NTT Security

Technische Hochschule Ingolstadt

# Technische Hochschule Ingolstadt

## Fakultät Institut für Akademische Weiterbildung

## Studiengang IT-Management (MBA)

# Masterarbeit

Thema: Defence in Depth für Fahrzeuge - Stand der Technik und zukünftige Möglichkeiten

Vor- und Zuname: Ralf Georg Graupner

ausgegeben am: 07.06.2018

abgegeben am: 12.07.2018

Erstprüfer: Prof. Dr.-Ing. Hans-Joachim Hof

Zweitprüfer: Prof. Dr. Jürgen Hofmann

Firmenbetreuer: René Bader

# Erklärung

Ich erkläre hiermit, dass ich die Arbeit selbständig verfasst, noch nicht anderweitig für Prüfungszwecke vorgelegt, keine anderen als die angegebenen Quellen oder Hilfsmittel benützt sowie wörtliche und sinngemäße Zitate als solche gekennzeichnet habe.

Ingolstadt, den 12.07.2018

Georg Graupner

# Kurzfassung

Sowohl Fahrzeuge als auch die Informationstechnologie sind unentbehrliche, essentielle Bestandteile in unserer modernen Gesellschaft. Da besonders die westliche Welt beides exzessiv nutzt, war es nur eine Frage der Zeit, bis diese beiden Technologien zusammenfinden. Dies fing beim einfachen Radio im Fahrzeug an, über Autotelefonie bis hin zu den heutigen, rundum vernetzten Fahrzeugen mit einer ständigen Verbindung zum Internet. Doch mit der Vernetzung sind Fahrzeuge auch Ziel von einer Gruppierung geworden, die sich bis dato wenig für Fahrzeuge interessiert hatten: Hacker. Während bis zu diesem Zeitpunkt das „Hacken“ eines Fahrzeugs in dessen Aufbruch und Diebstahl bestand, für welches der Hacker physisch am Fahrzeug sein musste, so gibt es heutzutage die Möglichkeit, Fahrzeuge auch aus der Ferne anzugreifen. Dies schafft neue Angriffswege, -gründe sowie neue Risiken und Bedrohungen, da bei diesen Angriffen im schlimmsten Fall das Leben von Personen gefährdet sein kann.

Bisher wurden Fahrzeuge von Automobilherstellern meist nicht als IT-System gesehen. Deshalb wurde auch bisher nur die funktionale Sicherheit (Safety) betrachtet und IT-Risiken waren maximal im Backendbereich ein Thema. Doch nicht zuletzt wegen einiger öffentlichkeitswirksamen Angriffe auf Fahrzeuge hat das Thema Security im Fahrzeug an Aufmerksamkeit gewonnen. Nun suchen die Hersteller nach Lösungen, wie sie ihre Fahrzeuge absichern können. An dieser Stelle ist ein ganzheitliches Sicherheitskonzept gefragt, welches Sicherheit in der Tiefe (Defense in Depth) bietet.

# Inhaltsverzeichnis

# Abbildungsverzeichnis

# Abkürzungsverzeichnis

| | |
|---|---|
| ACC | Adaptive Cruise Control |
| ADAC | Allgemeiner Deutscher Automobil Club |
| ANSI | American National Standards Institute |
| API | Application Programming Interface, Programmierschnittstelle |
| ASIL | Automotive Safety Integrity Levels |
| BYOD | Bring your own Device |
| CAN | Controler Area Network |
| CIA | Confidentiality, Integrity, Availability |
| CVE | Common Vulnerabilities and Exposures |
| CWE | Common Weakness Enumeration |
| DMZ | Demilitarisierte Zone |
| DSGVO | Datenschutzgrundverordnung |
| ECC | Elliptic Curve Cryptografie |
| ECU | Electronic Control Units |
| ENISA | European Union Agency for Network and Information Security |
| ETSI | Europäische Institut für Telekommunikationsnormen |
| ETW | Eintrittswahrscheinlichkeit |
| FOTA | Firmwareupdate Over the Air |
| HSM | Hardware Secure Module |
| HSPA | High Speed Packet Access |
| IDS | Intrusion Detection System |
| IEC | International Electrotechnical Commission |
| IEEE | Institute of Electrical and Electronics Engineers |
| IoT | Internet of Things |
| IPS | Intrusion Prevention System |
| ISA | International Society of Automation |
| ISO | International Organization for Standardization |
| ISO/OSI | ISO Open Systems Interconnection Modell |

| | |
|---|---|
| IT | Informationstechnologie |
| Kfz | Kraftfahrzeug |
| Lkw | Lastkraftwagen |
| MAC | Message Authentication Code |
| NHTSA | National Highway Traffic Safety Administration |
| NIST | National Institute of Standards and Technology |
| OBD | On-Board-Diagnose |
| OEM | Original Equipment Manufacturer |
| PDCA | Plan-Do-Check-Act |
| PKI | Public Key Infrastructure |
| Pkw | Personenkraftwagen |
| SAE | Society of Automotive Engineers |
| SIM | Subscriber Identity Module |
| SOC | Security Operation Center |
| SoC | System on Chip |
| SSDLC | Secure Software Developement Lifecycle |
| StGB | Strafgesetzbuch |
| StVG | Straßenverkehrsgesetz |
| TCU | Telematic Control Units |
| UMTS | Universal Mobile Telecommunications System |
| UN-TF CS/OTA | UN Task Force on Cyber security and OTA issues |
| USB | Universal Serial Bus |
| VPN | Virtual Private Network |
| WLAN | Wireless Local Area Network |

# 1 Einleitung

Der digitale Wandel hat unser aller Leben in den letzten Jahren und Jahrzehnten bestimmt. Produkte im Bereich der Consumer-Elektronik wie Laptops oder Handys, sowie die tägliche Nutzung des Internets sind aus dem täglichen Leben nicht mehr wegzudenken. Dieser Trend hat unlängst auch den Automobilsektor erreicht. Radio oder Navigationssysteme gehören schon lange zur Standardausstattung der meisten Fahrzeuge.

Mit dem Aufkommen von Smartphones Mitte der 2000er Jahre sowie dem damit verbundenen Ausbau des mobilen Datennetzes (wie zum Beispiel den Übertragungsstandards UMTS und HSPA) war es nur eine Frage der Zeit, bis das Internet auch in Fahrzeugen Einzug halten würde. Dementsprechend bietet heutzutage nahezu jeder Fahrzeughersteller digitale Features in seinen Fahrzeugen an. Diese reichen von USB, Bluetooth und WLAN, über Infrarot-, Laser- oder Radarsensoren bis zur Internetfähigkeit des Fahrzeuges selbst durch integrierte Datenmodule. Fahrzeuge erhalten somit permanent Informationen von externen Quellen.

Allerdings werden sie dadurch auch mögliche Ziele von Hackerangriffen. Die Motivation für solch einen Angriff kann verschiedene Hintergründe haben: Zum Beispiel kann ein Hacker versuchen, über Softwaremanipulation sein Fahrzeug aufzubessern (zu „tunen“), um mehr Leistung zu erhalten, den Tachostand zu manipulieren oder um die Abriegelung einer maximal möglichen Geschwindigkeit abzuschalten. Ein weiterer Grund kann sein, dass sich ein Hacker über Fahrzeugsysteme unerlaubten Zugang verschaffen will, um das Fahrzeug zu entwenden ohne Einbruchspuren zu hinterlassen. Im schlimmsten Fall wird der Hacker aber versuchen, sicherheitsrelevante Systeme[1] wie Lenkung oder Bremsen zu übernehmen, was im schlimmsten Fall zu Unfällen führen kann. Dies ist insbesondere im Hinblick auf zukünftige Stufen des autonomen Fahrens überaus riskant. Für eine Privatperson ist es zwar ärgerlich, wenn deren Laptop oder Smartphone gehackt wird und für Unternehmen kann dies einen wirtschaftlichen Schaden bedeuten, allerdings besteht, im Gegensatz zum Fahrzeug, bei diesen Angriffen selten eine Gefahr für Leib und Leben.

Das solche Hackerangriffe auf Fahrzeuge durch aus möglich und umsetzbar sind, haben in der Vergangenheit schon mehrere Versuche gezeigt: So hat der ADAC 2014 eine Sicherheitslücke im BMW System „ConnectedDrive“ gefunden, über die Fahrzeuge über

[1] Ein sicherheitsrelevantes System ist ein System, dessen Ausfall oder Fehlfunktion eine Gefahr für Leib und Leben bedeuten kann. (Benz, 2004)

Mobilfunk geöffnet werden konnten (ADAC, 2014). Die beiden IT-Experten Javier V. Vidal und Alberto G. Illera zeigen in einem Livehack auf der Defcon 2013, wie sie mit Equipment für nur 20 Euro in die Elektronik eines Fahrzeugs einbrechen konnten (Reißmann, 2013). Das wohl prominenteste Beispiel kommt von Charlie Miller und Chris Valasek, welche einen werksneuen Jeep Cherokee während der Fahrt übernahmen und Lenkung und Bremse steuerten (Greenberg, 2015).

Dementsprechend hoch sind auch die Bemühungen der Fahrzeughersteller, solche Gefahren abzuwenden. Dabei wird meist versucht, die derzeitige Fahrzeugarchitektur möglichst gut gegen Angriffe abzusichern. Dies gelingt allerdings nur partiell. Gründe hierfür gibt es mehrere:

1. Die derzeitige Fahrzeugarchitektur ist meist historisch gewachsen. Dabei stand stets die Funktionsorientierung der Systeme und deren funktionale Sicherheit (Safety) im Vordergrund und nicht die Informationssicherheit (Security). Das bedeutet, dass Fahrzeugsysteme ursprünglich gar nicht darauf ausgelegt waren, Schutz vor Cyberangriffen zu bieten. (Shen, 2015)
2. Derzeitige Schutzmaßnahmen beschränken sich darauf, den Zu- und Abfluss der Daten in und aus dem Fahrzeug zu kontrollieren (Perimeter-Schutz). Dabei wird aber nicht überprüft, wie die Daten sich im Fahrzeug selbst verhalten oder welche Aktionen sie dort ausführen.
3. Fahrzeughersteller haben nur eine eingeschränkte Kontrolle über Daten, welche von externen Quellen in das Fahrzeug eingespielt werden. Dies gilt zum Beispiel für Daten welche über die USB- oder Bluetooth-Verbindung mit einem Smartphone in das Fahrzeug gelangen.

Dementsprechend ist es für kommende Generationen von vernetzten (und autonomen) Fahrzeugen essentiell, IT-Sicherheitskonzepte gegen Hackerangriffe zu entwickeln. Dafür muss das funktionale Sicherheitskonzept um Informationssicherheitsmaßnahmen erweitert und verbessert werden. An dieser Stelle setzt Defense in Depth an, welches die bisher einzelne Schutzschicht um mehrere Schichten erweitert. Defense in Depth beschreibt dabei ein Security-Konzept, welches durch mehrere Schutzschichten für eine erhöhte Sicherheit sorgt.

In dieser Hinsicht stellen sich mehrere Fragen: Welche Defense in Depth Maßnahmen sind für eine angemessene Absicherung von Fahrzeugen gegen Angriffe notwendig? Und wie lassen sich diese in die Fahrzeugarchitektur integrieren?

Da es hierzu zwar vereinzelt, aber keine öffentlichen oder konkretisierten Konzeptionen für solche ein Sicherheitskonzept gibt, wird sich diese Masterarbeit dieser Problemstellung widmen.

Ziel der Arbeit ist die Konzeption von generischen Defense in Depth Mechanismen, welche derzeitige Fahrzeugarchitekturen und Automotive Cyber-Systeme gegen Angriffe absichern. Dafür werden auch Ansätze und Produkte von Herstellern von IT-Sicherheitsprodukten evaluiert und deren Umsetzung für die Praxis kritisch hinterfragt.

Dafür wurden zuerst die wichtigsten Begriffe, welche den Kern dieser Arbeit beschreiben, zusammengetragen und anschließend eine Definition dieser Begriffe erstellt. Mit diesen Begriffen wurde dann die Quellenrecherche begonnen, um die Definitionen zu schärfen und mit Quellen belegen zu können.

Im Anschluss ist eine Recherche nach adäquaten Studien zum Thema „IT-Sicherheit im Fahrzeug“ sowie zum Thema „Defense in Depth“ durchgeführt worden. Der Recherche lagen neben den zuvor verwendeten Quellen auch solche zugrunde, auf die in den ersten gefundenen Quellen verwiesen wurde. Es folgte eine Literaturauswertung der Quellen, welche ein Bild des aktuellen Forschungsstandes ergaben.

Auf dieser Basis wurde ein Vergleich angestellt, welcher den Ist-Zustand der IT-Sicherheit in Fahrzeugen gegenüber einem angestrebten Soll-Zustand betrifft, sowie ein Vergleich, inwiefern sich klassische IT-(Sicherheits)Architektur von der eines Fahrzeugs unterscheidet. Darauf aufbauend wurden IT-Sicherheitslösungen für Fahrzeuge analysiert und evaluiert. Zum Schluss wurde analysiert, wie über einen Defense in Depth Ansatz die IT-Sicherheitsarchitektur in Fahrzeugen verbessert werden kann.

In Kapitel zwei dieser Arbeit werden die theoretischen Grundlagen dieser Arbeit behandelt, welche für das weitere Verständnis notwendig sind. Dabei werden die wichtigsten Begriffe und deren Bedeutung definiert und voneinander abgegrenzt.

Im dritten Kapitel wird auf den aktuellen Forschungsstand eingegangen. Es werden ausgewählte Studien zur derzeitigen Situation im Bereich „Automotive Security“ dargestellt, zusammengefasst und anschließend ausgewertet. Auf dieser Basis werden Anforderungen und Rahmenbedingungen für die IT-Sicherheit in Fahrzeugen definiert und daraus die dort bestehende Forschungslücke hervorgehoben.

Im Mittelpunkt des vierten Kapitels steht das Beleuchten der in dieser Arbeit verwendeten Methoden. Es wird das Vorgehen bei der Analyse von Defense in Depth Mechanismen beschrieben sowie die Auswahl der gewählten Methoden begründet. Anschließend folgt die Darstellung von Hersteller-Lösungen für IT-Sicherheit in Fahrzeugen und Erkenntnisse über diese.

Die Erstellung von Modellen, eine Bedrohungs- und Risikoanalyse, die Konzeption von verschiedenen Security-Bausteinen sowie die Konzeption von Defense in Depth Mechanismen erfolgt im fünften Kapitel. Dort erfolgt auch eine Evaluierung und kritische Analyse der Lösungen und Mechanismen sowie ein Ausblick auf eventuellen weiteren Forschungsbedarf.

Das sechste Kapitel schließt mit einer Zusammenfassung der Ergebnisse, einer Schlussfolgerung, wie Fahrzeughersteller und deren Zulieferer die Erkenntnisse dieser Arbeit nutzen können sowie ein Ausblick auf die möglichen weiteren Entwicklungen.

# 2 Defense in Depth und Automotive Security - Theoretische Grundlagen

In diesem Kapitel werden die wichtigsten Begriffe beschrieben, welche für das Verständnis der Arbeit notwendig sind. Im Laufe der Arbeit verwendete Begrifflichkeiten werden sich stets auf die hier getroffenen Definitionen beziehen.

## 2.1 Defense in Depth – Bedeutung und Begriffsabgrenzung

**Defense in Depth** hat, je nach Einsatzgebiet, verschiedene Bedeutungen. In der Informationstechnologie (IT) beschreibt Defense in Depth ein umfassendes Security-Konzept (Kästner, 2007) für IT-Systeme. Dafür werden verschiedene Maßnahmen, auch Abwehr- oder Verteidigungslinien genannt, kombiniert, um Risiken für einen Angriff auf die IT zu minimieren (Lass, et al., 2014). Maßnahmen können sowohl IT-Maßnahmen sein, also zum Beispiel der Einsatz von Sicherheitssystemen für Verschlüsselung, Virenschutz, Berechtigungsmanagement etc., oder auch organisatorische Maßnahmen, wie das Schulen von Mitarbeitern bezüglich Security-Awareness oder dem Aufstellen von entsprechenden Dienstanweisungen. Wichtig ist auch, dass für einen erfolgreichen Defense-in-Depth-Ansatz alle Beteiligten mitwirken müssen: Ob Hersteller, Provider, Integratoren, Externe Ressourcen, IT-Mitarbeiter und Mitarbeiter aus anderen Bereichen (Kobes, 2016).

