. TÜV Rheinland, „HU-Adapter: Mehr Sicherheit bei der Prüfung von Assistenzsystemen - TÜV Rheinland - Pressemitteilung“, Pressebox 28.05.2015, 2015

<<http://www.pressebox.de/pressemitteilung/tuev-rheinland/HU-Adapter-Mehr-Sicherheit-bei-der-Pruefung-von-Assistenzsystemen/boxid/740702>> [zugegriffen 29 Mai 2015].

¹⁶ Quelle: u.a. (Linder, 2014); Lennart Lutz, „Rechtliche Herausforderungen auf dem Weg zu voll autonomen Fahrzeugen“, VDI Wissensforum, 2013.



3 Datenschutz-, IT-Sicherheits- und Forensiksicht

Wie bereits im einleitenden Kapitel als Motivation dargestellt, kann man die in Fahrzeugen bzw. mit diesen gekoppelte IT-Systeme und Dienstleistungen sowohl unter Aspekten des Datenschutz als auch der IT-Sicherheit kritisch betrachten. Und auch wenn diese Systeme und Datenspeicher vordergründig einen ganz anderen Sinn und Zweck haben, kann man sie prinzipiell für eine forensische Analyse heranziehen und auswerten. Zur Verdeutlichung der unterschiedlichen Blickwinkel sollen daher in diesem Kapitel zunächst die Grundlagen auf Normenbasis bzw. durch Klarstellung der Begrifflichkeiten angerissen werden.

3.1 Datenschutz-Sicht

Unter dem Begriff Datenschutz versteht man den Schutz von personenbezogenen Daten natürlicher, lebender Personen vor missbräuchlicher Nutzung durch die erfassenden oder weiter verarbeitenden Stellen. Beim Datenschutz stehen, anders als der Begriff zunächst vermuten lässt, nicht die Daten im Vordergrund, sondern die Personen, über die Informationen (Daten) verarbeitet werden. Rechtlicher Ausgangspunkt ist das Grundrecht auf informationelle Selbstbestimmung. Die Grundidee ist, dass der Einzelne die Möglichkeit haben soll, selbst zu bestimmen, wer bei welcher Gelegenheit welche Informationen über ihn erhält. Als besonders gefährdend werden die Situationen angesehen, in denen große Organisationen Informationen - möglicherweise ohne Kenntnis der betroffenen Personen - sammeln, speichern und auswerten (BigData). Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

3.1.1 Gesetzlichen Grundlagen: DS-GVO und BDSG

Update 05/2019: Am 25. Mai 2018 ist die EU Datenschutz-Grundverordnung (DS-GVO) in Kraft getreten. Der Text des nachfolgenden Kapitels wurde daher in der vorliegenden Ausgabe komplett überarbeitet.

Bis zum 25. Mai 2018 galt in Deutschland das Bundesdatenschutzgesetz vom 20.12.1990. Es wurde nach einer Neufassung im Jahr 2003 zuletzt am 25.02.2015 aktualisiert und mit Einführung der DS-GVO grundlegend überarbeitet und mündete in das BDSG neu. Das primäre Ziel sowohl der verschiedenen Versionen des BDSG als auch der DS-GVO ist nach wie vor dasselbe, auch wenn dies nur in der alten Fassung des BDSG so explizit formuliert wurde: „*Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.*“ (§1 BDSG alt).

Dem BDSG übergeordnet ist die DS-GVO. Da es sich bei der DS-GVO um eine Grundverordnung handelt, war diese in den EU-Staaten nicht in nationale Gesetzgebungen umzusetzen, sondern gilt unmittelbar. Die DS-GVO vereinheitlicht nun die Datenschutzregeln für alle EU-Staaten und findet auch für Anbieter Anwendung, die nicht in der EU ansässig sind, jedoch ihre Dienstleistungen in der EU anbieten bzw. erbringen – also beispielsweise auch Facebook und Google ohne eigenen Firmensitz innerhalb der EU. Die DS-GVO enthält sogenannte Öffnungsklauseln, die es den Mitgliedsstaaten erlaubt, Regelungslücken mit eigenen Gesetzen zu ergänzen bzw. die von der DS-GVO vorgegebenen Mindeststandards zu erhöhen. Ein Unterschreiten bzw. Aushebeln der Standards der DS-GVO ist jedoch nicht zulässig.

3.1.1.1 Zulässigkeit der Datenerhebung

§3 des BDSG besagt: Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem ange strebten Schutzzweck steht.

Die Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung regeln Art. 5 und 6 DS-GVO. Art 5 liefert folgendes:

(1) Personenbezogene Daten müssen

- a. auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);
- b. für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);
- c. dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
- d. sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);
- e. in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);
- f. in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

Art 6: Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

1. *Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;*
2. *die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;*
3. *die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;*
4. *die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;*
5. *die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;*
6. *die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.*

Zusammengefasst bedeutet dies, dass die oberste Prämisse die Vermeidung der Erhebung bzw. Speicherung von personenbezogenen Daten sein soll bzw., sofern dies nicht möglich ist, ansonsten die Datensparsamkeit an nächster Stelle steht. Dort wo möglich soll von der Möglichkeit des Anonymisierens von Daten Gebrauch gemacht werden. Des Weiteren ist eine explizite Einwilligung zum Erheben, Speichern und Verarbeiten personenbezogener Daten beim Betroffenen einzuholen und ihn über die Art und Weise, was mit seinen Daten passiert, transparent aufzuklären. Stillschweigend darf nicht von einer Zustimmung ausgegangen werden.

Der Betroffene hat das Grundrecht, von jeder verantwortlichen Stelle (also demjenigen, der die Daten erhoben, gespeichert oder verarbeitet hat) unentgeltlich Auskunft zu erhalten, welche Daten über ihn gespeichert sind und er kann verlangen, dass diese ggf. berichtigt oder gelöscht (gesperrt) werden.

Die DS-GVO erlaubt, dass Firmen und Institutionen sehr wohl personenbezogene Daten ihrer Kunden speichern und verwenden dürfen, sofern es zur Vertragserfüllung notwendig ist. Dies werden regelmäßig neben Namen und Titel die postalische Adresse sowie z.B. Geburtsdatum und Bankverbindung sein. Man soll dabei aber nur die Daten erheben und speichern, die man für die Pflege der Geschäftsbeziehung tatsächlich benötigt und hat die Verpflichtung, mit diesen sehr sorgfältig umzugehen.

3.1.1.2 Rechtsfolgen bei Missachtung der DS-GVO

Das BDSG in der alten Fassung war, was die Verhängung von Bußgeldern bei Verstößen anging, ein recht stumpfes Schwert. So wurden bisher meist nur Verstöße gegen Formalien mit Bußgeldern sanktioniert und es sind nur sehr wenige konkrete Fälle überliefert, in denen das tatsächlich passiert ist. Wurde z.B. kein betrieblicher Datenschutzbeauftragter bestellt und / oder es kam zu einer Datenschutzpanne, so konnten Bußgelder bis max. 300.000,-Euro bei Verstößen gegen das BDSG verhängt werden.

Etwas überraschend war jedoch, dass sich die Pönalisierung i.d.R. immer nur auf formale Aspekte bezogen hat und beispielsweise die Missachtung gängiger Standards im Bereich der IT-Sicherheit bei der Verarbeitung von personenbezogenen Daten durch das BDSG nicht mit Ordnungs- oder Bußgeldern bestraft wurde. So war beispielsweise das Speichern und Verarbeiten von Benutzerpasswörtern im Klartext bzw. unverschlüsselt selber nicht pönalisiert, obwohl dies nicht dem Stand der Technik entspricht und damit der technische Datenschutz missachtet wird. Dies wird im Kontext der Untersuchungen an Smartphone-Apps im weiteren Verlauf der Arbeit noch deutlich gemacht. Mit Einführung der DS-GVO hat sich dies erheblich gewandelt. Es sind nun Bußgelder bis 20 Mio. € oder 4% des Vorjahresumsatzes der gesamten Organisation/Firmengruppe (weltweit) möglich, wenn gegen die DS-GVO verstoßen wird. Zudem können Betroffene nun wahlweise den Verantwortlichen oder den Auftragsverarbeiter in Bezug auf Schadenersatzzahlungen in Regress nehmen. Insbesondere die Vertragsgestaltung zur Auftragsverarbeitung sowohl aus Sicht der Verantwortlichen Stelle als auch des Auftragsverarbeiters bedarf daher eines besonderen Augenmerks.

Zu begrüßen ist, dass die DS-GVO nun auch konkrete Maßnahmen zur Einhaltung eines Datensicherheitsniveaus bei Verantwortlichen und Auftragsverarbeitern fordert und sich allein schon aus der Missachtung dieser eigentlich selbstverständlichen Mindeststandards nun auch Ansätze für eine Belegung mit einem Bußgeld ergeben. Hier von wurde bereits nach Einführung Gebrauch gemacht und nun werden die in der Presse immer wieder publik werdenden, teils haarsträubenden Datensicherheits- und Datenschutz-Incidents auch wirksam pönalisiert. Zu kritisieren ist auch bei der DS-GVO und dem BDSG neu, dass die Aufsicht über die Einhaltung in Deutschland weiterhin föderalistisch geregelt und somit für jedes Bundesland ein eigener Landesdatenschutzbeauftragter zuständig ist.

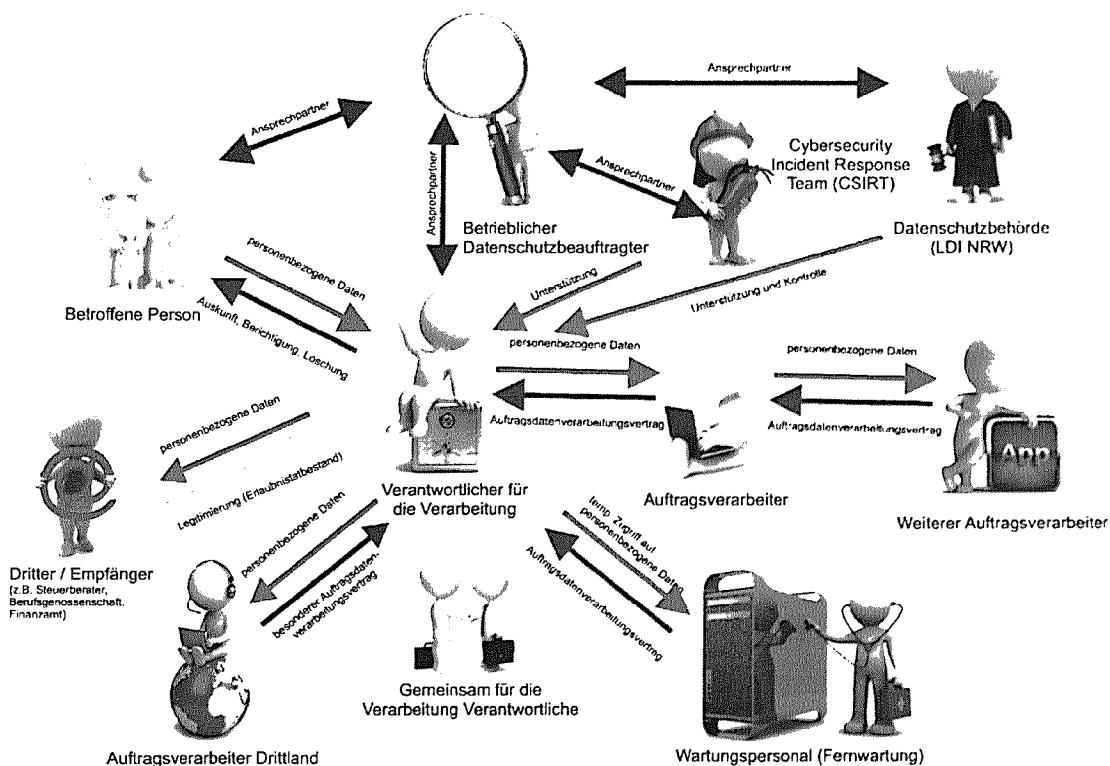


Abbildung 10: Wechselwirkungen und Zuständigkeiten bei der DS-GVO

3.1.2 Datenschutz im Automotiv-Umfeld

Die (ehemalige) Vorstandsvorsitzende der Daimler AG²⁷ und ehemalige Bundesverfassungsrichterin Frau Dr. Hohmann-Dennhardt forderte u.a. am 25.04.2014 in der Zeitschrift Autobild²⁸ eine gesetzliche Initiative bzw. Klarstellung zum Datenschutz im Automobil. Der Autor hat daraufhin die Daimler AG kontaktiert und ist in einen Gedankenaustausch zu diesem Thema u.a. mit dem Konzernbeauftragten für den Datenschutz der Daimler AG eingestiegen und zum Datenschutzkongress am 18.09.2014 eingeladen worden, bei dem die Fragen zu Datenschutz und Privacy von Technikern, Datenschützern und Politikern intensiv diskutiert wurden. Dieses Thema wurde – neben weiteren Aspekten des automatisierten Fahrens – in einem ausführlichen Gespräch seitens des Autors mit dem Bundesministerium für Verkehr und digitale Infrastruktur (Fachbereich Autonomes Fahren) am 21.01.2015 in Berlin diskutiert. Datenschutz bzw. der Umgang mit im Fahrzeug und damit verbundenen Systemen generierten und verarbeiteten Daten ist ein beherrschendes Thema sowohl in der Industrie und Politik auch als in der Wahrnehmung durch den Verbraucher.

Formal betrachtet greifen die Datenschutzgesetze hier jedoch nur indirekt, da die Normen nur die Daten natürlicher und lebender Personen regeln bzw. schützen, nicht jedoch technische Daten, die in einem Automobil anfallen oder in entsprechenden Infrastrukturen gesammelt und weiterverarbeitet werden. Erst durch die Kopplung eines bestimmten Fahrzeugs mit einer individuell bestimmbaren Person bekommt die Speicherung und Verarbeitung von fahrzeugspezifischen Daten eine datenschutzrechtliche Bedeutung.

Diese Verbindung entsteht in der Praxis durch die Identifizierung eines Fahrzeugs durch die eindeutig vergebene Fahrzeugidentifikationsnummer (VIN) mit dem Besitzer bzw. Benutzer des Fahrzeugs. Neben der VIN ist bei für den Straßenverkehr zugelassenen Fahrzeugen auch das amtliche Kennzeichen für die Identifikation und die Zuordnung zu einer Person (dem Halter) heranziehbar. Zwischen amtlichen Kennzeichen und VIN wird die Verbindung über die nationalen Zulassungsbehörden hergestellt. Ist ein Fahrzeug im Besitz einer juristischen Person (Firma, Verein, Behörde) bzw. auf diese zugelassen, so gelingt die Zuordnung meist erst über die Hinzuziehung weiterer Daten (z.B. primärer Nutzer / Fahrer des Fahrzeugs).

Hier gibt es eine Analogie aus der IT-Welt. Eine TCP/IP-Adresse ist (vor allem bei Verwendung des V4-Standards) rein technisch betrachtet kein personenbezogenes Datum, da diese Adresse i.d.R. nie einer natürlichen Person direkt bzw. eindeutig und exklusiv zugeordnet ist. So kann beispielsweise eine öffentliche IP-Adresse zwar zu einem bestimmten Zeitpunkt einem Anschlussinhaber einer Internetanbindung (z.B. Router, Smartphone) zugeordnet werden, jedoch nicht automatisch auch deren Nutzung durch eine bestimmte natürliche Person. Dennoch hat sich eine allgemein anerkannte Rechtsauffassung durchgesetzt (allerdings laut Berichterstattung in der c't 17/2015 nicht obergerichtlich abgesichert²⁹), dass eine IP-Adresse ein personenbezogenes Merkmal ist, da sie unter gewissen Einschränkungen eben oft genug zur Zuordnung einer Kommunikation zu einer bestimmten Person herangezogen werden kann. Genauso wird es sich bei der VIN verhalten.

²⁷ gem. Pressemeldung im Oktober 2015 zur Volkswagen AG gewechselt

²⁸ Quelle: (Hohman-Dennhardt, 2014)

²⁹ Quelle: (Schulzki-Haddouti & Härtig, 2015)

Der ehemalige Bundesdatenschutzbeauftragte Peter Schaar teilte auf dem Daimler Datenschutzkongress am 18.09.2014 auf Nachfrage die Einschätzung des Autors, dass die VIN als personenbezogenes Datum anzusehen ist. In der Konsequenz dieser These ergeben sich somit Auswirkungen für die automatisierte Erhebung, Verarbeitung, Auswertung und ggf. Weitergabe von Fahrzeugdaten an Dritte und die Anwendung der Datenschutzgesetze auch auf Daten aus dem Automotivumfeld.

3.1.3 Einschub: Besitz von Daten

Im Zusammenhang mit den öffentlich geführten Diskussionen über die Datenhoheit im Automobilumfeld hört man des Öfteren die Frage „**Wem gehören die Daten?**“. Diese Frage lässt sich formal gar nicht beantworten, weil bereits die Fragestellung an sich falsch ist. Besitz im juristischen Sinn kann man nur an einer Sache erlangen. Die Problematik beginnt hier bereits mit dem Begriff „Software“, da diese an sich nur eine Folge von Befehlen einer syntaktisch definierten Programmiersprache ist und diese allenfalls durch ihre Wirkung bei Ausführung auf einer entsprechenden Hardware bzw. Speicherung auf einem Datenträger manifestiert wird. Den Datenträger kann man in Besitz nehmen bzw. Besitz darüber erlangen. Tatsächlich relevant ist jedoch das Nutzungs- bzw. Verwertungsrecht der Software, dass seitens des Erstellers anderen eingeräumt werden kann. Analog dazu verhält es sich mit digitalen Daten. Auch diese manifestieren sich durch Speicherung in IT-technischen Systemen, sind faktisch jedoch nur virtuelle Abbilder mit unterschiedlichem Informationsgehalt der Realität. Erzeugt eine natürliche, lebende Person durch eine bewusste oder unbewusste Aktion digitale Daten in einem von ihr bewusst oder unbewusst genutzten System, so unterliegen diese Daten dem Datenschutz und die Person hat zunächst das alleinige Nutzungs- und Verwertungsrecht. Sie kann dieses Recht an andere übertragen und die eigenen Daten somit zur Nutzung überlassen.

Die Fragestellung muss daher lauten: **Wer darf die Daten (aus dem automobilen Umfeld) nutzen?** Die Frage ist deswegen so interessant und bisher durchaus kontrovers diskutiert, da in einem Automobil eine Vielzahl von Daten anfallen, die rein (betriebs-) technischer Natur sind (z.B. Betriebsparameter für die Menge eingespritzten Kraftstoffs in Abhängigkeit von Temperatur usw.) und andere, die direkt oder in der Folge auch für unterschiedliche Interessengruppen interessant sein können. Hier ist als Beispiel die Position und Geschwindigkeit zum Zeitpunkt eines Unfalls sowohl für die Unfallbeteiligten als auch für Polizei, Versicherer und Hersteller interessant.

3.2 Datensicherungs-Sicht

Um Daten vor Verlust jeglicher Form zu sichern, gilt es, diese – soweit technisch bzw. organisatorisch möglich und sinnvoll – durch digitale Kopien zu sichern. Auch wenn sich die technischen Möglichkeiten und Kapazitäten regelmäßig in rel. kurzen Zeiträumen um Größenordnungen verändern (vgl. Moorsches Gesetz³⁰), ist Speicherplatz und die Kapazität für eine nicht-flüchtige Sicherung von live anfallenden Daten immer limitiert.

³⁰ Quelle u.a. (Stiller, 2015)

So erzeugt ein automatisiert fahrendes Auto über die Umfeldanalyse mittels verschiedener Sensorsysteme (Kamera, RADAR, LIDAR³¹, Ultraschall usw.) Datenmengen, die mit heutigen Technologien weder technisch noch wirtschaftlich dauerhaft gespeichert werden können (Annahme Telekom von 2013: 5 GB / Monat³², Annahme Spiegel Online vom 09.01.2014: 1 GB / Minute³³). Auf der VDI/VW-Gemeinschaftstagung 2014 in Wolfsburg wurde eine Datenmenge von 430 Milliarden GB p.a. in bzw. durch Kfz erzeugte (nicht gespeicherte) Daten genannt.

Das Kfz wird damit nach den SmartMetern aus den Energieanlagen der zweitgrößte Datenlieferant im Internet der Dinge. Man wird daher auch im Automobilumfeld Datenextrakte identifizieren, die temporär (z.B. bis zur Weiterverarbeitung) bzw. dauerhaft gespeichert werden müssen. Wirklich relevante Parameter wird man zusätzlich über eine Datensicherung auf ein weiteres sekundäres Speichermedium vor Verlust sichern wollen. Hierbei sind sowohl rechtliche (Mindest- und Höchstdauer für Speicherung) als auch technologische Restriktionen zu beachten (limitierte Schreibzyklen bei Flash-Speichern oder begrenzte Haltbarkeit bei optischen Medien).

3.3 IT-Sicherheits-Sicht

Im Gegensatz zum Datenschutz, der eher ein Identitätsschutz ist, geht es bei der IT-Sicherheit bzw. Datensicherheit tatsächlich um den Schutz digitaler Daten vor Verlust, ungewollter Veränderung oder missbräuchlicher Verwendung / Diebstahl.

3.3.1 IT-Sicherheits-Normen und Gesetze

3.3.1.1 Das IT-Sicherheitsgesetz

Im Juli 2015 ist das sogenannte IT-Sicherheitsgesetz in Kraft getreten. Dies hat nicht nur Auswirkungen (u.a. Meldepflicht bei IT-sicherheitskritischen Vorfällen) für Betreiber kritischer Infrastrukturen aus den Bereichen Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen, sondern auch für Betreiber von On-Line-Shops, Hosting-Angeboten und Web-Sites. Alle Unternehmen, auf die die vorgenannten Kriterien zutreffen, haben nach dem ebenfalls neu definierten § 13 TMG "durch technische und organisatorische Vorkehrungen sicherzustellen, dass kein unerlaubter Zugriff auf die für die Telemedienangebote genutzten technischen Einrichtungen möglich ist". Hierzu sind u.a. Methoden zur Verschlüsselung nach dem Stand der Technik einzusetzen³⁴. Es ist zu begrüßen, dass offensichtliche Nachlässigkeiten beim Umgang mit Kundendaten, Passwörtern usw. nun auch mit diesem Gesetz geahndet werden können.

³¹ LIDAR: Light Detection And Ranging – dem RADAR ähnliche Methode zur Abstands- und Geschwindigkeitsmessung auf Basis von Laserstrahlen.

³² Quelle: (Telekom, 2013)

³³ Quelle: (Stockburger, 2014)

³⁴ Quelle u.a. (BSI, 2015)

Fast-Facts: IT-Sicherheitsgesetz (BRD)

- Einhaltung von Mindeststandards im Bereich IT-Security für Betreiber kritischer Infrastrukturen
- Meldepflicht für sicherheitskritische Vorfälle z.B. bei Telekommunikations- und Versorgungsunternehmen an das BSI (Kreis der meldepflichtigen Unternehmen wird zukünftig noch ausgebaut)
- Freiwillige Vorratsdatenspeicherung zur Abwehr von Störungen (3 Tage bis zu einem halben Jahr)
- Ca. 2.000 bis 18.000 Unternehmen betroffen (u.a. Zulieferer und Dienstleister: Beispiel SmartMeter)
- Betreiber von Online-Shops und Anbieter von Hosting-Produkten und Web-Servern fallen unter die Regelungen (Ausrüstung Stand der aktuellen Technik)

Auch wenn der umgangssprachliche Name des IT-Sicherheitsgesetzes etwas anderes suggeriert, gibt es weder in der EU noch in der BRD eine eigene Rechtsnorm, die die IT-Sicherheit bzw. deren Einhaltung gesetzlich und vor allem vollumfänglich regelt. Der Kern dieses Gesetzes liegt in der Anzeigepflicht systemrelevanter Unternehmen und Institutionen sicherheitskritische Angriffe auf deren IT einer zentralen Meldestelle beim BSI³⁵ anzugeben³⁶. Ob ein Automobil-Hersteller als systemrelevant einzustufen ist, wird sich dann zeigen, wenn ein großangelegter Hackerangriff ganze Automotive-Infrastrukturen lahmlegen wird. Dann wäre ggf. daraus eine bußgeldbewehrte Pflicht zur Sicherstellung der IT-Sicherheit ableitbar (vgl. § 16 Abs. 2 Nr. 3 TMG bzw. § 13 Abs. 7 TMG).

3.3.1.2 Anwendung anderer Gesetze und Normen

Aus letzterem lässt sich aber nach Ansicht des Autors ableiten, dass der fahrlässige Umgang bzw. die Nichtanwendung von Verfahren gemäß Stand der Technik im Hinblick auf Passwort-Speicherung und Übertragung incl. Hashing und Verschlüsselung künftig geahndet werden kann (z.B. auch im Rahmen des Wettbewerbsrechts). Entsprechende Verpflichtungen zur Sicherstellung von IT-Sicherheit leiten sich i.d.R. zudem aus anderen Gesetzen und Compliance-Anforderungen ab (z.B. aus dem Handelsrecht und GmbH-Gesetz³⁷ oder § 823 BGB und § 229 StGB), in denen durch allgemeine Verhaltensregeln von den handelnden Akteuren verlangt wird, Schaden von den ihnen anvertrauten Werten und Systemen abzuhalten.

3.3.1.3 Regelungsbedarf: Die DS-GVO als Referenznorm

Faktisch muss man mit Stand Mai 2019 konsternieren, dass es in der EU und in Deutschland keine eigenständige Rechtsnorm gibt, die – analog zur DS-GVO – die Regeln zur Einhaltung der Datensicherheit (IT-Security) vorschreibt und regelt. Eine entsprechende Initiative zur Erstellung und Verabschiedung einer solchen EU-weiten Norm wäre aus Sicht des Autors zu begrüßen, wenngleich sie mehr als die DS-GVO den Verwaltungs- und Administrationsaufwand gerade für kleinere Unternehmen und Institutionen auf ein angemessenes Maß begrenzen muss. IT-Sicherheit definiert sich nicht durch Dokumentation und Administration, sondern durch fachliche Expertise und deren tatsächliche Umsetzung.

³⁵ BSI: Bundesamt für Sicherheit in der Informationstechnologie.

³⁶ Quelle u.a. (BMI, 2015)

³⁷ Quelle u.a. (GmbH, 2007)

Bis es eine solche Norm gibt, kann die DS-GVO jedoch ggf. ersatzweise als Orientierung dienen und wird evtl. der (bußgeldbewährte) Hebel sein, um auch in der Automobilwelt für mehr Datensicherheit zu sorgen.

3.3.2 Bewertung von IT-Sicherheit in der Praxis

IT-Sicherheit definiert sich unabhängig von den Vorbemerkungen und den gesetzlichen Normen aus Anbietersicht jedoch immer auch aus der eigenen Anforderung und Motivation, die eigenen bzw. anvertrauten Daten vor fremden Zugriff und technisch bedingtem Verlust zu schützen. In der IT-Sicherheit werden Angriffe auf IT-Systeme als „Incident“ bezeichnet und nach Howard/Longstaff³⁸ mit einer Incident Taxonomie klassifiziert³⁹:

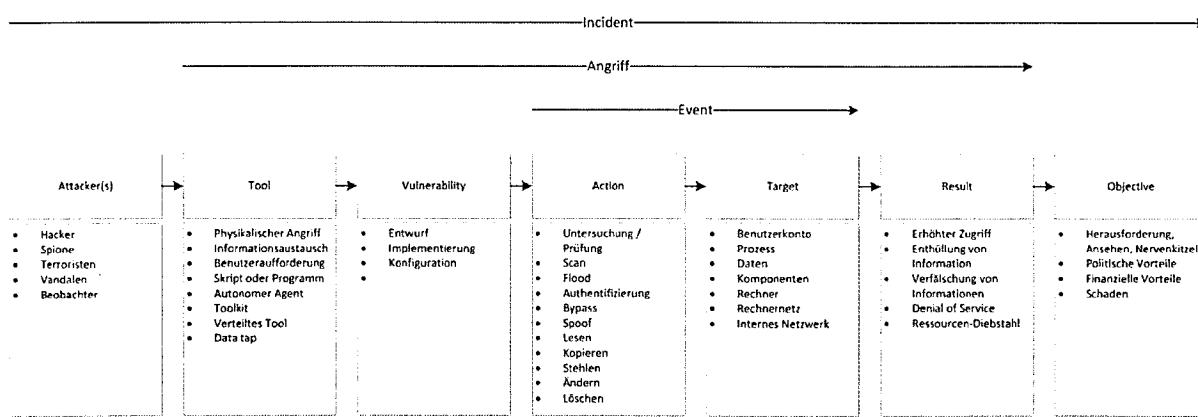


Abbildung 11: Incident Taxonomie⁴⁰

Diese Incident Taxonomie kann man auch für Angriffe auf IT-Infrastrukturen im automobilen Umfeld heranziehen (siehe auch Kapitel 4.2.3.1). Ein ungewollter Datenverlust kann nach dem Referenzprofil IT-System-Administratoren für die Personenzertifizierung nach ISO 17024⁴¹ drei Ausprägungen haben:

1. Daten sind verloren (Beispiel: Datei ist gelöscht).
2. Daten sind zerstört (Beispiel: Datei ist korrupt und unbrauchbar).
3. Daten wurden verändert (Beispiel: Datei enthält nicht die erwarteten / validen Daten).

Hierfür kann es wiederum drei Ursachen geben:

1. Verlust durch fehlerhaftes System verursacht (Beispiel: Festplattendefekt).
2. Verlust durch fehlerhafte Bedienung des Systems verursacht (Beispiel: versehentliches Löschen einer Datei durch einen Benutzer).
3. Verlust durch sicherheitsrelevantes Vorkommnis verursacht (Beispiel: Verlust durch Diebstahl durch einen Angreifer).

³⁸ vgl. (Howard & Longstaff, 1998)

³⁹ vgl. German Nemirovskij und Vasilios Tsantroukis, *Modul 9 SB 1 - IT-Sicherheit*, 2013.

⁴⁰ (Quelle: Masterstudiengang Digitale Forensik Modul 9 Kryptografie und IT-Sicherheit - SB 1)

⁴¹ Quelle: (Prehn, 2004)

Fasst man den Begriff „Verlust“ etwas weiter, so kann man das Modell auch allgemein für den Verlust der Integrität bzw. der alleinigen Hoheit über die Daten fassen. Dann ist auch der Usecase enthalten, dass die originalen Daten noch beim rechtmäßigen Nutzer vorhanden sind, es jedoch auch illegal angefertigte Kopien auf fremden Systemen gibt, die nicht unter dessen Kontrolle stehen. Die Identifizierung des Datenverlustes und die Verifizierung der Ursache resultieren in unterschiedlichen Handlungsplänen für die konkrete Reaktion (Incident Response) und der generellen Präventionsstrategie zur Verhinderung derartiger Ausfälle.

Ist erkennbar, dass ein Verlust auf ein fehlerhaftes System zurückzuführen ist, wird man einen Fault-Management-Prozess initiieren, der den Fehler beseitigt (z.B. Austausch der fehlerhaft arbeitenden Komponente). Hat eine fehlerhafte Bedienung zum Verlust geführt, resultiert dies – wenn möglich – in einer verbesserten Nutzerschulung bzw. Anwenderdokumentation oder organisatorischen Absicherung des Systems.

Ist die Ursache jedoch in einem sicherheitsrelevanten Vorkommnis zu suchen, so ist zunächst mittels Security-Management-Prozess die Systemsicherheit und -Integrität wiederherzustellen (z.B. durch Schließen der Sicherheitslücke und Entfernen der Schad-Software).

Ganz offensichtlich hat diese dritte mögliche Ursache für das weitere Handeln und in der öffentlichen Wahrnehmung die weitreichendsten Konsequenzen, ist jedoch bzgl. Detektion, Analyse und Gegenstrategie gleichzeitig auch am aufwendigsten, da ab einem gewissen Punkt am wenigsten vorhersehbar bzw. planbar. Es gilt, diesen Punkt bzw. das grundsätzliche Schutzniveau des IT-Systems im Design und im Betrieb so weit wie technisch möglich und wirtschaftlich vertretbar nach oben zu setzen, um die gesamte (Betriebs-) Sicherheit neben Verhinderung von technisch und organisatorisch bedingten Ausfällen zu maximieren.

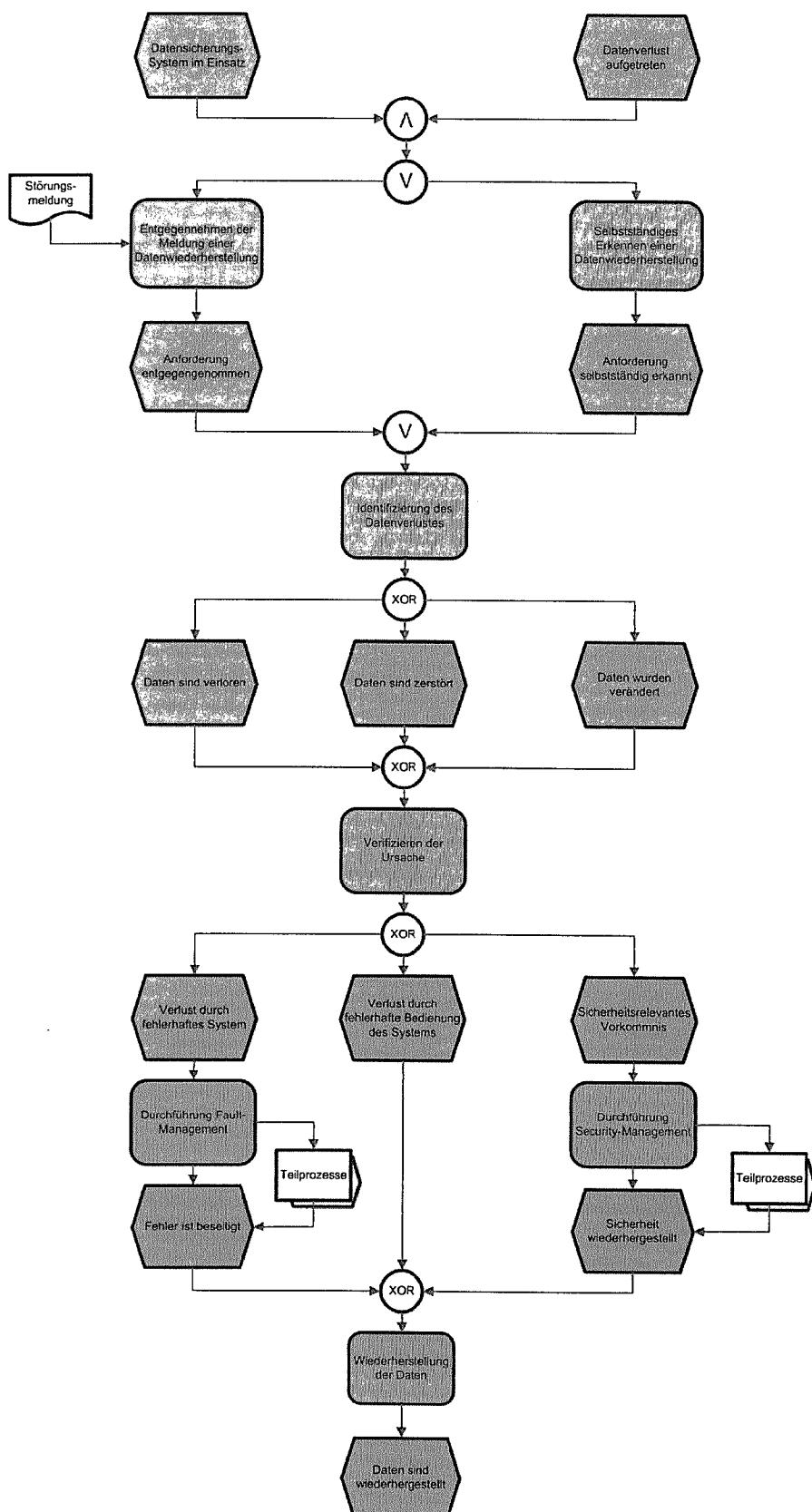


Abbildung 12: Vorgehensmodell Datenverlust nach ISO 17024 in EPK (Quelle: Fraunhofer ISST)

5.6 Mercedes Connect Me

Mercedes geht mit dem im Herbst 2014 gestarteten Dienst „Connect Me“ im Hinblick auf die Endgeräte einen anderen Weg als die Mitbewerber (hier insbesondere als BMW mit dem Dienst ConnectedDrive).