Defense in Depth ist, keine Erfindung der heutigen IT. Defense in Depth und dessen Konzept kommt aus dem Militärgebrauch und wurde schon im Mittelalter angewandt. Dort wurden Städte und Burgen nach dem Defense in Depth Konzept aufgebaut, wie Abbildung 1 zeigt.

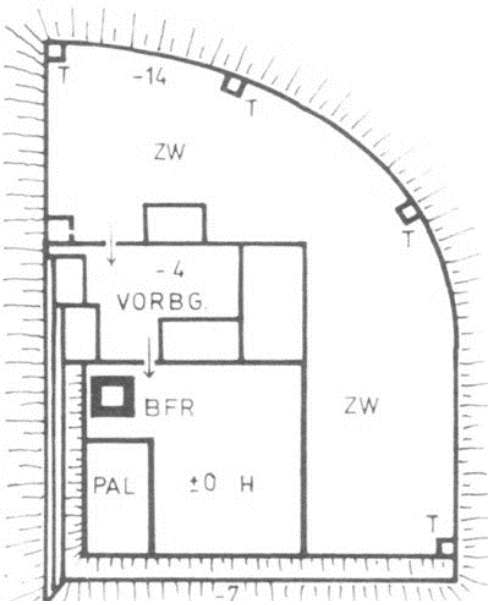


*Abbildung 1: Schematischer Aufbau einer Burg am Beispiel Burg Oberlauda (Krahe, 2000)*

Die äußerste Abwehrlinie war hier ein Graben, dann kam die erste Mauer mit Türmen, dann die Vorburg und zum Schluss die Hauptburg mit dem Bergfried als letzten Rückzugsort. Zwischen den einzelnen Bereichen gab es jeweils nur einen Zugang durch ein Tor wo kontrolliert wurde, wer reinkommt und wer rausgeht. Ein Angreifer konnte nicht gleich in das Innerste der Burg vordringen, sondern musste nach und nach die einzelnen Verteidigungsanlagen überwinden. Das gleiche Prinzip gilt noch heute in der IT.

Ein anderer Ansatz von Defense in Depth stammt von den schwedischen Wissenschaftlern Dr. Ulf Larson und Dennis Nilsson. Diese beschreiben Defense in Depth als das Zusammenspiel von verschiedenen Stufen oder Vorgehensweisen, um Angreifer abzuwehren. In ihrem Model gibt es drei Stufen, welche auch in dieser Reihenfolge greifen sollen: *Vermeidung* (Prevention), *Erkennung* (Detection) und *Ablenkung* (Deflection), wie. Abbildung 2 zeigt.

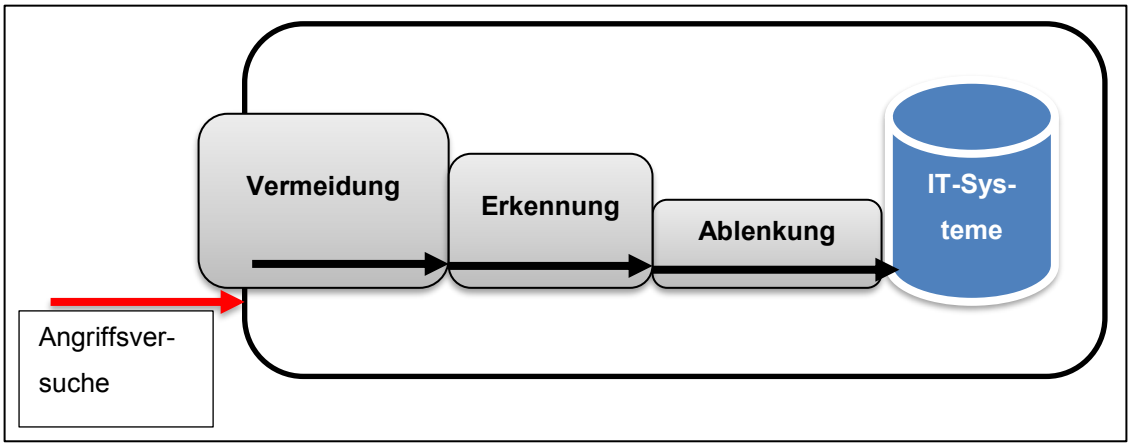


*Abbildung 2: Defense in Depth Ansatz. Nach (Larson, et al., 2009)*

Dabei gilt der Grundsatz, dass so viele Angriffswege wie möglich vermieden werden sollen. Angriffe, die nicht abgewehrt werden können, deren Schutz zu teuer ist bzw. die Kosten dafür nicht in Relation mit dem Sicherheitsgewinn stehen, diese sollen zumindest erkannt werden, um dann Maßnahmen treffen zu können. Ablenkung beschreibt das Aufstellen von sogenannten „*Honeypots*[2]“. Angreifer sollen so auf Systeme gelenkt werden, bei denen sie keinen Schaden anrichten können und um Sicherheitsexperten die Möglichkeit zu geben, den Angreifer und sein Vorgehen zu studieren.

Viele Unternehmen oder Systeme, die Defense in Depth noch nicht anwenden, beschränken sich darauf, dass geprüft wird, welche Daten zu- und welche abfließen, den

[2] Honeypots sind Server mit nur scheinbar wertvollen Daten wie Adressen und Dokumenten zur Täuschung von Angreifern. Mit ihnen soll von Systemen abgelenkt werden, die tatsächlich wertvolle Daten verarbeiten. (Stevens, et al., 2004)

sogenannten **Perimeterschutz**. Perimeterschutz ist als Schutz eines Objektes wie einem IT-System durch Vorkehrungen in dessen Umfeld gedacht (Kersten, et al., 2008) und soll Schutz vor unerlaubtem Eindringen bieten, die Grenze des Schutzraumes nach außen markieren und diese Grenze durch geeignete Überwachungsmaßnahmen überwachen (Schwarz, 2018).

Um Defense in Depth auch für Unternehmen, denen das Wissen oder der Ansatz für den Aufbau einer sicheren IT-Landschaft fehlt, besser verständlich zu machen, wurde von der International Electrotechnical Commission (IEC) in Zusammenarbeit mit dem American National Standards Institute (ANSI) und der International Society of Automation (ISA) ein Standard für Cyber Security entwickelt. Dieser Standard trägt die Normnummer **IEC62443**, bzw. ANSI/ISA-99, wenn man das Pendant des ANSI dazu nimmt. Der Standard ist in vier Kategorien aufgeteilt:

1. Generelles: Terminologie, Konzepte und Modelle
2. Richtlinien und Verfahren: Aufbauen von Kontroll-Systemen, eines Patchmanagements und Anforderungen an Service Provider
3. Systeme: Netzwerk- und Systemsicherheit, Security Technologien und Security-Anforderungen, Aufbau von Zonen und Security-Level
4. Komponenten: Anforderungen an einen sicheren Produktentwicklungslebenszyklus

Der Punkt, welcher den Grundgedanken von Defense in Depth am treffendsten beschreibt, nämlich den Aufbau eines Schichtmodelles mit verschiedenen Verteidigungslinien, ist im Standard IEC62443-3.2, bzw. ANSI/ISA-99-3.2 geregelt. Dort wird das Konzept von „Zones“ und „Conduits“ (z.dt. Zonen und Leitungen) wie folgt beschrieben:

- **„Zonen** sind Gruppierungen logischer oder physischer Anlagen mit gleichen Security Anforderungen. Eine Zone hat eine klar definierte Grenze (entweder logisch oder physisch), welche die Abgrenzung von enthaltenen und ausgeschlossenen Elementen darstellt.“ (Torfino Security, 2012)
- „Ein **Conduit** ist ein Pfad für den Fluss von Informationen zwischen zwei Zonen. Der Conduit kann Sicherheitsfunktionalitäten haben, welche die Kommunikation zwischen Zonen absichert. Daten zwischen Zonen dürfen ausschließlich über Conduits ausgetauscht werden.“ (Torfino Security, 2012)

Für jede Zone und für jeden Conduit kann es dann unterschiedliche Sicherheitsmaßnahmen geben. Bei Zonen kommt es auf deren Systeme an, welche sich in ihr befinden.

Eine Zone mit Webservern braucht andere Schutzmaßnahmen als eine Zone, in welcher Datenbanken mit hochkritischen Daten stehen. Ebenso gibt es für Conduits Sicherheitsfunktionen. Die am häufigsten genutzten sind hier Firewalls und VPNs. Firewalls überwachen und kontrollieren den Datenstrom zwischen Zonen, während der VPN dafür sorgt, dass Daten nur verschlüsselt und damit für Unbefugte nicht lesbar zwischen Zonen ausgetauscht werden.

Allerdings hat der Defense-in-Depth-Ansatz auch Nachteile. Ein Nachteil ist zum Beispiel die Geschwindigkeit. Je mehr Zwischenstationen und Prüfungen durchlaufen werden müssen, umso länger brauchen die Daten von ihrer Quelle zu ihrem Ziel. In Systemen oder Anwendungen, wo Zeit ein wichtiger Faktor ist, kann dies zum Problem werden. Dies gilt insbesondere bei Echtzeitanforderungen wie in Connected Cars. Ein weiterer Nachteil sind die Kosten. Mehr Sicherheit heißt in der Regel auch immer zusätzliche Investitionen. Und je mehr Zonen und Conduits es gibt, desto mehr Sicherheitskomponenten werden benötigt, um diese abzusichern. Es gilt also Kosten und Nutzen abzuwägen, ob mehr Sicherheitstechnik ab einem bestimmten Level das Sicherheitsniveau noch merklich hebt. Außerdem muss bei diesem Modell Sicherheit von allen Beteiligten gelebt und umgesetzt werden. Dazu müssen diese auch das benötigte Wissen und die Security-Awareness besitzen. Dies durchzusetzen ist oft eine organisatorische Herausforderung für Unternehmen.

## 2.2 IT-Sicherheit und ihre Komponenten

**IT-Sicherheit**, hier synonym mit Informationssicherheit und IT-Security verwendet, beschreibt den Schutz von Informationen, welche elektronisch gespeichert sind oder elektronisch transportiert werden, Dabei sollen vor allem Knowhow von Unternehmen sowie die Daten von Mitarbeitern, Kunden und Lieferanten geschützt werden, um wirtschaftliche Schäden zu verhindern (Prof. Dr. Eckert, 2013). Hierfür wird durch **Schutzziele** für IT-Sicherheit beschrieben, welche Systeme und deren abzusichernde Zustände und Eigenschaften (Bedner, et al., 2010) mit welchen Maßnahmen geschützt werden müssen.

Dazu werden zwei Arten von Schutzzielen beschrieben: Der Schutz von Privacy und der Schutz von IT-Systemen. **Privacy** beschreibt den Schutz von allen Daten, die als sogenannte personenbezogene Daten gelten. Dies gilt für alle Daten, die sich einer Person unmittelbar oder mittelbar zuordnen lassen, wie Name, Alter, Anschrift, aber auch IP-Adressen, GPS-Standort, Mails, Kalendereinträge, Einkaufsverhalten etc. Zum Schutz von IT-Systemen zählen alle Maßnahmen, die **IT-Systeme** jeglicher Art vor Angriffen schützen. Ein System kann dabei ein Server in einem Rechenzentrum, ein Smartphone

oder ein Sensor in einem Auto sein. Die Aufgabe von IT-Sicherheit dabei ist, einen möglichst umfassenden, effektiven und effizienten Schutz vor Angriffen zu bieten, ohne den Nutzer oder das System unnötig zu belasten und ohne unverhältnismäßige Kosten zu verursachen.

Um die Gliederung und Einführung von Maßnahmen zu vereinfachen, wurden Schutzziele in ursprünglich drei Hauptkategorien eingeteilt: *Vertraulichkeit* (Confidentiality), *Integrität* (Integrity) und *Verfügbarkeit* (Availability). Diese Einteilung wurde als „*CIA-Triade*“ bezeichnet. In der Literatur werden diese Schutzziele oft noch um weitere verschiedene Kategorien erweitert, wie zum Beispiel die „Nichtverfolgbarkeit bei Privatpersonen“ (Untraceability), „Verfolgbarkeit bzw. Revisionssicherheit bei Firmen“ (Traceability) und Verbindlichkeit (Liability). In dieser Arbeit werden aber nur die drei Schutzziele aus der CIA-Triade behandelt:

- **Vertraulichkeit** besagt, dass Daten nur von Personen oder Systemen gelesen werden dürfen, wenn diese dafür berechtigt sind. „Vertrauliche Informationen müssen vor unbefugter Preisgabe geschützt werden“. (BSI, 2018)
- **Integrität** beschreibt, dass Daten weder verloren gehen, noch auf dem Übertragungsweg unerlaubt verändert werden dürfen. „Die Daten sind vollständig und unverändert. Der Begriff ‚Information‘ wird in der Informationstechnik für ‚Daten‘ verwendet, denen je nach Zusammenhang bestimmte Attribute wie z. B. Autor oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert wurden oder Angaben zum Autor verfälscht wurden oder der Zeitpunkt der Erstellung manipuliert wurde.“ (BSI, 2018)
- **Verfügbarkeit** sagt aus, dass Dienstleistungen, Funktionen eines IT-Systems oder auch Informationen dem Benutzer zum geforderten Zeitpunkt zur Verfügung stehen. (BSI, 2018). Dies wird mit der Ausfallabsicherung, der Skalierbarkeit und der entsprechenden Flexibilität und Performance von Systemen erreicht.

Um diese Schutzziele zu erreichen, gibt es verschiedene Wege. Zum einen organisatorisch im Betrieb selber, durch das Umstellen von internen Strukturen und Prozessen, zum anderen durch Schulung und Sensibilisierung von Mitarbeitern. Ein anderer Weg ist die Investition in Hardware und Software, welche zur Erhöhung der Sicherheit beitragen oder das Beauftragen von Experten und externen Ressourcen.

Dabei kann zudem unterschieden werden in aktive und passive IT-Sicherheit. Aktive Sicherheitskomponenten sind solche, die aktiv und präventiv für eine erhöhte IT-Sicherheit

sorgen. Das können Infrastrukturkomponenten wie Firewalls, Virenscanner oder Public Key Infrastrukturen (PKIs) sein, aber auch Investitionen in Beratung, in ein Rollen- und Berechtigungsmanagement, in Systemhärtung und ähnliches. Passive Sicherheit umfasst zum einen alles, was im Falle eines Angriffs bzw. eines erfolgreichen Angriffs dabei hilft, dessen Auswirkungen abzuschwächen. Darunter zählen Backups, Log-Dateien, die ausgewertet werden können oder entsprechende Notfallpläne. Aber auch das IT-sicherheitskonforme Verhalten der Mitarbeiter im Berufsalltag trägt passiv zur Gesamtsicherheit bei.

Es ist aber auch anzumerken, dass hier eine Lösung zu wählen oder ein Weg einzuschlagen wieder nur zu einem unvollständigen Schutz führen würde. Erst das Zusammenspiel der einzelnen beschriebenen Komponenten bringt eine umfasse IT-Sicherheit hervor.

## 2.3 Fahrzeuge und Fahrzeugarchitektur – Grundlegende Bestandteile

Der Begriff **Fahrzeug** in dieser Arbeit ist gleichzusetzen mit einem Kraftfahrzeug (Kfz). Laut Straßenverkehrsgesetz (StVG) ist ein Kraftfahrzeug „ein durch Maschinenkraft angetriebenes, nicht an Gleise gebundenes Landfahrzeug“ (§ 1 II StVG), beziehungsweise beschreibt der Begriff Fahrzeug im Strafgesetzbuch (StGB) „nicht nur Kfz, sondern alle Fahrzeuge, die zur Beförderung von Personen oder Sachen dienen und am Verkehr auf der Straße teilnehmen“ (§315c Rn. 5 StGB). In dieser Arbeit wird sich der Begriff Fahrzeug allerdings auf Personenkraftwagen (Pkw) und Lastkraftwagen (Lkw) beschränken, da diese in erster Linie die Zielgruppe im Kontext der Arbeit ausmachen.