Anstatt eine betriebssystemabhängige App für die verschiedenen Smartphone- und Desktopbetriebssysteme anzubieten, wird der Telematiendienst (der mit Funktionen der Mitbewerber prinzipiell vergleichbar ist) über eine dynamisch geladene Web-App realisiert.

Dieser Ansatz ist aus Sicherheitssicht durchaus begrüßenswert, da er die Angriffsfläche reduziert und einen wesentlichen Analyse- und Missbrauchsansatz – nämlich den Zugriff auf eine lokal installierte Applikation mit den in den vorangegangenen Kapiteln und im Anhang gezeigten sehr mächtigen Analysewerkzeugen – unterbindet.

Eine Sicherheitsanalyse der Web-App verbietet sich aufgrund des Systemaufbaus (Hosting auf einem fremden System mit Zugangssicherung) für den Autor ohne ausdrückliche Erlaubnis des Herstellers / Betreibers (vgl. u.a. § 202a StGB). Mehrfache Anfragen bei Daimler, ob dem Autor valide Datensätze von Testfahrzeugen zur Analyse bereitgestellt werden und eine Sicherheitsüberprüfung erlaubt würde, wurden negativ beantwortet.



Abbildung 140: Mercedes Connect Me Startbildschirm

5.7 Audi MMI-Connect / myAudi

Auch Audi ist in der Zwischenzeit mit einem zu Mercedes und BMW vergleichbaren Dienst an den Start gegangen und ermöglicht beispielsweise das Öffnen und Schließen der Türen und Fenster oder das Abfragen von Betriebsparametern.

Da der Autor im Sommer 2016 nun auch Zugriff auf einen Audi A4 hatte, konnten – ähnlich zu den früheren Versuchen mit dem eigenen BMW – vergleichbare Untersuchungen auch mit diesem System durchgeführt werden.

Hierbei wurde die App MMI Connect im Sommer 2016 analog zu den Tests des BMW ConnectedDrive sowohl in der IOS-Version (z.B. mit Snoop-IT) als auch in der Android-Variante untersucht.

5.7.1 Findings bei der App

Negativ fällt auf, dass die Oberfläche der App nicht gesperrt / sperrbar ist und z.B. das Orten des Kfz oder die Abfrage, ob es verschlossen oder nicht ist, ohne Passwort möglich ist. Der Schutz der App (bzw. des Fahrzeugs) wird hier also komplett auf die Betriebssystem-Ebene des Smartphones abgewälzt.

Positiv festzuhalten ist, dass die Zertifikate für die SSL-Verschlüsselung offensichtlich gepinnt sind. Sie lassen sich in der Android-Version nicht austauschen und so schlägt eine Man-in-the-middle-Attacke zum Mitlesen der Kommunikation fehl. Damit war es dem Autor und seinem Team somit auch nicht möglich, das benutze Protokoll per Reverse-Engineering mitzulesen und nachzubauen.

Auch in dieser App sind jedoch zahlreiche Details zum Fahrzeug abgelegt. Unschön ist zudem, dass dasselbe Passwort für die Fahrzeugkommunikation zwischen App und Fahrzeug als auch für das Audi-Portal selber benutzt wird. Schafft es ein Angreifer, dass in der App gespeicherte Passwort auszulesen, so kann er dieses auch für die Portal-Kommunikation benutzen und so den regulären Benutzer praktisch ausschließen.

Tatsächlich kann das Passwort über externes Triggern von Methoden (wie im Kapitel zu BMW Connected-Drive ausführlich beschrieben) im Klartext ausgelesen werden (IOS-App via Snoop-It und Jailbreak). Die für das Öffnen des Fahrzeugs notwendige PIN konnte im App-Verzeichnis nicht gefunden werden. Mit dem gefundenen Passwort ist es jedoch möglich, die PIN im Portal zu ändern.

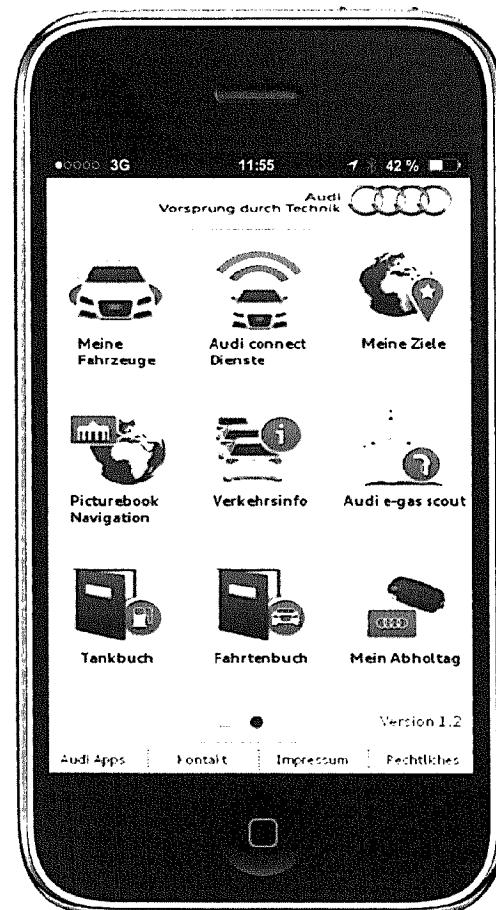


Abbildung 141: Audi App MMI Connect

Dipl.-Ing. Thomas Käfer, M.Sc. – Car-Forensics 5.0

Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, Kfz-Unfalldatenschreibern und Smartphone-Kopplung

ID	Action	Sec Class	Accessible	Timestamp
5	Read	kSecClassGenericPassword	unknown	08-09-16 14:50:46
6	Read	kSecClassGenericPassword	unknown	08-09-16 14:50:46
7	New	kSecClassGenericPassword	kSecAttrAccessibleAlways	08-09-16 14:50:46
8	Read	kSecClassGenericPassword	unknown	08-09-16 14:50:46
9	Read	kSecClassGenericPassword	unknown	08-09-16 14:50:46
10	New	kSecClassGenericPassword	kSecAttrAccessibleAlways	08-09-16 14:50:46
11	Read	kSecClassGenericPassword	unknown	08-09-16 14:50:46
12	Read	kSecClassGenericPassword	unknown	08-09-16 14:50:46
13	New	kSecClassGenericPassword	kSecAttrAccessibleAlways	08-09-16 14:50:46
14	Read	kSecClassGenericPassword	kSecAttrAccessibleAfterFirstUnlockThisDeviceOnly	08-09-16 14:50:46
15	Read	kSecClassGenericPassword	kSecAttrAccessibleAfterFirstUnlockThisDeviceOnly	08-09-16 14:50:46

Details

Timestamp: 08-09-16 14:50:47
Action: Read
Sec Class: kSecClassGenericPassword
Accessible: kSecAttrAccessibleAlways
AccessControl:
Query: class->emp_gen->AATMSGLogonManagerKeychainItem_m_Limit:m_LimitDir:_DataTrue
Data: data-RGFrXNOTWzCdw MTYh_snoop-it_string_data-DasistMist2016!

snoop-it_string_data=DasistMist2016!

Abbildung 142: Mitlesen des Passwortes beim Keychain-Zugriff

Abbildung 143: Methoden zum Auslesen des Passwortes via extern getriggerten Methodenaufruf

Gäbe es eine Trennung von Portal und App-Passwort und würde man auf Methoden verzichten, die das Passwort als Übergabeparameter herausgeben, dann wäre die Audi-App deutlich sicherer als die früheren Versionen z.B. von BMW und Ford (siehe vorangegangene Kapitel).

5.7.2 Findings Pairing-Mechanismus

Die Anbindung des Kfz an das Audi MMI bzw. an die Webschnittstelle von myAudi ist notwendig, damit man per Remote auf das Kfz zugreifen kann. Über die Webschnittstelle kann dann z.B. die Parkposition des Kfz ermittelt werden. Damit dies möglich ist, muss als erstes ein Benutzerkonto bei Audi erstellt werden. Diesem muss dann das Kfz sowie ein eigener PIN angefügt werden. Anschließend muss der Audi-Account als Hauptbenutzer im Kfz angelegt werden.

Zur tatsächlichen Kopplung des Smartphones mit dem Fahrzeug ist nun ein weiterer Konfigurationsschritt im Fahrzeug nötig. Dieser grundsätzlich zu begrüßende Vorgang, der verhindert, dass man ein fremdes Smartphone einfach nur durch Kenntnis der Portaldaten mit einem Fahrzeug koppeln kann, ist jedoch kompliziert gemacht und funktionierte bei erneuten Tests des Autors nach einem Zurücksetzen des Kfz auf Werkeinstellungen nicht auf Anhieb, was den Sicherheitsgewinn dann wieder durch mangelnde Usability in Frage stellt.

Laut Anleitung von Audi müsste man den Hauptbenutzer über die „Audi connect Nutzerverwaltung“ problemlos hinzufügen können. Im Kfz sind aber tatsächlich andere bzw. mehr Schritte notwendig. Da das Anlegen des Hauptbenutzers selbst nach mehrmaligen Versuchen nicht möglich war und immer in der gleichen „Endlosschleife“ endete, wurde der Kundensupport kontaktiert. Leider war es nicht möglich eine direkte Problemlösung bzw. einen Lösungsvorschlag zu bekommen. Die Mitarbeiterin nahm das Problem sehr genau auf, um es an die Technik-Abteilung weiter zu geben. Die konkrete Rückmeldung erfolgte erst etwa zwei Tage später und war auch noch falsch und nicht zielführend. Demnach sollte der Autor sich „vertrauensvoll“ an seine Vertragswerkstatt wenden, um dort ein notwendiges Update lokal einspielen zu lassen. Das ist an und für sich schon ein Anachronismus, denn warum kann man ein nötiges Software-Update nicht auch online einspielen. Zudem stellte sich heraus, dass die Kopplung ohne Änderung der Vorgehensweise ca. eine Woche später als der erste Versuch – wenn auch gleich umständlich – im Ergebnis problemlos gelang.

Eine solche fehlerhafte und umständliche Einrichtung ist kontraproduktiv und so ein „Kundensupport“ eines deutschen Premium-Herstellers nicht angemessen. Das wiederum führt dazu, dass man IT-Security mit umständlicher Bedienung verbindet und zugunsten der Usability oder im Marketing-Deutsch „Kundenerfahrung“ darauf verzichtet.

Fazit: Audi macht das hier etwas besser als BMW, aber auch noch nicht perfekt.



6 Technische Untersuchungen an Fahrzeugen

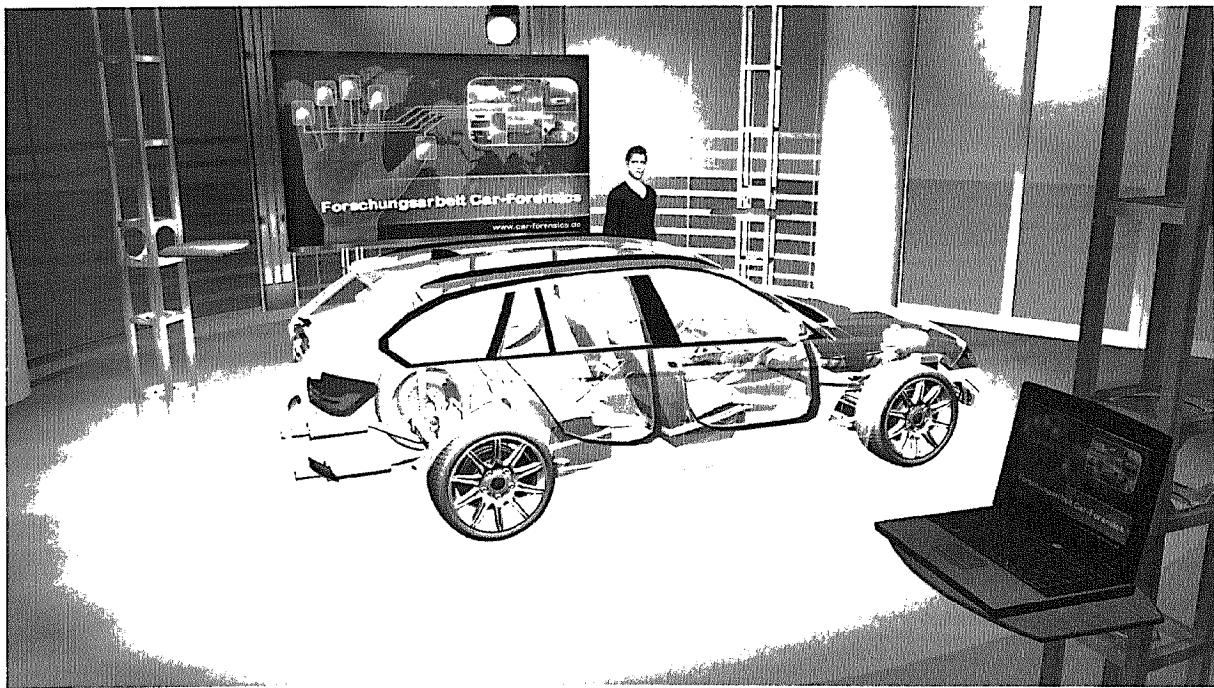


Abbildung 157: Virtuelles Labor des "Car-Forensics"-Projektes (Quelle: Eigene Visualisierung)

In diesem Kapitel wird anhand von Beispielen von Untersuchungen an Fahrzeugen bzw. Steuergeräten gezeigt, welche Angriffsvektoren für eine missbräuchliche Nutzung der Systeme bestehen bzw. denkbar sind und wie sie forensisch ausgewertet werden können.

6.1 Schnittstellen und Zugriffsmöglichkeiten

6.1.1 Zugriff auf das Fahrzeug via OBD-Schnittstelle

Ein typischer Ansatz beim Versuch, auf fahrzeuginterne Steuergeräte zuzugreifen, ist für den Forensiker genauso wie für den Hacker der Weg über die OBD-II-Diagnoseschnittstelle. Hierüber lässt sich bei allen modernen Fahrzeugen der Fehlerspeicher u.a. für die Emissionsdaten auslesen und meist auch ein erweiterter Systemzugang zumindest physikalisch herstellen. Das liegt daran, dass bei vielen Fahrzeugen heutzutage auf proprietäre Diagnoseschnittstellen verzichtet und stattdessen z.B. der CAN-Bus über freie Pins der OBD-Schnittstelle herausgeführt wird. Es kann aber auch sein, dass genau dieses nicht mehr passiert, weil die Hersteller erkannt haben, dass über diese nach außen geöffnete Schnittstelle eben auch Missbrauch betrieben werden kann und Dritte auf einfachste Weise auf den Fahrzeugbus zugreifen können. So führte beispielsweise ein Versuch, die CAN-Nachrichten mit einem über die OBD-II-Schnittstelle eines BMW-Fahrzeugs der Baureihe F31 angeschlossenen Protokoll-Analysers mitzulesen, zu keinem verwertbaren Ergebnis. Das liegt mutmaßlich an zwei Gründen. Zum einen wird der CAN-Bus möglicherweise über eine im zentralen Gateway implementierte Firewall-Funktion vor dem Mitlesen von außen abgeschottet und zum anderen erfolgt die Kommunikation über die OBD-II-Schnittstellen bei BMW-Modellen der F-Serien über ein ebenfalls dort anliegendes Ethernet-Signal.

6.1.2 Direkter Zugriff auf den CAN-Bus

Um diesem Problem zu begegnen, kann man versuchen, direkt auf den CAN-Bus im Fahrzeug zuzugreifen und die OBD-II-Schnittstelle und ein ggf. damit verknüpftes Gateway mit Firewall-Funktion zu umgehen. Dazu muss man den oder die CAN-Bus-Leitungen im Fahrzeug eben nur finden. Mit einem über das Internet für rd. 80,- € bezogenes Analysewerkzeug namens „ECS Can-Bus-Finder“ gelingt die Identifikation der CAN-Bus-Verkabelung in Fahrzeuskabelbäumen auf einfache Weise. Hierbei macht sich das Gerät die charakteristische Abstrahlung des CAN-Bus-Signals (Rechtecksignal zwischen CAN-High und CAN-Low) zu Nutze und signalisiert optisch-akustisch, wenn man sich mit dem Tester einem Kabelbaum nähert, welcher ein CAN-Signal führt. Separiert man dann die Adern noch etwas, so zeigt das Gerät an, welche der Adern CAN-High und welches CAN-Low führt.

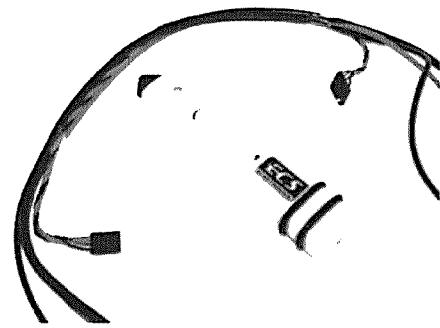


Abbildung 158: CAN-Bus-Finder
(Quelle: Eigene Aufnahme)

6.1.3 Zugriff auf Fahrzeugbusse am Beispiel von Ethernet

Ein CAN-Bus hat typischerweise eine Geschwindigkeit von bis zu 1 MBit/s. Durch Weiterentwicklung sind bis 8 MBit/s möglich. Gemessen an heute zur Verfügung stehenden Übertragungsraten im Office-Bereich von 1 bis 10 GBit/s und den auch im Fahrzeug immer wichtiger werdenden schnellen Datenleitungen (Verarbeitung von Bild- und Videodaten aus den Sensorsystemen), sind diese Datenraten aber viel zu niedrig. Daher halten nun auch im Kfz moderne Netzwerktechniken wie eben Ethernet Einzug. Teilweise wird das Ethernet-Protokoll nur für die Kapselung von CAN-Bus-Nachrichten genutzt, die nun schneller transportiert werden können. Teilweise haben die Steuergeräte aber bereits schon „echte“ Ethernet-Schnittstellen (zur Vermeidung von Flaschenhälsern bei der Übertragung der Daten zwischen den verschiedenen Systemen). Die Verwendung von Ethernet-Protokollen ist nun natürlich auch für den Hacker interessant, bedient sich die Automobilindustrie nun ihm wohl bekannter Übertragungstechniken.

Bei manchen Fahrzeugen wird über die OBD-II-Schnittstelle in Ergänzung des CAN-Bus-Signals nun auch ein Ethernet-Signal herausgeführt. Man kann sich darüber z.B. mit einem Diagnosegerät oder Notebook mit Analyse-Software via LAN-Kabel mit dem Auto verbinden. Das angeschlossene Notebook erhält via DHCP eine IP-Adresse vom Fahrzeug und ist dadurch physikalisch und logisch via Ethernet mit dem Kfz verbunden. Jetzt kann beispielsweise die Programmierung von Steuergeräten schnell und effektiv darüber abgewickelt werden. Das benötigte Kabel kann leicht selbst hergestellt oder über diverse Anbieter im Internet kostengünstig bezogen werden. Es besteht letztlich außer aus den entsprechenden Steckern und einem Stück Twisted-Pair-Kabel aus einem 510 Ohm-Widerstand, der an zwei Pins dem Fahrzeug signalisiert, dass nun ein Diagnosegerät angeschlossen ist.

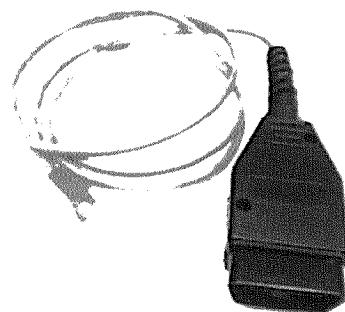


Abbildung 159: OBD-Ethernet-Kabel (Quelle: eigenes Foto)

6.2 Zugriff am Beispiel einer Head-Unit

In Zusammenarbeit mit dem Projekt ISiA (IT Security in Automotive) der Fachhochschule Aachen (Prof. Dr. Marko Schuba, Prof. Dr.-Ing. Frank Hartung, Prof. Dr.-Ing. Michael Hillgärtner und Prof. Dr.-Ing. Günter Schmitz) und auf Basis dort bereits erfolgter Abschlussarbeiten und Erkenntnisse erfolgte ein weiterer forensischer Untersuchungsansatz an einer Head-Unit durch den Autor. Hierbei wurde insbesondere die Fragestellung untersucht, ob und welche Daten aus einem im Fahrzeug eingebauten Navigationsgerät extrahiert und forensisch untersucht werden können.

Dabei interessieren den Forensiker vor allem die Daten, die über die Oberfläche des Gerätes nicht oder nicht mehr angezeigt werden. Das können z.B. gelöschte Navigationsziele oder angefahrenen Ziele sein, die nicht mehr in der Auflistung in der Benutzeroberfläche vorhanden sind, sowie weitere Spuren, die auf das Anfahren eines bestimmten Ortes (zu einer bestimmten Zeit) oder beispielsweise die Kopplung mit eindeutig bestimmten Endgeräten (wie z.B. Mobiltelefonen via Bluetooth) hinweisen. Des Weiteren ist interessant, ob Daten im Navigationsgerät tatsächlich gelöscht (also überschrieben) oder nur als gelöscht markiert werden (ähnlich dem Verfahren in anderen Betriebs- bzw. Dateisystemen).

6.2.1 Versuchsaufbau

Der Versuchsaufbau besteht hierbei aus einer handelsüblichen Head-Unit aus einem Mittelklassefahrzeug, einem dazu passenden fahrzeugspezifischen Bildschirm und der Tachoeinheit sowie der entsprechenden Kabelbäume. Im Rahmen vorheriger Abschlussarbeiten anderer Studierender wurde eine Restbussimulation entwickelt, die der Head-Unit und den Displays vorgaukelt, dass sie in einem reellen Fahrzeug verbaut sind. Die Steuerung der Head-Unit erfolgt über selbst entwickelte Software für die Restbussimulation und ein entsprechendes USB-to-CAN-Interface¹⁵³.

Die untersuchte Head-Unit beinhaltet neben einem DVD-Laufwerk für den Import von Navigations- und Mediadaten modular aufgebaute Teilsysteme zur Navigation, Medienwiedergabe und Fahrzeugkonfiguration. Die Head-Unit besitzt ein dediziertes Speichergerät in Form einer Festplatte sowie einen auf einen der Boards aufgelöteten Flash-Speicher. Hierdurch wird eine forensische Analyse des Flash-Speichers erschwert, da dieser ausgelöstet werden müsste, um ihn außerhalb des Systems untersuchen zu können. Im Rahmen einer Schwachstellenanalyse oder des Reverse-Engineerings wäre eine solche Maßnahme prinzipiell durchführbar, scheidet aber für eine übliche forensische Untersuchung aufgrund des Aufwands (vor allem initial) aus. Als Betriebssystem kommt QNX zum Einsatz, bei dem es sich um ein kommerziell vertriebenes und auf Automotive-Anwendungen angepasstes Linux-Derivat handelt. Der Autor hat eine entsprechende QNX-Lizenz für nicht-kommerzielle wissenschaftliche Zwecke beschafft, lizenziert und gesichtet.

Im Rahmen der vorherigen Abschlussarbeiten wurden verschiedene Wege zum Anschluss von Diagnosewerkzeugen an die Head-Unit erforscht und hierüber auch erfolgreich zum Zugriff auf die auf der Head-Unit enthaltenen Software und Daten eingesetzt. Es gelang den Forschern, Disk-Images der Head-Unit zu erstellen, die dem Autor nun zur weiteren Untersuchung zur Verfügung gestellt wurden.

¹⁵³ vgl. Peak, *PCAN-USB USB to CAN Interface User Manual*, 2014, I.

6.2.2 Untersuchung der Datenimages

Die Datenimages wurden vom Autor mit der Software X-Ways Forensics (Version 16.5 SR-9 x86) untersucht. Hierbei handelt es sich mutmaßlich um ein bootfähiges Image mit dem QNX Betriebssystem V 1.2b“.

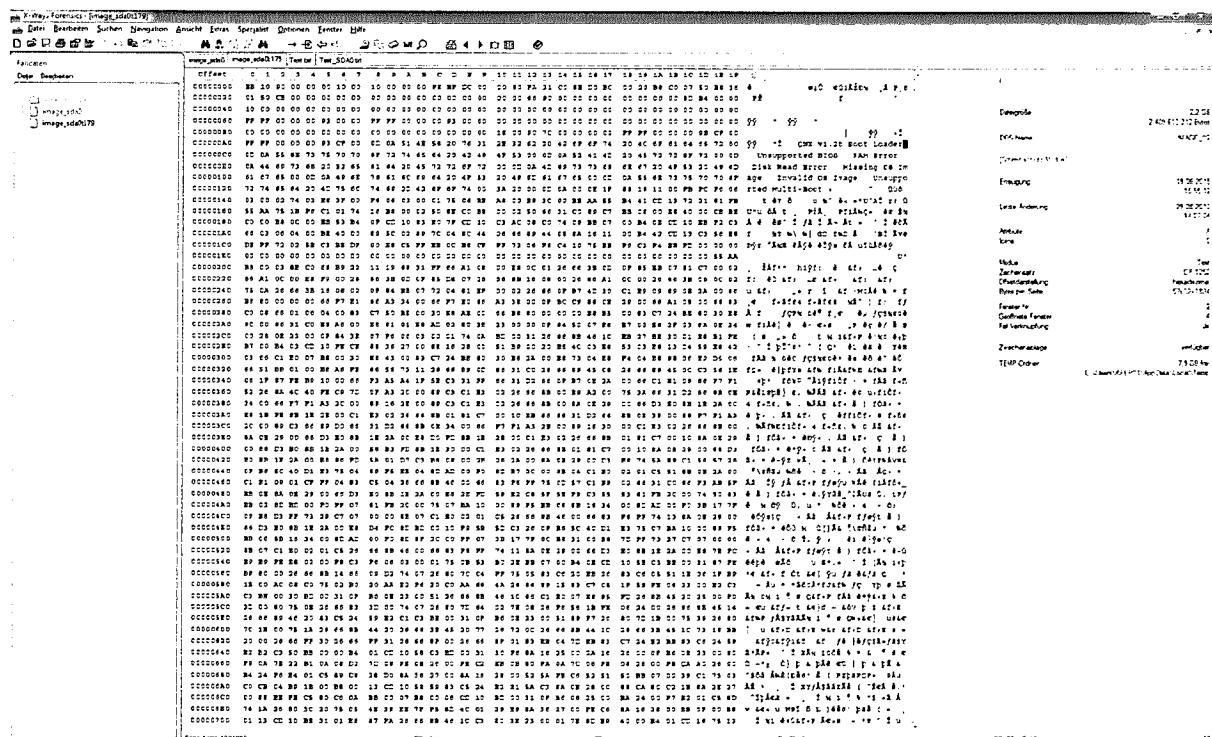


Abbildung 160: Auswertung der Images der Head-Unit via X-Ways Forensics

Mittels X-Ways-Forensic lassen sich rd. 19 MB Text (ab 10 aufeinander folgenden Zeichen) extrahieren, die teilweise zusammenhängende Informationen über Funktionsweise und weitere Fundstellen offenbaren. So findet sich unter dem Suchbegriff „select“ eine Reihe von Datenbankabfragen wie z.B. „Select Tripld From Trips where Trips.Type =? order by Trips.ArrivalTime“:

Abbildung 161: Textfundstellen Head-Unit

Diese Information könnte bei Auffinden der zugehörigen Datenbank hilfreich sein, um tatsächlich gespeicherte Daten zu finden.

6.2.2.1 Interessante Fundstellen

In dem Image „HU-Flash-Complete“ fanden sich nach Entpacken eine Reihe von interessanten Dateien (z.B. vier Dateien mit ssh-Konfiguration und RSA und AES Schlüsseln und Klingeltönen nach Marken sortiert). In der Oberfläche der Head-Unit kann man noch eine gespeicherte Bluetooth-Kopplung finden („XXXXXX iPhone“). Die Suche in X-Ways nach dem Namen des Forschers (XXXXXX) liefert 46 Fundstellen in drei Verzeichnissen und sechs Dateien:

Die Datei „LOG_00000001“ enthält Einträge für den Computer „XXXXXX-Laptop“ mit der IP-Adresse 172.16.222.106 incl. zugehöriger Mac-Adresse 00:21:6a:85:fc:08 sowie das iPhone „XXXXXX-iPhone“ mit der IP-Adresse 172.16.222.101 und der zugehörigen MAC-Adresse.

```
<GCF 000641 TS_10_0000020819>EVNT SGBluetoothGap_BSS_GAP_NAME=BSS_GAP_DEVICE_LIST_CHANGED name_list={ 'XXXXXX€'s iPhone', 'XXXXXX-LAPTOP', 'jehoBTTest0', 'HTC MSM8660' } address_list={ 'MAC XXXXXXXXXXXX', 'MAC XXXXXXXXXXXX', 'MAC XXXXXXXXXXXX', '18:87:96:48:76:A1' } class_of_device_list={ 7995916, 4063500, 4325900, 5898764 } security_list={ BSS_GAP_SECURITY_AUTH_SSP_UNTRUSTED, BSS_GAP_SECURITY_AUTH_SSP_UNTRUSTED, BSS_GAP_SECURITY_WEAK_UNTRUSTED, BSS_GAP_SECURITY_AUTH_SSP_UNTRUSTED } connection_list={ BSS_GAP_CONNECTION_NOT_IN_RANGE, BSS_GAP_CONNECTION_NOT_IN_RANGE, BSS_GAP_CONNECTION_NOT_IN_RANGE, BSS_GAP_CONNECTION_NOT_IN_RANGE } reason=BSS_INITIALIZATION;
<GCF 000628 TS_10_0000020819>EVNT MediaCtrl NAME=BSS_GAP_DEVICE_LIST_CHANGED name_list={ 'XXXXXX€'s iPhone', 'XXXXXX-LAPTOP', 'jehoBTTest0', 'HTC MSM8660' } address_list={ 'MAC XXXXXXXXXXXX', 'MAC XXXXXXXXXXXX', 'MAC XXXXXXXXXXXX', '18:87:96:48:76:A1' } class_of_device_list={ 7995916, 4063500, 4325900, 5898764 } security_list={ BSS_GAP_SECURITY_AUTH_SSP_UNTRUSTED, BSS_GAP_SECURITY_AUTH_SSP_UNTRUSTED, BSS_GAP_SECURITY_WEAK_UNTRUSTED, BSS_GAP_SECURITY_AUTH_SSP_UNTRUSTED } connection_list={ BSS_GAP_CONNECTION_NOT_IN_RANGE, BSS_GAP_CONNECTION_NOT_IN_RANGE, BSS_GAP_CONNECTION_NOT_IN_RANGE, BSS_GAP_CONNECTION_NOT_IN_RANGE }
```

In derselben Datei findet man auch eine Reihe von Einträgen ähnlich wie folgendes Beispiel: DAB¹⁵⁴ Info#AMS timeout valid on F=1466656 kHz FAST mit wechselnden Frequenzen.

These: Das System versucht offensichtlich systematisch, die aktuell empfangbaren Radiosender durch Abtasten der Frequenzen zu ermitteln und in eine Liste verfügbarer Sender zu speichern. Theoretisch wäre es nun möglich, den geografischen Aufenthaltsplatz des Fahrzeugs anhand der zum Zeitpunkt X gespeicherten Sender zu ermitteln, da es für jeden Punkt der Erde eine räumlich begrenzte Fläche gibt, in der nur ein ganz bestimmtes Set von Radiosendern (Frequenzen) empfangen werden kann. Dies könnte mit entsprechendem Aufwand dazu benutzt zu werden, um zu beweisen, dass sich ein Fahrzeug zu einem Zeitpunkt t in so einer Region befunden hat oder genau dies zu widerlegen. Dazu müsste jedoch auch ein Zeitstempel valide aus dem Dateidatum und den Logeinträgen abgeleitet werden können. Ob dies so ist, kann anhand dieses einen Images nicht festgestellt werden. Zudem wird diese Liste flüchtig sein. Eine forensische Analyse könnte also nur gelingen, wenn das relevante Set zum fraglichen Zeitpunkt „eingefroren“ worden ist und unmittelbar ohne erneutes Starten eines Scans ausgewertet wurde. Das stellt natürlich den Nutzwert des Untersuchungsansatzes wieder in Frage.

¹⁵⁴ DAB: Digital Audio Broadcasting

Unklar ist zudem derzeit, woher diese Logdatei stammt und ob diese bei jedem Systemstart erzeugt wird oder ob diese ggf. durch die Analyse eines anderen Forensikers vorher nur manuell initiiert wurde:

Header der Datei (auszugsweise):

```
<TraceRecorder (alias /dev/gnlogger), Version 0.0.0.1>
<Hostname 'hu-intel'>
<Starting UDP listener>
<Connecting 127.0.0.1:851>
<request debuglevel 2>
<<<time 01.01.2000 00:38:17>
```

Die Datei „devicelist.dat“ enthält bekannte / gekoppelte Geräte.

Die Datei pss_config.cfg enthält die Konfigurationsparameter u.a. für die Bluetooth- und WLAN-Verbindungen, so u.a. den IP-Adressbereich für DHCP-Leases 172.16.222.100, 172.16.222.110 bei einer Subnetmask 255.255.255.0 und einer Server-Adresse (incl. DNS und Standard Gateway) von 172.16.222.1.

```
#> PhoneService.DeviceName = /dev/sdn_ba
PhoneService.SvcCommandLine = /etc/init.d/phone_start, Phone2, Headset, Phone1, Phone3
PhoneService.ChannelQueueSize = 200
PhoneCtrl.SCOConnectTimeout = 50
PhoneCtrl.SCOConnectMode = 0
PhoneCtrl.SCOConnectType = 0
PhoneCtrl.SCOConnectType_BT
Phone3.Bluetooth = 1
Phone3.ProviderCodeFile = /opt/conn/etc/prvcode.tab
Phone3.Name = BluephoneSecondary
Phone3.Disposition = PHONE_DISPOS_DYNAMIC
Phone3.DHCP_DNS_Conce = 1
Phone3.DHCP_DNS_Servers = 172.16.222.1
Phone3.DHCP_Timer_ID = 4000
Phone2.Type = PHONE_TYPE_MAD
Phone2.ProviderCodeFile = /opt/conn/etc/prvcode.tab
Phone2.Name = MADPhone
Phone2.Disposition = PHONE_DISPOS_UNDEFINED
Phone2.DriverVendor = PHONE_VENDOR_STEER
Phone2.DriverModel = PHONE_MODEL_PHONE_TCS
Phone2.Disposition = PHONE_DISPOS_STATIC
Phone2.AttChannels = 1
Phone2.Bluetooth = 0
Phone2.BluetoothType = TYPE_BT
Phone1.Bluetooth = 1
Phone1.ProviderCodeFile = /opt/conn/etc/prvcode.tab
Phone1.Name = Bluephone
Phone1.Disposition = PHONE_DISPOS_DYNAMIC
Phone1.DHCP_DNS_Conce = 1
Phone1.DHCP_DNS_Servers = 172.16.222.1
Phone1.DHCP_Timer_ID = 4000
NetworkingService_wsp0.interrdhcp = manual
NetworkingService_wsp0.ipmode = static
NetworkingService_wsp0.ipaddress = 172.16.222.1
NetworkingService_wsp0.changrange = 172.16.222.100, 172.16.222.110
```

Abbildung 162: Konfigurationsparameter

6.2.3 Erkenntnisse

Alle diese Informationen können dazu benutzt werden, zu beweisen (oder ggf. zu widerlegen), dass ein bestimmtes Endgerät mit dem Fahrzeug gekoppelt war. Durch Austausch der entsprechenden Dateien im Image bzw. auf dem Livesystem ließe sich das HMI zumindest optisch und akustisch anpassen und allerlei Unfug treiben (Ansatz Scareware z.B. durch Austausch des Splashscreen o.ä.).

6.2.4 Systematischer Analyseansatz

Zur systematischen Analyse der in der Head-Unit gespeicherten Daten und Beantwortung der Frage, welche Bewegungsdaten gespeichert und wie diese gelöscht werden, ergibt sich folgende mögliche Strategie:

- A1 Herstellen einer physikalischen Diagnoseverbindung zur Head-Unit
- A2 Herstellen einer logischen Diagnoseverbindung zur Head-Unit
- A3 Ermitteln bzw. Brechen des Zugangsschutz
- A4 Login mittels einer Shell (Telnet, SSH), um auf die Daten zugreifen zu können.

Sind diese vorbereitenden Tätigkeiten erfolgreich abgeschlossen, so folgen nun die tatsächlichen Datenextraktionen.

1. Löschen aller Benutzerdaten über die Oberfläche der Head-Unit.
2. Kopieren der Daten auf einen angeschlossenen USB-Speicher (Image „Created“).
3. Erstellen von Nutzerdaten (Navigationsziele eingeben und speichern, Endgeräte koppeln, Anrufe tätigen, Adressbücher importieren, Musiksammlung importieren). Bei den Navigationszielen sind so viele Ziele einzugeben, dass die Liste „Letzte Ziele“ nicht mehr alle eingegebenen Ziele enthält.
4. Erneut Image erstellen (Image „Written“).
5. Vergleich der Images „Created“ und „Written“ zur Feststellung, welche Daten sich durch Benutzerinteraktion geändert haben bzw. neu hinzugekommen sind.
6. Einzelne Daten löschen.
7. Erneut Image erstellen (Image „Deleted“).
8. Vergleich der Images „Deleted“ und „Written“ zur Feststellung, welche Daten sich durch das Löschen geändert haben bzw. entfallen sind.
9. Forensische Suche, ob Daten wirklich gelöscht wurden oder nur als gelöscht markiert wurden.

Als Ergebnis könnte ermittelt und bewiesen bzw. widerlegt werden, welche Daten gespeichert werden und ob diese auch noch nach dem Löschen durch den Anwender Spuren hinterlassen haben.

6.2.4.1 Forensische Auswertung einer Head-Unit

Um eine solche systematische Untersuchung aus forensischer Sicht z.B. bei Vorliegen eines entsprechenden Gutachtenauftrages durchführen zu können, gilt es, eine physikalisch und logische Verbindung zwischen einer Forensik-Workstation und einer Head-Unit in einem Fahrzeug herzustellen. Diese sollte im Idealfall im eingebauten Zustand in einem reellen Fahrzeug stattfinden.

6.2.4.2 Zugriff auf die Head-Unit über Ethernet-Schnittstellen

Die Head-Unit wurde zerlegt und bzgl. ihrer Netzwerkschnittstellen analysiert. Demnach gibt es zwei Ethernet-Schnittstellen, über die die Head-Unit angesprochen werden kann. Zum einen kann das über eine im OBD-Stecker durchgeschliffene Ethernet-Schnittstelle erfolgen, die man mit einem OBD-auf-RJ45 Adapter und einem dort integrierten 510 Ohm-Widerstand zur Aktivierung der Diagnosefunktion nutzen kann. Zum anderen gibt es an der Head-Unit selber eine Rear-Seat-Entertainment Ethernet-Schnittstelle (RSE). Letztere kann über einen HSD-Rosenberg auf RJ45-Umsetzer und ein 1:1 Patchkabel an die Forensik-Workstation angeschlossen werden.

Erkenntnisse:

- Identifikation und Beschriftung der Ports anhand der Aufdrucke auf dem Mainboard. Hier: Identifizierung des Ethernet-Boards und Anschluss mittels HSD-Rosenberg auf RJ45-Umsetzer und 1:1 Patchkabel.
- Der QR-Code liefert keine direkt verwertbare Information und beinhaltet vermutlich eine Seriennummer zur Identifikation (180267064698410202359693).
- Untersuchung mittels Kali-Linux: Konfiguration der IP-Adresse des Forensik-PCs mittels sudo ip addr add 160.48.199.212/24 dev eth0.

- Programm netdiscover findet die Head-Unit offenbar über ein Abfangen eines Arp-Requests und bestätigt somit die These, dass es sich bei der Zieladresse um die 160.48.199.99 handelt.
- Es erfolgt ein nmap-Portscan über alle Ports 1-65535 mittels Befehl „nmap -v -p1-65535 160.48.199.99“
- Über RSE (Rear Seat Entertainment Schnittstelle) finden sich keine offenen, nutzbaren Ports.
- An der OBD-II-Schnittstelle liegt ebenfalls ein Ethernet-Signal an. Dessen Nutzungsmöglichkeit für forensische Aspekte war zu überprüfen.

6.2.4.3 Ausleseversuch der Festplatte

Die untersuchte Head-Unit besitzt eine 200 GB große SATA-Festplatte (Modell Toshiba), die unterhalb des DVD-Lesegerätes eingebaut ist. Die Harddisk wurde zu Analysezwecken ausgebaut und an den Forensik-PC des Autors angeschlossen. Ein Ausleseversuch mit X-Ways-Forensics scheiterte jedoch aufgrund von Lesefehlern.

Zu eruieren war, ob der Fehler auf Seiten des Auslese-Versuchsaufbaus liegt oder die Festplatte tatsächlich einen Defekt aufweist. Es könnte auch sein, dass der Fehler bewusst eingebaut ist und vom Zielsystem ignoriert wird (um dadurch eine forensische Analyse zu unterbinden).

Hierzu wurde der Versuchsaufbau mit und ohne installierte Festplatte gestartet.

Erkenntnis: Die Head-Unit bootet auch ohne installierte Festplatte, bei Zugriff auf Menüpunkt Multimedia/Musiksammlung ist jedoch kein Eintrag zu sehen (sonst Anzeige: 0/0). Bei Zugriff auf Navigations-Funktion erscheint die Meldung „Navigationssystem wird gestartet“. Mit installierter Harddisk erscheint ansonsten das Menü für die Eingabe der Ziele.

Da auch bei einer Internet-Recherche in einschlägigen Foren zwar das Problem, aber keine passende Lösung gefunden wurde und auch Klon-Versuche mit DD¹⁵⁵ und anderen gängigen Duplizierungswerkzeugen wegen der Lesefehler fehlschlug, hat der Autor die Versuche abgebrochen, die Festplatte auszulesen. Ohnehin wird hier nur erwartet, dass sie Mediendaten (hochgeladene Audiofiles und die Kartendaten des Navigationssystems) nicht aber die viel interessanteren Daten, wie z.B. die letzten Navigationsziele enthält. Diese werden auf dem Flash-Speicher der Head-Unit vermutet.

6.2.4.4 Einbinden des Images in die QNX-Entwicklungsumgebung

Zur weiteren Analyse könnte man das Image in eine mit der QNX-Entwicklungsumgebung ausgestatteten virtuellen Maschine (Oracle VM Box) importieren und dort in QNX laden.

Von diesem Versuch wurde mangels Generierungsfähigkeit neuer Images mit Prüfdaten Abstand genommen.

¹⁵⁵ DD: Tool zum Erstellen einer Bit-genauen Kopie einer Festplatte zur forensischen Auswertung (Wortbedeutung nicht exakt erklärt: duplicate data“, „disk dump“, „duplicate device“).

6.2.5 Untersuchung am Fahrzeug

An einem dem Autor zur Verfügung stehenden Fahrzeug mit baugleicher Head-Unit wurden nun weitere Untersuchungen und Zugriffsversuche unternommen.

6.2.5.1 Eingesetzte Werkzeuge

In einschlägigen Foren findet man Anleitungen zum Bau oder Bezug des benötigten OBD-Ethernet-Kabels und Download-Möglichkeiten für die zugehörige Diagnose-Software. Mit einer solchen Diagnosesoftware, wie sie auch bei Vertragswerkstätten eingesetzt wird, kann das Fahrzeug analysiert und Software-Parameter in verschiedenen Steuergeräten verändert werden.

Aber auch ein Angriff mit IT-Hackertools ist möglich. Mittels Werkzeugen aus der Kali-Linux-Distribution (u.a. netdiscover und nmap) lässt sich bei Anschluss eines PC an das Ethernet-Kabel die IP-Adresse des Fahrzeugs herausfinden (Zentrales Gateway). Ein anschließender Portscan mit nmap zeigte einen offenen Telnet-Port (23), der sich jedoch nicht für ein Login nutzen ließ (kein Login-Prompt).

Update 04/2019: In diesem Zusammenhang ist eine Forschungsarbeit von Compuhack aus dem Frühjahr 2018 interessant, bei die Forscher dort an Fahrzeugen anderer Hersteller offenbar einer ähnlichen Vorgehensweise gefolgt sind und hierbei tatsächlich einen Systemzugang herstellen konnten.

6.2.5.2 Forensische Zielsetzung

Eine mögliche Aufgabenstellung aus forensischer Sicht könnte lauten, digitale Spuren in der Head-Unit eines Fahrzeugs zu suchen, die eine bestimmte These erhärten oder widerlegen. Das könnten zum Beispiel Navigationsziele sein, die in der Oberfläche nicht mehr angezeigt werden (Liste ist auf x Einträge limitiert) oder bewusst über sie gelöscht worden sind. Genauso könnten Spuren gesucht werden, die auf eine Benutzung des Fahrzeugs durch eine bestimmte Person hinweisen. Hier wäre z.B. Name und Mac-Adresse eines dem Benutzer zugeordneten Smartphones in den Daten der Head-Unit zu suchen (vgl. Fundstellen aus Kapitel 6.2.2.1).

6.2.5.3 Analysestrategie

Die Erkenntnisse aus den Abschlussarbeiten des Projektes ISIA und der eigenen Untersuchungen am Fahrzeug des Autors legen nahe, dass entweder der Speicher, auf dem diese Daten permanent abgelegt werden, aus dem Fahrzeug / der Head-Unit entnommen und mit entsprechenden Werkzeugen direkt analysiert wird oder ein Diagnosezugang identifiziert werden muss, über den ein Zugriff bzw. Download der Daten gelingt.

Es wird vom Autor ja vermutet, dass es in der -Head-Unit zwei Arten von Speicher gibt: Einen fest auf einer Platine verlötzten Flash-Speicher, der mutmaßlich genau die Konfigurations- und Bewegungsdaten beinhaltet, die forensisch von Interesse sind und die bereits erwähnte Festplatte. Diese enthält ganz offensichtlich Kartendaten für die Navigation und mutmaßlich auch die Musiksammlung. Ob hier auch Navigationsdaten gespeichert sind, ist fraglich und eher unwahrscheinlich. Ein Auslösen des Flashspeichers und eine anschließende Analyse verbieten sich aus wirtschaftlichen Gründen, da dadurch das Mainboard der Head-Unit unbrauchbar wird.

Damit dies auch einen für die Praxis relevanten Bezug hat, müsste eine solche Analyse auch an einem Serienfahrzeug und ohne Ausbau der Head-Unit bzw. der Festplatte / des Flash-Speichers möglich sein. Hierbei wird unterstellt, dass es generell einen Entwickler- bzw. Werkstattzugang gibt, der über die Parametrierung des Steuergerätes freigeschaltet werden kann. Es könnte auch sein, dass die Head-Unit einen FTP-Server bereitstellt, über den Daten und Firmware-Updates hoch- und heruntergeladen werden können. Hierzu fanden sich nach Recherchen im Internet entsprechende Quellen und Tools.

Die verschiedenen Zugriffs- und Analyseversuche wurden, da sie mehrfach keinen Erfolg bzw. weiteren Erkenntnisgewinn für die zentralen Fragestellungen der Forschungsarbeit brachten, zunächst eingestellt.

6.2.6 Untersuchungen an anderen Fabrikaten

Im Laufe der Zeit wurden weitere Untersuchungen an Fahrzeugen verschiedener anderer Firmen vorgenommen, bei denen unterschiedlichste Adapter für die OBD-Schnittstelle eingesetzt wurden. Je nach Fabrikat und verfügbarer Software war es mehr oder weniger aufwändig, Veränderungen in der Codierung vorzunehmen oder Steuergeräte auszulesen.

Des Weiteren wurden zahlreiche Untersuchungen im Auftrag von Firmen (Pen-Tests) durchgeführt, über die leider an dieser Stelle nicht berichtet werden kann.

6.3 Forensische Auswertungsmöglichkeiten von fahrzeughnahen Systemen

Vor allem die konkreten Untersuchungen an Fahrzeugen, Steuergeräten und Head-Units sowohl durch die Kollegen des Projektes ISiA als auch durch den Autor selber zeigen sehr deutlich die Möglichkeiten aber auch die Grenzen für eine forensische Auswertung. Das Beispiel des Retrofit-Steckers mit der gekoppelten Smartphone-App zeigt auf der anderen Seite, wie schnell der vermeintliche Schutz eines proprietären Systems u.a. durch Verschleierung durchbrochen wird. Hier wird dann das unsichere Smartphone zum Zugangsschlüssel zu den begehrten Daten.

Mit zunehmender Digitalisierung der Fahrzeuge steigt auch die Zahl der Quellen an, die mit Werkzeugen der digitalen Forensik untersucht werden können. Jedoch ist der Aufwand im Einzelfall durchaus erheblich. Mangels bisher standardisierter Schnittstellen für einen Datenzugriff, einheitlichen Stellen, an den Daten im Automobil abgelegt werden (Systemprotokolle wie bei Office-Betriebssystemen) und frei zugänglicher Dokumentationen oder gar Unterstützung durch die Hersteller, muss der Forensiker i.d.R. das zu untersuchende System per Reverse Engineering analysieren, bevor er mit der eigentlichen Spurensuche und Auswertung beginnen kann. Hier „schützt“ die große Heterogenität der Embedded Systeme und die Abwehrhaltung der Automobilindustrie (Security by Obscurity) zunächst vor einer schnellen und erfolgreichen Analyse.

Spielt Zeit und damit Geld keine Rolle, so wird dieser letztlich schwache Schutz im Endeffekt meist dennoch zu brechen sein. Das erschwert eine sachverständige Bewertung und Sachverhaltsaufklärung, da sich der Aufwand vor allem bei einer zivilrechtlichen Auseinandersetzung in einem wirtschaftlich vertretbaren Maß zum eingetretenen Schaden bzw. Streitwert bewegen muss. Im Gegensatz dazu wird der Aufwand bei der Aufklärung eines Kapitalverbrechens oder gar eines schwerwiegenden Angriffs auf Staat und innere Sicherheit (Terror etc.) keine Rolle spielen und damit auch kein Hemmnis für die Ermittler darstellen.

Unbefriedigend für Verbraucher und Ermittler gleichermaßen ist, dass man mit ein wenig technologischem Verständnis zu dem Schluss kommen muss, dass auch in automobilen IT-Systemen Daten gespeichert werden und dass die Unterstellungen, dass dem so ist, nicht aus der Luft gegriffen sind. Allein – es fehlt der Beweis im Einzelfall bzw. ist dieser eben schwer zu erbringen. Und gibt es einen forensisch zu untersuchenden Fall, ist man vor Aufnahme der Untersuchung i.d.R. nicht sicher, ob man potentiell überhaupt Spuren finden kann, weil man nicht weiß, ob und wo das konkret zu untersuchende Fahrzeug bzw. Steuergerät bereits Daten im relevanten Umfang speichert. Das ist bei weitestgehend standardisierten und offengelegten Computer-Systemen im Industrie- und Office-Bereich anders. Der erfahrende Forensiker weiß, welche Betriebssysteme, Programme und Systeme wo welche Daten in welcher Detailtiefe potentiell aufzeichnen. Ob er dort dann auch verwertbare Spuren findet und wie diese zu interpretieren sind, ist seine eigentliche Arbeit. Im Automobilumfeld muss hier zunächst Know-How aufgebaut werden, diese Stellen zu identifizieren.

Eine freiwillige Unterstützung von Herstellerseite hat er wohl kaum zu erwarten, da dieser nicht nur die Sichtweise des Forensiker fremd ist, sondern sie mit dessen Erkenntnissen i.d.R. nicht arbeitet oder in Berührung kommt.

Dies ist meist erst der Fall, wenn es zu einem Incident gekommen ist und die Frage der Produkthaftung im Raum steht.

Interessanterweise beschäftigen sich auch die Kfz-Versicherer bereits mit dem Thema Produkthaftung. So teilte beispielsweise die Württembergische Versicherung ihren Kunden in einem Kundenbrief im Winter 2016¹⁵⁶ mit, dass sie gegenüber dem Hersteller Regressansprüche stellen wird, wenn diesem ein fehlerhaftes Produkt nachzuweisen ist. Die Aufklärung eines solchen behaupteten Produktmangel wird spannend. Und gleichzeitig – während die Versicherung den Kunden beruhigt, dass sie auch heute schon zahlt, wenn die Technik (Assistenzsysteme) versagt, rudert sie halb wieder zurück und weist darauf hin, dass der Autofahrer nicht aus seiner Verantwortung entlassen ist und den neuen Automatiksystemen gerade in der Einführungsphase besondere Aufmerksamkeit zu widmen ist.

Festzuhalten ist also schon einmal, dass es möglich ist, aus Fahrzeugen theoretisch und praktisch Daten zu extrahieren, aber der Aufwand nicht unerheblich ist. Bestimmte Sensorsysteme liefern aber entgegen der laienhaften Vorstellung keine oder nicht die erwarteten digitalen Spuren. So ist eine Auswertung einer in einem Fahrzeug verbauten Frontkamera mangels Daueraufzeichnung und weil sie kein wirkliches Videobild, sondern Objektlisten liefert, post mortem nach derzeitigen Erkenntnisstand aussichtslos.

Auch mittels Zugriff auf ein fest installiertes Navigationsgerät wird mangels standardisierter Export- bzw. Analyse-Schnittstelle nicht auf einfache Weise eine Liste aller vom Fahrer jemals angefahrenen Ziele (ggf. auch über die im HMI angezeigten Liste hinaus) zu erstellen sein. Und selbst wenn diese Liste per Reverse-Engineering aus einer Head-Unit extrahiert werden kann, ist immer noch fraglich, welchen Informationsgehalt sie für einen Rechtsfall hat. Fehlen nämlich valide Zeitstempel und Marker, ob das Ziel erreicht wurde, so handelt es sich nur um Indizien, dass ein bestimmter Ort als Navigationsziel eingeben wurde, nicht aber, dass er auch angefahren wurde und vor allem nicht von wem. Denn für letztere Aussage müsste es eine valide Kopplung zwischen individuellem Fahrer, Fahrzeug und Fahrziel bzw. Geokoordinaten geben.

Im Einzelfall kann man natürlich sehr wohl bei der Spurensuche erfolgreich sein und je nach Aufgabenstellung und zu bestätigender bzw. zu widerlegender These Indizien oder gar Beweise liefern.

In Anbetracht der in der Zukunft weiter zunehmenden Komplexität der Systeme und neuer Herausforderungen für zivil- und strafrechtliche Urteilsfindungen ist die derzeit zu praktizierende Vorgehensweise mit einem hohen Reverse-Engineering-Anteil nicht sinnvoll. Es gilt daher seitens des Gesetzgebers in einem fairen Interessenabgleich der unterschiedlichen Stakeholder Schnittstellen und Speicher zu definieren, die unter Beachtung von Datenschutz, Datensicherheit und rechtstaatlichen Prinzipien von Betroffenen, Ermittlern, Sachverständigen, Herstellern und Werkstätten für die Datenauswertung genutzt werden können.

¹⁵⁶ Quelle: (Württembergische, 2016)

Nachfolgend werden einige Beispiele von fehlerhaft bzw. unzuverlässig arbeitenden Assistenzsystemen am Beispiel eines Audi A4 Baujahr 2016 gezeigt und welche Probleme sich hierbei bei der forensischen Bewertung ergeben. Der Sachverständige kann allein die Effekte (an einem Vergleichsfahrzeug) nachvollziehen, nicht aber die konkrete (behauptete) Fehlfunktion zu einem Zeitpunkt X. Hier fehlt schlicht und ergreifend eine offengelegte und transparente Protokollierung der Betriebszustände und Fehler. Tatsächlich konnte vom Autor keiner der festgestellten Effekte durch korrespondierende digitale Spuren beim Auslesen von Fehlerspeichern nachgewiesen werden. Hier bleibt oft nur der Beweis über Videos oder Zeugen.

6.3.1 Fehlerhafte Umsetzung der StVO bei der Tempolimit-Erkennung

Die Verkehrszeichenerkennung und deren Anzeige im Fahrerinformationsdisplay bzw. Head-Up-Display bei Fahrzeugen der Marke Audi Typ A4/A4 Avant (Baureihe 8W-Baujahr 2016) in Verbindung mit der Übernahme des erkannten Tempolimits auf die aktivierte Geschwindigkeitsregelanlage ist fehlerhaft implementiert und entspricht nicht den Regeln der deutschen Straßenverkehrsordnung bzw. der zugehörigen Verwaltungsvorschrift und damit nicht dem Stand der Technik.

6.3.1.1 Problembeschreibung

Beispielhaft sind nachfolgend zwei konkrete Szenarien beschrieben und analysiert, die, soweit sich das Fahrzeug selber deterministisch verhält, reproduzierbare Resultate liefern. Bei Fahrten des Autors über bisher mehr als 15.000 km konnten zahlreiche ähnlich gelagerte Fälle beobachtet werden. Die Tempolimiterkennung ist an vielen Stellen fehlerhaft und zeigt sowohl zu niedrige als auch zu hohe Limitierungen an, die von dem ACC (Adaptive Cruise Control) bei Aktivierung auch automatisch durch Beschleunigen oder Abbremsen übernommen werden. Teilweise folgen widersprüchliche Anzeigen in kurzem Wechsel aufeinander (z.B. Wechsel von 50 auf 30 wieder auf 50 und 30 und wieder auf 50 km/h innerhalb von wenigen Metern). Die Fehlfunktionen konnten an vielen Stellen immer wieder beobachtet werden, so z.B. auch auf Autobahnfahrten, bei denen ohne erkennbaren Grund (kein Limit, kein Verkehrsschild, kein Fahrzeug voraus oder seitlich) z.B. von 120 km/h auf 60 km/h automatisiert heruntergebremst wurde. Auch in einem Tunnel konnte dieser Effekt bei erlaubten und gefahrenen 50 km/h beobachtet werden, bei dem das Fahrzeug wiederum ohne anderwärtige Anzeige abbremste und das Tempo manuell übersteuert werden musste, um einen Auffahrunfall zu vermeiden.

6.3.1.2 Missachtung von Tempo 30 Zonen

Beim Befahren der Tempo-30-Zone im Wohnort des Autors in 52146 Würselen (Bereich Wilhelmstraße von der Sebastianusstraße und Friedrichstraße vom Willy-Brandt-Ring kommend) ist zu beobachten, dass bei Erreichen des jeweiligen Zone-30-Schildes (Verkehrszeichen 274.1) kurzzeitig die korrekte Geschwindigkeitsbegrenzung 30 km/h im Fahrerinformationsdisplay bzw. Head-Up-Display angezeigt wird. Unmittelbar dahinter nach dem Abbiegen in die Wilhelmstraße bzw. Friedrichstraße schaltet die Anzeige auf 50 km/h um, obwohl dort keinerlei Aufhebungsschild (Verkehrszeichen 274.2) oder eine andere Geschwindigkeitsbegrenzung angezeigt wird. Bei aktivierter Geschwindigkeitsregelanlage (ACC) und eingeschalteter Option „Erkannte Tempo-Limits übernehmen“ beschleunigt das Fahrzeug dann selbstständig auf die fälschlicherweise detektierten und angezeigten 50 km/h.

Bei Ortsunkenntnis des Fahrers wird er diese Aktion i.d.R. nicht stoppen, da ihm ja über das im Display angezeigte Tempolimit 50 km/h suggeriert wird, dass er sich im zulässigen Geschwindigkeitsbereich bewegt und er das entsprechende Aufhebungsschild übersehen hat.

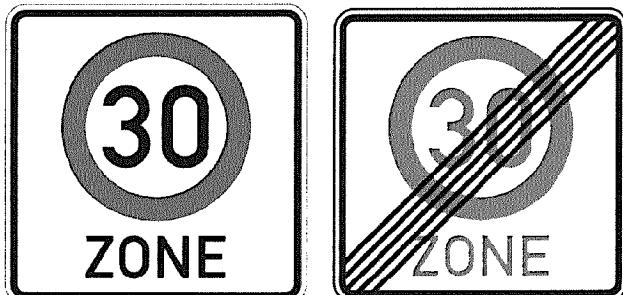


Abbildung 163: Zone 30 Verkehrszeichen 274.1 und 274.2

Gemäß StVO bzw. den Verwaltungsvorschriften der StVO wird eine Tempo-30-Zone durch das Verkehrszeichen 274.1 eingeleitet und durch das Zeichen 274.2 beendet. Die Aufhebung mittels Zeichen 274.2 ist entbehrlich, wenn die Tempo-30-Zone in eine Fußgängerzone oder einen verkehrsberuhigten Bereich übergeht.

Eine stillschweigende Aufhebung z.B. an der nächsten Kreuzung gibt es nicht. Streng genommen würde eine Tempo-30-Zone auch nicht durch ein aufgestelltes Geschwindigkeitsbegrenzungsschild mit 50 km/h oder durch ein Ortsausgangsschild aufgehoben. Da eine 30-er-Zone gemäß StVO außerhalb geschlossener Ortschaften nicht zulässig ist, wäre dies tatsächlich als impliziter Aufhebungsgrund zu sehen.

Offensichtlich sind auch in diesen Fällen die in der digitalen Karten hinterlegten Limits falsch bzw. veraltet (dann über mehr als 10 Jahre) und das System priorisiert hinterlegte Limits höher als detektierte. Durch den je nach Geschwindigkeitsunterschied zwischen gefahrenem und vermeintlich erlaubtem Tempo durchaus erheblichen Bremsereignis entsteht neben dem eindeutigen Komfortmangel ein hohes Unfallrisiko durch nachfolgende und auffahrende Fahrzeuge. Da das vorausfahrende Fahrzeug für den Nachfolger ohne ersichtlichen Grund gebremst hat und dies für ihn überraschend ist, ist davon auszugehen, dass bei einem tatsächlichen Unfall der Fahrer des vorausfahrenden Fahrzeugs eine (erhebliche) Mitschuld zugesprochen bekommt. Er wird sich dann nicht auf die Aussage zurückziehen können, dass das Fahrzeug ohne sein Zutun gebremst hat.

Der Algorithmus ist so zu ändern, dass eine per Verkehrszeichen 274.1 erkannte Tempo-30-Zone Vorrang vor allen in der Karte hinterlegten Limits beachtet wird. Solange kein Zeichen 274.2 optisch detektiert wurde, ist das Limit 30 km/h beizubehalten. Da es hierbei vorkommen kann, dass das entsprechende Aufhebungszeichen aufgrund von temporärer Verdeckung nicht erkannt werden kann, ist diese Limitierung erst dann aufzuheben, wenn dem widersprechende Verkehrszeichen (z.B. ein 50 km/h Schild, Ortsausgangsschild o.ä.) eindeutig optisch detektiert wurden. Auf digital hinterlegte Kartendaten darf erst dann zurückgegriffen werden, wenn diese eindeutig nicht im Widerspruch zu einer optisch detektierten Limitierung durch ein Verkehrszeichen stehen.

Dipl.-Ing. Thomas Käfer, M.Sc. – Car-Forensics 5.0
Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall,
Kfz-Unfalldatenschreibern und Smartphone-Kopplung

Eine verlässliche Datenquelle in Form von digitalen Kartendaten müsste hierbei täglich aktualisiert im Fahrzeug zur Verfügung stehen, nicht jedoch wie in der hier vorliegenden Form mit einem Fehler, der vermutlich schon seit mindestens 10 Jahren vorliegt. Das ist die mindestens die Zeit, in der die Tempo-30-Zone nach Erinnerung des Autors schon existiert.

Schaut man sich das zum Zeitpunkt der Untersuchung (Heruntergeladen am 09.10.2016) aktuellste und über das Audi Portal ladbare Kartenupdate mit einem Hex-Editor etwas genauer an, so stellt man fest, dass das als Version 2016/2017 deklarierte Kartenupdate offenbar Daten aus Q3/2015 enthält (Datei GermanyWest ADAS.pdf).

Abbildung 164: Versionskennung im Kartenmaterial von Q3/2015

Laut Website der Audi AG¹⁵⁷ sind bis zu fünf Kartenupdates, die im Halbjahresrhythmus erscheinen, nach der Auslieferung kostenlos: *Die aktuellen Kartenupdates können hier kostenfrei heruntergeladen und via SD-Karte im Fahrzeug installiert werden. Download und Installation können beliebig oft durchgeführt werden. Der Kartenupdate-Service umfasst die ersten fünf halbjährlich erscheinenden Updates, die der ab Werk installierten Kartenversion folgen.* Die am 09.10.2016 herunterladbare angeblich aktuelle Karte ist also tatsächlich über ein Jahr veraltet.

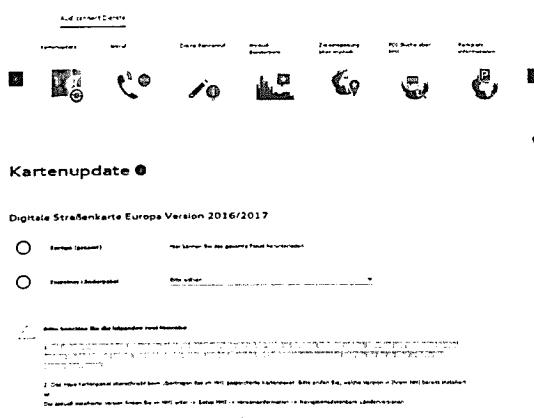


Abbildung 165: Kartenupdates der Audi AG

¹⁵⁷ https://my.audi.com/content/de/myaudi/de/home_user/vehicles/vehicle_detail.html?vin=xxxxxx#tab/services/service/kundenupdate_v1

6.3.1.3 Fehlinterpretationen vermeintlicher Tempolimits

Beim Befahren des Willy-Brandt-Rings in Richtung Aquana Freizeitbad aus Richtung Gewerbegebiet Würselen kommend zeigt das System das hinter dem Ortsausgangsschild stehende Schild 70 km/h korrekt an, zeigt dann aber in der darauffolgenden Linkskurve 50 km/h an und bremst den Wagen bei aktiviertem ACC auf 50 km/h ab, obwohl weder ein Ortseingangsschild noch ein entsprechendes Tempolimit vorhanden ist.

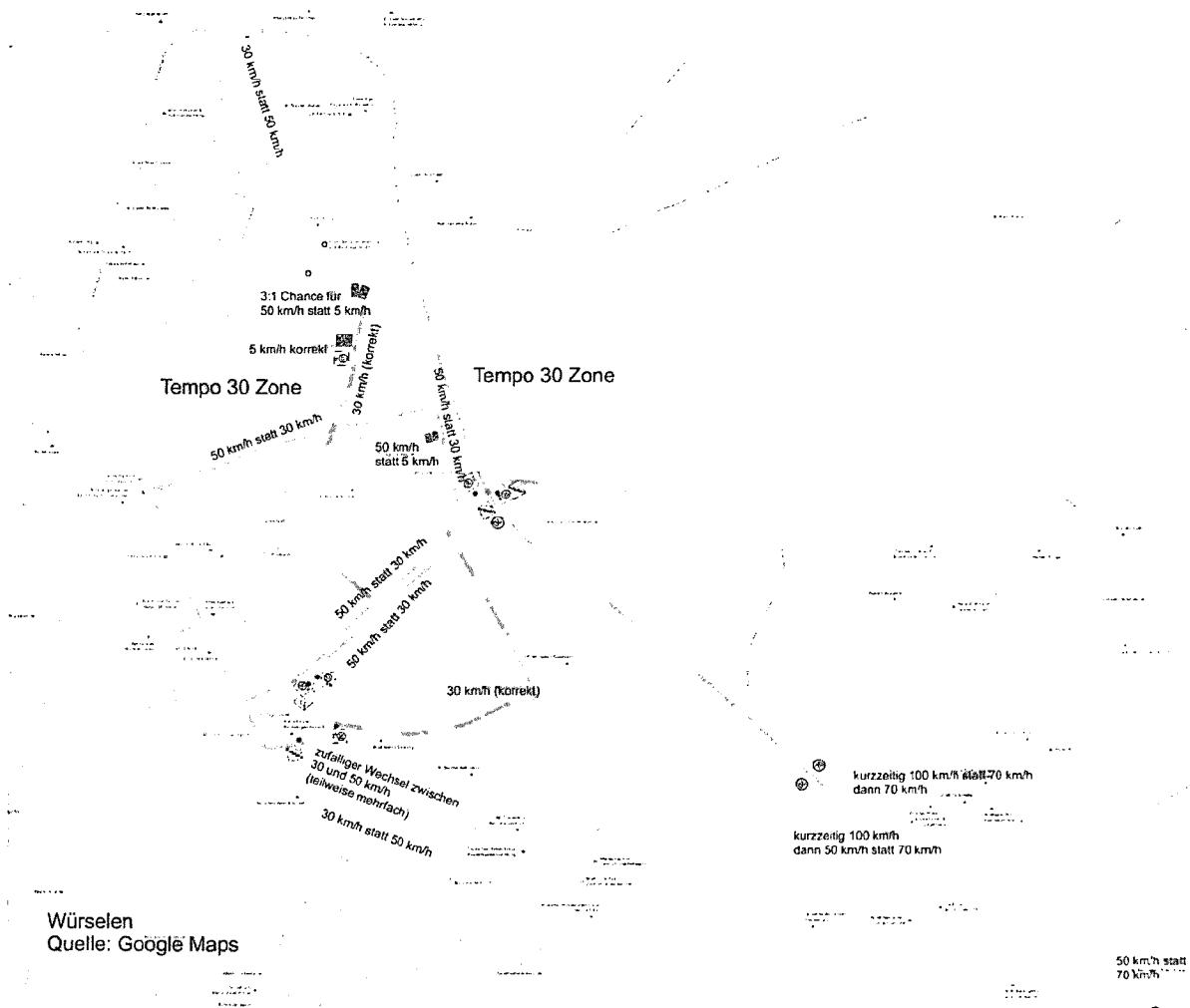


Abbildung 166: Fehlerhafte Tempolimiterkennung in Würselen

Der Vorausfahrende darf nicht ohne zwingenden Grund stark bremsen (§ 4 Abs. 1 S. 2 StVO). „Stark“ bremsen heißt: mehr als „normales“ Abbremsen, nicht unbedingt Vollbremsung (KG NZV 93, 478). Der Nachweis ist schwierig und häufig kann nur ein Gutachten helfen¹⁵⁸. Bei einem daraus resultierenden Auffahrungsfall wird dem vorausfahrenden Fahrer daher i.d.R. eine Mitschuld zugesprochen.