Unter die Bezeichnung eines Fahrzeugs fällt auch die Definition eines **Connected Car**. Bislang gibt es keine offizielle Definition, was ein Connected Car ist. Es ist mehr ein Sammelbegriff, welcher die Konnektivität eines Fahrzeugs mit seinen eigenen Systemen, mit seinem Fahrer und seiner Umwelt beschreibt (Dr. Löffler, et al., 2017). Die Konnektivität mit der Umwelt wird meist noch untergliedert in Begriffe wie Car-to-Car (meist geschrieben als Car2Car), Car2Infrastructure, Car2Pedestrian, Car2X etc.

In dieser Arbeit werden die Begriffe Connected Car und Fahrzeug synonym verwendet.

Ein Teil eines Fahrzeugs ist dessen Architektur. Die **Fahrzeugarchitektur** beschreibt den Aufbau des Fahrzeugs hinsichtlich seiner *E/E-Architektur*[3] (Elektrik-/Elektronik-Ar-

[3] Heutzutage teils auch als E/E/PE-Architektur (Elektrik-/Elektronik/Programmierbar elektronische-Architektur) bezeichnet

chitektur) und deren Funktionen. Dazu gehören alle elektrisch oder elektronisch gesteuerten oder ansteuerbaren Bauteile eines Fahrzeugs wie Fahrassistenz, Infotainment (Informations- und Entertainmentsystem), Controler-Area-Network-Bus-Systeme (CAN-Bus-Systeme), Aktoren, Sensoren, Electronic Control Units (ECUs[4]) und Telematic Control Units (TCUs) (Dégardins, et al., 2009); (Kerschenlohr, 2015). In der Fahrzeugarchitektur wird außerdem die Vernetzung im Fahrzeug und die Steuergerätetopologie beschrieben. Basis sind hier meist Anforderungen an Funktionen und technische Kriterien (Gerstel, 2016).

Die einzelnen Begriffe werden dabei wie folgt definiert:

- Ein **Sensor** ist eine technische Komponente, welcher einen bestimmten Umwelteinfluss meist physikalisch „wahrnimmt“ und darauf reagiert, in dem er den Einfluss in ein elektrisches Signal umwandelt. So gibt es zum Beispiel einen druckempfindlichen Sensor, welcher wahrnimmt, ob der Knopf für den Fensterheber betätigt wurde und einen optischen Sensor der merkt, wenn Regen auf die Frontscheibe tropft.
- Als **ECU** werden kleine Steuergeräte im Fahrzeug bezeichnet, die meist nur eine einzige spezifische Funktion haben. So gibt es zum Beispiel eine ECU, die steuert, ob ein Fenster auf- oder zugehen soll. Eine andere ECU entscheidet, ob die Scheibenwischer eingeschaltet sein müssen und mit welcher Geschwindigkeit sie wischen.
- Ein **Aktor** ist eine elektronische Einheit, welche ein Signal (meist aus einer ECU) in eine mechanische Aktivität umsetzt. Ein Aktor ist zum Beispiel der Motor, der das Fenster öffnet oder schließt. Ein anderer Aktor betreibt den Scheibenwischer.
- Als **TCU** werden jene Bauteile beschrieben, welche für die Kommunikation zwischen den verschiedenen Bus-Systemen, als auch mit externen Quellen über Funk, WLAN, Bluetooth usw. verantwortlich sind. Ein anderer häufig verwendeter Begriff ist demnach auch Kommunikationsmodul oder Com-Unit.

Abbildung 3 zeigt für beide aufgeführte Beispiele, wie die einzelnen Komponenten, Sensor, ECU und Aktor zusammenarbeiten. Der Sensor nimmt ein Umwelteinfluss wahr, in diesem Fall Regen. Er leitet diesen Eindruck elektrisch an die ECU weiter. Diese nimmt das Signal auf, interpretiert und kombiniert es mit Signalen von anderen Sensoren oder

[4] Teils wird mit „ECU“ auch die Engine Control Unit beschrieben, in dieser Arbeit wird aber stets die Electronic Control Unit gemeint sein

ECUs (z.B. ob die Zündung eingeschalten ist oder ob der Scheibenwischerhebel auf „Automatik“ steht).

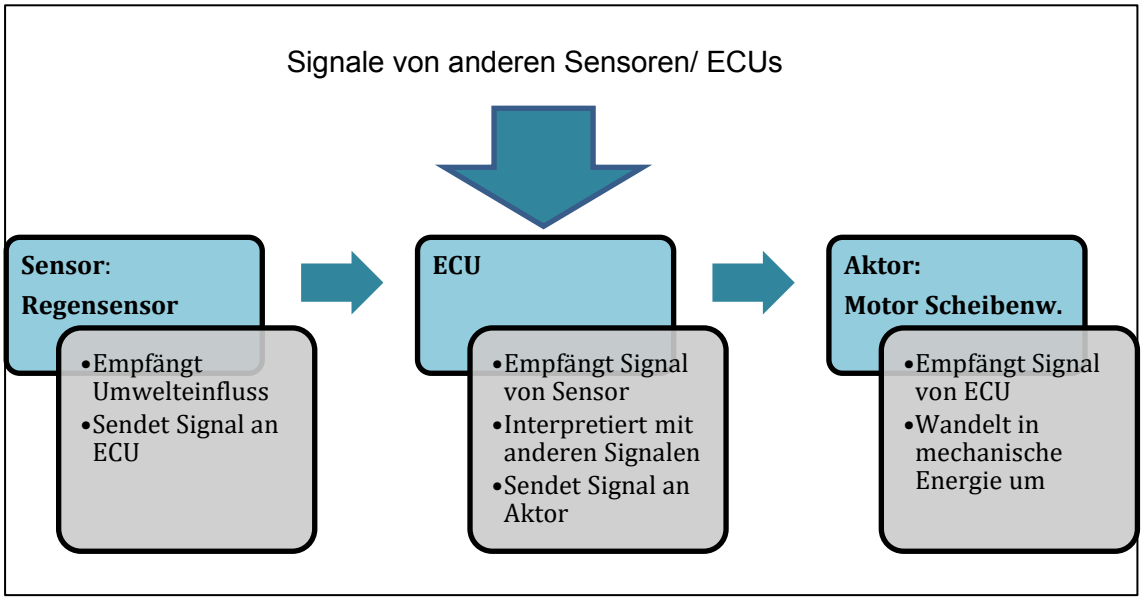


*Abbildung 3: Zusammenspiel von Sensor, ECU und Aktor*

Die ECU entscheidet, welches Signal an den Aktor weitergegeben wird, in diesem Fall „wischen in gewissen Abständen“, je nach benötigter Wischgeschwindigkeit. Der Aktor wandelt das Signal in Bewegungsenergie um. Der Scheibenwischer bewegt sich.

Über die letzten Jahre hat die Anzahl der Sensoren, Aktoren und ECUs stark zugenommen. Im Jahr 2003 waren in einem durchschnittlichen Mittelklassefahrzeug (z.B. Golf 3) noch rund 30 Sensoren, 50 bis 80 Aktoren und 35 ECUs verbaut. Zehn Jahre später, im Jahr 2013 waren es schon rund 75 Sensoren, 120 bis 150 Aktoren und 70 ECUs. Also eine Verdopplung der elektronischen Komponenten. Ein Connected Car aus dem Jahr 2016, wie der damals vorgestellte neue BMW 7er, mit Funktionen wie einer Gestensteuerung, Lenkassistent, Abstandstempomat, Stauassistent, adaptiven Scheinwerfern, ferngesteuertem Parken und vielen weiteren Funktionen, hat schon rund 130 Sensoren, 170 Aktoren und 120 ECUs, also teilweise nochmal eine Verdoppelung von elektronischen Komponenten in nur drei Jahren. Dazu ist zu sagen, dass dieser BMW 7er nur Level zwei der fünf Level des autonomen Fahrens[5] leisten kann. Es ist also anzunehmen, dass mit dem baldigen Aufkommen von Level-3-Fahrzeugen (wie dem 2018 vorgestellten neuen Audi A8) die Anzahl der Komponenten nochmal stark zunehmen wird.

[5] Die fünf Level sind:
1. Assistiert: Fahrer bekommt Unterstützung
2. Teilautomatisiert: Kfz kann Aktionen übernehmen, Fahrer behält Verantwortung
3. Hochautomatisiert: Kfz kann abschnittsweise selbst fahren
4. Vollautomatisiert: Kfz fährt Großteils selbstständig, Fahrer muss nur selten eingreifen
5. Autonom: Fahrzeug kann komplett selbstständig fahren (VDA, 2018)

Aber nicht nur die steigende Anzahl an Fahrassistenz- und Komfortsystemen sorgt dafür, dass die Fahrzeugarchitektur immer komplexer wird und somit auch die elektronischen Komponenten zunehmen. Ein anderer Grund ist auch der modulare Aufbau der Fahrzeuge. Zum einen werden immer mehr Komponenten zu Modulen zusammengefasst, da so der Einkauf wirtschaftlicher ist, Module innerhalb eines Konzerns für verschiedene Fahrzeugbaureihen oder Marken verwendet werden können, weil so die Reparatur schneller geht und weil es bei den meisten Fahrzeugen für verschiedene Module mehr als eine Auswahlmöglichkeit gibt. Letzteres ist der Tatsache geschuldet, dass Kunden, welche ein Neufahrzeug erwerben möchten, dieses auch nach eignen Wünschen und Vorstellungen selber konfigurieren und anpassen möchten. Dementsprechend gibt es in den Konfiguratoren der Fahrzeughersteller tausende verschiedene Möglichkeiten, wie das fertige Fahrzeug am Ende aussehen kann. Dabei unterscheidet sich dadurch auch die Architektur von Fahrzeug zu Fahrzeug. Wie Abbildung 4 zeigt, gibt es bei den Plattformen CAN-Antrieb, CAN-Komfort und CAN-Diagnose stets mehrere Möglichkeiten, welche der Kunde wählen kann. Teils können Module parallel genutzt werden, wie die Parksensoren, der Abstandsradar und der Spurhalteassistent beim CAN-Antrieb. Teils ist es aber auch eine Entweder-oder-Entscheidung: Entweder nur das Radio oder das Navigationssystem „Standard“ oder „Premium“ usw.

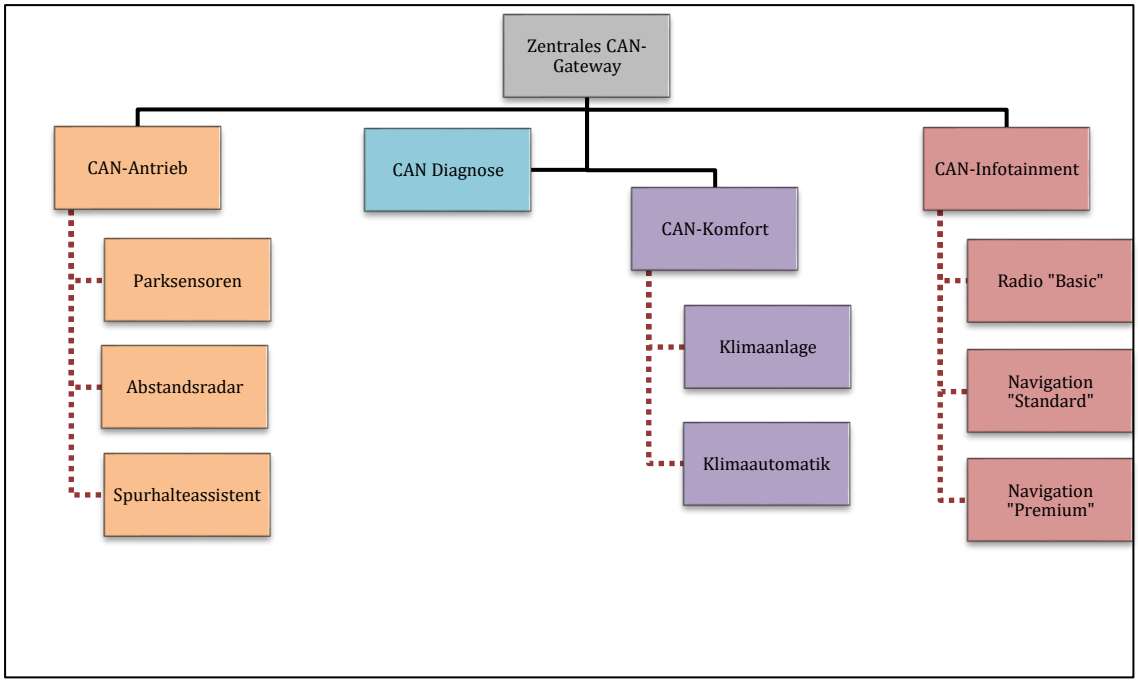


*Abbildung 4: Beispielhafte Vernetzung im Fahrzeug*

Deshalb ist es im Gegensatz zu den Fahrzeugen vor der Jahrtausendwende bei neueren Fahrzeugen unwahrscheinlicher, zwei Fahrzeuge desselben Modells zu finden, welche

eine identische Konfiguration haben. Trotzdem müssen alle Module, Komponenten und ECUs im Fahrzeug zusammenpassen, egal welche Konfiguration der Kunde wählt.

Aufgrund dieses Aufbaus mit Sensoren, Aktoren und ECUs werden Fahrzeuge heutzutage oft auch als **Automotive Cyber-System** bzw. Automotive Cyber-Physical-System bezeichnet. „Cyber-Physical-Systems adressieren die enge Verbindung eingebetteter Systeme zur Überwachung und Steuerung physikalischer Vorgänge mittels Sensoren und Aktuatoren über Kommunikationseinrichtungen mit den globalen digitalen Netzen (dem ‚Cyberspace')". (Broy, 2010)

Ein Automotive Cyber-System ist demnach das Zusammenspiel der elektronischen Komponenten (Aktoren, Sensoren, ECUs…) mit der digitalen Umwelt, mit welcher das Fahrzeug über Mobilfunk, WLAN etc. verbunden ist, wie Abbildung 5**Fehler! Verweisquelle konnte nicht gefunden werden.** schematisch zeigt. Der Kommunikator ist in diesem Fall die ECU, der Prozessor das zentrale CAN-Gateway. Die Zusammenführung von Umwelt und einem System, was diese selbstständig wahrnehmen und auf sie reagieren kann, ist eine Voraussetzung für die zukünftigen Level des autonomen Fahrens.

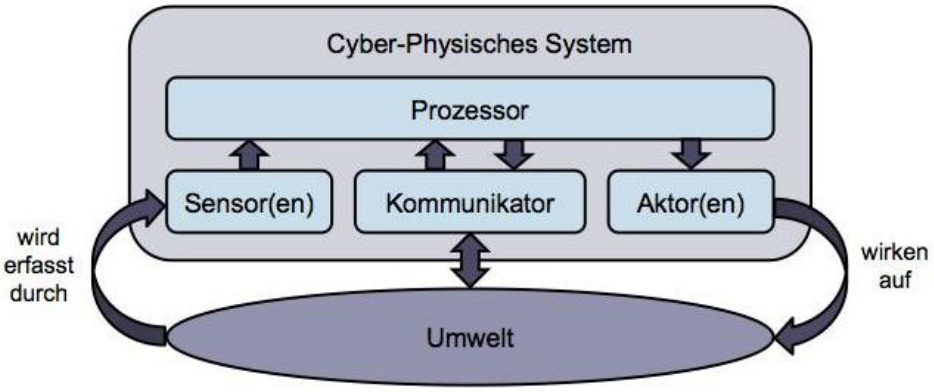


*Abbildung 5: Schematischer Aufbau eines Cyber-Physischen Systems. (Veigt, et al., 2013)*

Auch die Fahrzeughersteller haben erkannt, dass die steigende Komplexität durch immer neue Funktionen bald nur noch schwer zu managen ist. Deshalb gibt es Überlegungen und Konzepte, um die heutige E/E-Architektur weiter zu entwickeln. Wie häufig in der IT, wenn ein System in viele kleine Bestandteile aufgeteilt und dadurch eine hohe Komplexität erlangt hat, so geht auch bei Fahrzeugen der Trend wieder in Richtung Zentralisierung, wie die folgende Abbildung 6 zeigt.es autonomen Fahrens.

Wie schon beschrieben, sind ECUs derzeit modular aufgebaut und jede ECU hat meist nur eine einzige Funktion. Es gibt teils aber schon Ansätze, einzelne ECUs zu einem

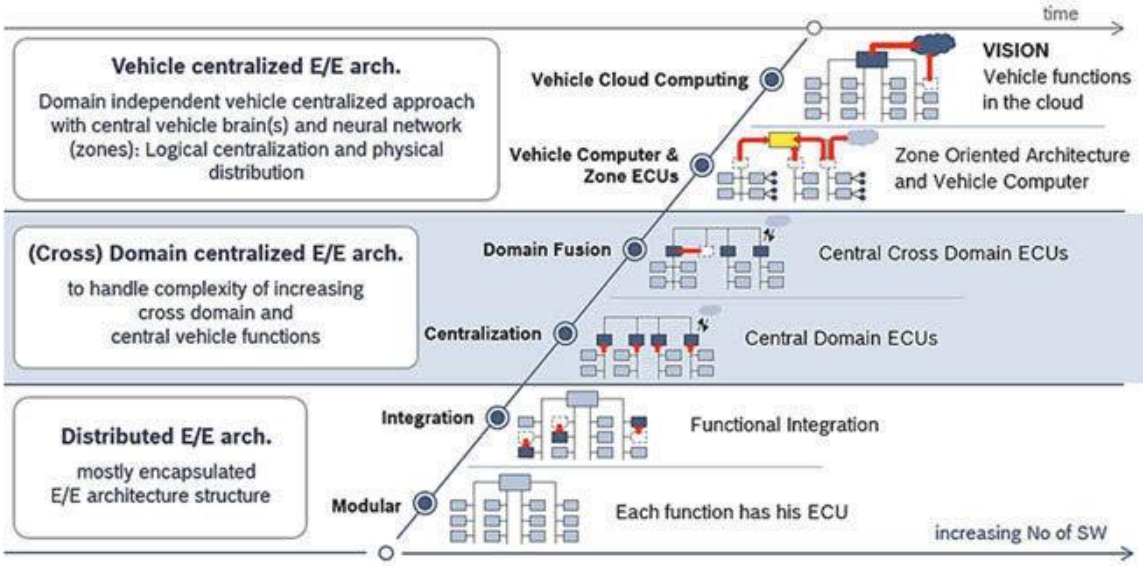


*Abbildung 6: Evolution von E/E-Architekturen in den nächsten Jahren. (Haas, et al., 2016)*

größeren Modul zusammenzufassen, die sogenannte funktionale Integration. Ein Beispiel hierfür ist die kombinierte Multifunktionskamera in der Frontscheibe, welche mehrere Aufgaben, die früher getrennt waren, inzwischen vereint und in einer gemeinsamen ECU verarbeitet (z.B. Lichteinfall, Regen und die Erkennung von Fahrstreifen).

Der nächste wahrscheinliche Schritt ist die Zusammenfassung von ECUs unter einer Master- bzw. Domain-ECU, welche alle Aufgaben einer Domäne bewältigt. Zum Beispiel eine ECU für die Domäne „Licht“ oder „Temperatursteuerung“. Auch die Fusionierung von Domänen ist denkbar, dass immer mehr Funktionen in einer zentralen Einheit verwaltet und gesteuert werden. Ein letzter Schritt könnte die Zusammenfassung zu Zonen sein, was einer Zone aus dem Defense in Depth Konzept gleichgesetzt werden kann: Domänen mit gleichen Security Anforderungen werden zusammengefasst und im allerletzten Schritt, sofern möglich, in der Cloud abgebildet. Bis dahin ist es allerdings noch ein weiter Weg. (Haas, et al., 2016)

Ein letzter Punkt, welcher in diesem Unterkapitel noch beleuchtet werden soll, ist der Unterschied zwischen **Safety** und **Security**. In der deutschen Sprache gibt es für beide Begriffe nur einen: Sicherheit. Dabei beschreiben Safety und Security zwar zwei zusammenhängende, aber doch unterschiedliche Dinge. Safety beschreibt ein System, das sich auf den Schutz von Menschen und Umwelt fokussiert, oft auch als funktionale Sicherheit bezeichnet wird (Lass, et al., 2014). Im automobilen Kontext fallen bislang fast alle Funktionen, die als „Sicherheitsfunktionen“ aufgeführt werden, in die Kategorie Safety. Für diese Kategorie gibt es auch eine international gültige Norm: Die ISO 26262 und die IEC61508, welche aufeinander aufbauen. Diese gliedert Safety in Automotive Safety Integrity Levels (ASIL) von A bis D, wobei ASIL A für ein niedriges Level steht

und ASIL D für ein hohes. Beispiele für Safety-Funktionen sind Airbags, die Knautschzonen des Fahrzeugs oder Notbremsassistenten.

Mit Security wird der Schutz eines Systems oder Informationen vor unerlaubten Zugriffen oder vor Manipulation beschrieben, ob durch Menschen oder die Umwelt (Lass, et al., 2014). In einem Fahrzeug wäre das zum Beispiel die Absicherung einer Mobilfunkschnittstelle gegen Angreifer. Grundsätzlich kann man, wenn man von Privacy mal absieht, bei Fahrzeugen davon ausgehen, dass alle Security-Maßnahmen der Safety gelten. Das heißt, durch Security-Maßnahmen, wie Zertifikate oder Verschlüsselung, wird zum Beispiel verhindert, dass Angreifer auf Safety-Features wie den Airbag zugreifen und diesen auslösen.

Eine ähnliche Einteilung, welche in der Literatur häufig zu finden ist, ist die Einteilung in sicherheitsbezogene- und sicherheitsrelevante Systeme, sowie in aktive und passive Sicherheit:

- Das sicherheitsbezogene System reduziert Risiken (zählt also zu Safety)
- Das sicherheitsrelevante System kann durch Fehlfunktionen Gefahren verursachen und muss deshalb entsprechend abgesichert werden (Benz, 2004)
- Aktive Sicherheit beinhaltet Systeme, die helfen, Unfälle zu vermeiden
- Passive Sicherheit beschreibt Systeme, die die Folgen eines Unfalls mindern

# 3 Aktueller Forschungsstand Automotive Security

In diesem Kapitel wird zunächst der aktuelle Forschungsstand ausgewertet. Es wird beschrieben, wie vorgegangen, welche Studien herangezogen und welche Erkenntnisse getroffen wurden. Im Anschluss werden die Erkenntnisse zusammengefasst und die Rahmenbedingungen um IT-Sicherheit in Fahrzeuge zu bringen, erläutert.

## 3.1 Vorgehen bei der Auswahl und Auswertung von Studien und wissenschaftlichen Artikeln

Die wichtigsten Schlüsselbegriffe bei der Suche waren zunächst einmal die Termini aus den Bereichen „Defense in Depth“ und „Fahrzeug Sicherheit“. Von diesen beiden Begriffen ausgehend wurden über Schlagwörter in den Dokumenten und über genannte Quellen weitere Begriffe identifiziert, nach denen im Anschluss ebenfalls gesucht wurde. Es stellte sich heraus, dass sich zwei Suchcluster voneinander unabhängig bildeten: Das eine beschäftigte sich mit IT und IT-Sicherheit, das andere mit Fahrzeugen und Unterthemen hierzu. Die beiden Suchcluster und die dazugehörigen Schlüsselwörter werden im Folgenden in Abbildung 7 und Abbildung 8 dargestellt.

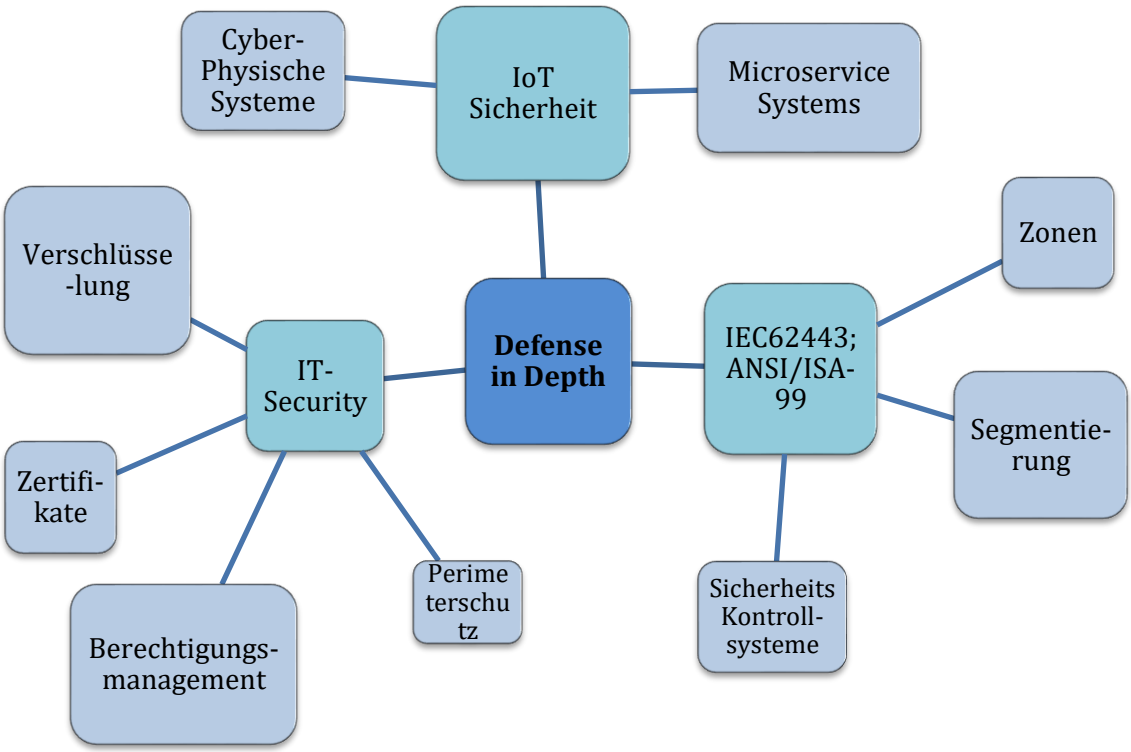


*Abbildung 7: Suchcluster "Defense in Depth"*

Anhand dieser Sammlung an Suchwörtern wurden dann Studien gesucht. Es wurden vorrangig Studien gewählt, welche mehr als eins der aufgezeigten Schlüsselwörter beinhalteten. Außerdem wurde auf eine möglichst hohe Aktualität der Studien geachtet. So

wurden nur Studien gewählt, welche nach 2005 veröffentlicht wurden. Dabei wurden ähnliche Studien, welche ein neueres Veröffentlichungsdatum aufwiesen, bevorzugt.

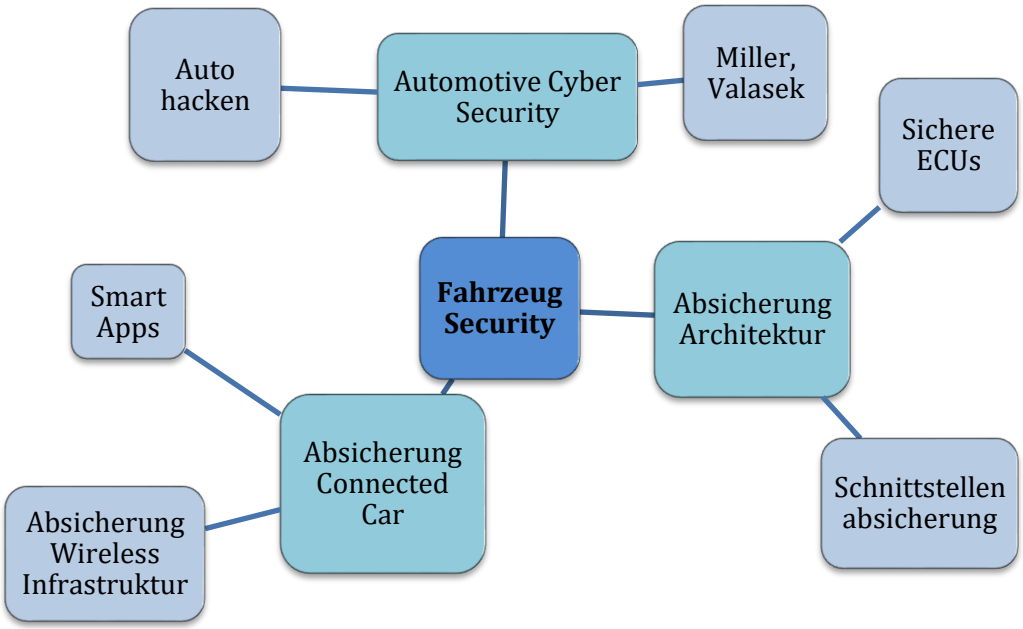


*Abbildung 8: Suchcluster "Fahrzeug Security"*

Die Studien wurden in erster Instanz nach Schlagworten durchsucht und dementsprechend gegliedert, ob sie sich eher mit „Fahrzeug Security“ oder mit „Defense in Depth“ beschäftigten. Die Studien, die beide Themen enthielten, sind die dritte Kategorie.

Es wurden schlussendlich acht Studien und Artikel ausgewählt, die hier im Folgenden dargestellt werden:

- Adler, Ebert: Automotive Cyber-Security-Erfahrungen für die Entwicklungspraxis
- Bouard, Graf, Weyl: Smart Apps in einem vernetzten (auto)mobilen Umfeld: IT-Security und Privacy
- Braunbach, Jander, Pokahr: Defense-in-depth and Role Authentication for Micro-service Systems
- Fabro, Kuipers: Control Systems Cyber Security: Defense in Depth Strategies
- Larson, Nilsson: A Defense-in-Depth Approach to Securing the Wireless Vehicle Infrastructure
- Kotarski, Lass: IT-Sicherheit als besondere Herausforderung von Industrie 4.0
- Miller, Valasek: A Survey of Remote Automotive Attack Surfaces
- Smith: A Car Hackers Handbook

## 3.2 Analyse ausgewählter Studien zu Automotive Security und Darstellung von deren Ergebnissen

### 3.2.1 Automotive Cyber-Security-Erfahrungen für die Entwicklungspraxis

Adler und Ebert (2016) zeigten in ihrem Artikel auf, wieso das Zusammenspiel von Connected Cars und IT-Sicherheit für Automobilhersteller so ein großes Problem ist und mit welchen Methoden gegen dieses Problem vorgegangen werden kann. Dabei fokussierten sie sich besonders auf die Phase der Fahrzeugentwicklung. Sie stellten fest, dass hardwareseitig insbesondere die hohe Komplexität, der hohe Vernetzungsgrad und Verknüpfungen von elektronischen, standardisierten Komponenten, sowie offene Schnittstellen diese zu einem sicherheitskritischen Ziel für Angreifer machen. Die bislang von den Automobilherstellern gelebte Sicherheit ist eine reine funktionale Sicherheit und hat mit IT-Sicherheit wenig zu tun. Wenn überhaupt, dann werden bisher nur Einzelkomponenten geschützt, was zu keinem sicheren Gesamtkonzept führen kann. Außerdem reichte es bislang zwar aus, Fahrzeuge vor direkten Angriffen, bei denen eine physikalische Anwesenheit des Täters nötig ist, zu schützen, aber mit Connected Cars und funkbasierten Verbindungen ist diese Annahme veraltet. Auf der Softwareseite ist das Problem, dass Änderungen an der Software im Fahrzeug oft spontan oder von Dritten durchgeführt würden ohne einen Security-Prozess zu durchlaufen.