¹⁵⁸ Quelle: Quelle <http://www.iww.de/va/archiv/unfallschadensregulierung-checkliste-auffahrungsfall-f44899>

6.3.1.4 Feststellungen bei einem Porsche Boxster S 781 Baujahr 2016

Update 10/2016: Bei einer weiteren Testfahrt, diesmal mit einem Leihwagen Porsche Boxster S Typ 781 Baujahr 2016, der ebenfalls mit einer Verkehrszeichenerkennung – jedoch ohne Übernahmemöglichkeit auf den Tempomat – ausgestattet ist, konnten im Prinzip ähnliche Erkenntnisse gesammelt werden.

Auch das Porsche-Fahrzeug ist nicht in der Lage, die geltenden und deutlich sichtbaren Tempolimits auch nur annährend zuverlässig zu erkennen. Das deckt sich also mit den Erfahrungen im BMW 330d touring BJ 2013 und dem Audi BJ 2016. An manchen Stellen zeigen sich exakt dieselben Fehlerbilder wie beim Audi A4, an manchen abweichende Symptome. So wird z.B. beim Porsche das Zusatzschild „Gültig für Gefahrguttransporte“ unterhalb des 30er-Schildes auf der Oppener Strasse in Würselen übernommen, was der Audi korrekt ignoriert. Beim Einfahren in die Mittelstraße von der Friedrichstraße kommend wird als Tempolimit 5 km/h angezeigt, obwohl dort kein entsprechendes Schild steht oder eine Verkehrsberuhigte Zone ist. Beide Straßen befinden sich in der 30er Zone. Manche Fehldetektionen sind zudem nicht deterministisch und nicht immer reproduzierbar (Beispiel 20 km/h-Schild in Privatstraße, in die nicht eingefahren wird, bzw. 10 km/h auf einem Tankstellengelände abseits der Straße wird mal angezeigt und beim nächsten Versuch wiederum nicht). Offenbar nutzt Porsche die gleichen falschen Kartendaten und mutmaßlich auch die gleich falschen Algorithmen zur Tempolimitdetektierung. Dies wäre angesichts der Konzernzugehörigkeit nicht verwunderlich und lässt vermuten, dass die Fehler auch bei anderen Fahrzeugen aus der VW-Gruppe auftreten.

6.3.1.5 Empfehlungen

Die zahlreichen Fehldetektionen und vor allem das oft nicht reproduzierbare Verhalten entbehren nicht einem gewissen Unterhaltungswert. Sie dienen jedoch nicht dazu, das Vertrauen in diese System zu stärken, wie hier ein recht aktuelles Beispiel mit einer nun neuen Detektion von 5 km/h in der 30er Zone zeigt, die ansonsten bisher immer mit 50 km/h ebenso falsch eingestuft wurde (Würselen Bahnhofstrasse vor Einmündung Nordstraße).



Abbildung 167: Detektion von 5 km/h in 30er Zone, die sonst mit 50 km/h detektiert wird

Abhilfe:

1. Die Qualität und Aktualität der in den Karten hinterlegten Information muss dringend überarbeitet werden und für Fahrzeuge mit Online-Verbindung täglich automatisiert zur Verfügung gestellt werden.
2. Die Algorithmen für die Entscheidungsfindung sind so zu ändern, dass Sie konform zur StVO (in allen zugelassenen Ländern) gehen und das Fahrzeug bei unklarer Datenbasis nicht fehlerhaft selbst beschleunigen oder bremsen lassen. Detektierte Verkehrszeichen gehen immer vor Kartendaten.
3. Ist die Gefahr gegeben, dass Verkehrszeichen, die nur einer Nebenspur gelten fehlerhaft detektiert werden können, so ist auf diese Datenquelle für den Anwendungsfall Beschleunigung entweder zu verzichten oder der Fahrer auf die unklarer Datenbasis durch ein geeignetes Piktogramm hinzuweisen.
4. Wird ein Bremseingriff rein auf Basis von Kartendaten ausgelöst, so hat dies mit Vorwarnung des Fahrers (optisch) verzögert zu erfolgen bzw. es wird allein dem Fahrer die Entscheidung überlassen und es erfolgt kein automatischer Bremsengriff. Dies gilt umso mehr, wenn durch den Bremseingriff ein erheblicher Unterschied zur vorher gefahrenen Geschwindigkeit ausgelöst wurde. Ggf. ist allein nur ein Unterbrechen des Antriebs statt eines zusätzlichen Bremseingriffs sinnvoll (Ausrollen incl. entsprechender Anzeige).
5. Den Fahrern sollte es auf einfache Weise möglich sein, offensichtliche Karten-datenfehler an eine zentrale Stelle zu melden (z.B. durch Drücken eines Soft-buttons im Bedienmenü wie z.B. bei Smartphone-Apps). Der Kartendienstleister erhält die Daten und würde bei vermehrten Meldungen verschiedener Fahrer (anonymisiert) verdichtete Hinweise bekommen, dass die gemeldete Position zu überprüfen ist. Ein Update der Daten müsste dann in kürzester Zeit (tages-aktuell) automatisiert bereitgestellt werden. Eine Updatefrist von einem Jahr und eine umständliche und aufwändige Meldeprozedur wie bisher, ist in der heutigen Zeit und angesichts der enorm hohen Aufpreise für fest installierte Navigationsgeräte und Online-Dienste im Fahrzeug nicht mehr akzeptabel.

Mit Ausblick auf autonom fahrende Fahrzeuge sind solche Fehldetections gar nicht mehr akzeptabel, da dann ja auch der menschliche Fahrer als Korrektiv entfällt. Selbst bei teil- oder vollautomatisiert fahrenden Fahrzeugen wird von ihm nicht zu verlangen sein, die Assistenzsysteme in solcher Detailtiefe ständig zu überprüfen. Dann kann er auch gleich wieder selber fahren.

6.3.2 Fehlfunktionen Active Lane Assist und Stau-Assistent

Die im vorangegangenen Kapitel aufgezeigten Probleme mit den Assistenzsystemen bei einem Audi A4 Baujahr 2016 finden ihre Fortsetzung im aktiven Spurhalte- und Stau-Assistenten. Dieses Assistenzsystem soll das Fahrzeug durch aktiven, korrigierenden Lenkeingriff in der erkannten Spur halten und den Fahrer bei Überfahren der Fahrbahnmarkierungen ohne gesetzten Blinker durch ein im Lenkrad spürbares Moment warnen. Das System krankt jedoch an einer unerwartet niedrigen Erkennungsrate der visuell deutlich sichtbaren Spuren. Selbst bei besten Lichtverhältnissen und Trockenheit ist nicht immer gewährleistet, dass die Spuren korrekt erkannt werden. Signalisiert wird dies durch farbige Spurssymbole im Cockpit und dem optional erhältlichen Head-Up-Display.

Da der Wechsel zwischen Erkennen und Nicht-Erkennen der Fahrbahnmarkierungen fließend ist, muss der Fahrer also ständig prüfen, ob die Symbole noch aktiv sind. Bei Regen und Dunkelheit sowie in Baustellen mit gelben Markierungen, also dann, wenn so ein Assistenzsystem seine Daseinsberechtigung besonders verdient, funktioniert das System noch unzuverlässiger. Hier sind sogar komplette Systemausfälle zu beobachten (analog auch beim ACC bei extrem schwachen Schneefall oder starkem Regen zu beobachten). Schlimmer noch wiegt, dass selbst bei besten Bedingungen eine fehlerhafte Führung des Fahrzeugs zu beobachten ist. So konnte der Autor mit einem Vergleichsfahrzeug Audi A4 Allroad Baujahr 2016 in Würselen K 30 Abfahrt Aquana zur Friedrichstraße reproduzierbar ein Lenkmoment beobachten, welches das Fahrzeug aktiv über eine durchgezogene Linie auf eine Sperrfläche bis in den Gegenverkehr führte.

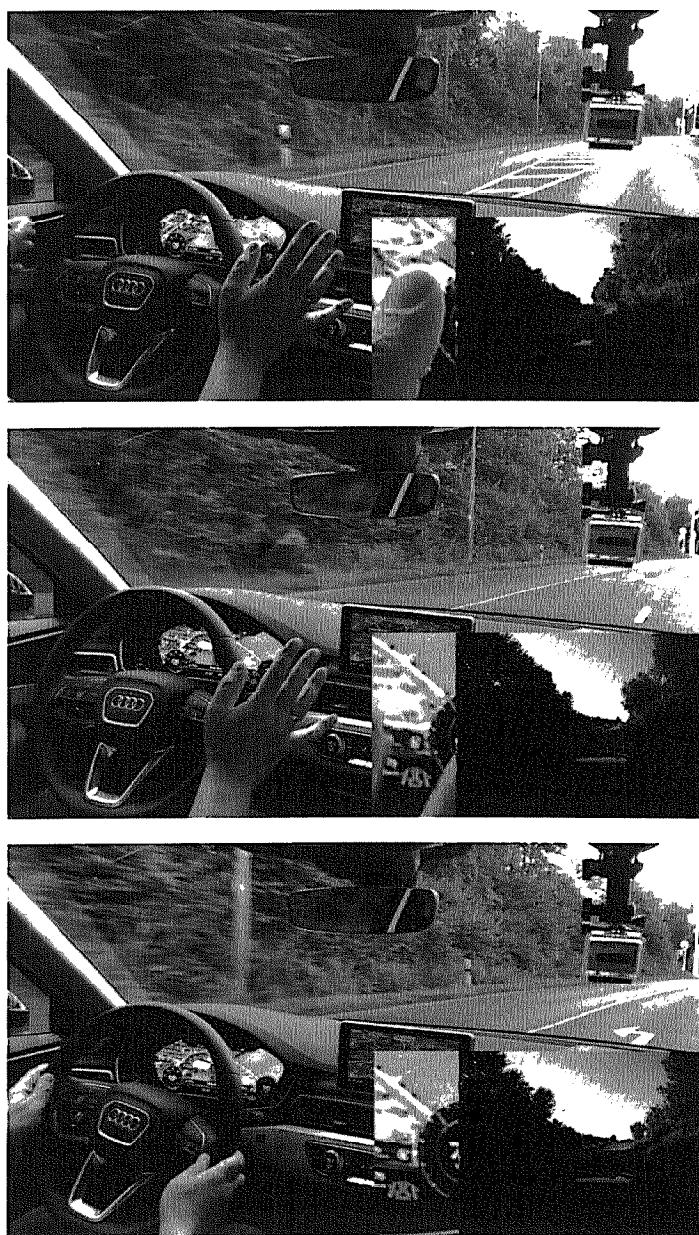


Abbildung 168: Bildsequenz aktives Überfahren Sperrfläche

Bei Regen und der Gefahr von Aquaplaning weiß der Fahrer dank ständiger (subtiler) Lenkeingriffe des Active Lane Assist übrigens nicht, ob sich die gefühlte Schwammigkeit der Lenkung auf das System oder ein Aufschwimmen der Räder zurückzuführen ist. Auch das trägt nicht zur Akzeptanz des Systems bei. Ähnliche Effekte konnten auf zahlreichen Fahrten z.B. auch auf Landstraßen beobachtet werden, bei dem sogar doppelt durchgezogenen Linien mit Nagelreihen aktiv vom System überfahren wurden. Und auch die Sinnhaftigkeit des Stauassistenten ist in Frage zu stellen. Dieser soll gem. Aussage des Herstellers¹⁵⁹ dem Fahrer die Steuerungsaufgabe abnehmen:

Audi A4 Stauassistent: Im Geschwindigkeitsbereich bis 65 km/h kann der Stauassistent, eine weitere Funktion der ACC, auch die Lenkarbeit ähnlich wie beim Audi active lane assist übernehmen, solange der Verkehr zähflüssig ist. Das System nutzt die Radar- und Ultraschallsensoren sowie die Frontkamera. Es führt das Auto durch sanfte Lenkeingriffe und folgt der vorausfahrenden Kolonne innerhalb der Systemgrenzen. Dabei orientiert sich der Stauassistent an den Fahrbahnmarkierungen und an den anderen Fahrzeugen auf der Straße. Wenn der Stauassistent seine Systemgrenzen erreicht – etwa, wenn sich der Stau auflöst oder eine enge Kurve vor ihm liegt, muss der Mensch am Steuer die Fahraufgabe wieder selbst übernehmen. Unterstützend warnt ihn das System in mehreren Stufen. Als letzte Maßnahme bringt es den A4 und A4 Avant selbsttätig zum sicheren Stillstand.

Was der Hersteller unterschlägt, ist, dass der Fahrer nach einer relativ kurzen Zeit (ca. 30 Sekunden) ein aktives Gegenlenkmoment am Lenkrad aufbauen muss, um dem Fahrzeug die Einsatzbereitschaft des Fahrers anzuzeigen. Das alleinige Festhalten des Lenkrades mit beiden Händen (z.B. wie bei einem kapazitiv arbeitendem System) ist nicht ausreichend. Man muss unnötigerweise Gegenlenken. Auch das Anfahren nach einem Stopp von mehr als 1-2 Sekunden muss manuell initiiert werden. Da zudem die Lenkbewegungen des Assistenzsystems deutlich stärker ausfallen, als aufgrund der Verkehrslage nötig und von einem menschlichen Fahrer gewöhnt, wird so ein System ad absurdum geführt. Das Vertrauen darin wird zudem erschüttert, wenn hierbei der zur Verfügung stehende Raum der Fahrspur maximal bis an die Begrenzungen (seitlich oft ohne Abstand zu daneben fahrenden Fahrzeugen oder festen Begrenzungen) „ausgenutzt“ wird oder sich das System schlagartig und nicht deterministisch abschaltet.

Um die persönlichen Erfahrungen nicht nur qualitativ, sondern auch quantitativ nachvollziehbar zu machen, wurden Messfahrten mit einem Diagnosegerät auf Video aufgenommen und typische Stausituationen sowohl mit als auch ohne Stauassistent dokumentiert und verglichen. Hierbei kam ein Diagnosegerät nebst Software der Firma Stemei zum Einsatz, mit dem man u.a. den Lenkwinkel incl. Zeitstempel kontinuierlich aufzeichnen kann. Mittels Timecode im Video (iPhone 6s mit der App Vidometer) ist ein Abgleich der Daten mit der Fahrsituation möglich.

Für den qualitativen Vergleich, wie gut der Mensch oder das Assistenzsystem die Steuerungsaufgabe gemeistert hat, kommt es offenbar auf die Anzahl und die Stärke der Lenkradbewegungen an.

¹⁵⁹ vgl. <http://www.audi-technology-portal.de/de/elektrik-elektronik/fahrerassistenzsysteme/audi-a4-stauassistent-de>

Der Test wurde am 21.11.2016 bei Trockenheit und guten Sichtbedingungen am Tag zwischen 16:03 Uhr und 16:36 Uhr auf der Autobahn A4 bei Aachen zwischen der Auffahrt Aachen-Krefelder Straße bis zur Einmündung der A4 ins Autobahnkreuz Aachen (Schilderbrücke) durchgeführt.



Abbildung 169: Testfahrt Audi Active LaneAssist ohne manuellen Lenkeingriff

Die Strecke wurde zunächst mit und anschließend ohne aktiviertem Active Lane Assist mit einem Audi A4 Baujahr 2016 durchgeführt. Die Stausituation hat sich in der Zeit nicht verändert und so ergaben sich für beide Durchgänge für die ca. 3,6 km etwa 11 Minuten Fahrzeit. Hierbei wurde in Höhe der Autobahnbrücke über die Haaler Straße ein manueller Spurwechsel von der rechten auf die linke Spur durchgeführt, um beide Situationen zu berücksichtigen. Beide Messfahrten wurden auf Video aufgezeichnet und die aufgezeichneten Messdaten der Lenkwinkel so getrimmt, dass sie zum gleichen Startpunkt beginnen und am gleichen Punkt enden. Der Spurwechselvorgang wurde komplett aus den Daten entfernt, um die Extremwerte der Messung nicht zu verändern. Bei der Fahrt mit aktiviertem LaneAssist und aktiviertem ACC (Tempomat) musste dem System durch ein kleines Lenkmoment signalisiert werden, dass der Fahrer die Fahraufgabe noch überwacht, da sich das System sonst abschaltet (erkennbar an den einzelnen deutlich hervorstechenden Spitzen). Bei der manuellen Fahrt (auch ohne ACC) wurden nur die absolut notwendigen Lenkbewegungen durchgeführt, so wie das ein guter menschlicher Autofahrer üblicherweise machen würde.

Man erkennt, dass die korrigierenden Lenkbewegungen des Assistenzsystems deutlich stärker ausfallen, als die des menschlichen Fahrers. Das deckt sich auch mit der Wahrnehmung im Fahrzeug, bei dem das automatisiert gesteuerte Fahrzeug deutlich unruhiger und mit merkbaren Lenkausschlägen agiert, als der menschliche Fahrer.

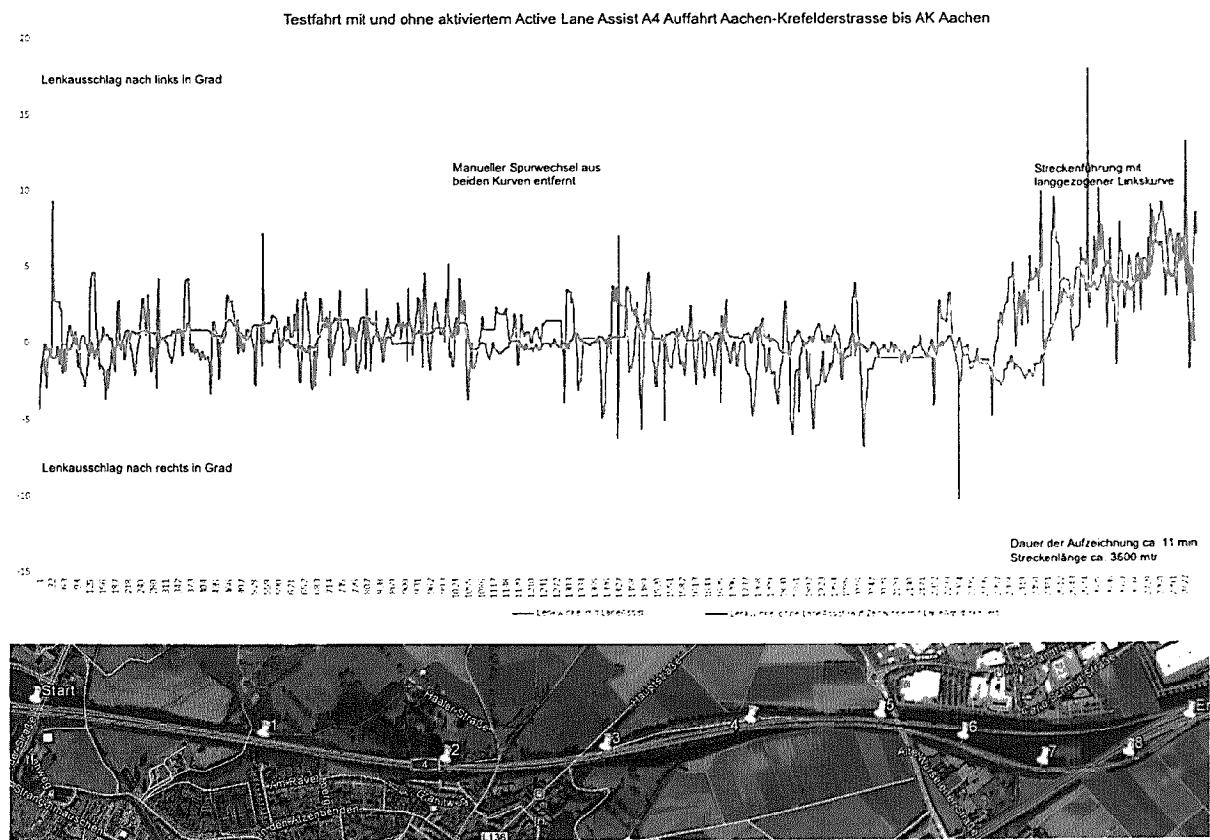


Abbildung 170: Testfahrt Audi Active Lane Assist

Fasst man die Absolutwert (ohne Vorzeichen) Blockweise für ca. 30 Sekunden zusammen und ermittelte daraus den jeweiligen Maximalwert, so erhält man für den Teilbereich der Messstrecke, (ohne enge Kurven) die auf der nächsten Seite dargestellten maximalen Lenkausschläge in Grad. Man erkennt, dass der Lenkradausschlag bei aktiviertem LaneAssist mit $4,26^\circ$ um etwa 171% höher liegt (also fast das Dreifache) als beim menschlichen Fahrer, der im Schnitt $1,57^\circ$ Lenkbewegung vornimmt. Diese Lenkbewegung wird vom Fahrer im Lenkrad deutlich wahrgenommen und als störend empfunden. Teilweise ist die Schlingerbewegung so stark, dass sie auch optisch anhand des Fahrwegs von Beifahrern und Außenstehenden wahrgenommen werden kann.

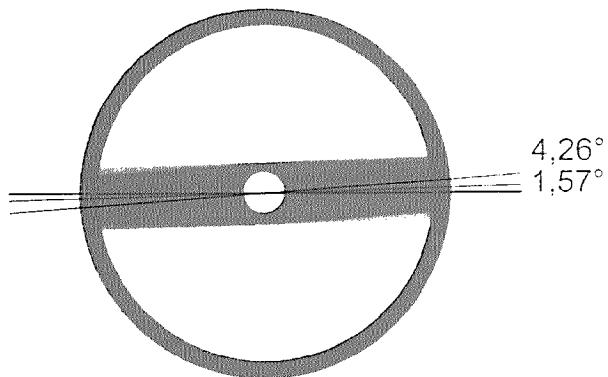


Abbildung 171: Unterschiedlicher Lenkradausschlag

— Mit LaneAssist — Ohne LaneAssist

Gemittelte Absolutwerte (Max. ohne VZ) Event 1-2000

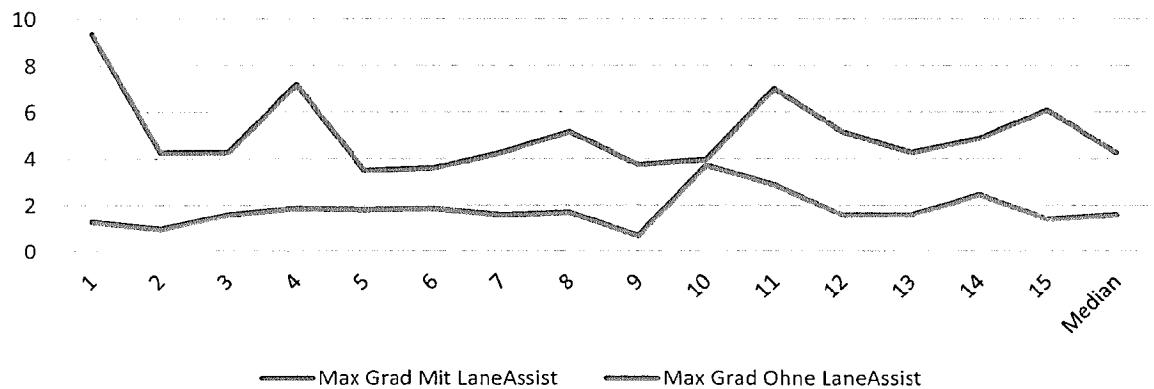


Abbildung 172: Gemittelte Maximalwerte (Median)

Teilbereich	Max Grad Mit LaneAssist	Max Grad Ohne LaneAssist	Mehrausschlag LaneAssist Mit zu Ohne
1	9,352	1,272	635%
2	4,256	0,952	347%
3	4,256	1,568	171%
4	7,168	1,848	288%
5	3,472	1,792	94%
6	3,584	1,848	94%
7	4,256	1,568	171%
8	5,152	1,68	207%
9	3,736	0,672	456%
10	3,96	3,696	7%
11	7	2,856	145%
12	5,136	1,568	228%
13	4,256	1,568	171%
14	4,856	2,448	98%
15	6,088	1,384	340%
Median	4,256	1,568	171%

6.3.3 Fehlfunktionen Pre-Sense-System

In den entsprechenden Testfahrzeugen Audi A4 und Audi A4 Allroad ist des Weiteren ein sogenanntes „Pre-Sense“-System verbaut. Diese soll den Fahrer vor drohenden Kollisionen im Front- und Heckbereich soweit beim Linksabbiegen bei Gegenverkehr durch eine Aufmerksamkeits- bzw. Notbremsung warnen und schützen. Beim Fahrzeug des Autors konnten über rund 15.000 gefahrene Kilometer über 40 Fehlauslösungen ohne einen einzigen tatsächlich begründeten Notfall beobachtet werden. Gleichwohl reagierte das System bei vergleichbaren Situationen, bei denen eine Warnung nach den offensichtlich hinterlegten Kriterien angebracht gewesen wäre, nicht. Oft waren die als Hindernis erkannten Fahrzeuge nicht oder nicht mehr im Gefahrenbereich und die Detektion erfolgte ohne erkennbaren Sinn. In einem Fall war eine Aufmerksamkeitsbremsung bei rund 180 km/h beim Überholen eines LKW auf einer zweispurigen Autobahn ohne sonstigen Verkehr zu beobachten, weil sich das Auto wohl „erschrocken“ hatte. Das ist alles andere als vertrauenserweckend.

Das Funktionieren des sogenannten Abbiegeassistenten, der im Fahrzeug des Autors im Assistenzpaket Tour enthalten ist, konnte hingegen weder im Alltag noch bei konkret bei Tests mit einem Dummy-Objekt eine Auslösung festgestellt werden. Dieses System soll vor drohenden Kollisionen mit dem Gegenverkehr beim Linksabbiegen schützen. Bei Tests wurde zunächst eine Schaumstoffrolle auf einem Rollbrett von einem Helfer als simulierter Gegenverkehr links am Testfahrzeug vorbeigezogen. Trotz gesetztem Blinker konnte keine Warnung oder Notbremsung des Pre-Sense-Systems festgestellt werden. Das Fahrzeug wäre ohne manuelle Bremsung in den Schaumstoffkörper hineingefahren. Auch bei Tests mit einem mit Alufolie umwickelten Körper reagierte das Pre-Sense-System nicht. Erst unmittelbar (wenige Zentimeter) reagierte der Parkassistent mit dem typischen Piepsen, was nichts mit dem Pre-Sense-System zu tun hat.



Abbildung 173: Abbiegeversuch mit Dummy-Objekt

Anschließend wurden die Versuche mit einem echten Fahrzeug als „Gegner“ an insgesamt drei verschiedenen Kreuzungen wiederholt. Der eingeweihte Fahrer des entgegenkommenden Fahrzeugs bremste dabei entweder noch rechtzeitig ab oder wich dem Testwagen aus, denn in keinem der rund 15 Versuche an zwei verschiedenen Tagen konnte ein Ansprechen des Abbiegeassistenten festgestellt werden.

Laut Werbeaussage der Audi AG sollte das System genau vor diesen Abbiegeunfällen schützen: *Audi A4 Abbiegeassistent¹⁶⁰: Der Abbiegeassistent, eine weitere Audi-Innovation, überwacht beim Linksabbiegen im Geschwindigkeitsbereich zwischen zwei und zehn km/h den Gegenverkehr. In einer gefährlichen Situation bremst er zum Stillstand. Das System wird im Hintergrund aktiv, sobald der Fahrer den Blinker zum Linksabbiegen setzt:*



Abbildung 174: Animation Audi Abbiegeassistent - Sollzustand

In einer exakt wie in der Werbevisualisierung nachgestellten echten Situation auf der Straße wurde das Testfahrzeug (jeweils oben im Bild) jedoch nicht gebremst bzw. der Fahrer gewarnt.



Abbildung 175: Auszug aus dem Video zu den Fahrversuchen (www.Car-Forensics.de)

¹⁶⁰ Quelle: (Audi-AG, 2016)

Bei schlechten Witterungsbedingungen kommen Assistenzsysteme – wie hier im Beispiel des Audi A4 Baujahr 2016 – komplett an ihre Grenzen. Starker Regen oder etwas stärkerer Schneefall lassen bereits das Abstandsradsystem ausfallen und eine nur leicht schnee-bedeckte Fahrbahn stellt ein Spurhaltesystem vor ein unlösbare Problem. Und aus unerfindlichen Gründen arbeitet dann auch das Pre-Sense-System nicht mehr. Das ist umso bedauerlicher, als das der Fahrer gerade in solchen schwierigen Situationen auf einen elektronischen Helfer gerne zurückgreifen würde. Wie sollen damit erst vollständig automatisch oder autonom fahrende Fahrzeuge umgehen? Sind das nur Schönwettersysteme und braucht man dann im Winter ein „altes“ Auto, welches sich noch herkömmlich bewegen lässt?



Abbildung 176: Ausfall der Audi Assistenzsysteme bei Schnee

6.3.4 Auslesen von Steuergeräten

Die beobachteten Mängel und Fehlfunktionen an Assistenzsystemen sind äußerst schwierig zu dokumentieren und forensisch aufzuklären, da sie oft nicht reproduzierbar und deterministisch auftreten und es an einer geeigneten offen gelegten Protokollierung der Fehlfunktionen fehlt. Viele vom Fahrer bemerkte Fehler werden vom System erst gar nicht als solche detektiert und die teilweise in den Fehlerspeichern der betreffenden Steuergeräte zu findenden Meldungen sind so oberflächlich, dass sie für eine detaillierte Analyse unbrauchbar sind (u.a. fehlende absolute Zeitstempel).

STG Nr.	8W0907217B
Name	R242_BVS
Codierung	0404090200000404022023A7AD0000FCB0F0C020E280
Software	0042
Fehler gefunden	
1122612(\$112134):08 (U112100) Datenbus fehlende Botschaft unplausibles Signal Lamp OFF Status unbekannt	
1123600(\$112510):08 (B163002) Prädiktive Streckendaten Signalfehler unplausibles Signal Lamp OFF Status unbekannt	
1123601(\$112511):08 (B163002) Prädiktive Streckendaten Signalfehler unplausibles Signal Lamp OFF Status unbekannt	
665(\$000299):08 (C110AF0) Steuergerät für Kamera Eingeschränkte Sicht unplausibles Signal Lamp OFF Status unbekannt	

Abbildung 177: Exemplarischer Fehlerspeicherbericht für Motorsteuergerät

Bei der Suche nach den Steuergeräten und Sensordaten, die für ein bestimmtes Assistenzsystem zuständig sind, helfen entsprechende Werkstattdiagnosegeräte, die es sowohl vom Hersteller als auch von Drittanbieter zu kaufen gibt. Im Fall des untersuchten Audi A4 8W wurde ein Diagnosegerät der Firma Stemei eingesetzt. Über die Gateway-Funktion können alle im Fahrzeug verbauten Steuergeräte aufgelistet werden. Die Steuergeräte können hinsichtlich ihrer Parameter, Fehlercodes und Live-Daten ausgelesen und codiert werden. Hierzu ist teilweise ein Login-Code notwendig, der recherchiert oder ermittelt werden muss.

STG-Liste aus Gateway						
Verbaute STGs		Name	Status	Bus	Fehler	Codierung
Adresswort	StG					
01	Motorelektronik		Kommunikation OK	CAN_PVRT	!	✓
02	Getriebeelektronik		Kommunikation OK	CAN_PVRT	!	✓
03	Bremselektronik		Kommunikation OK	CAN_PVRT	!	✓
08	Klima-/ Heizungselektronik		Kommunikation OK	CAN_PVRT	!	✓
09	Elektronische Zentralelektrik		Kommunikation OK	CAN_PVRT	!	✓
13	Distanzregelung		Kommunikation OK	CAN_PVRT	!	✓
15	Airbag		Kommunikation OK	CAN_PVRT	!	✓
16	Lenksäulelektronik		Kommunikation OK	CAN_PVRT	!	✓
17	Schalttafeleinsatz		Kommunikation OK	CAN_PVRT	!	✓
19	Diagnoseinterface für Datenbus		Kommunikation OK	CAN_PVRT	!	✓
3C	Spurwechselassistent		Kommunikation OK	CAN_PVRT	!	✓
42	Türelektronik Fahrer		Kommunikation OK	CAN_PVRT	!	✓
44	Lenkhilfe		Kommunikation OK	CAN_PVRT	!	✓
46	Zentralmodul Komfortsystem		Kommunikation OK	CAN_PVRT	!	✓
52	Türelektronik Beifahrer		Kommunikation OK	CAN_PVRT	!	✓
5F	Informationselektronik 1		Kommunikation OK	CAN_PVRT	!	✓

Abbildung 178: Auszug aus Übersicht gefundener Steuergeräte

Mit etwas Aufwand bei der Suche findet man in den Steuergeräten moderner Fahrzeuge eine Reihe von aufgezeichneten Betriebsparametern, die Aufschluss über die Fahrweise des Fahrers bzw. die Belastung des Fahrzeugs geben können.