Adler und Ebert schlagen daher vor, ein Konzept für den gesamten Produktlebenszyklus zu gestalten, um den Sicherheitsanforderungen gerecht zu werden. Sie benennen dafür einzelnen Maßnahme, insbesondere für die frühen Phasen des Produktlebenszyklus, also Design und Entwicklung. Diese Maßnahmen sehen die Absicherung von Komponenten (z.B. sichere ROM und Flash Module), Schlüsselprüfungen zur Laufzeit Intrusion Detection Systeme (IDS), Verschlüsselung und Penetration Tests vor. Außerdem setzen sie auf eine Sensibilisierung der Mitarbeiter in der Entwicklung sowie auf die Einführung von verbindlichen Design und Coding Standards.

### 3.2.2 Smart Apps in einem vernetzten (auto)mobilen Umfeld: IT-Security und Privacy

Der Ansatz von Bouard, Graf und Weyl (2012) beschäftigt sich mit Apps, welche für die Kommunikation mit dem Fahrzeug gedacht sind, um damit entweder Daten aus dem Fahrzeug zu erhalten oder Daten einzuspeisen. Dabei betrachten sie neben IT-Sicherheitsaspekten dieser Apps auch deren Privacy-Aspekte. Sie zeigen auf, dass insbesondere personenbezogene Daten des Fahrers ins Visier von Angreifern geraten könnten,

die Daten wie Fahrverhalten, Fahrrouten, Kontakte oder Bezahldaten selbst verwerten oder an interessierte Dritte weiterverkaufen könnten, welche wiederum diese dann für Werbung oder ähnliches nutzen. In Bezug auf IT-Security stellen sie besonders das Problem der Validität von Nachrichten oder Daten aus Apps dar. Sie fragen sich, wie ein Fahrer sich zum Beispiel sicher sein kann, das eine Warnung über eine Gefahrenstelle tatsächlich auch wahr und valide ist, und nicht manipuliert. Um darum die Apps besser abzusichern, schlagen die Autoren mehrere Maßnahmen vor: Zum einen sollten Sicherheitskomponenten modularisiert werden, um diese besser anpassen und optimal konfigurieren zu können. Dadurch sind einzelne Module auch besser und schneller austauschbar. Schnittstellen sollten zudem vereinfacht werden, um eine Integration erfolgreich zu machen. Dafür stellen sie ein Schichtenmodell vor, welches auf dem ISO/OSI-Schichtenmodell basiert. Zwischen den dort aufgezeigten einzelnen Units sind einheitliche Schnittstellen (Layer-Enforcement-Points) definiert. Für die Einbindung von externen Modulen ist eine Adapter-API angedacht. Damit könnten auch Apps von OEMs die Security-Features des Modells verwenden. Im Anschluss beschreiben die Autoren die einzelnen Komponenten, sowie den Ablauf des Datenflusses für dieses Modell.

### 3.2.3 A Defense-in-Depth Approach to Securing the Wireless Vehicle Infrastructure.

Mit einem ähnlichen Thema beschäftigten sich auch Larson und Nilsson (2009). Bei ihnen standen aber nicht die Apps, sondern die Verbindung dieser zum Fahrzeug im Vordergrund. Sie beschäftigten sich mit der Frage, wie Funkzugänge zu einem Fahrzeug abgesichert werden können, auch wenn dazu gesagt werden muss, dass ihre Ausarbeitung schon von 2009 ist.

Die erste Erkenntnis, welche Larson und Nilsson ziehen, ist, dass sich mit dem Einzug von Funktechnologie in Fahrzeuge neue Wege für Angreifer öffnen werden. In-Car-Netzwerke wurden bislang als isoliert betrachtet und auch nur dementsprechend geschützt. Zwar bringen neue Techniken wie „Firmwareupdate Over the Air“ (FOTA) Vorteile für Hersteller und Kunden, dabei sollte aber nicht vergessen werden, solche Technologien auch entsprechend sicher auszugestalten. Außerdem bemängeln sie, dass jede ECU eine eigene Firmware hat und somit auch jede ECU einzeln abgesichert werden muss, zumal ECUs sowieso nur eine limitierte Leistung haben und die Echtzeitübertragung von Daten trotz Security-Maßnahmen weiter gegeben sein muss. Datenverkehr zwischen ECUs erfolgt zudem nicht nur auf IP, sondern auf CAN-Ebene und muss daher auch anders als klassischer IP-Verkehr abgesichert werden.

Nach ihrem schon in Abbildung 2 vorgestellten Modell schlagen sie drei Stufen vor, um Funkverbindungen und ECUs abzusichern: In der ersten Stufe (Prevention) sollte es die Möglichkeit von Secure-FOTA geben. Dabei setzen sie auf die Maßnahmen Verschlüsselung, Hashfunktionen und digitale Signaturen. Über einen von ihnen definierten Prozess soll es somit möglich sein, Firmware-Updates über Funk einzuspielen, ohne dass ein Angreifer dieses manipulieren kann. Für die Verbindung zwischen ECUs schlagen sie eine Verschlüsselung basieren auf Message Authentication (MAC)-Blöcken und MAC-Keys vor. In der zweiten Stufe (Detection) wird die Einführung eines IDS empfohlen, wobei dies so designt wird, dass die Detektoren jeweils direkt an den ECUs andocken, um eine korrekte Zuordnung von richtigen und manipulierten Datenströmen machen zu können. In der dritten Stufe (Deflection) wird der Aufbau eines „Honeypots“ dargestellt, inklusive Logging-Funktionalitäten für eine Analyse im Nachgang.

### 3.2.4 A Survey of Remote Automotive Attack Surfaces.

Einen anderen Ansatz verfolgen Miller und Valasek (2014), welche durch ihren medienwirksamen Jeep-Hack Bekanntheit erlangt haben. Diese Vorgehensweise sowie ihre Untersuchungen an insgesamt 14 Fahrzeugen werden in ihrer Studie vorgestellt. Dabei analysieren sie die Fahrzeuge und zeigen dabei auf, über welche Komponenten sie sich in die Fahrzeuge einhacken konnten.

Miller und Valasek haben als ihren Ausgangspunkt festgestellt, dass manche ECUs sowohl nach außen (Funk, WLAN, Bluetooth…) als auch nach innen in das In-Car-Network eine direkte Verbindung haben. Das macht diese ECUs besonders anfällig für Angriffe. Dabei beschreiben sie ihren Angriffsweg: Zunächst einmal wird eine ECU, welche eine Verbindung nach außen hat, kompromittiert. Dies kann zum Beispiel bei einer ECU im Listening-Mode durch Code-Injection geschehen. Über diese ECU wird im zweiten Schritt versucht, auf ECUs vorzudringen, welche sicherheitskritische Funktionen (wie Lenkung, Bremsen oder Gas) haben. Dabei wird versucht, auch in diese ECU wieder Schadcode einzubringen und somit eine Verbindung zwischen den Angreifer und der Ziel-ECU aufzubauen. Der letzte Schritt ist, die Ziel-ECU dazu zu bringen, eine sicherheitskritische Aktion auszuführen. Dies kann entweder durch manipulierte Signale (z.B. das Signal „Notbremsung einleiten“) oder durch ein aufspielen von manipulierter Firmware („flashen“) geschehen. Manchmal reicht es aber scheinbar auch aus, nur eine ECU anzugreifen, wenn diese schon die Informationen beinhaltet, auf die es der Angreifer abgesehen hat (wie z.B. Telemetriedaten).

Im Anschluss werden verschiedene Möglichkeiten und Wege beschrieben, über die ein Auto angegriffen werden kann, wie die Diebstahlsicherung, Reifendruckkontrolle, Keyless-Entry-Systeme, oder wie schon angesprochen Funk, WLAN und Bluetooth und viele mehr.

In einer anschließenden Studie von 14 Fahrzeugen unterschiedlicher Marken werden jeweils die Angriffsmöglichkeiten, die verwundbaren ECUs, der Entry-Point und der Angriffsweg dargestellt. Das Ergebnis ihrer Studie war, dass durch die starke Zunahme von ECUs die Angriffsoberfläche ebenso stark zugenommen hat. Zwar unterscheiden sich die getesteten Fahrzeuge von einander, was den Aufbau ihrer Systeme und ihrer Netzwerk-Topologie anbelangt, ähneln sich aber in den einzelnen Regionen (US/Japan/Deutschland) wieder sehr stark. Neuere Modelle haben teils schon eine Segmentierung von Systemen. Angreifbar waren aber alle getesteten Autos. Zum Schluss schlagen Miller und Valasek einige Punkte vor, mit denen Hersteller ihre Fahrzeuge gegen die von ihnen versuchten Angriffe besser schützen können. Die Maßnahmen sind dabei nicht überraschend: Remote-Endpoints sollen besser abgesichert werden, es sollte Maßnahmen gegen Injection auf CAN-Systemen geben, Nachrichten im Fahrzeug sollten verschlüsselt, die Netzwerk-Architektur verbessert und eine Angriffserkennung (IDS) implementiert werden.

### 3.2.5 A Car Hackers Handbook

Eine ähnliche Studie hat auch Smith (2014) veröffentlicht. Er selber nennt es „Handbuch, um Autos zu hacken“, die Grundidee, welche Miller und Valasek mit ihrer Studie hatten, ist dieselbe. In seiner Studie erläutert er, was man unter Angriffsoberfläche in der IT versteht und welche Angriffsmöglichkeiten und -wege es bei Fahrzeugen gibt.

Angriffswege, so beschreibt er es, sind alle Möglichkeiten, um ein bestimmtes Ziel anzugreifen, in diesem Fall ein Fahrzeug. Ob von außerhalb über Radiofunkwellen, Bewegungssensoren etc. oder von innerhalb über Audio-Input wie CD oder USB, die OBD-Schnittstelle oder Internetverbindungen. Smith sortiert und gruppiert dann verschiedene Angriffsmöglichkeiten anhand der In-Car-Systeme, welche Ziel der Angriffe sind. Das sind zum Beispiel das Infotainment System, das fahrzeuginterne Kommunikationssystem, die Motorsteuerung, der CAN-Bus oder ECUs. Er beschreibt für die einzelnen Kapitel dann Schritt für Schritt Wege, Methoden und benötigte Hard- und Softwaretools, um das Fahrzeug anzugreifen. Methoden, wie Hersteller die aufgezeigten Lücken schließen können, stellt er nicht vor.

### 3.2.6 Defense-in-depth and Role Authentication for Microservice Systems

Eine eher lösungsorientierte Studie haben Braunbach, Jander und Pokahr (2018) veröffentlicht, welche sie auf der ANT[6]-2018 vorstellten. Sie beschäftigten sich mit der Analyse von Sicherheitslücken in Microservice Systemen und wie man diese mit einem Defense-in-Depth-Ansatz absichern könnte. Zwar sind in einem Fahrzeug nicht unbedingt die Microservices präsent, welche in der Studie erwähnt werden, trotzdem sind viele Parallelen sichtbar.

Bei Microservices geht es um ein System, welches aus mehreren Softwarekomponenten oder Services besteht, welche von unterschiedlichen Teams entwickelt und gewartet werden. Dabei erbringt jedes Team sowohl die Entwicklung als auch den Betrieb ihres Services (DevOps) aus einer Hand. Dabei werden alle Microservices dem Kunden zusammen als ein Service angeboten, ohne dass dieser mitbekommt, dass verschiedene Teams oder Hersteller dahinterstecken. Dieser gemeinsame Service wird meist nur durch einen Perimeterschutz geschützt. Die einzelnen Microservices selber werden nur teilweise abgesichert. Die Autoren machten auf die Gefahr bei diesem Vorgehen aufmerksam. Ein Angreifer muss bei diesem Vorgehen nur das schwächste Glied in der Kette attackieren und hat somit Zugriff auf die anderen Microservices, welche eventuell kritische Daten oder Funktionen enthalten. Die Autoren schlagen deshalb einen Defense-in-Depth-Ansatz vor: Alle Microservices müssen IT-Security-Maßnahmen implementieren sowie dafür Sorge tragen, dass die Strecken zwischen den Services ebenfalls abgesichert sind, auch wenn dies für jedes beteiligte Team einen erhöhten Aufwand sowie zusätzlich benötigtes Knowhow bedeutet.

Dabei schlagen sie verschiedene Maßnahmen vor. Diese sollten in erster Linie rollenbasierte Authentifizierung und Verschlüsselung von Services sein. Um diese Maßnahmen umzusetzen ist auch die Einführung einer PKI vorgesehen. Es wird weiterhin beschrieben, wie für Microservices dieses Konzept umgesetzt werden kann. Ihr Ansatz basiert dabei auf TCP/IP und HTTP Verbindungen und wie diese Abgesichert werden können. Dabei setzen sie auf das Jadex Active Component Framework. Mit diesem Framework wird der Aufbau einer sicheren, verschlüsselten Verbindung zwischen zwei Microservices mittels Authentifizierung (über PKI) realisiert.

[6] ANT ist die „International Conference on Ambient Systems, Networks and Technologies"

### 3.2.7 Control Systems Cyber Security: Defense in Depth Strategies

Eine Defense-in-Depth-Strategie stellten auch Fabro und Kuipers (2006) vor, wobei der Schwerpunkt ihrer Studie auf der Absicherung von Kontrollsystemen[7] liegt. Die Autoren erläutern, dass Unternehmen die IT traditionell darauf ausrichteten, Daten nicht nach außen gelangen zu lassen, da es keine Verbindung nach extern gab. Dementsprechend waren die IT-Systeme eher nach Funktionen aufgeteilt, wie das Corporate LAN oder Serversysteme und Datenbanken. Die einzelnen Bereiche hatten dabei meist keine Verbindungen untereinander. Heutzutage gibt es mehr und mehr Verbindungen zwischen den einzelnen Bereichen, sowie Verbindungen nach extern. Durch diese neuen Verbindungen ohne zusätzliche Sicherheitsmaßnahmen werden die IT-Systeme von Unternehmen angreifbarer. Es werden verschiedene Angriffsmöglichkeiten wie Angriffe über Backdoors, Angriffe über Datenbank SQL Injection und Angriffe auf externe, mit dem Unternehmensnetz verbundene Geräte erklärt und wie es darüber möglich ist, über mehrere Stationen von extern auf kritische Systeme wie Datenbanken zu gelangen.

Als Lösungsansatz wird von den Autoren Defense in Depth vorgeschlagen. Dies bedeutet in erster Linie, dass Systeme in verschiedene Zonen unterteilt und isoliert werden. Dabei sollen Zonen hinsichtlich ihrer Konnektivität und Kritikalität unterteilt werden: Eine Zone für die Kommunikation mit dem Internet, eine für externe Verbindungen mit anderen Unternehmen und externen Services, eine für die interne Unternehmenskommunikation (mit evtl. Anbindung an das Internet, also der erstgenannten Zone) und eine Zone für kritische, interne Systeme. Dabei wird zwischen den Zonen nur noch über abgesicherte, dedizierte Strecken kommuniziert. Diese Strecken sind mit adäquaten Firewalls (Stateful Inspection Firewalls, Proxy Firewalls, Package Filter Firewalls) sowie IDS ausgestattet. Davon versprechen sich die Autoren, dass alle Datenpakete, welche im Firmennetzwerk versendet werden, überwacht werden können und Angriffe somit erkannt und abgewehrt. Als letzten Punkt, welcher auch noch als wichtiger Bestandteil von Defense in Depth angesehen wird, sind organisatorische Maßnahmen wie das Erstellen von Security Policies, Security Training für Mitarbeiter und ein definierter Incident Response Prozess. Am Ende sollte ein proaktives Security Modell stehen, an dem alle Beteiligten gemeinsam mitwirken.

[7] Ein Kontrollsystem in diesem Kontext ist dafür zuständig, Zugriffsversuche auf Anlage oder Systeme zu prüfen, zu loggen, zu regulieren und im Zweifel zu verweigern.

### 3.2.8 IT-Sicherheit als besondere Herausforderung von Industrie 4.0

Kotarski und Lass (2014) untersuchten, welche Herausforderungen es für Industrie 4.0 hinsichtlich IT-Sicherheit gibt. Dabei wurde eine Lösung der Absicherung von „Internet of Things (IoT)"-Geräten angestrebt. Sie stellen fest, dass bisherige IT-Sicherheitsmodelle entweder sehr generell gehalten oder hauptsächlich auf Standart- und Office-IT beschränkt und auf IoT-Geräte nur bedingt übertragbar sind. Da bei vielen IoT-Geräten die Echtzeitfähigkeit zwingend erforderlich ist, sind Security Maßnahmen, welche die Datenübertragung und -verarbeitung stark verlangsamen würden, keine Option. Außerdem ist entgegen der Standard-IT der Lebenszyklus eines IoT-Gerätes häufig deutlich länger, insbesondere bei Industrieanlagen. Deshalb muss gewährleistet sein, dass über einen langen Zeitraum IoT-Geräte aus unterschiedlichen Generationen weiterhin gewartet und mit Sicherheitsupdates versorgt werden können. Ein weiterer Risikofaktor ist der Mensch, ob Kunde oder Mitarbeiter. Dadurch das diese sich über Bring-your-own-Device (BYOD) mit ihrem Laptop oder Smartphone drahtlos mit IoT-Geräten verbinden können, kann über diese Verbindungen Schadcode in das IoT-Gerät gelangen.

Deshalb schlagen die Autoren als Lösung einen Defense-in-Depth-Ansatz vor. Nach ihren Einschätzungen sollte die IT und auch die IoT-Geräte nach ANSI/ISA-99 bzw. IEC62443 (vgl. Kapitel 2.1) in Zonen segmentiert werden. Die einzelnen Zonen und darin enthaltenen IoT-Geräte werden über den Einsatz von gezielten, passenden Maßnahmen wie Paket Filter, deaktivierten Schnittstellen wie Bluetooth, WLAN oder USB, IDS und Access Control Systeme abgesichert. Um diese Maßnahmen bestmöglich zu integrieren, schlagen sie vor, diese bereits bei der Planung und Entwicklung von IoT-Komponenten und deren Vernetzung zu berücksichtigen.

## 3.3 Zusammenfassung der Anforderungen und Rahmenbedingungen für IT-Sicherheit in Fahrzeugen

### 3.3.1 Anforderungen an Fahrzeugarchitekturen

Zwei Faktoren sind in den Studien als besonders kritisch eingestuft worden, wenn es um Anforderungen an eine Fahrzeugarchitektur ging. Der erste Faktor war das Thema **Echtzeitfähigkeit**. Diese Anforderung erscheint logisch, wenn man bedenkt, wie viel in nur einer Sekunde passieren kann, wenn sich ein Fahrzeug mit 200 km/h oder mehr bewegt. In dieser Sekunde werden bei Tempo 200 über 55 Meter zurückgelegt. Dementsprechend performant müssen manche Komponenten, wie zum Beispiel ein Abstandsradar sein. Ihre Reaktionszeiten dürfen maximal im Millisekunden-Bereich liegen. Ein zweiter

Faktor war die **Ausfallsicherheit** von kritischen Komponenten. Für diese Komponenten muss es im Falle eines Ausfalls zumindest einen „Plan B“ geben, um einen Schaden abzuwenden. So gibt es zum Beispiel bei dem Ausfall der Hauptbremsen immer noch die Möglichkeit, das Fahrzeug mit der Handbremse zum Stehen zu bringen.

Neben diesen kritischen Faktoren gibt es noch weitere, welche ein Fahrzeug erfüllen muss. Ein Faktor ist der **modulare Aufbau** der Architektur. Dies ist wichtig, weil zum einen Kunden ihr Fahrzeug selber konfigurieren wollen und bestimmte Module (z.B. Navigationssystem oder Klimaanlage) in verschiedenen Ausfertigungen in die Gesamtarchitektur passen müssen, zum anderen weil viele Module von unterschiedlichen Zulieferern kommen und es hier die Möglichkeit geben muss, diese ohne großen Aufwand in das Fahrzeug und auch in verschiedene Fahrzeugbaureihen zu integrieren. Außerdem muss ein Fahrzeug **vernetzt** sein und mit seiner Umwelt kommunizieren können. Dazu gibt es Schichten und Kommunikationsprotokolle, wie Abbildung 9 zeigt.

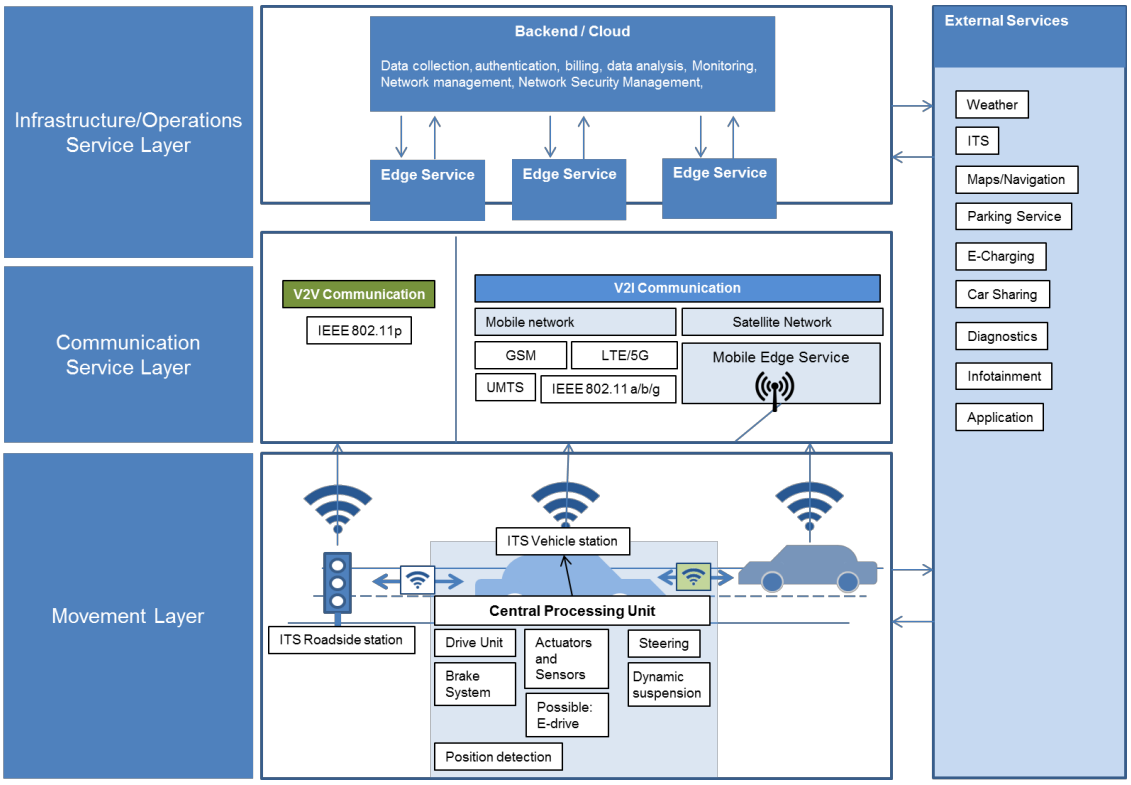


*Abbildung 9: Infrastruktur-Schichten (NTT Data Deutschland GmbH, 2018)*

Auf der untersten Schicht, dem „Movement Layer“ geht es um die drahtlose Kommunikation mit der unmittelbaren Umwelt (die sogenannte Short-Distance-Communication) wie zum Beispiel Ampeln oder einem anderen Fahrzeug in unmittelbarer Nähe (bis 50 Meter) sowie die Einflüsse auf das Verhalten des Fahrzeugs in Bezug auf diese. Wenn die Ampel vor dem Fahrzeug auf Rot schaltet oder das vorausfahrende Fahrzeug

bremst, wird unmittelbar auch ein Befehl zum Bremsen ausgelöst. Übertragungstechnologie für Kurzstreckenkommunikation kann zum Beispiel Bluetooth oder WLAN sein. Daraus resultierende Anforderungen für die Architektur ist die Möglichkeit, auf kurze Distanz Echtzeitkommunikation zu ermöglichen.

In der zweiten Schicht geht es um die Kommunikation mit weiter entfernten Objekten (Long-Distance-Communication) wie anderen Fahrzeugen oder der Infrastruktur. Hier kommt Mobilfunk- und Satellitentechnologie zum Einsatz, welche schnelle Kommunikation über längere Strecken ermöglichen. Die Anforderungen hier ist eine stabile, sichere und ständige Kommunikationsmöglichkeit mit der Ausfalloption, wenn einmal kein Netz verfügbar ist, trotzdem zu funktionieren.

Die dritte Schicht ist die Kommunikation mit dem Backend oder der Cloud beim Hersteller. Hier können zudem weitere, externe Services angebunden und genutzt werden. Die Anforderung hier ist zwar keine dauerhafte Verbindung, aber die Möglichkeit, auch größere Datenpakete sicher austauschen zu können.

### 3.3.2 Anforderungen an IT-Sicherheit in einem Fahrzeug

Um Fahrzeuge vor Angriffen zu schützen, wurden verschiedene Faktoren genannt, welche IT-Sicherheit für eine reibungslose Integration in ein Fahrzeug aufweisen muss. Zum einen müssen IT-Sicherheitskomponenten für die **Absicherung von Schnittstellen** mit Verbindung nach außen sorgen. Dies gilt sowohl für drahtlose als auch für drahtgebundene Schnittstellen. Zum anderen muss IT-Sicherheit ein Konzept für eine sinnvolle **Segmentierung** von Fahrzeuginternen Komponenten in einzelne Zonen bereitstellen. Verbindungen zwischen den Zonen müssen mit IT-Security Maßnahmen entsprechend kontrolliert werden können. IT-Sicherheitskomponenten müssen außerdem über die gesamte Lebensdauer des Fahrzeugs auf einem aktuellen Stand der Technik[8] sein – ohne die Komponenten dafür wechseln zu müssen. Dazu soll IT-Sicherheit auch einen Prozess definieren, wie IT-Sicherheit über den gesamten Produktlebenszyklus – von den ersten Entwürfen über die Entwicklung, Herstellung, Nutzung bis zur Verschrottung – implementiert und umgesetzt werden kann. Dabei muss auch beachtet werden, dass sich während des langen Lebenszyklus externe Faktoren unvorhergesehen verändern können. So kann es zum Beispiel sein, dass ein Fahrzeug nicht mehr erreichbar ist, weil der Besitzer die Mobilfunkeinheit abgeschaltet hat, diese defekt ist oder das genutzte

[8]Definition: Der Stand der Technik […] ist der auf den einschlägigen wissenschaftlichen Erkenntnissen beruhende Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen, Bau- oder Betriebsweisen, deren Funktionstüchtigkeit erprobt und erwiesen ist. (§71a östr. GewO)

Funktionen nicht mehr zur Verfügung stehen (z.B. durch die Abschaltung von UMTS oder wenn ein Krypto-Verfahren kompromittiert wird).

Es müssen dabei möglichst alle **Angriffswege** bedacht werden. Diese wurden insbesondere in den Studien (Miller, et al., 2014) und (Smith, 2014) aufgezeigt. In Abbildung 10 werden verschiedene Angriffswege und Ziele aufgezeigt.

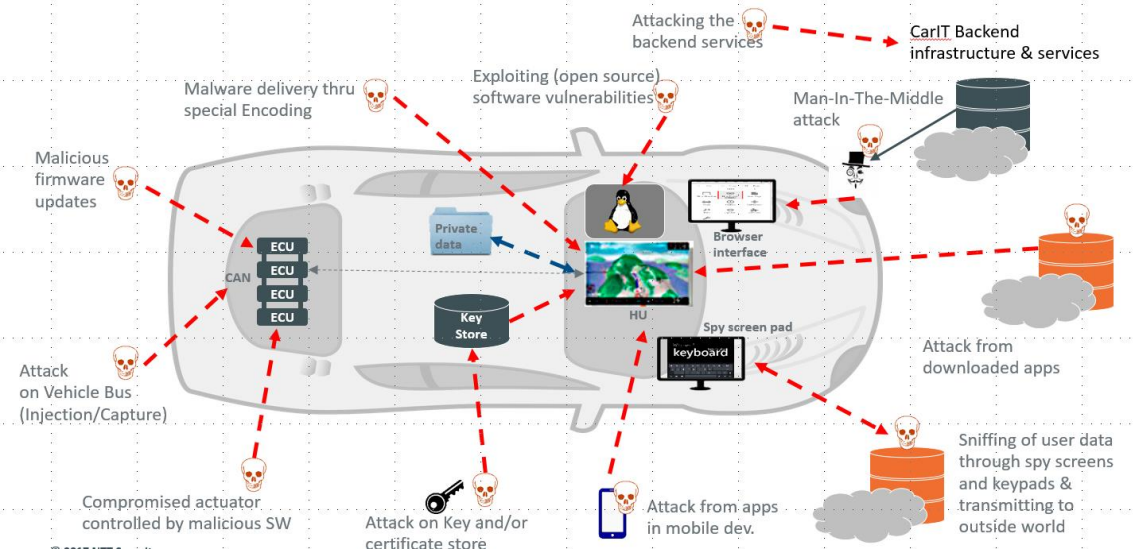


*Abbildung 10: Angriffswege Fahrzeug (NTT Security (Germany) GmbH, 2018)*

1. Angriffe auf ECUs und den CAN-Bus
    a. Es wird fehlerhafte Software mit Sicherheitslücken aufgespielt: Diese Schwachstelle können Angreifer missbrauchen, um gezielt nach diesen Lücken zu suchen und ausnutzen. Dadurch könnten sie Zugriff auf kritische ECUs bekommen und so in sicherheitsrelevante Systeme des Fahrzeugs eingreifen.
    b. CAN-Bus ist nicht abgesichert: Über CAN-Injection/ CAN-Capture Angriffe können Angreifer versuchen, Zugriff auf den CAN-Bus und darüber auch auf kritische ECUs zu erlangen. So könnten eventuell sie auf sicherheitsrelevante Systeme zugreifen.
    c. Schadhafte/Fehlerhafte Firmware oder Firmware Updates: Es könnte passieren, dass entweder eine fehlerhafte Firmware vom Hersteller selber schon ein schädigendes Ereignis auslöst oder das ein Angreifer versucht, eine Firmware mit Schadcode auf ECUs aufzuspielen und so wie schon zuvor beschrieben, Zugriff auf diese zu erlangen.
2. Angriffe auf die Head-Unit und damit verbundene Funktionen
    a. Ausnutzen von Open Source Software-Exploits: Wenn im Fahrzeug Open Source Software eingesetzt wird (z.B. ein Linux System) für welches es

bekannte Schwachstellen gibt, könnte ein Angreifer versuchen, diese Exploits auszunutzen und sich Zugriff auf Fahrzeugsysteme zu verschaffen.

b. Ausspähen von privaten Daten: Ein Angreifer könnte versuchen, personenbezogene Daten auszuspähen. Dies kann entweder über einen Keylogger passieren, welcher die Eingaben des Fahrers mitschneidet oder über Fernzugriff auf im Fahrzeug gespeicherte Daten des Fahrers.

c. Angriffe auf Schlüssel und Zertifikate: Durch einen Angriff auf die PKI im Fahrzeug könnte ein Angreifer an Schlüssel oder Zertifikate gelangen, die es ihm ermöglichen, mit diesen auf andere Systeme zuzugreifen oder sich als „das Fahrzeug“ auszugeben und so von Dritten unerlaubt Informationen abzugreifen.