Hierzu gab es 2016 bereits eine Veröffentlichung der FIA¹⁶¹ in Bezug auf Modelle des Herstellers BMW. Aber auch bei Audi werden solche Daten nach Untersuchung des Autors aufgezeichnet (und möglicherweise online an den Hersteller übertragen). So wird z.B. im Steuergerät 13 (Distanzregelung) beim Audi A4 8W die Nutzungsdauer des ACC in Minuten aufgeteilt nach den verschiedenen Modi „Dynamic“, „Comfort“, „Auto“ und „Efficiency“ geloggt:

ACC gesamt:	2.807 (Minuten) davon:
Dynamic:	2.496 Minuten
Comfort:	270 Minuten
Auto:	36 Minuten
Efficiency:	5 Minuten

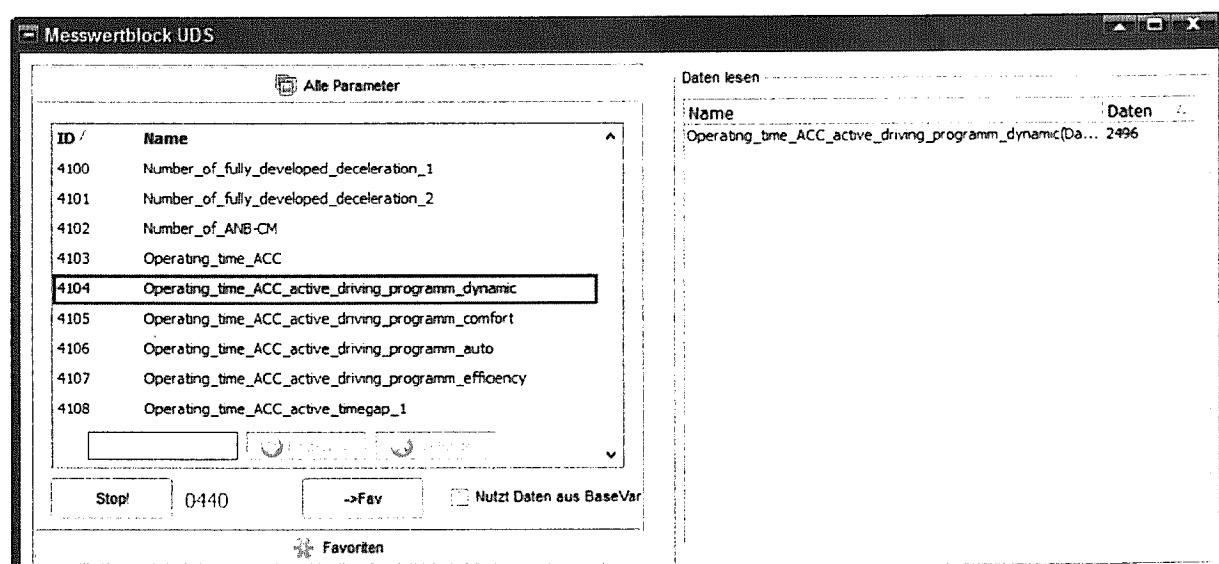


Abbildung 179: Nutzungsdauer ACC im Modus "Dynamic"

Die Systemlaufzeit des Fahrzeugs (Betriebsstundenzähler) beträgt 9703 Minuten (Messwert 970,3 muss mit 10 multipliziert werden).

Man kann daraus also ablesen, dass das ACC etwa 29% der Betriebszeit aktiviert war und es dabei in rund 89% der Zeit im Modus "Dynamic" benutzt wurde. Der Fahrer fährt also knapp ein Drittel der Zeit mit aktiviertem Tempomat und Abstandsradar, gehört aber offenbar zur eher dynamischen Sorte. Warum der Hersteller Audi dies aufzeichnet, darf sich der Leser nun selber überlegen.

Ob das System zu einem bestimmten Zeitpunkt aktiv war (z.B. zum Unfallzeitpunkt), lässt sich hingegen aus den Daten nicht ermitteln.

Überraschend ist, dass neben den betroffenen Herstellern offenbar auch noch keiner der staatlichen Stellen und Prüforganisationen aufgefallen ist, dass diese Systeme unzuverlässig bzw. fehlerhaft arbeiten (KBA, Bundesministerium für Verkehr und digitale Infrastruktur, TÜV/Dekra & Co).

¹⁶¹ Quelle u.a. (Zeit/ADAC, 2016)

6.4 Auswertung des tödlichen Unfalls des Uber-Volvo

Update 04/2018: Am 18.03.2018 verunfallte ein voll-automatisiert fahrendes Fahrzeug der Marke Volvo Typ XC90 SUV bei Testfahrten des Fahrdienstanbieters Uber in Tempe, Arizona (USA). Hierbei wurde eine 49-jährige Fußgängerin beim Überqueren der mehrspurigen Straße vom Fahrzeug erfasst und getötet.

Es ist nach Ansicht des Autors bemerkenswert, wie viel man aus den öffentlich zugänglichen Quellen und dem von der Polizei in Tempe veröffentlichten Video mit weiteren Meta-Daten des Fahrzeugs bereits herauslesen und somit bei sorgfältiger und richtiger Interpretation des Materials die bisher weitestgehend oberflächliche bis falsche Berichterstattung in den Medien widerlegen kann.

Für eine weitere Ursachenforschung, was innerhalb des Fahrzeugsystems passiert ist, muss man selbstverständlich Zugang zu selbigem und den darin gespeicherten Informationen haben. Dies hatte der Autor (bisher) aus naheliegenden Gründen nicht.

Die Polizei von Tempe hat kurz nach dem Unfall ein Video veröffentlicht, welches die Sicht sowohl nach vorn aus dem Fahrzeug als auch auf die Fahrerin vor und zum Zeitpunkt des Unfalls zeigt. Auf Basis dieses Videos, welches von einer Vielzahl von Nachrichtensendern aufgegriffen und verbreitet wurde, und den ersten Informationen der Polizei wurde eine Reihe von Behauptungen und Vermutungen hinsichtlich des Ablaufes des Unfalls und der Schuldfrage aufgestellt, die sich bei näherer Betrachtung und Auswertung des original Videomaterials als oberflächlich, irreführend und teilweise falsch herausstellen.

Mit Blick auf die Akzeptanz von voll automatisiert oder autonom fahrenden Fahrzeugen ist der erste Unfall eines solchen Fahrzeugs mit Todesfolge für einen unbeteiligten Fußgänger für das gesamte Projekt Vision Zero¹⁶² ein schwerer Rückschlag. Gerade in Bezug auf die vollmundige und nach wie vor gültige Werbeaussage von Volvo aus dem Jahr 2010, dass ab 2020 niemand mehr in einem dann neuen Volvo-Fahrzeug ernsthaft verletzt oder gar getötet wird, zeigt der Unfall, dass man von diesem Ziel offenbar noch weit entfernt ist. Daher gilt es, diesen Vorfall sorgfältig zu analysieren und aufzuklären.

Des Weiteren eignet sich der Fall ungeachtet der menschlichen Tragödie gut, um die Möglichkeiten und Grenzen der Aufklärung eines solchen Unfalls aufzuzeigen und wie auf Basis unvollständiger bzw. falscher Informationen vorschnell vollkommen falsche Schlüsse gezogen werden.

¹⁶² Reduzierung der Verkehrstoten auf Null

6.4.1 Behauptungen und Pressemeldungen

Folgende Aussagen wurden offenbar zunächst auf Basis der ersten Aussagen der lokalen Polizei in den USA und dem Videomaterial verbreitet:

1. Die verunfallte Fußgängerin (die ihr Fahrrad schiebend über die Fahrbahn gegangen ist) soll plötzlich aus dem Schatten hervorgetreten sein¹⁶³.
2. Das Fahrzeug soll im voll-automatisierten Modus mit umgerechnet 64 km/h (40 mph) anstatt der am Unfallort erlaubten 56,3 km/h (35 mph) unterwegs gewesen sein¹⁶⁴.
3. Das Fahrzeug soll weder nennenswert verzögert noch eine Ausweichbewegung vorgenommen haben¹⁶⁵.
4. Der/die zur Überwachung an Bord des Fahrzeugs befindliche Fahrer(in) soll nicht eingegriffen haben¹⁶⁶.
5. Der Unfall wäre auch von einem menschlichen Fahrer nicht vermeidbar gewesen¹⁶⁷.
6. Die Polizei von Tempe, Arizona (Sylvia Moir) sagte aus, dass es danach ausgehe, dass Uber keine Schuld an dem Unfall trage und eine Anklage gegen den Fahrer nicht ausgeschlossen werde¹⁶⁸.
7. Das Fahrzeug war mit RADAR-Sensoren, Kameras und einem LIDAR-System ausgestattet.¹⁶⁹
8. Am 27.03.2018 wurde Uber die Erlaubnis für weitere Testfahrten mit autonom fahrenden Fahrzeugen bis auf weiteres entzogen¹⁷⁰.
9. Uber hat das Fahrzeug mit eigener Hardware bzw. Software ausgestattet und das serienmäßige Kollisionssystem von Volvo abgeschaltet¹⁷¹.

¹⁶³ diverse Quellen, beispielhaft (Forbes, n.d.)

¹⁶⁴ diverse Quellen, beispielhaft (WDR, 2018)

¹⁶⁵ diverse Quellen, beispielhaft (Newsweek, 2018)

¹⁶⁶ diverse Quellen, beispielhaft (Newsweek, 2018)

¹⁶⁷ diverse Quellen, beispielhaft (Autobild, 2018)

¹⁶⁸ diverse Quellen, beispielhaft (Network, 2018)

¹⁶⁹ diverse Quellen, beispielhaft (Bloomberg, 2018)

¹⁷⁰ diverse Quellen, beispielhaft (Spiegel, 2018)

¹⁷¹ diverse Quellen, beispielhaft (Coppola & King, 2018)



Abbildung 180: Unfallfahrzeug bei der Untersuchung durch Polizei und Spezialisten

6.4.2 Eigene Untersuchungen und Auswertungen

Erwartungsgemäß hat die teils reißerische und widersprüchliche Berichterstattung der Medien über den Unfall das Interesse des Autors Thomas Käfer geweckt und ihn veranlasst, eigene Auswertungen der öffentlich zugänglichen Quellen vorzunehmen.

Besonders auffällig ist nach einer ersten Sichtung des im Internet frei verfügbaren Videomaterials zu dem Crash, dass gerade das Bild der Frontkamera sehr dunkel ist und die Fußgängerin tatsächlich erst unmittelbar vor dem Zusammenprall aus dem Schatten herauszutreten scheint. Das nährt zunächst die These, dass der Unfall auch für einen menschlichen Fahrer unvermeidbar gewesen wäre:



Abbildung 181: Ausschnitt Dashcam-Video (Quelle YouTube - Auflösung 636 x 360 px)

Versuche, das Video durch Nachbearbeitungsfilter aufzuhellen, scheitern aufgrund des qualitativ schlechten Ausgangsmaterials. In allen im Internet zugänglichen Quellen sind die Zusatzinformationen am Bildrand zudem verpixelt.

Der Autor hat daher die Polizei in Tempe, Arizona angeschrieben und um Zusendung des originalen Bildmaterials aus der Pressemitteilung gebeten. Tatsächlich erhielt er einen Tag nach seiner Anfrage eine qualitativ bessere Version mit einer Auflösung von 848 x 480 und 25 fps¹⁷², die zudem die Zusatzinformationen im Klartext unverpixelt enthielt (Frontkamera):

Die zu diesem forensischen Bericht zugehörigen Videos in Deutsch und Englisch sind unter www.car-forensics.de abzurufen.

Link: <https://www.kaeferlive.de/index.php/medien-forensik/videos-und-webcasts>

Direkter Link zum Video (Deutsche Version): <https://youtu.be/wTJAHHNrDtM>

¹⁷² fps: frames per second – Eine Sekunde Filmmaterial besteht hier aus 25 Einzelbildern.



Abbildung 182: Ausschnitt Dashcam-Video (Quelle Polizei Tempe - Auflösung 848 x 480 px)

Im Gegensatz zu dem verkürzten Video auf YouTube beginnt das Video früher (unmittelbar vor dem Unterfahren der Brücke) und es werden daher wichtige Details für die weitere Analyse sichtbar.

Zunächst fällt auf, dass beim Schnitt zwischen der Außen- und Innenansicht und am Ende des Videos kurz das Hintergrundbild des Windows Mediaplayers sichtbar wird:

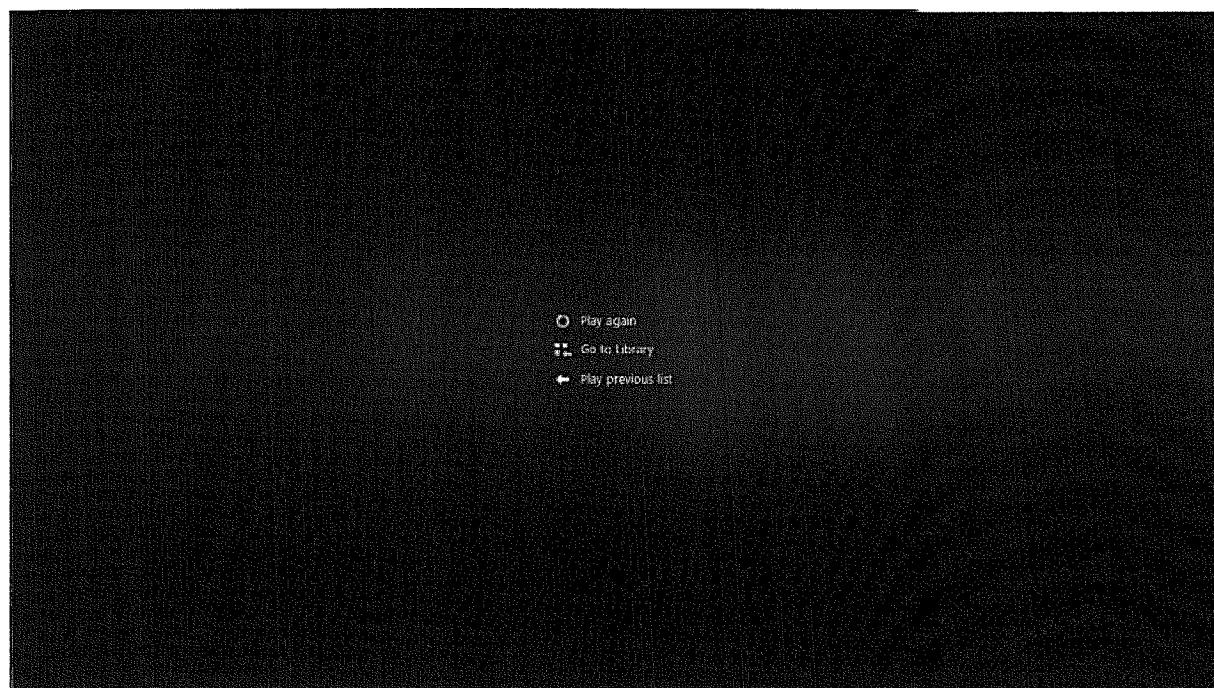


Abbildung 183: Medioplayer Screen am Ende der Video, die die Polizei verbreitet hat

Vergleicht man dessen Qualität (und Helligkeit) mit der eines Screenshots auf dem Auswertungs-PC des Autors nach Abspielen des Original-Videos, so erkennt man, dass letzteres qualitativ klarer und etwas heller ist. Das führt zu dem Schluss, dass die Polizei nicht das Original-Video aus dem Fahrzeug ausgewertet bzw. verbreitet hat, sondern dieses von einem PC vermutlich mittels Screen-Recorder aufgenommen und geschnitten wurde. Dabei und dem dann nachfolgend erfolgten Export des geschnittenen Videomaterials ist es offenbar zu einem Qualitätsverlust gekommen. Denkbar ist sogar, dass das Original-Video mit einer Video-Kamera oder einem Smartphone abgefilmt wurde. Das wäre dann in Bezug auf die Auswertung ein äußerst fahrlässiges und unprofessionelles Verfahren.

Äußerst fraglich ist also, warum nicht die digitale Ausgangsdatei in der höchstmöglichen Auflösung verwendet wurde. Man könnte unterstellen, dass das Video bewusst auf einem PC abgespielt wurde und hierbei bereits Helligkeits- und Qualitätsreduzierungen absichtlich oder mindestens fahrlässig in Kauf genommen wurden.

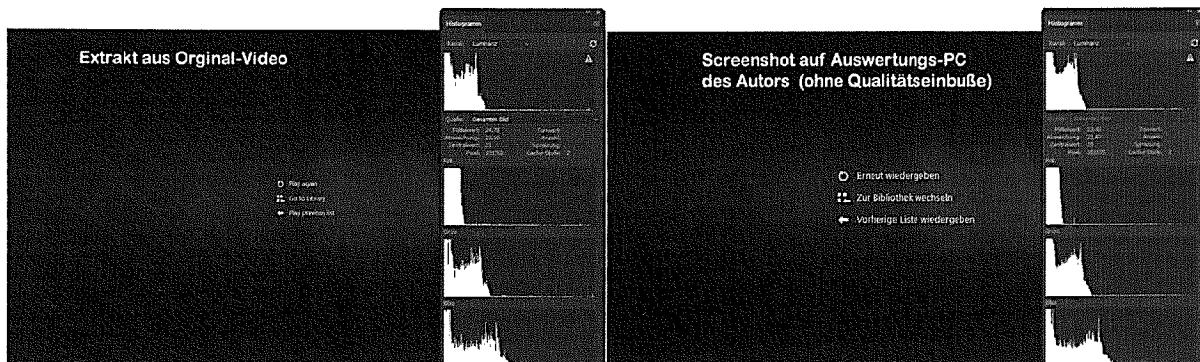


Abbildung 184: Vergleich reduzierte Qualität Polizei-Video zu möglicher Auflösung/Helligkeit

Anhand der Histogramme erkennt man die etwas höhere Dynamik des Screenshots (rechts) mit weniger Rauschen gegenüber dem von der Polizei zur Verfügung gestellten Video (links)¹⁷³.

Sollte das Video dennoch tatsächlich die realen Lichtverhältnisse 1:1 abbilden, so würde dies wiederum bedeuten, dass die Sichtweite nur bis zur Grenze des Fahrlichts (hier offenbar Abblendlicht) gereicht hat. Da man nur so schnell fahren darf, dass man das Fahrzeug jederzeit innerhalb der Sichtweite anhalten kann, würde dies bedeuten, dass man bei diesen Lichtverhältnissen hätte deutlich langsamer fahren müssen. Die Sichtweite lässt sich anhand der Mittelstreifen im Video und dem Vergleich mit Google Earth auf rund 25 m vermessen. Das wiederum führt bei konventionellen Annahmen (1 s Reaktionszeit, 6 m/s² Verzögerung auf trockenem Asphalt) zu einer maximal zulässigen Geschwindigkeit von höchstens 45 km/h (entspricht knapp 28 mph¹⁷⁴).

¹⁷³ Anmerkung: Die Auswertung der Bilder wurde mit Photoshop im Einzelbildmodus ohne jegliche weitere Veränderung des Ausgangsmaterials vorgenommen. Die Unterschiede sind in einem gedruckten Bericht nicht so deutlich sichtbar wie am Bildschirm.

¹⁷⁴ Umrechnung 1 mph = 1,60934 km/h

Dipl.-Ing. Thomas Käfer, M.Sc. – Car-Forensics 5.0

Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall,
Kfz-Unfalldatenschreibern und Smartphone-Kopplung

Geschwindigkeit:	44	km/h
Reaktionszeit:	1	s
Bremsverzögerung:	6	m/s ²
Reaktionsweg:	12.22	m
Bremsweg:	12.45	m
Anhalteweg:	24.67	m
Anhaltezeit:	3.04	s
Hindernisentfernung:	25	m
Aufprallgeschwindigkeit:	0	km/h
Dauer bis zum Aufprall:	-----	s
Äquivalente Fallhöhe:	0	m

Abbildung 185: Berechnung Anhalteweg bei Sichtweite 25m¹⁷⁵

Aus den am Bildrand enthaltenen Metadaten kann man weitere Informationen ablesen und diese zur Auswertung weiterverarbeiten. So zeigt der Zeitstempel, dass der Unfall am 19.03.2018 um 04:58:50 UTC (entspricht 00:58:58 Ortszeit) im Bereich der Geo-Koordinaten LAT 3326.1456 LON 11156.5195 mit einer Geschwindigkeit von 40 mph erfolgte (Wie sich später herausstellte, ist das Datum und die angezeigte Uhrzeit falsch. Der Unfall ereignete sich lt. Polizeibericht am 18.03.2018 um 22:00 Uhr):



Abbildung 186: Bild aus dem Polizeivideo unmittelbar beim Aufprall

Die Werte X, Y und Z geben mutmaßlich die Beschleunigung in der Längs- und Querachse bzw. senkrecht nach unten (Erdbeschleunigung) an und mit dem Wert „sum“ wird daraus eine Vektorsumme (mathematisch Betrag) für die resultierende Beschleunigung ermittelt. Mit 8,25 m/s² ist dieser Wert gegenüber den Normalwerten bei einer Fahrt deutlich erhöht und zeigt auf den Aufprall hin.

¹⁷⁵ Quelle: <http://www.kfz-handwerk.de/bremsweg.php>

Bei der Interpretation der Geo-Koordinaten, die offenbar von einem internen GPS-Empfänger im Fahrzeug stammen, muss man sehr aufpassen, nicht versehentlich das falsche Maßsystem anzuwenden, da hier keine Einheiten-Notation angegeben ist.

Aus den ungefähren Ortsangaben der Presseberichterstattung weiß man, dass der Unfall in Tempe, Arizona in der Nähe des Marquee-Theatres passiert ist.

Interpretiert man die Werte als Grad, Minuten, Sekunden und hierbei die Sekunden als Dezimalwert, so führt das zu $33^{\circ} 26' 14.56''$ N $111^{\circ} 56' 51.95''$ W. Diese Werte liegen rund 500 m abseits des tatsächlichen Unfallorts. Das ist deutlich mehr als der übliche Fehler des GPS-Signals von unter 15 m.

Deutet man die Werte jedoch als Grad und Minuten und hierbei die Minuten als Dezimalwert mit Nachkommastellen, so führt das zu $33^{\circ} 26.1456'$ N $111^{\circ} 56.5195'$ W. Dieser Wert ist plausibel, da er auf dem Fahrweg des Fahrzeugs liegt. Jedoch beträgt der Abstand zum tatsächlichen Unfallpunkt zu diesem Zeitpunkt rd. 108 m (Strecke 2 in Abbildung 187).

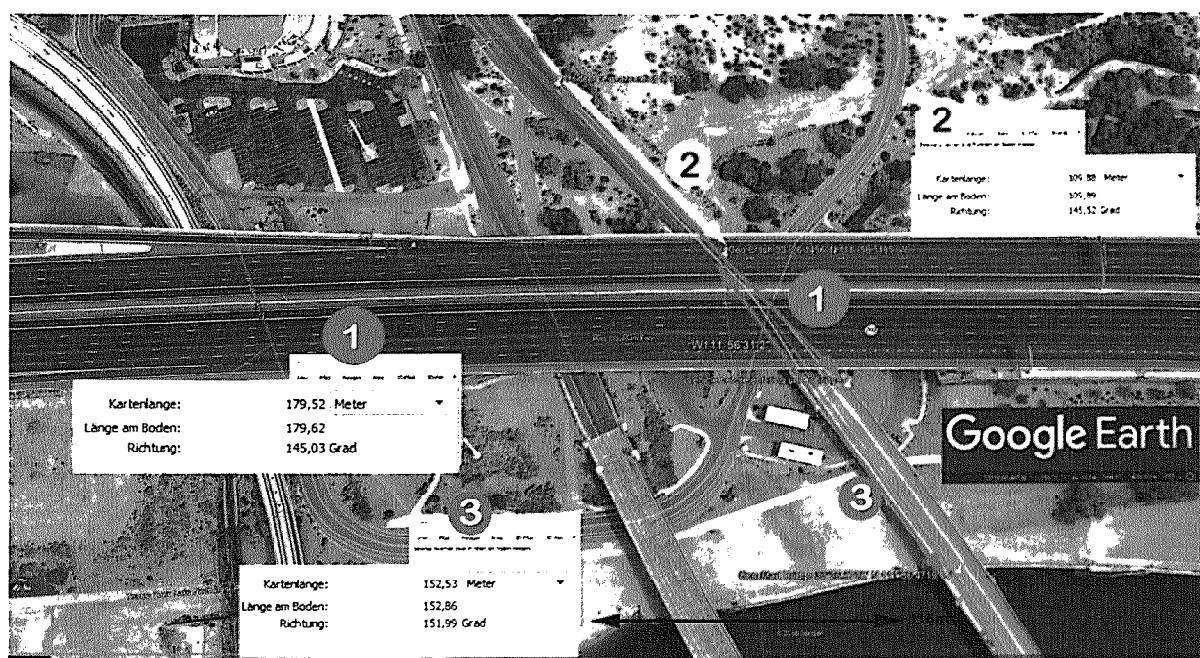


Abbildung 187: Abweichung angegebliche Geo-Position zu tatsächlicher Position

Ein weiterer Prüfpunkt wurde zu Beginn des Videos unmittelbar vor dem Unterfahren der Brücke untersucht. Laut Video befindet sich das Fahrzeug zu diesem Zeitpunkt bei $33^{\circ}26.0720'$ N $111^{\circ}56.4719'$ W und tatsächlich rund 76 m vom tatsächlichen Standpunkt entfernt.

Berechnet man nun anhand dieser beiden Geo-Koordinaten-Paare die Geschwindigkeit zwischen dem Zeitpunkt Brücke bis Unfall, so erhält man von den im Video eingeblendeten Speed-Werten deutlich abweichende Durchschnittsgeschwindigkeiten.

Das Pärchen der angegebenen Geo-Koordinaten ergibt gem. mit Google Earth eine Strecke von rd. $s_{Geo} = 152 \text{ m}$ ¹⁷⁶ (Strecke 3 in Abbildung 187). Das Pärchen der gem. Video ermittelten Geopositionen ergibt rund $s_{Video} = 179 \text{ m}$ (Strecke 1 in Abbildung 187). Laut Timecode im Video dauert die Fahrt zwischen diesen beiden Punkten exakt $t = 10$ Sekunden. Somit ergeben sich folgende Geschwindigkeiten:

$$v_{Geo} = s_{Geo}/t = 152 \text{ m} / 10 \text{ s} = 15,2 \text{ m/s} = 54,72 \text{ km/h} = 34 \text{ mph}$$

$$v_{Video} = s_{Video}/t = 179 \text{ m} / 10 \text{ s} = 17,9 \text{ m/s} = 64,44 \text{ km/h} = 40,04 \text{ mph}$$

Die im Video enthaltenen Metadaten sind also mit größter Vorsicht zu behandeln – auch was die daraus mutmaßlich errechnete Geschwindigkeit angeht. Diese bezieht sich offenbar auf den Bereich vor dem Unterfahren der Brücke.

In diesem Bereich gilt bis zur Brücke ein Tempolimit von 35 mph, was den rechnerisch ermittelten Wert v_{Geo} von 34 mph plausibel erscheinen lässt. Die Abweichung bzw. der Versatz um rd. 76 m bzw. 108 m auf dem Fahrstrahl ist durch eine verzögerte Berechnung der Geschwindigkeit auf Basis von um wenige Sekunden veralteten GPS-Daten zurückzuführen. Die Geschwindigkeit per GPS gemessen berechnet sich immer aus zwei zurückliegenden Geo-Positionen und der dafür benötigten Zeit. Bei langsamer Aktualisierung der Werte entspricht die so ermittelte Geschwindigkeit damit immer der vor x Sekunden. Anhand des Videos kann man die Koordinaten des Aufpralls sehr exakt durch Vergleich der Fahrbahnmarkierung mit den Bildern aus Google Earth ermitteln:



Abbildung 188: Kartierung des Unfalls mittels Google Earth

¹⁷⁶ Bei der Ermittlung von Distanzen auf der Erdkugel anhand von Geo-Daten und natürlich bei der Verwendung von Google Earth mit dem Lineal-Werkzeug sollte man immer eine gewisse Ungenauigkeit von einigen wenigen Metern berücksichtigen. Da dieser Fehler jedoch systematisch bei allen Messungen vorhanden ist und die Messungen zeitlich und örtlich nahe beieinanderliegen, kann er hier weitestgehend ignoriert werden.

¹⁷⁷ Umrechnung m/s in km/h: $\times 3,6$; Umrechnung 1 mph = 1,60934 km/h

Misst man im Video die Zeit, die das Fahrzeug kurz vor dem Unfall für das Abfahren der Strecke von 6 Mittelpurmarkierungen benötigt hat, so führt das zu einer höheren Geschwindigkeit:

Strecke gemessen mit Google Earth 71,59 m (Abweichung zugunsten des Fahrzeugs 70 m):

$$v_1 = s_1/t = 71,59 \text{ m} / 3,52 \text{ s} = 20,34 \text{ m/s} = 73,21 \text{ km/h} = 45,49 \text{ mph}$$

$$v_2 = s_2/t = 70 \text{ m} / 3,52 \text{ s} = 19,87 \text{ km/h} = 71,59 \text{ km/h} = 44,48 \text{ mph}$$

D.h., das Fahrzeug hat in den letzten 70 m vor dem Aufprall eine Geschwindigkeit von etwa 45 mph gehabt. Laut Anzeige im Video (Metadaten) beschleunigte das Fahrzeug in diesem Bereich von 34 mph auf ca. 40 mph unmittelbar beim Aufprall und erhöhte die Geschwindigkeit dann noch auf 42 mph nach dem Unfall. Letzteres ist vollkommen unplausibel, da das bedeuten würde, dass das Auto beim Überfahren des Opfers noch mal Gas gegeben hätte. Tatsächlich wird es allein durch den Aufprall abgebremst worden sein.

Durch die Erkenntnisse auf der vorherigen Seite erklärt sich aber auch dieser scheinbare Widerspruch. Die im Video eingeblendeten Geschwindigkeitswerte sind im Gegensatz zu den zeitnah erfassten Beschleunigungswerten X, Y und Z um mehrere Sekunden veraltet und beziehen sich auf den Fahrweg rund 76 m bis 108 m weiter vor dem Unfall. Dass das Fahrzeug dort beschleunigt hat, ist auch plausibel, da ab dem Unterfahren der Brücke das Speed-Limit von 35 mph auf 45 mph angehoben wurde, wie gleich gezeigt wird.



Abbildung 189: Frontkamerabild ca. 120 m vor dem Unfallort



Abbildung 190: Frontkamerabild unmittelbar beim Aufprall

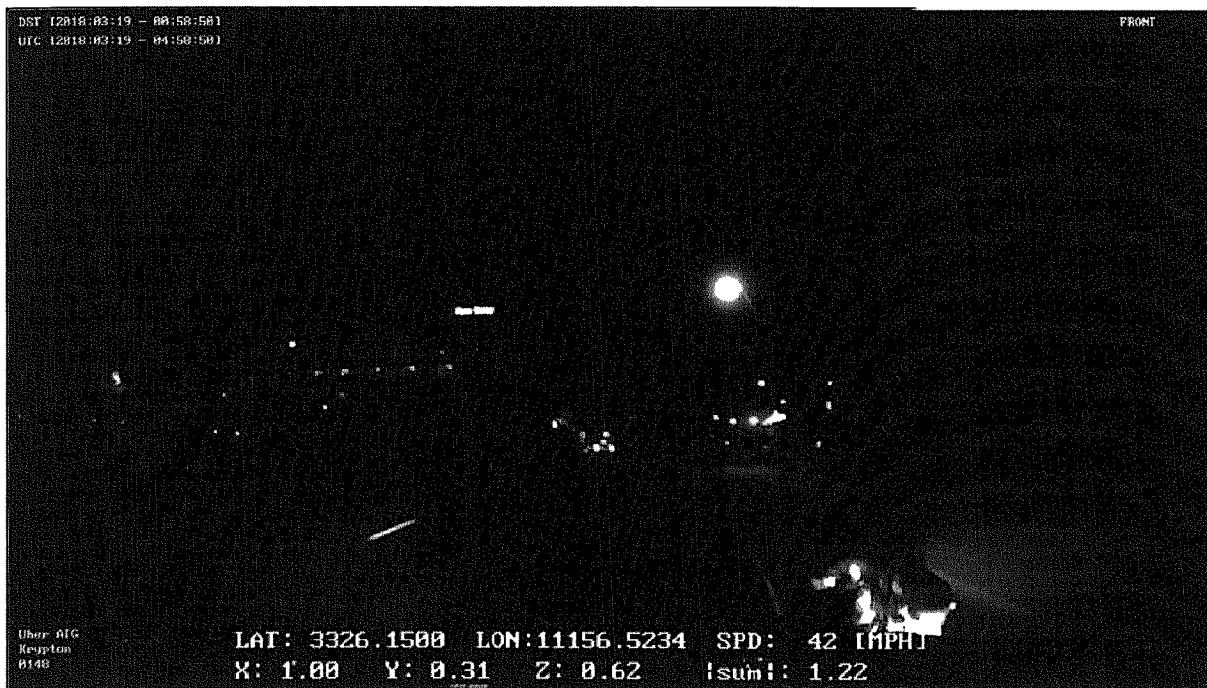


Abbildung 191: Frontkamerabild unmittelbar nach dem Aufprall

Damit kann mit hoher Wahrscheinlichkeit davon ausgegangen werden, dass das Fahrzeug zum Zeitpunkt des Unfalls zwischen 42 und 45 mph schnell war. Nun wurde auch seitens der Polizei zunächst behauptet, dass an dieser Stelle ein Tempolimit von 35 mph besteht. Damit wäre das Fahrzeug automatisiert zu schnell gewesen.