3. Angriff auf Schnittstellen
    a. Direkter Angriff, drahtlos: Ein Angreifer könnte versuchen, offene Schnittstellen wie WLAN, Bluetooth oder NFC direkt und drahtlos anzugreifen und über diese Verbindungen ins Fahrzeug-Netz einzudringen. Solche Angriffe können auch über eine Zwischenstation wie Ampeln, andere Fahrzeuge etc. (V2X) erfolgen. Dabei könnte er versuchen, entweder Daten auszuspähen oder in tieferliegende, sicherheitsrelevante Systeme vorzudringen.
    b. Direkter Angriff, drahtgebunden: Über Schnittstellen direkt am Fahrzeug wie USB, OBD-Schnittstelle oder außenliegende und leicht zugängliche ECUs/Sensoren/Aktoren (z.B. im Außenspiegel oder die Reifendruckkontrolle) auf Fahrzeugsysteme zu gelangen und hier ebenfalls Daten auszuspähen oder weitere Systeme zu kompromittieren. Durch die Tatsache, dass es gesetzliche Rahmenbedingungen gibt, die eine teilweise Offenheit von OBD vorsehen, ist die Absicherung an dieser Stelle komplizierter.
    c. Indirekter Angriff: Über schadhafte Apps auf mobilen Geräten des Fahrers (Smartphone), welches dieser mit dem Fahrzeug verbunden hat oder über Schadcode in Mediadateien könnte ein Angreifer versuchen, diesen Schadcode in das Fahrzeug einzuschleusen und so eine Hintertür zu öffnen, um über andere Wege (wie einem Angriff über WLAN) das Fahrzeug weiter zu kompromittieren.
4. Angriffe auf das Backend
    a. Direkter Angriff auf das IT-Backend beim Hersteller: Wenn ein Angreifer sich Zugang zum IT-Backend des Herstellers verschaffen kann, so könnte er über diesen Weg auf das Fahrzeug zugreifen und entweder

Daten mitlesen oder versuchen, Firmware oder Software in das Fahrzeug einzuspielen und dort zu manipulieren. Durch einen Angriff auf das Backend ist es außerdem sehr wahrscheinlich, dass dadurch nicht nur ein einzelnes Fahrzeug, sondern die gesamte Flotte des Herstellers betroffen ist.

b. Man-in-the-Middle: Über eine ungesicherte Verbindung zwischen Backend und Fahrzeug könnte ein Angreifer versuchen, den Datenverkehr mitzulesen und so an wichtige Informationen zu gelangen (personenbezogene Daten) oder die Informationen für weitere Angriffe zu nutzen.

c. Schadhafte Apps im App-Store des Fahrzeugherstellers: Über das veröffentlichen von Apps mit Schadcode im App-Store eines Herstellers könnte ein Angreifer versuchen, diesen Schadcode in das Fahrzeug einzuschleusen und sich wie beim indirekten Angriff (3c) beschrieben, Zugang zu verschaffen.

Wie es schon im vorhergehenden Abschnitt teilweise beschrieben wurde, gibt es neben verschiedenen Angriffswegen auch unterschiedliche **Angriffsreichweiten**. Diese sind in Abbildung 11 dargestellt. Angriffe auf das „Vehicle Layer“ beziehen sich direkt auf das

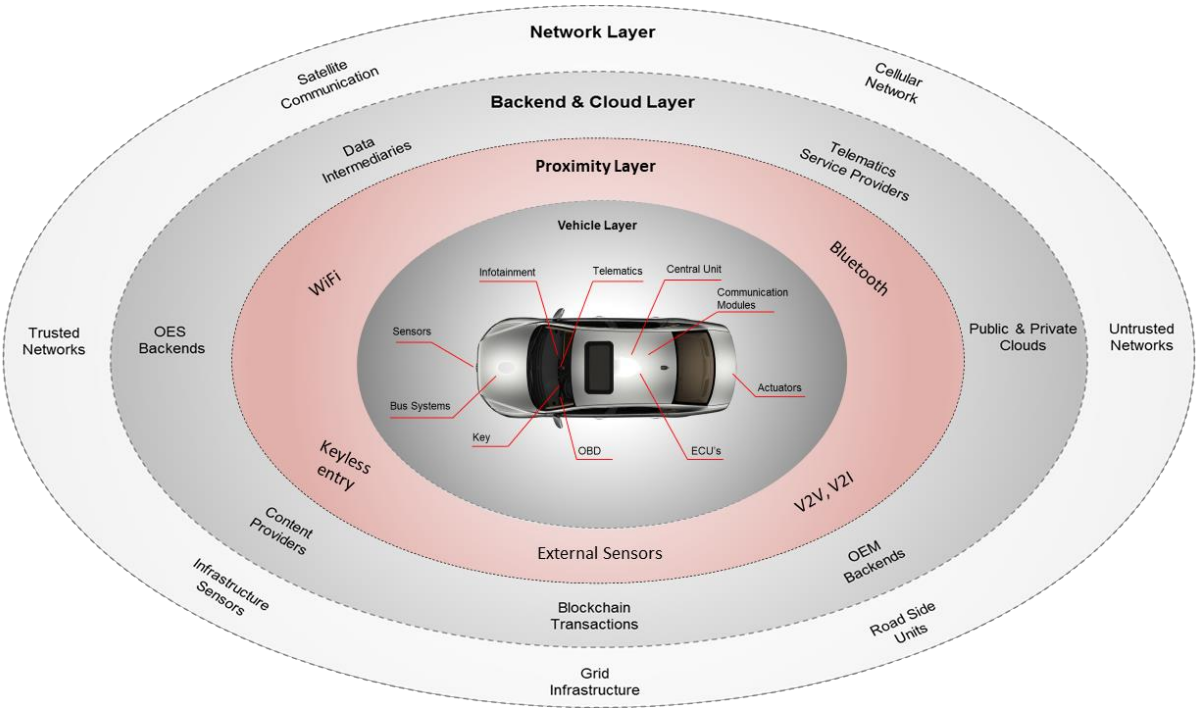


*Abbildung 11: Angriffsreichweiten (NTT Data Deutschland GmbH, 2018)*

Fahrzeug. Anders gesagt: Das Fahrzeug ist das direkte Ziel eines Angriffs. Es wird versucht, über verschiedene Wege das Fahrzeug zu kompromittieren. Dafür ist teils eine physische Präsenz am Fahrzeug nötig. Angriffe auf die „Proximity Layer“ sind Angriffe

auf und in der näheren Umgebung um das Fahrzeug. Es wird versucht, Technologie wie WiFi oder Bluetooth zu kompromittieren und so Zugang zu Fahrzeugsystemen zu erhalten. In der „Backend & Cloud Layer“ wird das Fahrzeug nicht unmittelbar angegriffen, sondern dessen Backend Infrastruktur beim Hersteller oder Service Providern. Auch hier kann versucht werden entweder über diese Wege Zugriff auf Fahrzeugsysteme zu erhalten oder aber Daten aus dem Backend auszuspähen (wie z.B. Daten über den Fahrer bei dem Service Provider „Versicherung“). In der „Network Layer“ werden weitgespannte Netzwerke ausgenutzt. Dabei muss nicht immer ein bestimmtes Fahrzeug das Ziel eines Angriffs sein, sondern es kann auch versucht werden, über Scans potentielle Opfer zu lokalisieren.

### 3.3.3 Neue Rahmenbedingungen im Automobilsektor

Zusätzlich zu den Anforderungen an die bisherige Fahrzeugarchitektur und IT-Sicherheitsmaßnahmen für diese, ändern sich durch vernetzte Fahrzeuge auch die Rahmenbedingungen. So kann man die Entstehung von neuen Geschäftsmodellen beobachten, sowohl bei Herstellern, Zulieferern und verschiedenen Service Providern, teils auch in Kombination zusammen. So kann man in Fahrzeugen mit integrierter SIM-Karte heute schon Datenpakete bei Mobilfunkanbietern buchen und diese über den WLAN Hotspot des Fahrzeugs mit einem Tablet oder Laptop nutzen. Es ist abzusehen, dass solche zahlungspflichtigen Extradienste mehr und mehr zunehmen werden (pay-by-use-Prinzip) (Bosler, et al., 2018). Weitere Dienste könnten zum Beispiel das Freischalten von Extra-PS für den Wochenendausflug oder das zeitweilige Zubuchen von Assistenzsystemen für eine lange Autobahnfahrt sein.

Außerdem hat auch die Politik erkannt, dass eine Rechtsgrundlage für autonomes Fahren und Connected Cars geschaffen werden muss und ist inzwischen in der Entwicklung von entsprechenden gesetzlichen Richtlinien[9]. In den USA sind das:

- Der SPY CAR Act, welcher IT-Security und Privacy Standards für Fahrzeuge setzen soll. (US Kongress, 2017)
- Der Autonomous Vehicle Privacy Protection Act für den Schutz von Kunden- bzw. Fahrerdaten (Privacy). (US Kongress, 2015)

[9] Zum Zeitpunkt der Erstellung dieser Arbeit gab es von den überarbeiteten Regulatorien noch keine verabschiedeten Fassungen.

- Die National Highway Traffic Safety Administration (NHTSA) hat Richtlinien für IT-Sicherheit in Fahrzeugen erstellt. (United States Department of Transportation, 2017)
- Das National Institute of Standards and Technology (NIST) hat ein Security-Framework entwickelt, welches auch für Fahrzeuge gilt. (United States Department of Transportation, 2017)

Auch in der EU gibt es neue Richtlinien für dieses Thema:

- Die Datenschutzgrundverordnung (DSGVO) setzt neue Richtlinien für den Schutz von personenbezogenen Daten fest. (intersoft consulting, 2018)
- Die European Union Agency for Network and Information Security (ENISA) hat Guidelines für Automotive Cyber-Security veröffentlicht. (European Union Agency for Network and Information Security, 2017)
- Das British Department for Transport hat in einer Studie „Schlüsselprinzipien für IT-Sicherheit in vernetzten und autonomen Fahrzeugen“ veröffentlicht. (British Department for Transport, 2017)
- Die UN Task Force on Cyber security and OTA issues (UN-TF CS/OTA) arbeitet an einem Standard für Sicherheit im Bereich Autonomes Fahren und Updates-OTA. (UN ECE, 2016)

Und in Japan gibt es vom Ministerium für innere Angelegenheiten und Kommunikation (MIC) die „Automotive Cyber Security“ Richtlinie. (Ministry of Internal Affairs and Communications , 2014)

Auch verschiedene Standardisierungsorganisationen haben sich dem Thema angenommen und sind dabei, passende Standards zu schaffen:

- Die Internationale Standardisierungsorganisation (ISO) hat schon 2009 ISO26262 herausgebracht. Dieser fokussiert sich aber auf funktonale Sicherheit (Safety) und ist für Automotive Cyber Security nur bedingt geeignet. (International Organization for Standardization, 2011)
- Auf dieser Basis hat der Verband der Automobilingenieure (SAE) 2016 den Standard SAE J3061 entwickelt, welcher speziell für Cyber Security in Fahrzeugen ausgelegt ist (SAE, 2016). Derzeit wird ein Mapping zwischen ISO26262 und SAE J3061 gemacht, um einen heterogenen Standard zu erhalten. (SAE International, 2012)
- Das Europäische Institut für Telekommunikationsnormen (ETSI) hat mehrere Standards für verschiedene Bereiche herausgebracht, welche meist zwar nicht

ausschließlich für Fahrzeuge gedacht sind, aber Technologien betreffen, welche in Fahrzeugen verbaut sind. Das sind zum Beispiel Standards unter dem Oberbegriff „Automotive Radar“, welche sich mit der Standardisierung von Radartechnologie für weite und für kurze Strecken beschäftigen – in der Automobilindustrie meist als „Adaptive Cruise Control“ (ACC) bzw. „Parksensoren“ und „Notbremsassistent“ bezeichnet (ETSI, 2018). Des Weiteren gibt es eine ganze Reihe Standards, welche sich mit Cyber Security beschäftigen und dabei sich auch um eine Annäherung an das amerikanische Pendant Institute of Electrical and Electronics Engineers (IEEE) bemühen. Diese Standards beschäftigen sich zum Beispiel mit der Kommunikation zwischen zwei Fahrzeugen und einem Austausch von Zertifikaten und Signaturen zwischen diesen (ETSI TS 103 097) oder der Entwicklung eines Trust-Modells für Car2Car Kommunikation (u.a. ETSI TS 102 941) (Lonc, 2018)

### 3.3.4 Unterschiede zwischen Standard-IT-Architektur und Fahrzeug-IT-Architektur

Zunächst einmal stellt sich hier die Frage: Was ist Standard-IT-Architektur? Die IT Architektur eines Fahrzeuges wurde bereits in Kapitel 2.3 erläutert. Die IT-Architektur ist ein Teil der Architektur des Gesamtunternehmens und leitet sich dementsprechend aus dieser ab. Oder anders gesagt: Die IT-Architektur leitet sich aus einer IT-Strategie ab. Und diese wird wiederum von der Unternehmensstrategie bestimmt. Dabei gibt es in der IT-Architektur verschiedene Ebenen, wie Abbildung 12 zeigt (Durst, 2007).

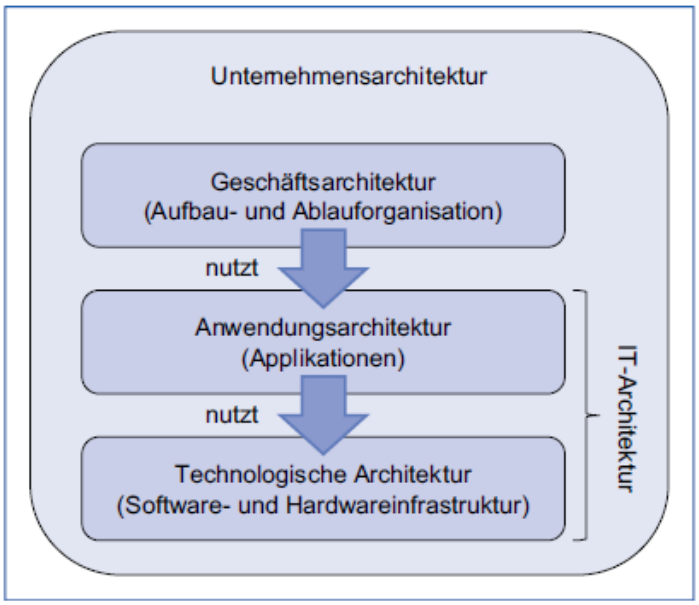


*Abbildung 12: IT-Architektur eines Unternehmens. (Dern, et al., 2009)*

Im Gegensatz dazu wird eine Fahrzeugarchitektur nicht von der Unternehmensarchitektur abgeleitet, sondern aus dem Eigenschaftskatalog für das zu entwickelnde Fahrzeug (Kerschenlohr, 2015). Im Gegensatz zur Unternehmensstrategie und dem daraus resultierenden Aufbau der IT-Architektur, welche meist auf einen Zeitraum von fünf Jahren und länger ausgelegt ist, ist die Architektur im Fahrzeug eher kurzlebig, da sie mit jedem neuen Modell und jeder neuen Modellpflege wieder überarbeitet wird. Des Weiteren gibt es nicht „die Eine“ IT-Architektur im Fahrzeug, sondern jedes Modell eines Herstellers hat seine eigene Architektur. Dementsprechend aufwändig ist hier auch die Pflege und Wartung von vielen IT-Architekturen parallel.

Ein weiterer Punkt ist, dass nicht nur der Automobilhersteller allein am Aufbau der Fahrzeugarchitektur und deren Komponenten hinsichtlich Sicherheit beteiligt ist, sondern auch die Zulieferer, welche die meisten Teile und Module inklusive der passenden Software bereitstellen. Zwar gibt es das Konzept in der Standard-IT mit IT-Service-Providern ebenfalls, doch hier sind die Unternehmen schon einen Schritt weiter und verpflichten die Service Provider auf die Einhaltung von Security-Standards und überwachen dies auch. Im Fahrzeugbereich ist diese Praxis noch nicht oder nur wenig vorhanden. Entweder gibt es beim Zulieferer wenig Awareness für das Thema Security oder es gibt Probleme bei dem Transfer von sicherheitskritischen Informationen (wie z.B. Schlüsseln oder Passwörtern) zwischen Zulieferer und Hersteller. Außerdem ist der Aufbau von Security-Maßnahmen ein Kostentreiber und wird deshalb sowohl von Herstellern als auch den Zulieferern bisher gescheut. Denn schon eine Verteuerung von nur 1 Euro pro ECU oder Sensor etc. würde bei der Menge an ECUs pro Fahrzeug mal die Menge aller Produzierten Fahrzeuge einen Millionenbetrag an Mehrkosten mit sich bringen.