Es gibt drei Gegenbeweise, die alle zeigen, dass an dieser Stelle 45 mph das zulässige Limit ist und damit das Fahrzeug nicht zu schnell unterwegs war:

Zum einen liefert Google Earth in der Streetview-Ansicht ein vollkommen klares Bild der Beschilderung vor der Brücke (also ca. 200 m vor dem Unfallpunkt). Das Bild stammt von Juli 2017 (also deutlich vor dem Unfallzeitpunkt). Aber auch auf dem Unfallvideo ist das 45 mph-Schild gut erkennbar:

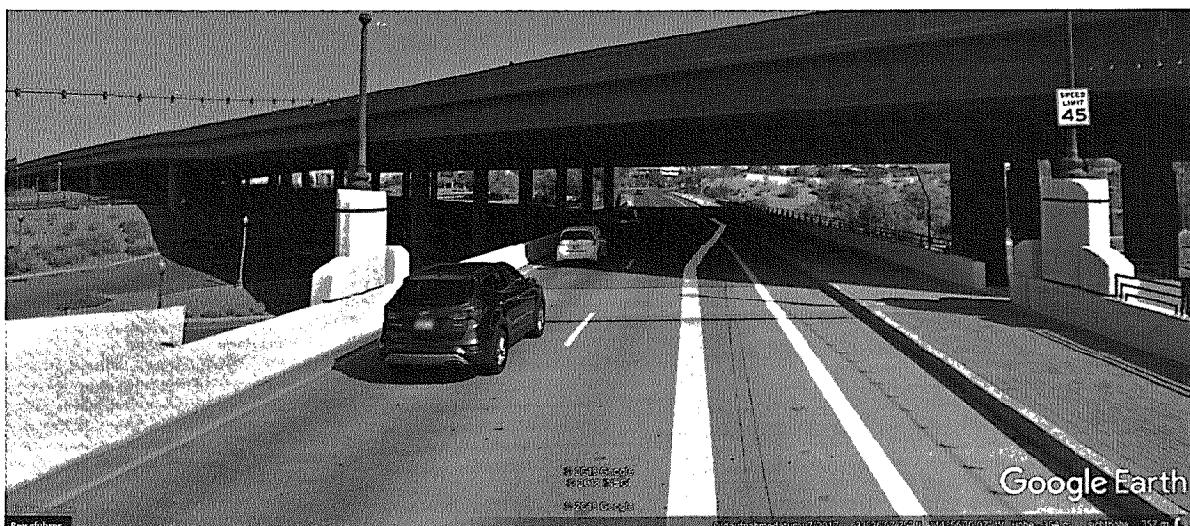


Abbildung 192: Google-Streetview Aufnahme des 45 mph-Schildes bei Tag



Abbildung 193: Aufnahme des 45 mph Schildes aus dem Unfallauto

Und auch auf einem weiteren im Internet aufgetauchten Video der Situation bei Nacht (aufgenommen am 21.03.2018 von Brian Kaufman¹⁷⁸ erkennt man die 45 mph-Limitierung¹⁷⁹.

¹⁷⁸ Quelle: <https://www.youtube.com/watch?v=CRW0q8i3u6E>

¹⁷⁹ Anmerkung: Sichtbarkeit im Ausdruck stark eingeschränkt, am Bildschirm besser sichtbar



Abbildung 194: Aufnahme des 45 mph-Schildes aus einem Vergleichsfahrzeug bei Nacht.

Aus demselben Video kann man zudem zu Beginn der Fahrt erkennen, dass mehrere hundert Meter vor der Brückenunterquerung ein 35 mph-Limit besteht:



Abbildung 195: Aufnahme des vorherigen 35 mph-Schildes aus Vergleichsfahrzeug bei Nacht

Da dieses Video auch den Bereich hinter dem Unfall zeigt, wird deutlich, dass nach dem 45 mph-Limit bis zum Unfallpunkt keine neue abweichende Geschwindigkeitsbeschränkung besteht. Damit ist bewiesen, dass am Unfallort eine Limitierung von 45 mph und nicht, wie vielfach fälschlich behauptet, 35 mph bestand.

Das Video von Brian Kaufmann liefert aber noch eine wesentlich wichtigere Erkenntnis. Die optische Situation in der Nacht ist bei weitem nicht so dunkel, wie es das von der Polizei verbreitete Video scheinen lässt:



Abbildung 196: Tatsächliche Lichtsituation am Unfallort bei Nacht ca. 120 m vor dem Unfallort

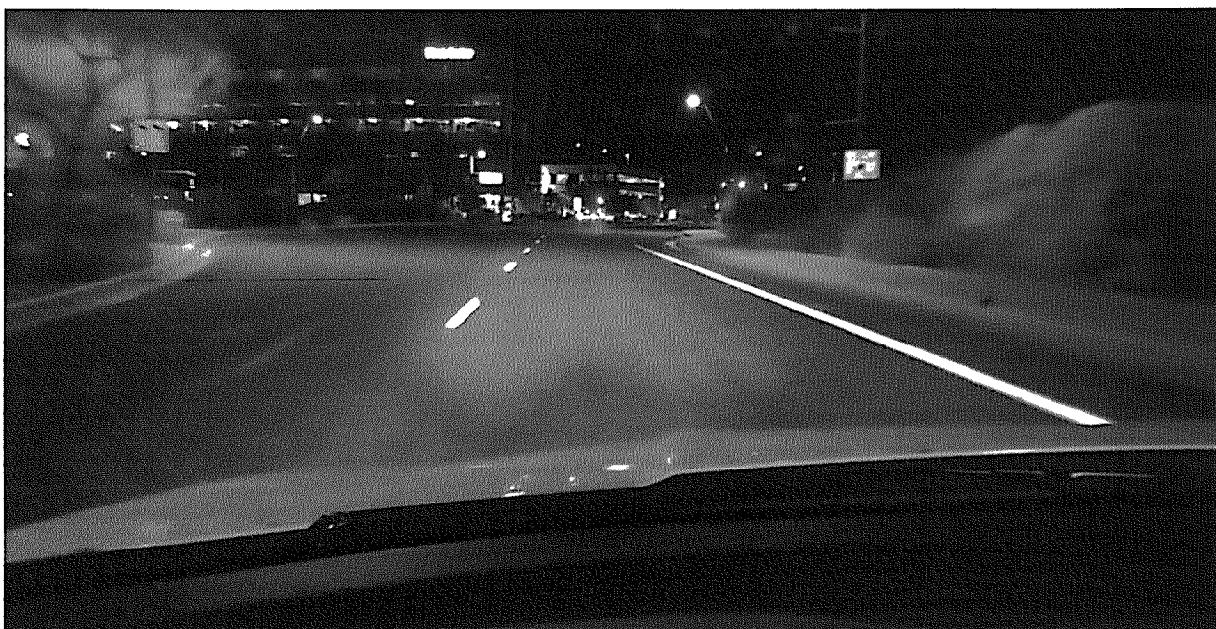


Abbildung 197: Tatsächliche Lichtsituation am Unfallort bei Nacht ca. 40 m vor dem Unfallort

Durch Auszählen der Mittelmarkierungen und dem Abmessen der Markierungen mittels Google Earth kann man in Verbindung mit der benötigten Zeit für das Abfahren der Strecke auch hier die Durchschnittsgeschwindigkeit des Vergleichsfahrzeugs bestimmen. Diese liegt bei etwa 40 bis 42 mph und somit also in etwa im gleichen Geschwindigkeitsbereich wie das Unfallfahrzeug. Daher kann man die Videos gut nebeneinander legen und die Positionen annährend exakt (bis auf wenige Meter) bestimmen.



Abbildung 198: Tatsächliche Lichtsituation am Unfallort

Man erkennt deutlich, dass die gesamte Straße sehr gut ausgeleuchtet ist und ein Hindernis, wie z.B. eine querende Person, die ein Fahrrad schiebt, sehr leicht erkennbar wäre. Google Earth liefert in der Streetview-Ansicht auch hier wertvolle Hinweise zur Situation am Unfallort (hier selbstverständlich bei Tag):

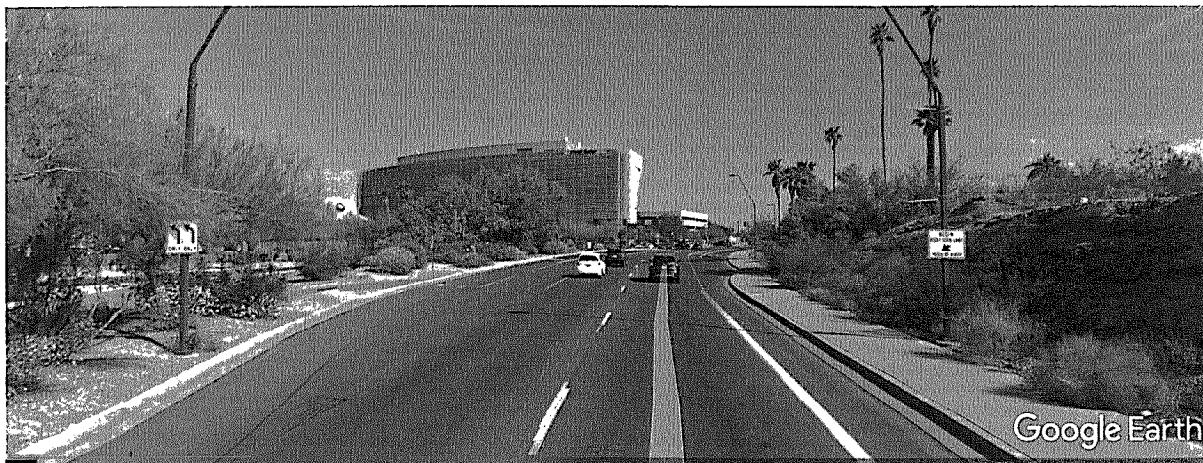


Abbildung 199: Unfallort bei Tag (Google Streetview)

Im von der Polizei zur Verfügung gestellten Video sieht es so aus, als ob die Frau mit dem Fahrrad erst ca. 1,5 s vor dem Aufprall sichtbar gewesen wäre (Zeitpunkt im Analysevideo des Autors von Timecode 00:00:12:19 bis 00:00:14:05). Auf dem Video erkennt man, dass sie in dieser Zeit drei Schritte von links nach rechts auf der rechten Fahrspur (Spur 1) macht. Das entspricht in etwa einer Strecke von 2,1 m (0,7 m pro Schritt). Damit bewegt sich das Unfallopfer mit $v = 2,1 \text{ m} / 1,5 \text{ s} = 1,4 \text{ m/s}$. Extrapoliert man diese Geschwindigkeit auf den Zeitraum vor dem Sichtbarwerden in die Richtung nach links (von wo sie mutmaßlich hergekommen ist), so hat sie sich 3 s früher etwa 2,8 m (Spur 2) und 6 s früher etwa 5,6 m (Spur 3) weiter links befunden.



Abbildung 200: Berechnete Bewegung der Fußgängerin über die Fahrspuren hinweg

Die Frau war also mindestens 7,5 s vor dem Aufprall bereits auf der Fahrbahn unterwegs. Das Fahrzeug war zum Zeitpunkt des Unfalls im ungünstigsten Fall 45 mph = 72,42 km/h = 20,12 m/s schnell. Damit hat es sich 7,5 s vor dem Aufprall rund 150 m vom Unfallort entfernt befunden. Dieser Punkt liegt unter der Brücke:



Abbildung 201: Übersicht des Unfallortes via Google Earth

Nun kann man noch den notwendigen Sichtwinkel ermitteln, ab dem das Unfallopfer in den Sichtbereich des Fahrzeugs getreten ist, das auf der rechten Spur 1 unterwegs war. Man stellt fest, dass die Fußgängerin spätestens mehr als 80 m vor dem Aufprallort in einem Sichtwinkel von < 4° (von der Normalen in der Mitte aus gesehen) erkennbar und nicht durch feststehende Hindernisse verdeckt war. Bei einem Sichtwinkel von 6° wäre sie auch dann noch sichtbar gewesen, wenn sie sich zu diesem Zeitpunkt noch auf Spur 4 befunden hätte. Um dann aber den Aufprallpunkt auf Spur 1 zu erreichen, hätten sie über die Straße rennen müssen, was das Video klar widerlegt. Die Sichtwinkel von 4° bzw. 6° deutlich unter der tatsächlichen Objektivöffnung der Dashcam.

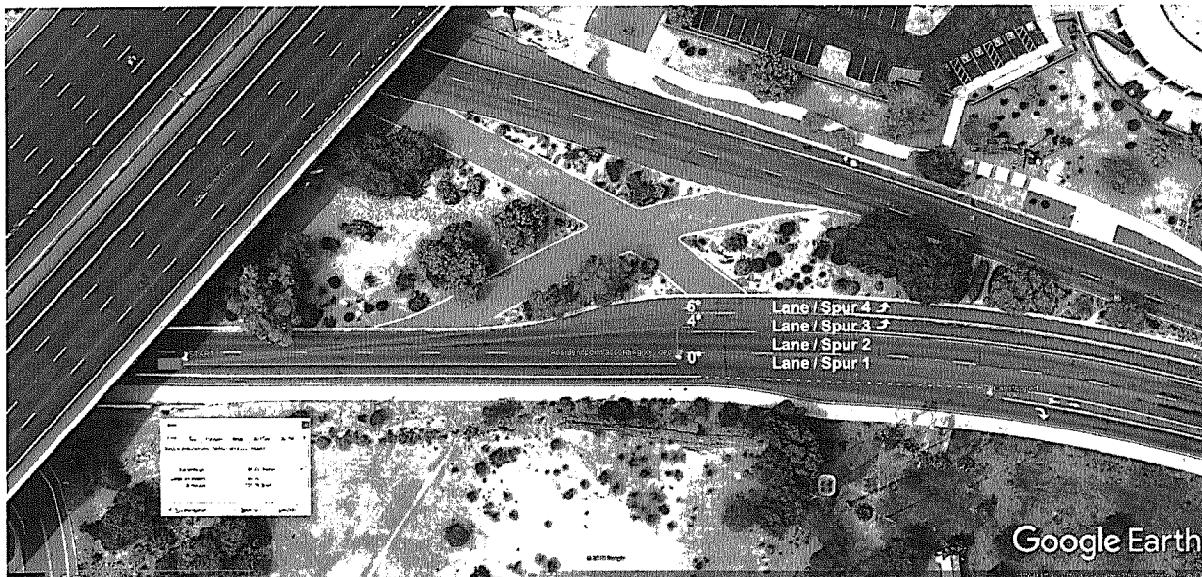


Abbildung 202: Ermittlung des Sichtwinkels

Zur weiteren Visualisierung hat der Autor die Videos / Ansichten auf einem Bildschirm zusammengefügt, synchronisiert und mit einem Timecode versehen.

Aus der zusammengesetzten Animation der Videos erkennt man, dass die Fahrerin des Uber-Fahrzeugs vor dem Unfall genau an dieser Stelle (Timecode 00:00:06:13) letztmalig auf die Fahrbahn geschaut und dann bis kurz vor dem Aufprall nicht mehr hochgeschaut hat.



Abbildung 203: Zusammengesetzte und synchronisierte Videodarstellung

Das hellere Vergleichsvideo zeigt, dass zu diesem Zeitpunkt der Bereich der Abbiegespuren links von den Hauptspuren weder für Sensoren wie einem LIDAR noch für einen menschlichen Fahrer einsehbar waren. Die Frau befand sich zu diesem Zeitpunkt also tatsächlich noch im Sichtschatten.

Vier Sekunden später (Timecode 00:00:10:13) und damit noch etwa vier Sekunden vor dem Zusammenprall (Timecode 00:00:14:05) befand sich das Fahrzeug somit noch mindestens 80 m vom Unfallpunkt entfernt.

Der Anhalteweg errechnet sich unter ungünstigen Bedingungen (1 s Reaktionszeit, 6 m/s² für den Mindestwert einer Verzögerung bei trockenem Asphalt) zu 53,84 m. D.h., dass das Fahrzeug, wenn es zu einem Zeitpunkt, zu dem das Unfallopfer definitiv spätestens sichtbar gewesen sein muss, eine Gefahrenbremsung vorgenommen hätte, rund 24 m vor der Frau zum Stehen gekommen wäre. Somit gilt auch, dass eine Reaktion des Fahrzeugs bzw. der menschlichen Fahrerin spätestens 4,35 s vor dem tatsächlichen Aufprall ausgereicht hätte, einen Unfall zu verhindern. Geht man in der Praxis von noch höheren möglichen Verzögerungswerten von 9 m/s² oder darüber hinaus aus, so reduziert sich der Anhalteweg sogar auf 42,6 m.

Geschwindigkeit in km/h	<input type="text" value="72.42"/> km/h	
Reaktionszeit in Sekunden	<input type="text" value="1"/> s	0.67 s Kuratorium für Verkehrssicherheit 0.8 s MA 46, Wien (Verkehrssicherheitsreferat) 1 s Deutscher Verkehrssicherheitsrat
Bremsverzögerung	<input type="text" value="6"/> m/s ²	m/s ² Eigenschaft 6.0 - 9.0 Asphalt, Beton trocken 5.0 - 7.0 Asphalt naß 4.0 - 6.0 alter Beton naß 6.0 - 8.0 neuer Beton naß 4.0 - 8.0 Pflasterstein naß/trocken 4.0 - 6.0 festgefahrener Kies/Sand 3.0 - 6.0 Wiese fester Untergrund 2.0 - 3.0 fester Erdboden naß 2.0 - 3.0 Schneefahrbahn 0.5 - 3.0 Eis (je nach Temperatur)
Hindernis-entfernung in Meter	<input type="text" value="80"/> m	<input type="checkbox"/> Das Fragezeichen (?) berechnet das Hindernis dort, wo das Fahrzeug zum Stillstand kommt.
Geschwindigkeit: <input type="text" value="72.42"/> km/h Reaktionszeit: <input type="text" value="1"/> s Bremsverzögerung: <input type="text" value="6"/> m/s ² Reaktionsweg: <input type="text" value="20.12"/> m Bremsweg: <input type="text" value="33.72"/> m Anhalteweg: <input type="text" value="53.84"/> m Anhaltezeit: <input type="text" value="4.35"/> s Hindernisentfernung: <input type="text" value="80"/> m Aufprallgeschwindigkeit: <input type="text" value="0"/> km/h Dauer bis zum Aufprall: <input type="text" value="-----"/> s Äquivalente Fallhöhe: <input type="text" value="0"/> m		

Abbildung 204: Berechnung von Anhalteweg und Bremsweg¹⁸⁰

Tatsächlich hat die menschliche Fahrerin erst gut eine Sekunde vor dem Aufprall wieder auf die Fahrbahn geschaut und damit die gesamte einem menschlichen Fahrer zugebilligte Reaktionszeit von einer Sekunde verbraucht, bis eine Reaktion erfolgen konnte / erfolgt ist.

¹⁸⁰ Quelle: <http://www.kfz-handwerk.de/bremsweg.php>

Dipl.-Ing. Thomas Käfer, M.Sc. – Car-Forensics 5.0
Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall,
Kfz-Unfalldatenschreibern und Smartphone-Kopplung

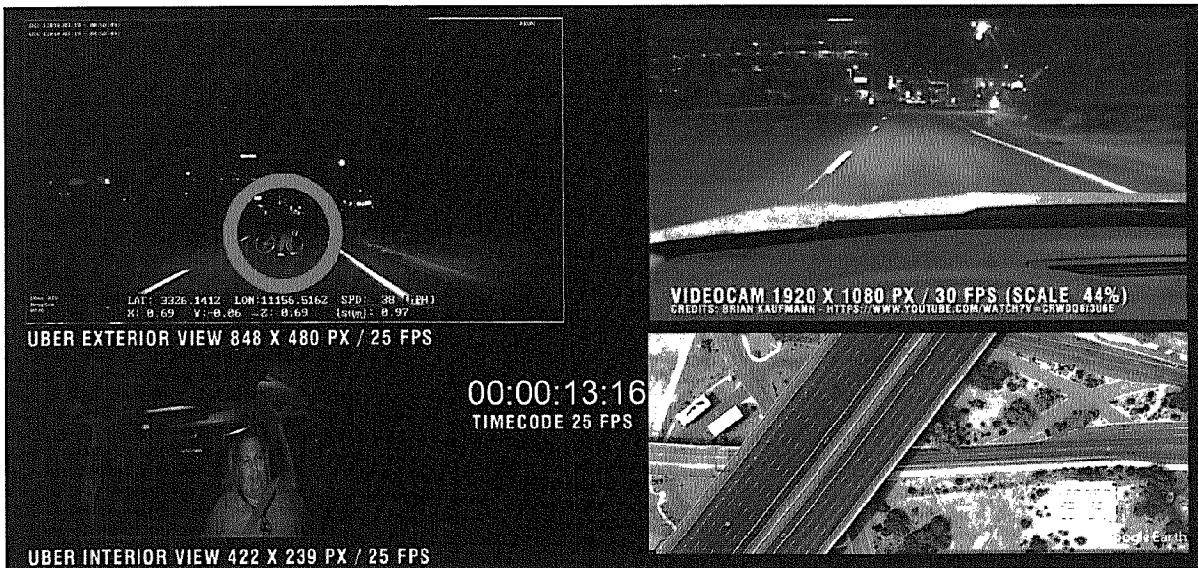


Abbildung 205: Synchronisierte Videodarstellung zum Zeitpunkt kurz vor dem Unfall

Der Aufprall ist etwa 1 Sekunde später mit Timecode 00:00:14:04 dokumentiert.



Abbildung 206: Synchronisierte Videodarstellung zum Zeitpunkt des Aufpralls

Allerspätestens bei Timecode 00:00:12:20 und damit 1,4 Sekunden vor dem Aufprall ist das Unfallopfer auch in dem dunklen Video des Uber-Fahrzeugs sichtbar und definitiv im Erfassungsbereich der Sensoren selbst eines heutzutage in modernen Fahrzeugen üblichen Frontkollisionswarners auf Radar- und/oder Kamerabasis.



Abbildung 207: Spätester Zeitpunkt Sichtbarwerden im Polizeivideo

1,4 Sekunden vor dem Aufprall hatte das Fahrzeug noch einen Abstand von mindestens 28 m zum Unfallopfer. Dies hätte für ein Ausweichmanöver entgegen der Laufrichtung der Frau und bei einem gleichzeitigen Bremsvorgang zu einem reinen Bremsweg von rund 33,7 m geführt. Die Restgeschwindigkeit bei einem Aufprall nach 28 m hätte hierbei nur noch knapp 30 km/h anstatt 72 km/h betragen, was zu weniger als einem Viertel der kinetischen Energie beim Aufprall geführt hätte. Möglicherweise hätte das allein verhindert, dass die Fußgängerin tödlich verletzt worden wäre.

Geschwindigkeit:	72.42	km/h
Reaktionszeit:	0	s
Bremsverzögerung:	6	m/s ²
Reaktionsweg:	0	m
Bremsweg:	33.72	m
Anhalteweg:	33.72	m
Anhaltezeit:	3.35	s
Hindernisentfernung:	28	m
Aufprallgeschwindigkeit:	29.83	km/h
Dauer bis zum Aufprall:	1.97	s
Äquivalente Fallhöhe:	3.5	m

Abbildung 208: Berechnung des reinen Bremswegs und der Aufprallgeschwindigkeit

Ein erfolgreicher Ausweichvorgang selbst 1,4 Sekunden vor dem Aufprall hätte den Unfall vollständig verhindert.

Analysiert man nun noch die Beschleunigungswerte, die im Video des Unfallfahrzeugs in der Fußzeile eingeblendet sind, so stellt man folgendes fest:

Zunächst werden die Beschleunigungswerte deutlich zeitnäher und schneller aktualisiert, als die GPS-Geschwindigkeitswerte. Das kann man am Video ablesen, bei dem beim optisch erkennbaren Aufprall die Beschleunigungswerte signifikant nach oben schnellen. Dass die Beschleunigungswerte schneller aktualisiert werden, erklärt sich dadurch, dass Beschleunigungssensoren eine viel geringere Latenz haben und nicht die zurückgelegte Strecke über ein nennenswertes Zeitintervall gemessen werden müssen. Damit nämlich überhaupt zwei räumlich voneinander getrennt liegende Geo-Positionen zur Geschwindigkeitsmessung heran gezogen werden können, muss bei Messung mittels GPS der systemimmanente Fehler durch ein zeitlich und räumlich ausreichend großes Delta kompensiert werden (mehrere Sekunden und mehr als die Systemgenauigkeit von ca. 15 m).

Die Beschleunigungswerte hinken der tatsächlichen Position im Video also deutlich weniger stark hinterher, als die GPS-Speed-Werte.

Während der gesamten Fahrt vor dem Unfall liegt der Wert für die Beschleunigung in X-Richtung im positiven Bereich (meist unter 1.00). Damit wird der X-Wert mutmaßlich die Beschleunigung des Fahrzeugs in Fahrtrichtung repräsentieren. Y wird die Beschleunigung zur Seite und Z nach unten darstellen.

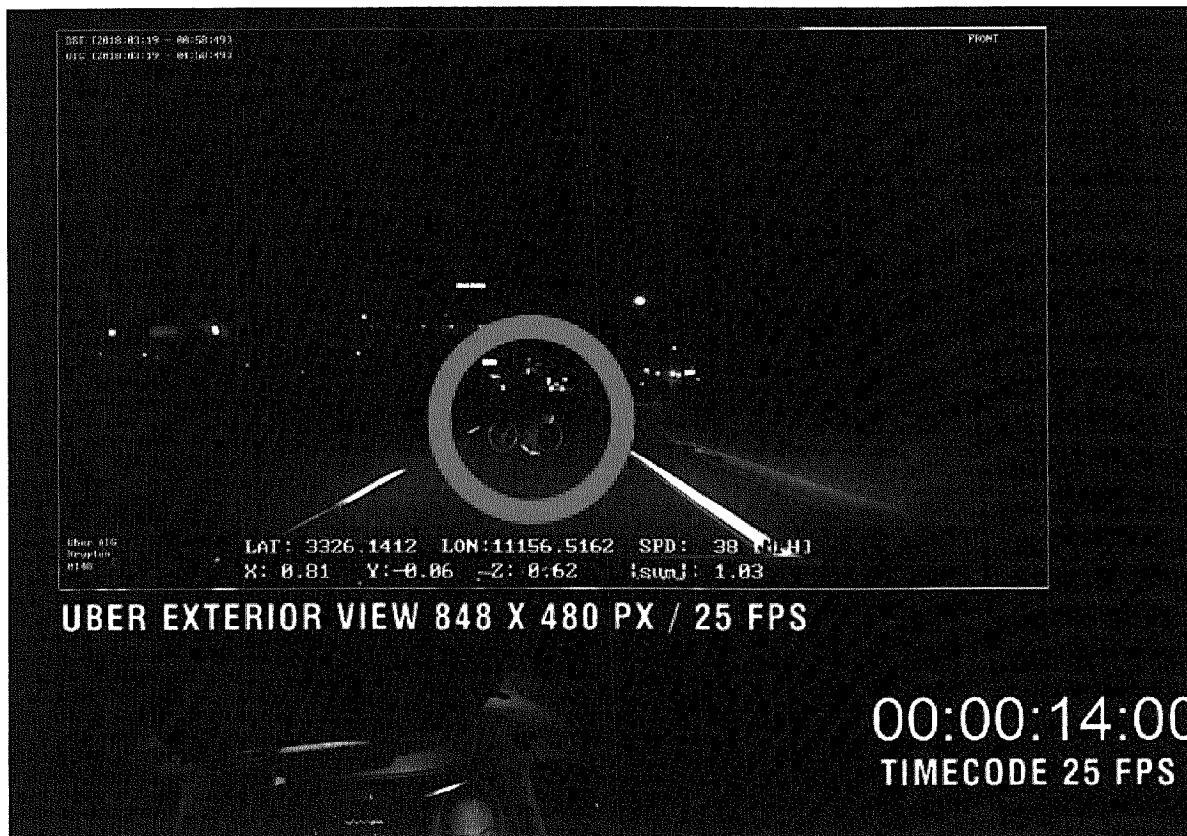


Abbildung 209: Positive Beschleunigungswerte vor dem Unfall

Genau beim Aufprall steigt X auf ein Maximum von -5.62 (Y auf -5,9 und Z auf -2.0). D.h. das Fahrzeug wird deutlich verzögert (negative Beschleunigung) und bekommt einen Drehimpuls nach recht (-Y) und nach unten (-Z):

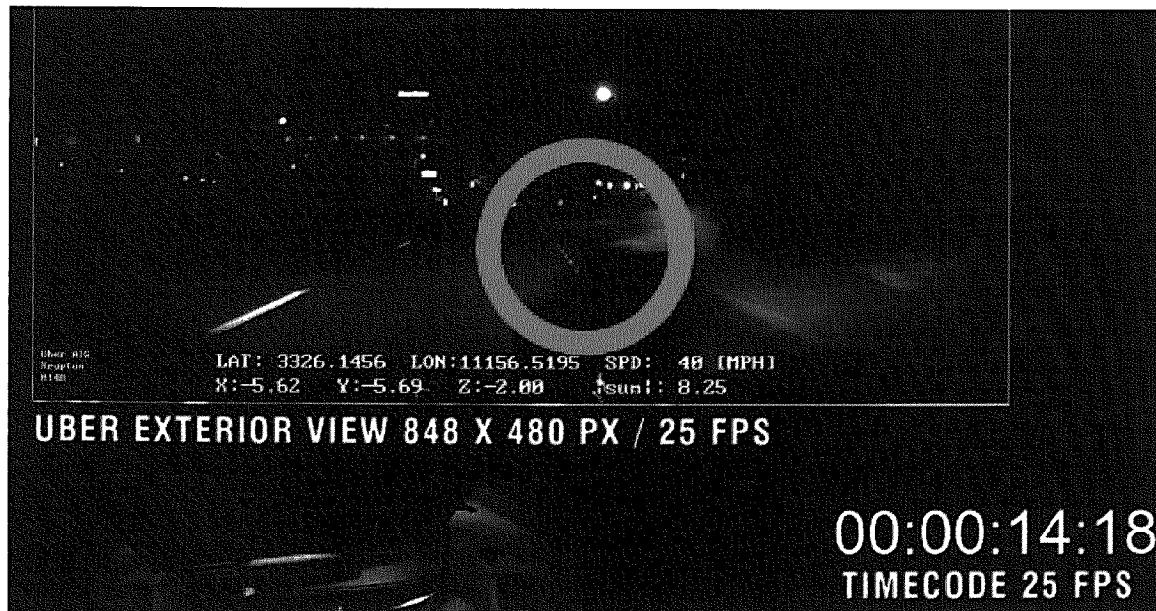


Abbildung 210: Negative Beschleunigungswerte beim Aufprall

Unmittelbar nach dem Aufprall verändern sich die Werte wieder positiv und erreichen in etwa die Beträge vor dem Unfall:

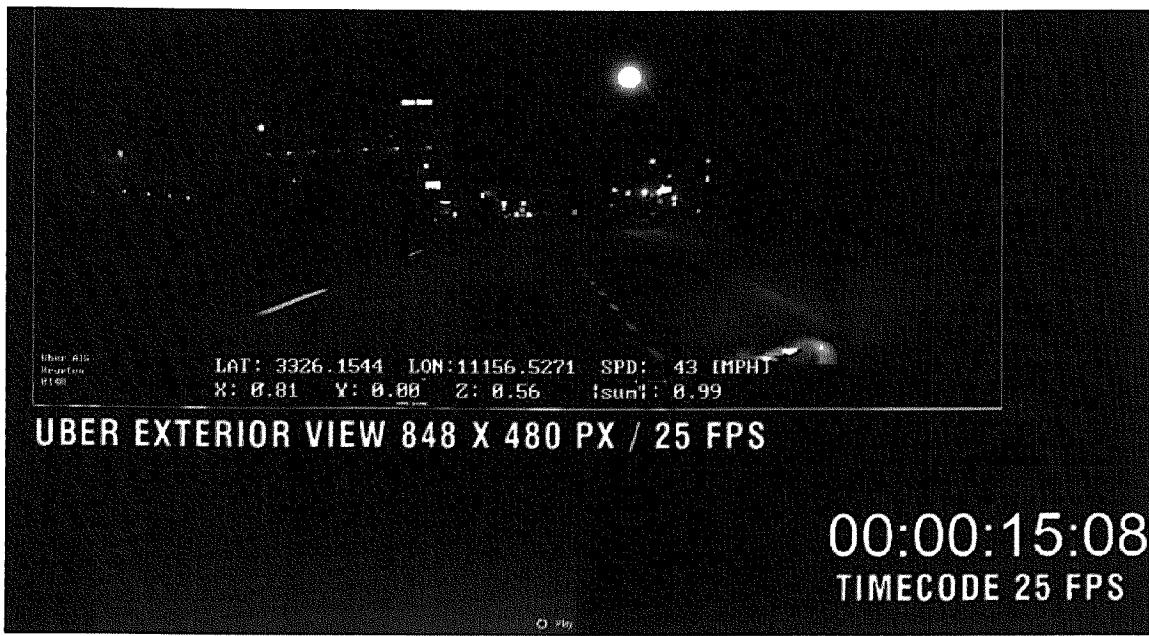


Abbildung 211: Positive Beschleunigungswerte nach dem Aufprall

Ermittelt man dann noch anhand der Fernsehberichterstattung und einem Vergleich mit Google Earth den Punkt, an dem das Fahrzeug offenbar aufgefunden wurde, kommt man unweigerlich zu dem Schluss, dass das Fahrzeug direkt nach dem Unfall die vorher gewählte Geschwindigkeit wieder aufzunehmen versucht und Gas gegeben hat.

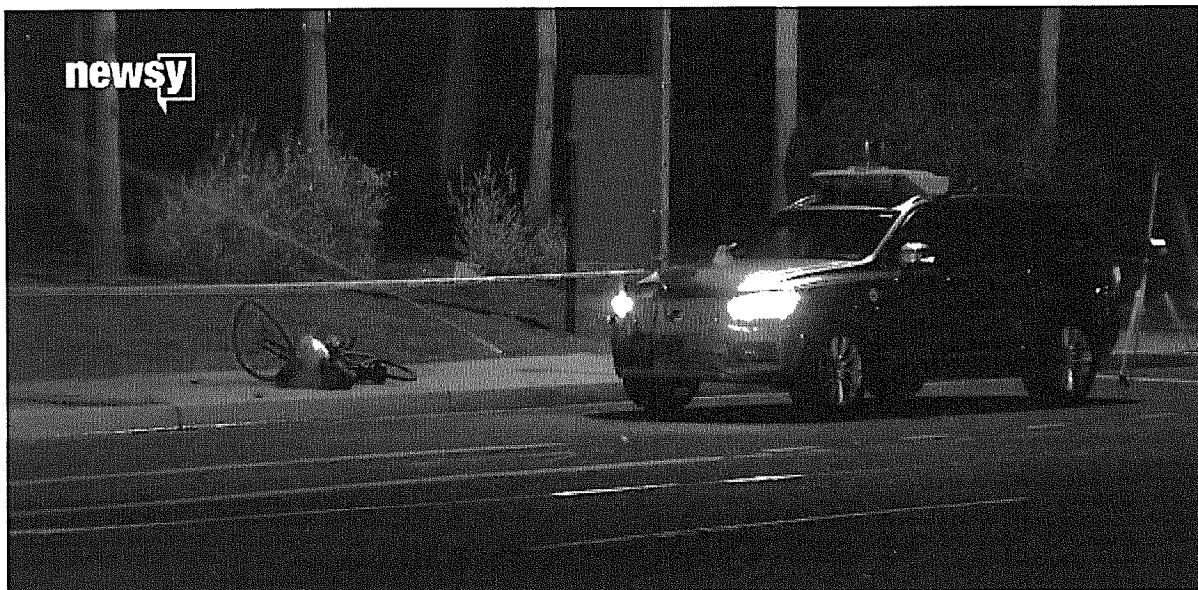


Abbildung 212: Bild der mutmaßlichen Auffindestelle des Fahrzeuges (Quelle: newsy)

Dieser Punkt liegt (abgeschätzt mit Google Earth) mehr als 50 m hinter dem Unfallpunkt. Diese Distanz entspricht in etwa dem Anhalteweg aus $72 \text{ km/h} = 45 \text{ mph}$ (Reaktions- und Bremsweg).

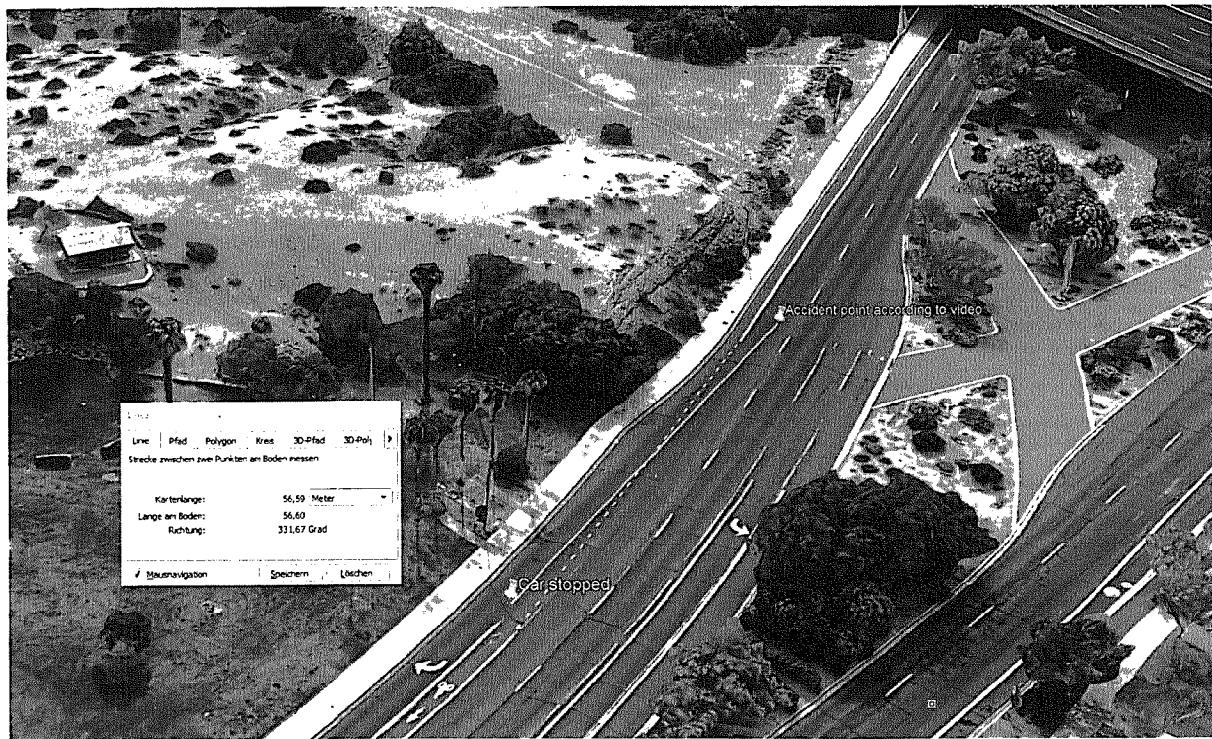


Abbildung 213: Ausmessen der Distanz zwischen Aufprall- und Auffindestelle

Zu vermuten ist, dass die menschliche Fahrerin erst ab dem Moment des Aufpralls wirklich reagiert und dann mit einer Verzögerung von etwa einer Sekunde manuell eine Notbremsung eingeleitet hat.

Das führt wiederum zu einem weiteren Indiz, dass das Fahrzeug das Unfallopfer überhaupt nicht detektiert hat und unbeirrt seinen Weg fortsetzen wollte bzw. hat.

6.4.3 Bewertung des Videomaterials

Beim Studium des Videomaterials und dem Vergleich des Videos des YouTube-Users Brian Kaufmann stellt man sich unweigerlich die Frage, warum die Aufnahmen aus dem Unfallfahrzeug so dunkel sind und ob das Material bewusst oder unbewusst manipuliert oder einfach schlicht ungeeignete Hardware für Videoaufnahmen in der Nacht benutzt wurde. Man könnte auch zu dem Schluss kommen, dass das Vergleichsvideo von Brian Kaufmann deutlich zu hell aufgenommen wurde (große Blende) und die Lichtverhältnisse für das menschliche Auge tatsächlich so schlecht waren, wie aus dem von der Polizei verbreiteten Video hervorgeht.

Der Autor Thomas Käfer hat daher versucht, in seinem Heimatort eine in etwa vergleichbare ausgeleuchtete Straße bei Nacht abzufahren und die subjektive Wahrnehmung der Sichtweite und der Lichtverhältnisse mit zwei Kameras synchron aufgenommen¹⁸¹. Das Ergebnis ist in folgender Darstellung visualisiert:



Abbildung 214: Kameravergleich

Links oben sieht man das Video von Brian Kaufmann und rechts daneben, dieselbe Stelle im Video aus dem Unfallfahrzeug. Darunter sieht man eine beleuchtete Landstraße in Würselen (Deutschland), die links mit einer Sony Videokamera und rechts mit einer einfachen ca. 30 € teuren Action-Cam aufgenommen wurde. Man erkennt beim Vergleich der unteren Bilder auch hier den qualitativen Unterschied vor allem in Bezug auf die Helligkeit. Das Bild der einfachen Action-Cam ist dunkler, mit einer geringeren Auflösung und qualitativ schlechter, hat jedoch ein größeres Weitwinkelobjektiv (ähnlich einer Dashcam). Tatsächlich kann man aber bei beiden Vergleichskameras deutlich über die Reichweite des Abblendlichtes hinaus bis mindestens 100 m weit nach vorn schauen. In der Realität ist die Sichtweite für den menschlichen Fahrer sogar noch weiter und die Szenerie deutlich heller und kontrastreicher.

¹⁸¹ Verwendetes Fahrzeug: Alfa Romeo Stelvio SUV mit Xenon-Scheinwerfern und Abblendlicht

Das zeigt, dass das Vergleichsvideo von Brian Kaufmann nach Ansicht des Autors nicht unnatürlich oder übertrieben hell ist und der Bereich um den Unfallpunkt ausreichend gut ausgeleuchtet war, um das Unfallopfer früh genug für ein Brems- und/oder Ausweichmanöver zu erkennen. Dies gilt umso mehr für RADAR- und LIDAR-Sensoren, die unabhängig von den Lichtverhältnissen arbeiten und bei Dunkelheit eine noch bessere Sensorik besitzen, als ein menschliches Auge. Das Unfallopfer war also für einen aufmerksamen menschlichen Fahrer genauso rechtzeitig erkennbar, wie von den Sensorsystemen des Fahrzeugs und der Unfall damit definitiv vermeidbar.

6.4.4 Zwischen-Fazit

Die Berichterstattung wenige Tage nach dem Ereignis ist tatsächlich nicht nur oberflächlich gewesen, sondern kam tatsächlich in vielen Fällen zu den vollkommen falschen Schlüssen. Zu befürchten ist, dass auch die Polizei zu den falschen Schlüssen kommen wird, wenn sie das Material nicht ebenso sorgfältig und aufwändig auswertet wie der Autor. Ihr ist in jedem Fall zu empfehlen, die Auswertung anhand binär-identischer Kopien der originalen Videos aus dem Fahrzeug vorzunehmen bzw. sich diese unter Aufsicht von unabhängigen Fachleuten herausgeben zu lassen. Der Grund für die deutlich zu dunkle Darstellung ist in jedem Fall aufzuklären, da sie entscheidend für die Beurteilung des Unfalls und dessen Vermeidbarkeit ist.

Als gesichert gelten folgende Erkenntnisse:

1. Das Unfallfahrzeug ist unmittelbar vor dem Unfall mindestens 42 mph und maximal 45 mph schnell gewesen und lag damit innerhalb des an dieser Stelle zulässigen Limits von 45 mph.
2. Das von der Polizei veröffentlichte Video ist mindestens einmal verlustbehaftet kopiert worden und insgesamt wesentlich dunkler, als es die Lichtverhältnisse zum Unfallzeitpunkt hergegeben haben. Tatsächlich ist die Unfallstelle mehr als ausreichend gut durch Straßenlaternen ausgeleuchtet und über einen Weg von mindestens 80 m vor dem Unfallort über alle Fahrspuren bis zu den Fahrbahnrandern einsehbar.
3. Dieser Sichtbereich von mindestens 80 m hätte sowohl für ein automatisiert fahrendes Fahrzeug als auch für ein von einem durchschnittlichen Autofahrer gesteuertes Fahrzeug bei der Geschwindigkeit von max. 45 mph vollkommen ausgereicht, um die Fußgängerin auf der Fahrbahn wahrzunehmen und rechtzeitig vor ihr zum Stehen zu kommen oder ihr auszuweichen.
4. Die menschliche Fahrerin des Unfallfahrzeugs, deren Aufgabe es offensichtlich war, die korrekte Funktion des voll-automatisiert fahrenden Fahrzeugs zu überwachen, war vor dem Unfall für mindestens sechs Sekunden abgelenkt und hat möglicherweise auf ein Smartphone oder Tablet geschaut. Das lässt sich bereits aus dem Gesichtsausdruck ablesen. In diesen sechs Sekunden hat das Fahrzeug rund 120 m zurückgelegt, ohne dass eine Kontrolle der Fahraufgabe erfolgt ist.
5. Das Sensorsystem des voll-automatisiert fahrenden Fahrzeugs hat offenbar keinerlei Reaktion auf die den Fahrweg kreuzende Fußgängerin gezeigt und zu keinem Zeitpunkt abgebremst oder rechtzeitig eine Warnung zum Eingreifen für die menschliche Fahrerin ausgegeben.

Da die Fußgängerin sogar ein Fahrrad geschoben hat, ist davon auszugehen, dass sie ein mehr als ausreichendes Signal sowohl für optisch als auch auf LASER-, RADAR- oder Ultraschallbasis arbeitende Systeme abgegeben hat.

6. Es ist keine Verzögerung vor dem Unfall bzw. durch ein Bremsmanöver im Video erkennbar. Die Verzögerungswerte in den Metadaten stammen offenbar vom Aufprall des menschlichen Körpers. Aufgrund der nacheilenden Geschwindigkeitsanzeige im Video ist davon auszugehen, dass der PKW beim Aufprall nicht 40 oder 42 mph, sondern 45 mph schnell war. Offenbar hat das Fahrzeug unmittelbar nach dem Aufprall wieder versucht, die zuvor eingestellte Geschwindigkeit von 45 mph zu erreichen und kam erst über 50 m nach dem Aufprall mutmaßlich durch eine verspätete Notbremsung der menschlichen Fahrerin zum Stehen.

Diese Erkenntnisse wiederum münden in drei Aussagen:

1. Die Bereitstellung bzw. Veröffentlichung des offenbar unnatürlich dunklen Videos der Frontkamera führt zu Fehldeutungen, dass der Unfall auch für einen menschlichen Fahrer unvermeidbar gewesen wäre und das Unfallopfer unvermindert und plötzlich in den Fahrweg getreten ist. Das ist falsch und widerlegt.
2. Die Sensorik bzw. die Steuerung des mutmaßlich voll-automatisierten Fahrzeugs hat komplett versagt oder war gar nicht eingeschaltet. Dann stellt sich die Frage, wer das Fahrzeug überhaupt auf dem Fahrweg gehalten hat. Für eine weitere Ursachenforschung, was genau im Fahrzeug versagt hat, ist eine aufwändige forensische Untersuchung des Fahrzeugs nötig, die der Autor allein auf Basis der Videoaufnahmen und allgemein zugänglichen Quellen nicht leisten kann.
3. Die menschliche Fahrerin hat ihre Kontrollaufgabe nachweislich nicht wahrgenommen und durch ihre Fahrlässigkeit den Ausfall der Sensorik nicht erkannt und somit den drohenden Unfall nicht verhindert.

6.4.5 Bewertung der Thesen aus den bisherigen Veröffentlichungen

1. Die verunfallte Fußgängerin (die ihr Fahrrad schiebend über die Fahrbahn gegangen ist) soll plötzlich aus dem Schatten hervorgetreten sein.

Diese Aussage ist insofern falsch und widerlegt, da die Fußgängerin bei den tatsächlichen Licht- und Straßenverhältnissen deutlich sichtbar die Fahrbahn überquert hat und bereits mindestens 80 m vor dem Unfallort für Mensch und Maschine erkennbar gewesen sein muss.

2. Das Fahrzeug soll im voll-automatisierten Modus mit umgerechnet 64 km/h (40 mph) anstatt der am Unfallort erlaubten 56,3 km/h (35 mph) unterwegs gewesen sein.

Diese These ist falsch. Am Unfallort waren 45 mph erlaubt und das Fahrzeug fuhr zum Zeitpunkt des Unfalls zwischen mindestens 42 und maximal 45 mph.

3. Das Fahrzeug soll weder nennenswert verzögert noch eine Ausweichbewegung vorgenommen haben.

Das ist korrekt. Es ist keine Verzögerung oder Ausweichbewegung erkennbar. Stattdessen ist anhand der im Video eingebblendeten Beschleunigungswerte sogar noch eine leichte Geschwindigkeitserhöhung unmittelbar nach dem Aufprall feststellbar.

4. Der/die zur Überwachung an Bord des Fahrzeugs befindliche Fahrer(in) soll nicht eingegriffen haben.

Diese These ist korrekt.

5. Der Unfall wäre auch von einem menschlichen Fahrer nicht vermeidbar gewesen.

Diese These ist definitiv falsch. Ein aufmerksamer durchschnittlicher Fahrer hätte den Unfall problemlos durch Bremsen und/oder Ausweichen frühzeitig verhindern können. Das gleiche gilt auch für ein voll-automatisiert fahrendes Fahrzeug, wenn dessen Sensoren und Steuerung richtig funktioniert hätten.

6. Die Polizei von Tempe, Arizona (Sylvia Moir) sagte aus, dass es danach ausgehe, dass Uber keine Schuld an dem Unfall trage und eine Anklage gegen den Fahrer nicht ausgeschlossen werde.

Diese These ist nicht haltbar. Zweifellos hat die Fahrerin ihre Kontrollpflicht drastisch verletzt, da sie vor dem Unfall für mindestens 6 Sekunden und rund 120 m Fahrweg nicht auf die Fahrbahn geschaut hat. Faktisch hätte aber das Fahrzeug die Fußgängerin erkennen und darauf reagieren müssen. Da dies offenbar nicht passierte, ist nun zu klären, wer diesen Fehler zu verantworten hat (Uber, Volvo, Zulieferer).

7. Das Fahrzeug war mit RADAR-Sensoren, Kameras und einem LIDAR-System ausgestattet.

Die Aussage wird korrekt sein, lässt sich aber vom Autor nicht objektiv überprüfen.

8. Am 27.03.2018 wurde Uber die Erlaubnis für weitere Testfahrten mit autonom fahrenden Fahrzeugen bis auf weiteres entzogen.

Die Aussage wird korrekt sein, lässt sich aber vom Autor nicht objektiv überprüfen.

9. Uber hat das Fahrzeug mit eigener Hardware bzw. Software ausgestattet und das serienmäßige Kollisionssystem von Volvo abgeschaltet.

Die Überprüfung dieser These wird elementar für die weitere Ursachenforschung und Schuldermittlung sein.

6.4.6 Erkenntnisse nach Auswertung des Polizei-Berichts

Am 22.06.2018 erhielt der Autor einen 318 starken Abschlussbericht, der weitestgehend angeschwärzt die Ermittlungsergebnisse der Polizei und der beauftragten Forensiker im Detail wiedergibt. Des Weiteren waren Aufnahmen der Bodycams der am Unfallort tätigen Polizeibeamten, die Notrufe und einige weitere Fotos vom Unfallort und des Unfallfahrzeugs beigefügt. Dieses Material wurde vom Autor ausgewertet und mit den eigenen Erkenntnissen abgeglichen.

Hierbei stellte sich zunächst heraus, dass sowohl das in der Dash-Cam angegebene Datum 19.03.2018 als auch die Uhrzeit offenbar falsch waren. Laut Polizeibericht ereignete sich der Unfall am 18.03.2018 gegen 22.00 Uhr Ortszeit. Dieser Fehler wurde am 06.08.2018 bereits im Originalbericht des Autors korrigiert.

6.4.6.1 Auswertung der Dash-Cam

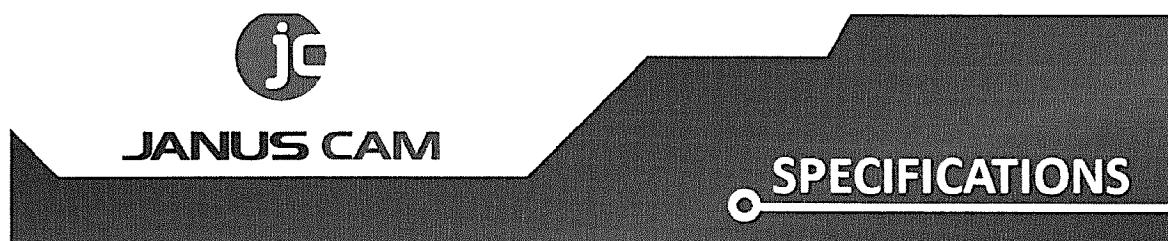
Typ und Funktionen der installierten Dash-Cam

Laut Polizeibericht war im Unfallfahrzeug eine kommerzielle Dash-Cam Janus V3 installiert. Diese verfügt über eine Kamera, die nach vorne und eine, die nach hinten in den Innenraum gerichtet ist, sowie GPS und Beschleunigungssensoren. Offenbar war noch eine weitere Rückfahrkamera extern angeschlossen, deren Bilder aber nicht veröffentlicht wurden und nach Aussage der Beamten offenbar auch keine verwertbaren Informationen zeigten.



Abbildung 215: Originalbild Polizei Tempe - Visualisierung Thomas Käfer

Die Spezifikationen können dem Datenblatt des Herstellers entnommen werden.



The cover of the Janus Cam V3 data sheet features the Janus logo (a stylized 'j' and 'c') at the top left, followed by 'JANUS CAM' in bold capital letters. To the right, a large section titled 'SPECIFICATIONS' is displayed above a photograph of the Janus V3 dashcam unit, which has a black rectangular body with a small screen and several buttons.

Features

- Optimal Audio and Day/Night time recording
- Tamper Proof: Lens and all wires secured with security bracket
- Supports up to 128GB Memory Storage
- Google Maps GPS
- Adjustable Camera Angles
- Optional Third Lens

Category	Descriptions	Remarks
CPU	Cortex-A8 (800MHz) Processor	Linux ARM
1st-Front Camera	1.3 MEA Pixels HD CMOS Sensor	1280 x 720p (HD)
2nd-In-Cabin Camera	1.3 MEA Pixels HD CMOS Sensor	1280 x 720p (HD)
3rd-Rear Camera	NTSC Analog Or Composite	CV 720 x 480p, Optional
Camera Angle	114.34(H, 81.08(V), 134.4(D)	
DDR3RAM	256 MB	GDDR3
Nand Flash Memory	128 MB	Samsung
G-Force Sensor	3-Axis Acceleration Sensor	up to 16G
Speaker / MIC	Mono Speaker / Internal MIC	
Beeper Capacitor	DC 5V over 5F	+44.1 to +85.1 Industrial Level
GPS Module Ant.	GNSS / External GPS Antenna Support	
Removable Storage	micro SD+COMIC x 2 slots	64GB support // Total 128GB use
Video Output	NTSC/PAL	Ear phone Jack to RCA
External Interface		
GPS Signal	2.0M 4PIN ear phone jack	
USB	USB Type-A	USB2.0 support
Rear Camera	2.0M 4PIN ear phone jack	Vehicle back gear signal support
Micro USB	Micro-USB Type B	USB2.0 support
DC Inpux	3.00 DC Input Jack	
AV-Out	2.50 4PIN ear phone jack	Y type cable use for foot use
Format	mp4 / H.264	
Mode	2 Channel use	3 Channel use
Video Encoder	Front: 4Mbps / @30fps	4Mbps / @30fps
In-Cabin	2Mbps / @30fps	2MbpsMax / @15fps
Rear		512bpsMax / @10fps

Category	Descriptions	Remarks
Audio Encode	PCM	Monaural, 22.05Khz, 16bits
Recording	All 5ms Recording	One file / min(62sec/s)
	Button_Event Recording	
	Panic_Event Recording	Before 15 sec. so 0.25s after 15 sec. 28.25s (total 30 sec.)
	G-sensor_Event Recording	
	Battery for RTC Backup	3.7v over 600mAh primary battery -40°C to +125°C Military spec.
Devices in DR	Push button for manual event recording	
	Over 4 IR LEDs for In-Cabin cameras	IR LEDs are turned on and off automatically depends on surrounding luminance
Operating Power Voltage	DC 8V - 32V	DC 12V / DC 24V support
Operating Temperature	-20° to +65°	
Storage Temperature	-30° to +95°	
Dimension (mm)	109(W) x 82(H) x 19(D)	Main body except projection of camera
	121.9(W) x 104.2(H) x 46.1(D)	Main body including GPS cradle and cover case except projection of camera
Weight	Main device: 138g / GPS Cradle : 42g	Assembled all the part: 180g
Warranty Period	1 year after purchase	
Market Defect Rate	Under 0.2%	
UL Standard	UL94-V0	
Certificate	Kohs, CE, FCC	
Product Origin	South Korea	

Janus Cam | 31 Airport Blvd., Suite G2 | South San Francisco, CA 94080 Tel: 650-871-8696 | Fax: 650-871-5914

www.januscam.com | Email Address: info@januscams.com

Abbildung 216: Datenblatt Janus V3 Dash-Cam

Demnach verfügen beide eingebauten Kameras über eine Auflösung von 1,3 Megapixel bei 1200x720p bei 4 Mbps/@30 fps für die externe und 2 Mbps/@30 fps für die interne Kamera. Des Weiteren sind IR-Dioden verbaut, die sich je nach Lichtbedingungen bei der Innenkamera hinzuschalten.

Die Dash-Cam zeichnet nicht nur Unfalldaten sondern kontinuierlich alle Fahrbewegungen incl. Geopositionen, Beschleunigungen und Geschwindigkeit für eine spätere Auswertung auf und ist u.a. für den kommerziellen Einsatz in Fahrzeugflotten gedacht. Die gesammelten Bewegungsdaten (Videos, Audio, Geopositionen etc.) werden in einem Dateiformat „KDS“ auf einer Speicherkarte abgelegt und können mit einem Viewer-Programm des Herstellers angezeigt, ausgewertet und exportiert werden. Durch Integration der Sensorwerte für Geschwindigkeit und Beschleunigung in die Videodarstellung kann ein Event im Detail nachvollzogen werden.



Abbildung 217: Beispielvideo (Auflösung 1200x720p im Video)

Ein ebenfalls von der Herstellerseite heruntergeladenes Video zeigt die Nachtansicht, leider in noch geringerer Auflösung als die Tagesansicht als Demo:

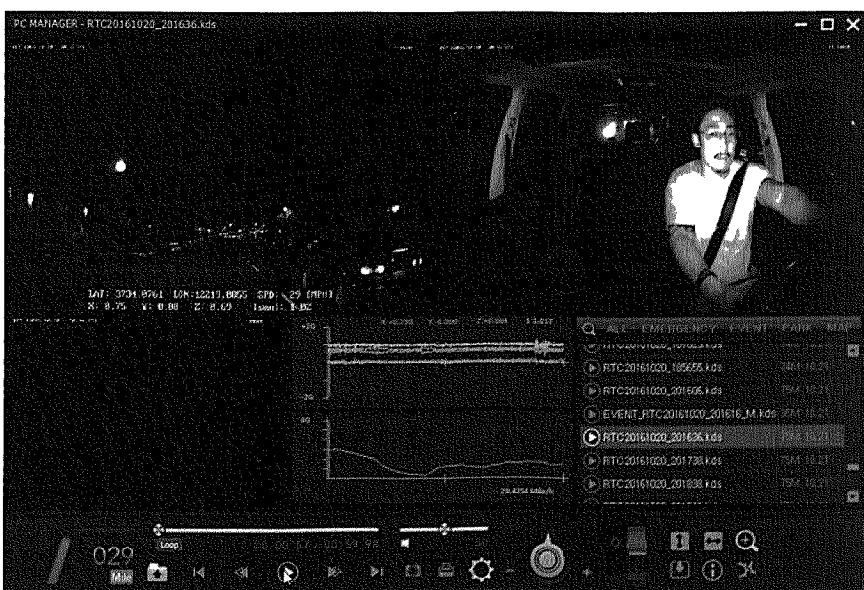


Abbildung 218: Beispielvideo (Auflösung ca. 668 x 454 px im Video)

Der Autor hat eine originale KDS-Datei incl. der Viewer-Software beim Hersteller angefordert, um sich ein eigenes Bild über die Videoqualität beim Export der einzelnen Videos machen zu können. Eine Antwort erhielt er nicht.

Auswertungsergebnisse der Polizei in Tempe

Die Forensiker der Polizei in Tempe haben die SC-Card der im Fahrzeug verbauten Janus V3 Dash-Cam sichergestellt und ausgewertet. Hierbei haben sie die Viewer-Software des Herstellers benutzt (PCMangerInstall-1.6.2.27.exe). Sie ermittelten, dass auf der SC-Card praktisch die gesamten Fahrbewegungen des Fahrzeugs der Nacht aufgezeichnet waren und sich die Fahrerin eindeutig identifizieren ließ.

Sie stellten fest, dass die drei Videos (Front, In-Cabin, Rear) nicht 100% sauber synchronisiert zueinander und dass die eingeblendeten Geschwindigkeitsdaten offenbar nicht vertrauenswürdig waren, da diese weder offensichtlich plausibel waren noch zu den ebenfalls ausgewerteten Daten des Event-Data-Recorders des Airbag-Moduls passten (EDR, siehe weiteres Kapitel im Folgenden).

Den Beamten fiel des Weiteren auf, dass die Fahrerin auffallend oft auf etwas im Bereich unterhalb des Armaturenbretts schaute, teilweise mit einem Lächeln reagierte und werteten die Häufigkeit, wie oft der Blick von der Fahrbahn auf diesen Bereich gesenkt und wie oft und wie lange sie auf die Fahrbahn oder das Armaturenbrett geschaut hat, statistisch aus.

Sie kamen zum Ergebnis, dass die Fahrerin für 31% der rund 21 Minuten und 48 Sekunden dauernden Fahrt vor der Kollision und vor allem mindestens 5,2 Sekunden der 5,7 Sekunden vor dem Zusammenprall nicht auf die Straße geschaut hat. Die Ermittler vermuten, dass die Fahrerin eines der beiden sichergestellten Smartphones während der Fahrt benutzt und sich dieses in ihrer Hand unterhalb des Armaturenbretts befunden hat.

6.4.6.2 Forensische Auswertung der Smartphones

Die Polizeibeamten stellten vor Ort zwei Smartphones bei der Fahrerin sicher und werteten diese im Nachgang forensisch aus. Hierbei stellten sie fest, dass es auf einem Smartphone Hinweise für die Nutzung der Streaming-Dienste YouTube, Netflix und Hulu gab. Daraufhin extrahierten sie die Nutzungshistorie und glichen diese mit den bei den Providern zum Benutzer-Account der Fahrerin gespeicherten Zugriffen ab.

Letztlich stellte sich heraus, dass die Fahrerin mit an Sicherheit grenzender Wahrscheinlichkeit unmittelbar vor dem Unfall eine Folge der Talentshow „The Voice“ auf Hulu angeschaut hat.

6.4.6.3 Untersuchung des EDR des Airbag-Moduls

Im Unfallfahrzeug war im Airbag Modul ein Unfalldatenschreiber des Zulieferers Bosch verbaut, der sich forensisch auslesen ließ.

Hiernach fuhr das Fahrzeug 5 Sekunden vor dem Zusammenstoß 44,1 mph (also knapp unterhalb des dort erlaubten Limits). Man erkennt, dass die Geschwindigkeit etwa 3,5 Sekunden vor dem Impact leicht zu sinken beginnt, um 0,5 Sekunden vor dem Aufprall immer noch 37,3 mph aufzuweisen.

Dipl.-Ing. Thomas Käfer, M.Sc. – Car-Forensics 5.0
 Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall,
 Kfz-Unfalldatenschreibern und Smartphone-Kopplung

2 Sekunden vor dem Aufprall gab es einen 1% Lenkeinschlag nach links, 1 Sekunde vorher einen Wert von 2% nach links und 0,5 Sekunden vor dem Aufprall einen Input von 4% Lenkwinkel nach rechts. Zum Zeitpunkt des Aufpralls gab es dann wieder einen Lenkimpuls von 2% nach links. Erst unmittelbar zum Zeitpunkt des Aufpralls wurde der Aufzeichnung des EDRs zufolge die Bremse betätigt.

 TEMPE POLICE DEPARTMENT General Offense Report	GO# TE 2018-32694																																																																																																																						
Operational Status: ADMINISTRATIVE																																																																																																																							
<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> BOSCH <i>18-32694</i>  </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="2">Pre-Crash Data -1 Sec (Event Record 1)</th> </tr> </thead> <tbody> <tr> <td>Safety Belt Status: Driver</td> <td>On</td> </tr> <tr> <td>Safety Belt Status: Passenger</td> <td>On</td> </tr> <tr> <td>Front Airbag Warning Lamp</td> <td>Off</td> </tr> <tr> <td>Front Airbag Deployment Status: Front Passenger</td> <td>Off</td> </tr> <tr> <td>Seat Belt Position Sensor: Frontmost, Status: Driver</td> <td>Not Equipped</td> </tr> <tr> <td>Seat Belt Position Sensor: Frontmost, Status: Front Passenger</td> <td>No</td> </tr> <tr> <td>Occupant Size Right Front Passenger: Child</td> <td>No</td> </tr> <tr> <td>Occupant Size Right Front Passenger: Child</td> <td>No</td> </tr> </tbody> </table> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="2">Pre-Crash -5 to 0 sec (Event Record 1)</th> </tr> <tr> <th>Time (sec)</th> <th>Speed, Vehicle Indicated (mph)</th> <th>Accelerator Pedal (% Full)</th> <th>Service Brake (0% off)</th> <th>Steering Input (%)</th> <th>ABS Activated</th> <th>Stability Control Status</th> </tr> </thead> <tbody> <tr> <td>-5.0</td> <td>44.1 (71.0)</td> <td>0.0</td> <td>Off</td> <td>0.0</td> <td>On</td> <td>On</td> </tr> <tr> <td>-4.5</td> <td>44.1 (71.0)</td> <td>0.0</td> <td>Off</td> <td>0.0</td> <td>On</td> <td>On</td> </tr> <tr> <td>-4.0</td> <td>44.1 (71.0)</td> <td>0.0</td> <td>Off</td> <td>0.0</td> <td>On</td> <td>On</td> </tr> <tr> <td>-3.5</td> <td>43.5 (70.0)</td> <td>0.0</td> <td>Off</td> <td>0.0</td> <td>On</td> <td>On</td> </tr> <tr> <td>-3.0</td> <td>43.5 (70.0)</td> <td>0.0</td> <td>Off</td> <td>0.0</td> <td>On</td> <td>On</td> </tr> <tr> <td>-2.5</td> <td>43.5 (70.0)</td> <td>0.0</td> <td>Off</td> <td>0.0</td> <td>On</td> <td>On</td> </tr> <tr> <td>-2.0</td> <td>41.8 (66.0)</td> <td>0.0</td> <td>Off</td> <td>0.0</td> <td>On</td> <td>On</td> </tr> <tr> <td>-1.5</td> <td>40.4 (65.0)</td> <td>0.0</td> <td>Off</td> <td>0.0</td> <td>On</td> <td>On</td> </tr> <tr> <td>-1.0</td> <td>37.9 (61.0)</td> <td>0.0</td> <td>Off</td> <td>-1.0</td> <td>On</td> <td>On</td> </tr> <tr> <td>-0.5</td> <td>37.3 (60.0)</td> <td>0.0</td> <td>Off</td> <td>-1.0</td> <td>On</td> <td>On</td> </tr> <tr> <td>0.0</td> <td>35.6 (56.0)</td> <td>0.0</td> <td>On</td> <td>-2.0</td> <td>On</td> <td>On</td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> <td>-4.0</td> <td>On</td> <td>On</td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> <td>-2.0</td> <td>On</td> <td>On</td> </tr> </tbody> </table>		Pre-Crash Data -1 Sec (Event Record 1)		Safety Belt Status: Driver	On	Safety Belt Status: Passenger	On	Front Airbag Warning Lamp	Off	Front Airbag Deployment Status: Front Passenger	Off	Seat Belt Position Sensor: Frontmost, Status: Driver	Not Equipped	Seat Belt Position Sensor: Frontmost, Status: Front Passenger	No	Occupant Size Right Front Passenger: Child	No	Occupant Size Right Front Passenger: Child	No	Pre-Crash -5 to 0 sec (Event Record 1)		Time (sec)	Speed, Vehicle Indicated (mph)	Accelerator Pedal (% Full)	Service Brake (0% off)	Steering Input (%)	ABS Activated	Stability Control Status	-5.0	44.1 (71.0)	0.0	Off	0.0	On	On	-4.5	44.1 (71.0)	0.0	Off	0.0	On	On	-4.0	44.1 (71.0)	0.0	Off	0.0	On	On	-3.5	43.5 (70.0)	0.0	Off	0.0	On	On	-3.0	43.5 (70.0)	0.0	Off	0.0	On	On	-2.5	43.5 (70.0)	0.0	Off	0.0	On	On	-2.0	41.8 (66.0)	0.0	Off	0.0	On	On	-1.5	40.4 (65.0)	0.0	Off	0.0	On	On	-1.0	37.9 (61.0)	0.0	Off	-1.0	On	On	-0.5	37.3 (60.0)	0.0	Off	-1.0	On	On	0.0	35.6 (56.0)	0.0	On	-2.0	On	On					-4.0	On	On					-2.0	On	On
Pre-Crash Data -1 Sec (Event Record 1)																																																																																																																							
Safety Belt Status: Driver	On																																																																																																																						
Safety Belt Status: Passenger	On																																																																																																																						
Front Airbag Warning Lamp	Off																																																																																																																						
Front Airbag Deployment Status: Front Passenger	Off																																																																																																																						
Seat Belt Position Sensor: Frontmost, Status: Driver	Not Equipped																																																																																																																						
Seat Belt Position Sensor: Frontmost, Status: Front Passenger	No																																																																																																																						
Occupant Size Right Front Passenger: Child	No																																																																																																																						
Occupant Size Right Front Passenger: Child	No																																																																																																																						
Pre-Crash -5 to 0 sec (Event Record 1)																																																																																																																							
Time (sec)	Speed, Vehicle Indicated (mph)	Accelerator Pedal (% Full)	Service Brake (0% off)	Steering Input (%)	ABS Activated	Stability Control Status																																																																																																																	
-5.0	44.1 (71.0)	0.0	Off	0.0	On	On																																																																																																																	
-4.5	44.1 (71.0)	0.0	Off	0.0	On	On																																																																																																																	
-4.0	44.1 (71.0)	0.0	Off	0.0	On	On																																																																																																																	
-3.5	43.5 (70.0)	0.0	Off	0.0	On	On																																																																																																																	
-3.0	43.5 (70.0)	0.0	Off	0.0	On	On																																																																																																																	
-2.5	43.5 (70.0)	0.0	Off	0.0	On	On																																																																																																																	
-2.0	41.8 (66.0)	0.0	Off	0.0	On	On																																																																																																																	
-1.5	40.4 (65.0)	0.0	Off	0.0	On	On																																																																																																																	
-1.0	37.9 (61.0)	0.0	Off	-1.0	On	On																																																																																																																	
-0.5	37.3 (60.0)	0.0	Off	-1.0	On	On																																																																																																																	
0.0	35.6 (56.0)	0.0	On	-2.0	On	On																																																																																																																	
				-4.0	On	On																																																																																																																	
				-2.0	On	On																																																																																																																	
<small>TYB00PLSH14950</small> <small>Page 3 of 15</small> <small>Printed: Tuesday March 20 2018 at 11:11:30</small>																																																																																																																							

Abbildung 219: Auszug aus EDR-Auswertung (Quelle Polizei, Tempe)

Anmerkung des Autors: Auch wenn ein Report eines validierten EDRs grundsätzlich eine verlässliche Datenquelle darstellt, stehen die Daten in gewissem Widerspruch zu dem, was man aus dem Video ablesen kann. Dort ist weder eine nennenswerte Seitwärtsbewegung noch die Verringerung der Geschwindigkeit ablesbar. Zu einer weiteren Bewertung müsste ein längerer Videoausschnitt bis zum vollständigen Stillstand des Fahrzeugs bereitgestellt werden.

6.4.6.4 Untersuchungen am Unfallort

Befragung der Fahrerin

Der Auswertung der Bodycams bei der Befragung der Fahrerin und den Berichten der den Unfall aufnehmenden Polizeibeamten kann man entnehmen, dass die Fahrerin grundsätzlich körperlich in der Lage war, das Fahrzeug zu steuern bzw. zu beaufsichtigen.

Sie befand sich nach eigener Aussage auf der dritten Runde einer Testfahrt für Uber und hatte beim Systemstart keine Auffälligkeiten am Fahrzeug bzw. Computer für die automatische Fahrfunktion festgestellt.

Die Fahrerin gab an, dass das Unfallopfer „aus dem Nichts“ vor ihr aufgetaucht wäre und sie konnte auch nicht angeben, woher die Person gekommen war. Unmittelbar beim oder nach dem Aufprall hätte sie manuell gebremst und wäre daraufhin zum Stehen gekommen. Dann hat sie die Notrufnummer gewählt, jedoch keine weitere Notfallmaßnahme am Unfallort eingeleitet.

Bei näherer Befragung, wo ihre Hände zum Zeitpunkt gewesen wären, gab sie an, dass diese „über das Lenkrad gehovert“ wären. Wie sich später bei Inaugenscheinnahme der Arbeitsanweisungen von Uber für Testfahrten herausstellte, wird dort die Anweisung gegeben, dass der Fahrer die Fahraufgabe des automatisch fahrenden Fahrzeugs durch ständiges „Hovern“ mit den Händen über das Lenkrad und mit den Füßen über die Pedale „begleiten“ soll, um im Fehlerfall schnell eingreifen zu können.

Berechnung der Geschwindigkeit anhand der Unfallspuren

Die Polizei kommt nach Auswertung rein der physikalischen Spuren zu dem Ergebnis, dass der Aufprall zwischen Fahrzeug und Fußgängerin/Fahrrad mit einer Geschwindigkeit von 39 mph erfolgte.

Dieser Wert liegt etwas unter dem Wert, der sich auf Basis der Auswertung des Videomaterials und der Aufzeichnungen der Dash-Cam-Sensoren sowie des EDR's ergeben. Sie sind aber von der Größenordnung vollkommen plausibel und mit einer höheren Ungenauigkeit zu bewerten, da die Berechnung rein auf der Auswertung von Effekten (Auffindestellen, Spurenlage) basiert und nicht zum Zeitpunkt des Events explizit gemessen wurde.

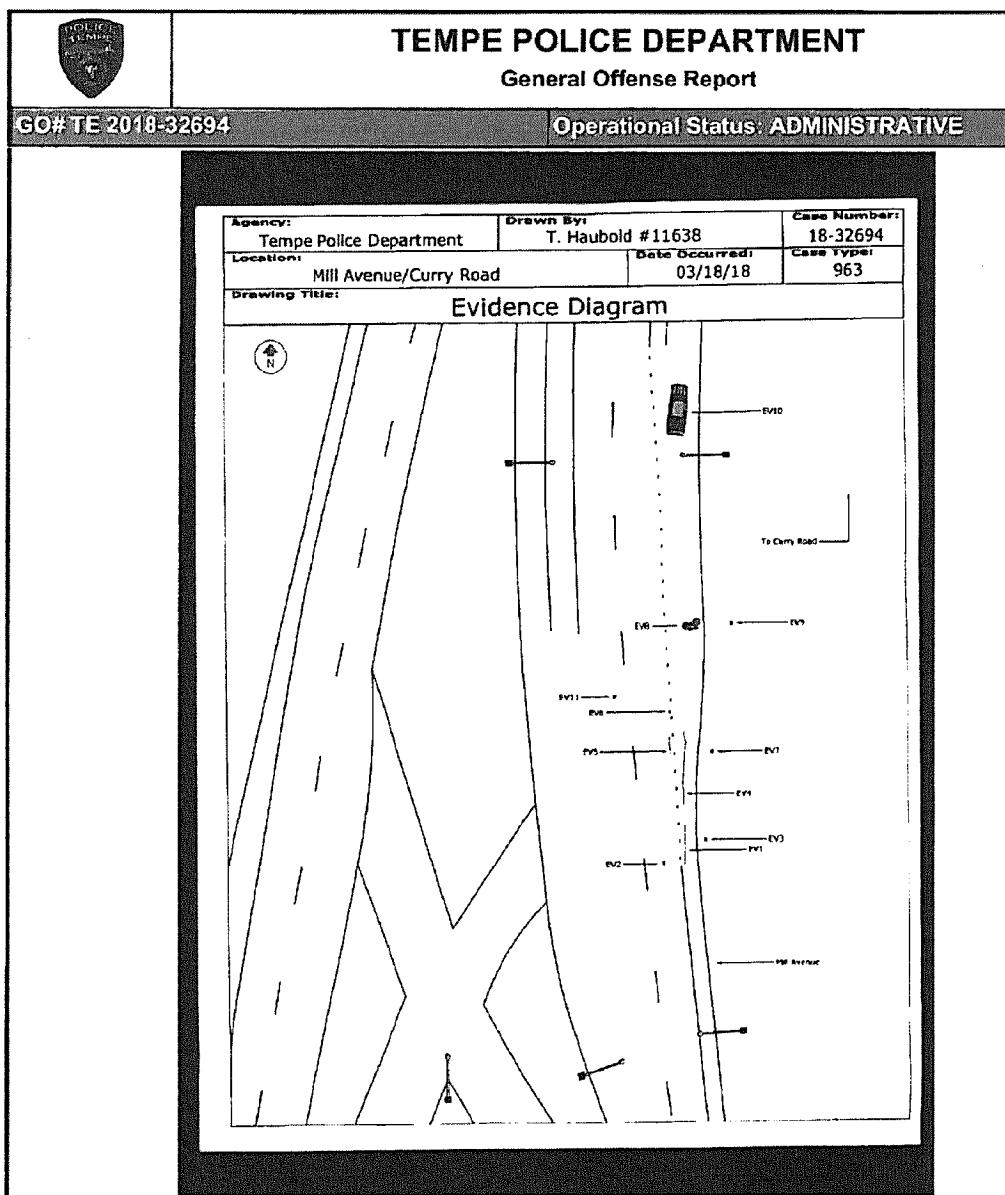


Abbildung 220: Skizze des Unfallortes (Quelle: Polizei, Tempe)

Sichtbedingungen und Bremsweg

Die Polizei hat am 22.03.2018 wenige Tage nach dem Unfall die Unfallszene vor Ort nachgestellt und hierbei sowohl die Sichtweite als auch den Fahrbahnzustand hinsichtlich möglicher Bremsverzögerung untersucht.

In Bezug auf die Sichtbedingungen und damit die Frage, ob und wann die Fußgängerin für Mensch und Fahrzeug erkennbar war, stellten die Ermittler fest, dass die generelle Sichtweite 637,3 ft (= 194,25 m) beträgt. Unter Abzug typischer Faktoren und Berücksichtigung der konkreten Situation jeweils zu Ungunsten einer früheren Detektierung kamen die Ermittler dann zu dem Ergebnis, dass das Opfer mindestens 143,4 ft (43,68 m) vor dem Aufprall zu sehen gewesen sein muss. Das Fahrzeug hat zu diesem Zeitpunkt laut EDR des Airbag-Moduls eine Geschwindigkeit von 43,5 mph gehabt.

Auf Basis des vor Ort durchschnittlich gemessenen Verzögerungswertes von 0,92 g und einer Reaktionszeit von 1,25 Sekunden kam man zu dem Ergebnis, dass das Fahrzeug bei einer so ausgelösten Vollbremsung am Punkt des theoretischen Aufpralls eine Restgeschwindigkeit von 12 mph gehabt hätte.

Da sich die Fußgängerin jedoch von links nach rechts mit 3.18 mph (= 5,12 km/h) gehend während des Vorgangs bewegt hat und das Fahrzeug durch den hypothetisch eingeleiteten Bremsvorgang erst 0,57 s später am gedachten Impact-Punkt angekommen wäre, wäre die Fußgängerin zu diesem Zeitpunkt schon außerhalb der Fahrlinie gewesen und nicht getroffen worden.

6.4.6.5 Positive Ergebnisse der Polizei

Die Polizei kommt in ihrem Abschlussbericht zu folgenden Ergebnissen:

Der Unfall war definitiv vermeidbar.

1. Das Unfallopfer hat die Straße an einer nicht dafür zugelassenen Stelle überquert und nicht den markierten Überweg benutzt.
2. Die Fahrerin des Unfallfahrzeugs war unaufmerksam, während sie das Fahrzeug geführt hat (im rechtlichen Sinn Fahrzeugführerin).
3. Die Fahrerin war für 31% der 21 Minuten und 48 Sekunden dauernden Fahrt vor dem Unfall abgelenkt und hat nach unten geschaut.
4. Die Fahrerin war 5,2 der 5,7 Sekunden vor dem Unfall abgelenkt und hat nach unten geschaut.
5. Der Fehler lag bei der Fahrerin darin, dass sie die Kontrolle hätte übernehmen müssen, um den Unfall zu verhindern.
6. Die Fahrerin ignorierte die zugewiesenen Jobfunktionen, um in einer gefährlichen Situation einzutreten.

Der Fall wurde an das zuständige Gericht zur Anklage gegen die Fahrerin weitergeleitet.

Based on this investigation, the following factors lead to the crash that resulted in the death of Elaine Herzberg:

1. Herzberg unlawfully crossing the road at a location other than a marked crosswalk.
2. Vasquez's inattention to the roadway conditions while operating the vehicle.
3. Vasquez was distracted and looking down for 31% of the 21 minutes and 48 seconds prior to the collision.
4. Vasquez was distracted and looking down for 5.2 seconds of the 5.7 seconds prior to impact.
5. Failure on the part of Vasquez to take control of the vehicle and avoid the crash.
6. Vasquez's disregard for assigned job function to intervene in a hazardous situation.

	TEMPE POLICE DEPARTMENT General Offense Report	
GO# TE 2018-32694	Operational Status: ADMINISTRATIVE	
This case is being submitted to the Maricopa County Attorney's Office for review for charges against Rafael Vasquez		

Abbildung 221: Ergebnisse des Polizeiberichtes

6.4.6.6 Negative bzw. fehlende Ergebnisse der Polizei

Der mit 318 Seiten sehr umfangreiche Abschlussbericht der Polizei in Tempe, Arizona lässt einige wesentliche Dinge vollkommen unberücksichtigt.

Zum einen wird mit keinem Wort darauf eingegangen, warum die Sensoren bzw. die Steuerungssoftware des voll-automatisch fahrenden Fahrzeugs nicht auf die querende Fußgängerin reagiert haben. Es wird lediglich festgestellt, dass laut Aussage von Uber die Sensorik des Basisfahrzeugs (Volvo) abgeschaltet und durch Uber-eigene Systeme ersetzt worden war. Ob für die Fehlfunktion nun ein Ausfall eines Sensorsystems, widersprüchliche Sensorinformationen oder eine Fehler in der Auswertungs- und Steuerungs-Software die Ursache für die nicht detektierte Kollisionssituation waren, wurde von der Polizei nicht untersucht oder hinterfragt.

Überhaupt verwundert den Leser des Berichtes die auffallende Zahl von Schwärzungen in selbigem, u.a. dann, wenn es hierbei um die Rolle der Firma Uber geht (z.B. im Rahmen einer Mitarbeit bei der Auswertung).

Auf die schlechte Video-Qualität der veröffentlichten Videos geht der Bericht genauso wenig ein, wie auf die konkrete Methode, wie diese Videos tatsächlich generiert wurden. Es ist hierbei nur die Rede davon, dass drei zusammengesetzte Videos in einem Viewer-Programm nicht sauber synchronisiert sind und dann (ebenfalls als eine zusammengesetzte Ansicht) in ein AVI-File exportiert wurden. Wie daraus die veröffentlichten Einzelvideos entstanden und warum diese deutlich schlechter aufgelöst und ausgeleuchtet sind, als es das Ursprungsmaterial hergibt (immerhin nur 848 x 480 statt der möglichen 1200 x 720 Pixel pro Video), bleibt unklar.

6.4.6.7 Vergleich der Erkenntnisse der Polizei und des Autors

Nicht nur für den Forensiker ist interessant, in wieweit die Thesen und Erkenntnisse des Forensikers Thomas Käfer allein auf Basis der Auswertung des Videomaterials und Abgleich mit Daten z.B. aus Google Earth aus der entfernten Betrachtung mit den Berichten der Ermittler vor Ort übereinstimmen und wo sie differieren.

Geschwindigkeit des Fahrzeugs vor und während des Unfalls

Die Polizei geht von einer Geschwindigkeit von 44,1 mph vor und ca. 37,9 bis 43,5 mph unmittelbar zum Zeitpunkt des Unfalls aus. Der Autor ermittelte mindestens 42 und maximal 45 mph.

Geschwindelt und Laufweg des Opfers

Die Polizei ermittelte, dass das Unfallopfer mit einer Geschwindelt von 5,12 km/h die Strasse von links nach rechts querte. Der Autor berechnete $1,4 \text{ m/s} = 5,04 \text{ km/h}$.

Aufmerksamkeit der Fahrerin

Die Polizei ermittelte als Zeitspanne 5,2 Sekunden von 5,7 Sekunden vor dem Unfall, in der die Fahrerin nicht auf die Straße geschaut hat. Der Autor kommt auf 6 Sekunden. Beide stellen übereinstimmend fest, dass die Fahrerin regelmäßig für längere Zeit nach unten geschaut und vermutlich ein Smartphone genutzt hat. Die Polizei findet ergänzend heraus, dass sie eine Folge der Talentshow „The Voice“ geschaut hat.

Sichtbarkeit des Unfallopfers

Die Polizei ermittelte eine grundsätzliche Sichtweite von 194,25 m, in der die Person bei den an der Unfallstelle vorherrschenden Bedingungen sichtbar war. Im ungünstigsten Fall hätte sie spätestens 43,68 m vor dem Aufprall erkennbar sein müssen, was diesen bei einer dann eingeleiteten Vollbremsung komplett verhindert hätte. Der Autor kommt auf eine Sichtbarkeit von mindestens 80 m.

Vermeidbarkeit des Unfalls

Der Unfallbericht der Polizei kommt genauso wie der Autor aber abweichend zur Presseberichterstattung auf Basis der ersten Pressemitteilungen der Polizei zu dem Schluss, dass der Unfall für Mensch und Maschine vermeidbar war.

6.4.6.8 Stellungnahme von Uber

Uber hat sich zu dem Unfall bisher nicht im Detail geäußert und auch keine Details darüber veröffentlicht, warum das System die Fußgängerin nicht als Hindernis erkannt und darauf reagiert hat.

Die Firma hatte zunächst ihre Testfahrten generell eingestellt. In Arizona waren diese Testfahrten von der Administration nach dem Unfall ohnehin vorerst verboten worden.

Am 26.07.2018 hat Uber angekündigt¹⁸², die Tests wieder aufzunehmen. Diesmal sollen aber Fachleute am Steuer sitzen, die jederzeit eingreifen können. Hier stellt sich die Frage, welche Qualifikation die bisherigen Test-Fahrer hatten.

6.4.7 Zusammenfassung

Aus diesem Unfall kann man somit zwei Lehren ziehen:

1. Tests von voll-automatisiert fahrenden Fahrzeugen im regulären Verkehr sind nur unter durchgängiger und andauernder Überprüfung durch einen aufmerksamen menschlichen Fahrer zulässig, der während der Fahrt keine anderen Aufgaben oder Sidetasks wahrnehmen darf.
2. Die Inbetriebnahme von voll-automatisiert bzw. autonom fahrenden Fahrzeugen hat zu unterbleiben, wenn aus „Sicherheitsgründen“ noch ein Mensch zur Beobachtung mitfahren soll. Entweder kann das Fahrzeug jede Situation vollständig eigenständig meistern oder nicht. Ein Fallback auf einen menschlichen Fahrer kann es bei einem autonom fahrenden Fahrzeug ja schon per Definition nicht geben. Und das Beispiel des Uber-Crash hat auf traurige Weise gezeigt, dass ein mit einem Sidetask beschäftigter Backup-Fahrer nicht schnell genug einschreiten kann, wenn das Fahrzeug in eine für es selber nicht lösbare Situation oder in eine nicht detektierte Gefahrensituation gerät.

Die gesellschaftliche Akzeptanz eines von einer Maschine verursachten tödlichen Unfalls, den ein Mensch problemlos hätte vermeiden können, liegt nahe Null und gefährdet damit das gesamte Projekt zum automatisierten und autonomen Fahren.

¹⁸² Quelle: <https://www.businessinsider.de/uber-resumes-testing-self-driving-cars-pittsburgh-2018-7?r=US&IR=T>

Der Polizeibericht lieferte weitere Belege für ein nach Ansicht des Autors angebrachte kritische Bewertung von Tests bzw. den Betrieb von voll-automatisiert fahrenden Fahrzeugen auf öffentlichen Straßen. Der Unfall und das Verhalten der menschlichen Fahrerin zeigen deutlich, dass es unseriös ist, anzunehmen, dass eine Person, die eine offensichtlich und leider im wahrsten Sinne des Wortes „tod-langweilige“ Kontrollaufgabe zu erfüllen hat, diese nicht ermüdfrei und ohne Ablenkung wahrnehmen wird. Wenn das Fahrzeug in 99,99% der Fälle jede Situation fehlerfrei meistert, dann bedeutet das „nur“ noch einen manuellen Eingriff für 100 m auf 1.000 gefahrene Kilometer. Wann dieser statistische Wert jedoch in umgerechnet vielleicht 20-30 Stunden Fahrtzeit auftritt, ist ungewiss und völlig überraschend. Und mit steigender Zuverlässigkeit tritt ein Problem vielleicht erst nach Wochen ansonsten zuverlässiger automatisierter Fahrt auf. Welcher Mensch wird dann auf den Punkt und ohne regelmäßige eigene Fahrpraxis besser und vor allem noch rechtzeitig reagieren als die Maschine? Die Anweisung der Firma Uber an ihre Testfahrer, dass sie mit Händen und Füßen über Lenkrad und Pedale „hovern“ sollen, um rechtzeitig eingreifen zu können, mag rechtlich begründet sein, ist aber vollkommen praxisfern.

Des Weiteren ist es eine nach Ansicht des Autors logische Konsequenz, auf Basis des bisher vorliegenden Materials eine Anklage gegen die Fahrerin des Uber-Fahrzeugs zu erheben. Sie hat nach der Beweislage ihre Kontrollpflicht der Fahraufgabe in nicht ausreichender Weise nicht durchgängig wahrgenommen und hätte den Unfall bei aufmerksamer Beobachtung des Umfeldes durch einen manuellen Eingriff problemlos vermeiden können.

Sie als Alleinschuldige hinzustellen und die Firma Uber aus dieser Betrachtung herauszunehmen, greift jedoch viel zu kurz. Es ist aufgrund der offiziellen Berichte nach wie vor vollkommen unklar, warum das Fahrzeug nicht auf die offensichtlich auf Kollisionskurs befindliche Fußgängerin mit Fahrrad reagiert hat. Das Unfallopfer war deutlich sichtbar (sowohl für optisch als auch mit RADAR oder Ultraschall arbeitende Systeme) und die Situation hätte in jedem Fall zu einer Bremsung und/oder Ausweichbewegung führen müssen.

So bleiben nur Mutmaßungen darüber, warum dies nicht erfolgte und gerüchteweise steht die Aussage im Raum, dass Uber die Software wegen zu vieler vorheriger „False Positives“, also Fehlalarmen, die fälschlicherweise eine Bremsung ausgelöst hatten, zu unsensibel eingestellt hat.

Diese Fehlalarme sind ein durchaus jetzt schon bei mit Assistenzsystemen ausgerüsteten teil-automatisiert fahrenden Fahrzeugen auch deutscher Hersteller zu beobachten. Regelmäßig im Abstand von etwa 800 bis 1.000 km konnte der Autor an eigenen Fahrzeugen feststellen, dass die Front-Kollisions-Warner fälschlicherweise Hindernisse anzeigen oder gar eigenständig Teil- und Aufmerksamkeitsbremsungen einleiteten oder aufgrund von harmlosen Witterungsbedingungen ausfielen. Die falsche Einstellung der Sensorik hinsichtlich „False Positives“ führt dann zum Abschalten der Systeme oder dazu, dass diese als unsicher bzw. unkomfortabel generell abgelehnt werden.

6.5 Missbrauchsszenarien bei Angriffen auf fahrzeugnahe Systeme

Wie in den vorherigen Kapiteln skizziert, muss der Forensiker einen nicht unerheblichen Aufwand für die Analyse eines Fahrzeugs bzw. damit gekoppeltem IT-System betreiben, bis er es für seine Zwecke und Sichtweisen benutzen kann. Genauso verhält es sich beim böswilligen Angreifer. Hat er ein lohnenswertes Geschäftsmodell entdeckt, so wird er den Initialaufwand gerne investieren, wenn er anschließend – selbstverständlich illegal – die Früchte seiner Arbeit ernten kann.

Neben den bereits bekannten und praktizierten böswilligen Attacken wie Chip-Tuning, Tachomanipulationen, Umgehung der Wegfahrsperren usw. kommen nun neue Angriffsvektoren hinzu und die Angriffsfläche vergrößert sich.

Jede neue Funktionalität und Technologie kann – vor allem wenn sie sich einer Funkübertragung und / oder informationstechnischer Netze und Systeme bedient – auch für böswillige Angriffe missbraucht werden.

Lange Zeit wurden Sicherheitsfachleute, die auf diese neuen Gefahren hingewiesen haben, als Schwarzmauer und die Angriffe als theoretisch möglich, aber nicht praktisch relevant abgetan. Stereotyp wurde und wird betont, dass man den Datenschutz sehr ernst nimmt, alles Erdenkliche für die Datensicherheit tut und – einem Totschlagargument gleich – es ja bisher in der Praxis noch zu keinem entsprechenden Angriff gekommen ist.

Spätestens mit der Vorstellung des Hacks auf einen Jeep Cherokee via Internet und Mobilfunkschnittstelle und der Manipulation von Antrieb und Bremse wurde von Miller und Valasek im Juli 2015 eindrucksvoll gezeigt, dass es praxisrelevante Angriffe gibt, die eben nicht auf der Verkettung mehrerer Angriffe beruhen, sondern bequem vom heimischen Laptop erfolgen¹⁸³. Hier musste man nicht zuerst das Fahrzeug orten und öffnen, um dann eine lokale Manipulation am Fahrzeug durchzuführen). Nach Ansicht des Autors sind für den „Erfolg“ eines solchen Hacks zwei wesentliche Gründe zu nennen. Zum einen ist die ansteigende Komplexität vernetzter Systeme im und um das Auto herum eine enorme Herausforderung – auch hinsichtlich der IT-sicherheitstechnischen Absicherung – und zum anderen wird im Automotivumfeld noch viel zu wenig von etablierten Sicherungsmaßnahmen wie Verschlüsselung, Firewalls, Intrusion-Detection-Systemen und Virenschutz oder Beratung durch Forensiker Gebrauch gemacht.

Es gibt hierzu Lösungsansätze, die teilweise bereits auf entsprechenden Konferenzen vorgestellt wurden (siehe auch nächstes Kapitel).

¹⁸³ siehe auch Stellungnahme (Tagesthemen, Eberl, & Käfer, n.d.) und (Karbach & Käfer, 2015)



Abbildung 222: BKA-Trojaner im Auto (Quelle: Eigene Visualisierung)

Beispiel für einen Angriff: Ein lohnenswertes Geschäftsmodell für einen Angriff auf ein HMI eines Fahrzeugs durch Einschleusen eines Trojaners wäre es, den Fahrer mit sogenannter „Scareware“ (vgl. BKA-Trojaner auf dem PC) zur Zahlung eines gewissen Obolus zu nötigen. Besonders eindringlich und überzeugend würde ein solcher Angriff, wenn die Schad-Software den Weg zur nächsten Tankstelle anzeigen würde, an der man die meist für solche Zwecke eingesetzten Prepaid-Karten (Ukash, Paysafecard usw.) kaufen kann. Die verbleibende Restfahrstrecke bis zur angedrohten Stilllegung des Fahrzeugs wird im HMI anzeigen. Ohne im PC bereits etablierte Funktionen wie Firewalls und Virenscanner könnte solch ein Szenario im Auto schneller funktionieren, als manchem lieb ist. Und mit tatsächlichem Zugriff auf die Steuerung (wie beim Jeep Cherokee) wird aus einem theoretisch denkbaren ein in der Praxis vermutlich bestens funktionierender Hack.

6.6 Absicherungsmöglichkeiten von Steuergeräten

Die Kommunikation innerhalb eines Fahrzeugs verläuft in der Vielzahl der Fälle vollkommen unverschlüsselt und Steuergeräte sind meist nur durch geheim gehaltene Zugangsmechanismen rudimentär vor Angriffen geschützt (z.B. Seed and Key-Verfahren). Eine echte Verschlüsselung findet nur partiell statt bzw. bedient sich nicht etablierter, sondern proprietärer Methoden, die meist angreifbar sind. Vollkommen untauglich sind beispielsweise triviale Kodierungen zum Verstecken von Menüfunktionen im HMI, da zu deren Aktivierung meist nach kurzer Zeit in einschlägigen Foren die Entsperr-Codes publiziert werden.

Beispiel 1: BMW F31 - Verstecktes Kombi-Instrument-Menü (u.a. Fehlerspeicher):

"To bring up this menu, press and hold the trip reset button between 10-12 seconds, with engine or ignition on. Ignore the engine oil reset opportunity and keep the button held until the menu appears. Press the trip reset button to navigate. Hold the trip reset button to enter and exit menus."

Der Entsperr-Code errechnet sich aus der Quersumme der letzten 6-7 Ziffern der VIN.

Beispiel 2: Verstecktes Menü im HMI (BMW F31 Serie u.a. mit Navigationssystem Professional)

This implies that you have an iDrive-controller that can slide up and down

iDrive-Controller:

- Call up Start (main) menu
- Push controller in up direction for at least 10 s
- Rotate controller, 3 notches to the right
- Rotate controller, 3 notches to the left
- Rotate controller, 1 notch to the right
- Rotate controller, 1 notch to the left
- Rotate controller, 1 notch to the right
- Press controller once
- The Service menu is now added as the last submenu to "Settings"

Bessere Ansätze als diese zum Scheitern verurteilten Versuche zur Verschleierung wurden u.a. von Alexander Kiening (Fraunhofer AiseC) auf der VDI/VW-Tagung 2014 in Wolfsburg vorgestellt. Steuergeräte könnten Manipulationen durch sogenannte Remote Attestation (aus dem Bereich des Trusted Computing) erkennen. Sicherheitsmodule müssten in Steuergeräten integriert sein, die eine Manipulation möglichst selbstständig erkennen und durch Secure Boot Prozesse die Korrektheit der einzelnen Bootphasen der Software prüfen. Wird ein unsicherer Zustand erkannt, so fällt das Steuergerät in einen Fail-Safe-Modus zurück und informiert den Fahrer über das HMI und ggf. den Hersteller via Datenverbindung (vgl. Tesla, die Modifikationen am Fahrzeug auf diese Art bereits detektieren). Software-Updates müssen durchgängig valide signiert und durch kryptografische Verfahren (z.B. Hashing) abgesichert werden (was vielfach schon passiert).

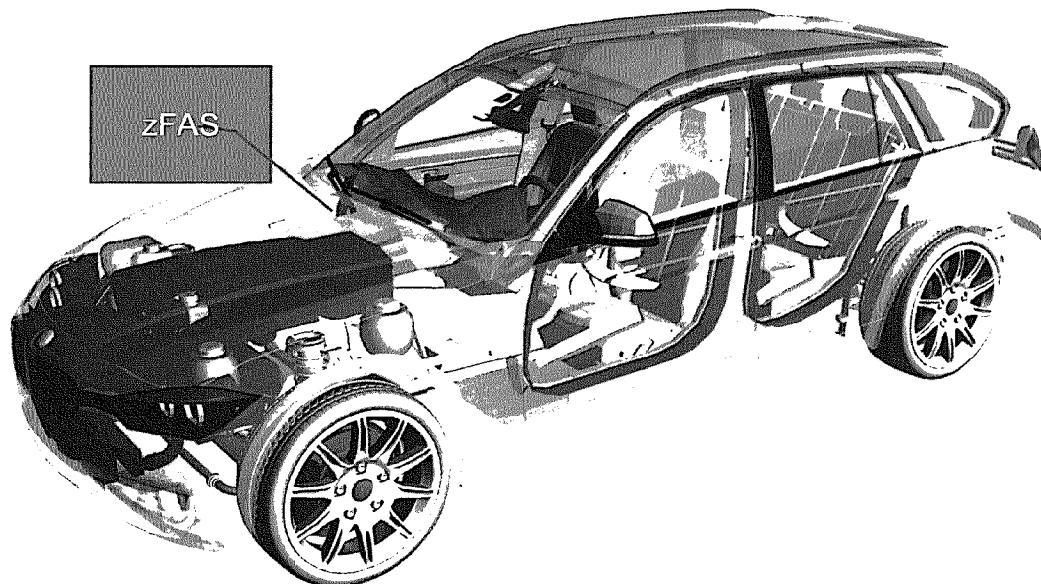


Abbildung 223: Reduzierung von X Steuergeräten zu einem zFAS (Quelle: Eigene Visualisierung)

Ein weiterer Ansatz zur Verbesserung der IT-Sicherheit bei Steuergeräten ist deren Zusammenfassung in ein zentrales Fahrrassistentsteuergerät (bei Audi „zFAS“ genannt), welches die Angriffsfläche nach außen reduziert und die Kommunikation der einzelnen Bereiche durch einen internen, schnellen und beherrschbar abzusichernden Bus optimiert. Ein solches zFAS müsste dann wiederum die typischen Sicherungsmechanismen wie Firewall, IDS, Virenschutz usw. besitzen, die aber einfacher bei einem einzelnen Gerät zu handhaben sind als bei einer verteilten Infrastruktur (wie derzeit üblich). Letztlich sollte man sich auch darüber Gedanken machen, ob man wirklich sicherheitsrelevante Systeme (Road-Safety) nicht – wie bei Flugzeugen üblich – redundant auslegt und ob man eben die gesamte Struktur auch übergeordnet von einem Monitoringsystem überwachen lässt (incl. Logging). Ein gem. eines Konferenzbeitrags offenbar praktiziertes Vorgehen bei der Entwicklung ist, dass System A von B programmiert und C implementiert wird und dieses Konstrukt von System X gecovert wird, dass von Y programmiert und Z implementiert wurde. Das ist ein durchaus sinnvoller Ansatz. Ohne ein ständig aktives Monitoring ergibt sich nach Ansicht des Autors jedoch nur eine statistische und ggf. trügerische Sicherung gegen systematische Fehler.

6.7 Verschlüsselung im Fahrzeug

Bzgl. Verschlüsselung gab es auf den verschiedenen vom Autor besuchten Kongressen durchaus kritische und gegensätzliche Einschätzungen der Fachleute. So schätzte Dr. Ilja Radusch (Fraunhofer/Daimler) die derzeit Security-Lage für Car2X als ausreichend ein, betrachtete aber IT-Sicherheit auch als einen kontinuierlichen Prozess. Christian Löper (German Aerospace / DLR) sah auf der VDI Tagung im Mai 2014 die Nutzung eines Smartphones für Car2X und Steuerung eines Fahrzeugs als nicht sicher an (Akku, Absturz). Alexander Kiening (LMU / Fraunhofer Aisec) hielt die Verschlüsselung im Fahrzeug aus Performancegründen als entbehrlich (VDI/VW Tagung 2014). Demgegenüber steht die Ansicht von Prof. Hillgärtner (FH Aachen ISiA), der zumindest die Absicherung der Außenschnittstellen von Fahrzeugsystemen forderte (9. Dortmunder Autotag 2014).

Ein wirksame Verschlüsselung der Daten auf dem aus heutiger Sicht veralteten CAN-Bus ist praktisch unmöglich und scheitert an dem viel zu kurzen Payload (Standard 8 Byte) eines CAN-Pakets. Selbst der neuere CAN FD Bus besitzt mit 64 Byte eine für eine zukunftssichere Verschlüsselung zu kurze Paketlänge.

Da für viele Steuergeräte das CAN-Protokoll jedoch der gemeinsame Nenner ist, ist zu erwarten, dass dieses auch in zukünftigen Fahrzeuggenerationen noch zu finden sein wird.

Abhilfe verspricht hier das Kapseln und Übertragen von CAN-Nachrichten über Ethernet. Das Ethernet-Protokoll ist zusammen mit der entsprechenden Übertragungstechnik schnell genug (typisch bis 10 GBIT/s) und bietet ausreichend große Paketgrößen, um CAN-Nachrichten zu verschlüsseln und im Fahrzeug schnell(er) zu transportieren. In dem Moment wo aus technischen Gründen bereits Ethernet o.ä. eingesetzt wird, sollte man sich daher auch umgehend Gedanken über wirksame Verschlüsselung im Fahrzeug machen.

Das ist natürlich auch nicht trivial, da man auch das Problem des sicheren Schlüsselaustauschs bzw. Speichern der Schlüssel lösen muss. Hierbei kann man sich z.B. in der IT etablierter Verfahren wie z.B. symmetrischer, asymmetrischer und hybrider Verschlüsselung mit digitalen Zertifikaten und Signaturen (PKI) bedienen.