Aber auch die Kunden tragen zum Aufbau der IT-Architektur im Fahrzeug bei. Anders als in Unternehmen lassen sie sich hier nicht oder nur teilweise vorschreiben, welche Sicherheitsregeln eingehalten werden müssen. Wenn zum Beispiel ein Unternehmen per Dienstanweisung festlegt, dass Mitarbeiter keine USB-Geräte oder private Smartphones mit IT-Geräten des Unternehmens verbinden dürfen, so haben alle Mitarbeiter sich daran zu halten. Wenn ein Automobilhersteller seinen Kunden verbieten würde, private Geräte an das Auto anzuschließen, dann würde dieser sich eine andere Marke suchen, die dies nicht verbietet. Genauso verhält es sich mit der OBD-Schnittstelle im Fahrzeug: Es gäbe durchaus Maßnahmen, diese besser abzusichern, z.B. durch entsprechende Autorisierungen, sodass nur autorisierte Benutzer (Werkstätten) über diese Schnittstelle Änderungen an Fahrzeugparametern und -software vornehmen können. Aber dann würden die Hersteller die Kunden verlieren, welche sich bestimmte Fahrzeuge nur kaufen, weil diese sich besonders gut tunen lassen.

Es lässt sich gut erkennen, dass Automobilhersteller also zwischen Sicherheit auf der einen Seite, und Kundenzufriedenheit und Anforderungen wie Echtzeitfähigkeit auf der anderen einen Weg finden müssen, um beides bestmöglich zu vereinen.

## 3.4 Forschungslücke im Bereich Automotive Security

Aus den vorgestellten Studien und den daraus resultierenden Überlegungen zur Fahrzeugarchitektur und IT-Sicherheit in Fahrzeugen lässt sich eines gut erkennen: Einen ganzheitlichen und generischen Ansatz gibt es bisher nicht. Die einen beschränken sich darauf, Angriffswege und Angriffsszenarien auf Fahrzeuge darzustellen (Miller/Valasek und Smith). Andere bieten zwar Lösungen, aber nur für einen Teilbereich des Gesamtproblems. Bouard, Graf und Weyl beschränken sich nur auf die Entwicklung eines Frameworks für sichere Apps, Larson und Nilsson bieten einen guten Ansatz für Wireless FOTA, das aber ohne Defense in Depth Ansatz und ohne das dazugehörige Schichtenmodell. Außerdem ist der von ihnen geforderte FOTA-Ansatz nach dem Dieselskandal nicht mehr so leicht umzusetzen, da Updates an der Flashware im Fahrzeug auch unmittelbare Auswirkungen auf die Emissionen haben können und sowohl Hersteller als auch Behörden an dieser Stelle inzwischen sehr empfindlich sind. Hier fehlt ein entsprechender Nachweisprozess, der FOTA transparent und nachvollziehbar macht. Braunbach, Jander und Pokahr bieten eher einen prozessualen Ansatz ohne wirklich technische Maßnahmen einzubeziehen. Es wird von ihnen zum Beispiel kein Konzept geliefert, wo und wie Krypto-Schlüssel sicher gespeichert werden können, um diese vor Manipulationen zu schützen. Fabro und Kuipers erläutern das Defense in Depth Modell mit Zonen und Conduits, sagen aber nichts über die Sicherheit und Absicherung von Einzelkomponenten. Ebert und Adler haben zwar Maßnahmen definiert, aber es gibt keine konkreten Design- oder Umsetzungsvorschläge. Der Ansatz von Kotarski und Lass ist zwar richtig, was IoT-Komponenten anbelangt, aber eine Fahrzeugarchitektur besteht aus mehr Komponenten, welche sich mit diesem Ansatz nicht abdecken lassen.

Ein weiterer Punkt ist bei der Auswertung der Studien aufgefallen: Bestimmte Lösungen und Forderungen sind in fast allen Studien zu lesen. Dies ist zum einen das Konzept von Zonen und Conduits, was immer wieder gefordert wird. Zum anderen sind es Securitymaßnahmen wie Verschlüsselung, Zertifikate oder die Einführung einer PKI und eines IDS. Trotz dieser vielen Empfehlungen seit Jahren wird dies aber in der Automobilindustrie bis heute nur vereinzelt umgesetzt. Das Problem liegt an dieser Stelle vermutlich darin, dass die Hersteller und Zulieferer ihre Fahrzeuge und Komponenten nicht als IT-System sehen, sondern eher aus funktionaler Ingenieurssicht. Die Entwicklung eines

Fahrzeugs liegt auch traditionell in der Hand von Ingenieuren und selten sind hier ausreichend IT-Fachkräfte mit entsprechendem Security Knowhow beteiligt.

Was deshalb Ziel dieser Arbeit sein wird, ist ein Zusammenspiel aller Lösungen, Vorgehensweisen und Methoden aus den vorgestellten Studien zu finden und einen ganzheitlichen Ansatz für Security in Fahrzeugen und damit Defense in Depth in Fahrzeugen zu finden.

# 4 Methodenauswahl und Marktstudie für Defense-in-Depth-Möglichkeiten

## 4.1 Vorgehen bei der Analyse für Defense-in-Depth-Mechanismen

Für die Analyse standen verschiedene Methoden zur Auswahl. Dies war zum einen die Auswertung von vorhandener Literatur, von Fallstudien und die Internetrecherche. Zum anderen war das die Befragung von Experten aus der Automobilbranche und deren Zulieferern. Eine dritte Methode war der Vergleich und die Evaluation von Quellen hinsichtlich ihrer Unterschiede, Gemeinsamkeiten und Relevanz für das Thema. Auch die Aktualität der Quellen war ein Kriterium, da in der Informationstechnologie Neuerungen bekanntermaßen in kurzen Zeitintervallen erfolgen und Quellen, welche älter als fünf bis zehn Jahre sind, oft als veraltet gelten.

## 4.2 Auswahl und Begründung der gewählten Methoden

Die beiden wesentlichen Methoden der Arbeit waren die systematische Auswertung von Quellen und der Vergleich und die Evaluation von Herstellerlösungen, sowie das Erstellen von Bedrohungs- und Risikoszenarien und dazu passenden Schutzmaßnahmen im zweiten Schritt. Diese Methoden wurden vor allem gewählt, weil so auf das möglichst aktuellste Material zugegriffen sowie am besten die Lücken in der bisherigen Forschung aufgezeigt werden konnten. Um Besonderheiten und Unterschiede zu identifizieren, wurde ein Vergleich von klassischen IT-Sicherheitsarchitekturen mit Fahrzeugarchitekturen durchgeführt sowie ein Vergleich des heutigen Ist-Zustandes mit einem potentiellen Soll-Zustand.

Eine Befragung von Experten wurde nicht durchgeführt. Dies lag vor allem daran, dass die Experten bei den Autoherstellern oder den Zulieferern aus Sicherheitsgründen keine Informationen über genaue Fahrzeugarchitekturen nach außen geben durften.

Im Folgenden werden verschiedene Herstellerlösungen analysiert, verglichen sowie evaluiert in punkto Umsetzbarkeit für ein ganzheitliches Defense-in-Depth-Konzept.

## 4.3 Marktstudie von Hersteller-Lösungen

Es gibt bereits einige Hersteller von Security-Produkten, welche das Potential von IoT und Fahrzeug-Security-Lösungen erkannt haben und diese entsprechend in ihr Portfolio

aufgenommen haben. Da in diesem Bereich der Security-Branche neue Produkte in hoher Schlagzahl an den Markt kommen, besteht die nachfolgende Auflistung von Security-Herstellern und deren Lösungen aus einer Bestandsaufnahme zum Zeitpunkt der Erstellung dieser Arbeit im Juni 2018.

### 4.3.1 Argus Cyber Security

Argus[10] ist ein Security Unternehmen, welches sich auf Security-Lösungen für Fahrzeuge spezialisiert hat. Sie wurde 2013 in Israel gegründet und gehört inzwischen als Tochter zur Continental AG. Das Unternehmen beschäftigt sich ausschließlich mit Security für Fahrzeuge und bietet neben verschiedenen Security-Lösungen auch Beratung in diesem Umfeld an. Dabei bietet Argus Lösungen aus zwei Kategorien an: Eine Lösung für Automotive FOTA, sowie verschiedene Sicherheitskomponenten für das Fahrzeug selber.

**Software Updates OTA**

Dieses Tool bietet eine ganzheitliche Lösung für die Implementierung, die Überwachung und das Management von Software Updates an. Diese Lösung hat mehrere Komponenten: Ein Monitoring System, ein System für die Planung und Verwaltung von Updates und ein In-Car Modul, um eine sichere Übertragung und Implementierung von Updates sicherzustellen.

**Connectivity Protection**

Diese Lösung überwacht und schützt Schnittstellen und angebundene Infotainment- und Telematik-Systeme vor Angriffen, bzw. stellt ein Monitoring zur Verfügung, um Angriffe zu erkennen. Dabei wird zum einen auf die Absicherung von Anwendungen gesetzt, z.B. auf deren Härtung und das Überprüfen auf „Trusted Apps“ (nur authentifizierte Anwendungen dürfen auch ausgeführt werden), zum anderen auf Sicherheit auf dem Netzwerk-Layer mit Network Access Filtering und Network Thread Detection. Auch enthalten ist eine Technologie, um ein End-to-End VPN mit dem Herstellerbackend aufzubauen.

**In-Vehicle Network Protection**

Eine Ebene tiefer setzt die In-Vehicle-Network-Protection an. Diese bietet auf Netzwerkebene eine Firewall zur CAN-Bus-Absicherung, eine dazu passende Segmentierung, ein IDS/ IPS sowie Monitoring des Netzwerks auf Ethernet-Ebene an.

[10] https://argus-sec.com/

**ECU Protection**

ECU Protection sichert ECUs durch eine dedizierte ECU Firewall und Validierung von ein- und ausgehenden Nachrichten ab. Dabei wird auf Hardware-Secure-Modules (HSM-Module) von Drittanbietern gesetzt.

**Lifespan Protection**

Lifespan Protection ist die Flottenlösung von Argus. Es bietet ein Monitoring der Flotte auch durch ein Argus-eigenes Security Operation Center (SOC) an.

**Aftermarket Protection**

Diese Lösung ist für bereits im Umlauf befindliche Fahrzeuge konzipiert, welche noch keine Security-Komponenten von Werk aus erhalten. Dabei wird über die OBD-Schnittstelle ein Dongle angeschlossen, welches verschiedene Schutzmaßnahmen mitbringt, wie Netzwerkschutz, Überprüfung von ein- und ausgehenden Nachrichten oder Angriffe auf den Dongle oder die OBD-Schnittstelle.

Alles in allem bietet Argus eine umfangreiche Lösung für viele Bereiche der In-Car-Security an, welche schon sehr nah an eine Defense in Depth Lösung herankommt. Diese funktionieren allerdings nur dann einwandfrei, wenn die gesamte Suite von Argus eingesetzt wird und der Kunde schon einen gewissen Reifegrad in seiner Security-Architektur erreicht hat, was heute aber bei vielen OEMs und Zulieferern wahrscheinlich eine große Umstellung von Architekturen und Prozessen bedeutet. Außerdem sind trotz des Umfangs nur einzelne Teile abgedeckt, welche für ein umfassendes Defense in Depth Konzept notwendig wären.

### 4.3.2 Autotalks

Autotalks[11] ist eine 2008 gegründete israelische Firma, welche Halbleiterprodukte herstellt. Sie haben sich im Automobilbereich auf die Herstellung von sicheren Chipsets und HSM-Modulen spezialisiert. Diese können entweder eigenständig arbeiten oder in vorhandene ECUs integriert werden.

Dabei wird von Autotalks nicht nur das HSM angeboten, sondern auch Funktionen, die unmittelbar damit zusammenhängen, wie Secure Boot, Kryptografie, Secure Storage und Netzwerk Security.

[11] https://www.auto-talks.com/

**HSM-Module**

Diese sind mit Elliptic Curve Cryptografie (ECC) ausgestattet, um eine leichtgewichtige, low-latency Möglichkeit für Verschlüsselung von V2X Kanälen zu bieten. Außerdem sind sie durch ein abgesichertes Hardware-Interface von anderen Systemen isoliert und so gegen Side-Channel-Angriffe abgesichert.

**Kryptografie**

Die Autotalks Kryptografiemethode beruht auf ECC. Dabei wird auf „Verify-all“ gesetzt, wobei alle eingehenden Pakete verifiziert werden müssen, im Gegensatz zu Verify-on-Demand. Damit sind Kernapplikationen vor nicht verifizierten Daten geschützt.

**Secure Storage**

Ein sicherer Speicher wird von Autotalks durch Zertifikate und einer Autorisierung-Engine abgebildet, welche Daten innerhalb des HSM verschlüsseln. Damit soll sichergestellt werden, dass keine unverschlüsselten Daten das HSM verlassen.

**Secure Boot**

Durch eine digitale Signierung des Firmware-Images sowie eines Authentizitäts- und Integritätschecks während des Bootprozesses soll sichergestellt werden, dass nur autorisierte Firmware installiert und gebootet werden kann. Dazu ist der initiale Boot-Code separat gesichert, dass dieser nicht verändert werden kann.

**Netzwerk Security**

Diese stellt kein Produktbestandteil dar, sondern beschreibt lediglich den Aufbau von ECU und HSM Einheiten hinsichtlich Zoning und eines Master-and-Slave Konzeptes.

Autotalks bietet demnach abgesicherte Chipsets an, welche ein Teil einer sicheren Fahrzeugarchitektur sein müssen. Diese Hardware kann die Grundlage dafür sein, ECUs gegen Angriffe abzusichern. Ein umfassendes Schutzkonzept gibt es hier aber nicht.

### 4.3.3 Gemalto

Gemalto[12] ist ein niederländisches Unternehmen, welches sich hauptsächlich mit digitaler Sicherheit durch Authentifizierungs- und Autorisierungstechniken sowie Datenschutzprodukten wie entsprechender Software und Verschlüsselungslösungen beschäftigt.

[12] https://www.gemalto.com/

Dazu gehören vor allem elektronische Chip oder Magnetstreifenkarten wie Personalausweise, Pässe, SIM-Karten, Kredit- und EC-Karten.

Auch im Connected-Car-Umfeld bietet Gemalto dementsprechend Lösungen für einen Authentifizierungs-Lebenszyklus an, sowohl für das Fahrzeug, dessen Hersteller wie auch für den Fahrer. Das reicht von der initialen Zertifikatsausstellung über dessen Gültigkeitsdauer oder dessen Erneuerung bis zu dessen Lebensende. Die Gemalto Zertifikatslösung bietet sichere Identitäten für Geräte im Fahrzeug, Fahrzeuge und Fahrer, eine PKI für eine entsprechende Verschlüsselung, ein sicheres Key-Management und eine entsprechende Backend Applikation für die Hersteller.

Die Gemalto-Lösung ist im Endeffekt einen Baustein für eine sichere Fahrzeugarchitektur. Für ein umfassendes Schutzkonzept sind allerdings noch andere Lösungen im Zusammenspiel mit der von Gemalto nötig.

### 4.3.4 Harman

Harman[13] ist ein US-amerikanisches Unternehmen, welches seit 2017 zu Samsung gehört. Neben Produkten aus dem Audio- und Infotainmentbereich für Fahrzeuge, bietet Harman auch Cyber-Security-Lösungen im Automobilbereich an. Dabei setzt Harman auf zwei Produkte: Den Harman Shield und den Harman Hypervisor.

**Hypervisor**

Die Hypervisor-Technologie nutzt die Leistungsfähigkeit moderner Prozessoren mit System-on-Chip und HSM, und baut auf diesem einen virtuellen Stack auf. Dadurch können auf einem Prozessor mehrere Betriebssysteme oder Softwarestacks parallel betrieben werden, ohne dass Daten unkontrolliert zwischen den Stacks ausgetauscht werden können. Dabei werden sicherheitskritische Daten in einer Trusted Partition verwaltet, die Medienwiedergabe oder heruntergeladene Apps in einer anderen Partition. Damit wird sichergestellt, dass Malware und manipulierte Daten nicht auf wichtige Systemdaten zugreifen können. (Shen, 2015)

**Harman Shield**

Harman Shield ist eine IDS/IPS Lösung für Fahrzeuge. Diese zielt auf den Schutz von ECUs, TCUs, Gateways und Infotainmentsysteme ab. Shield bietet neben Funktionen für das Sammeln und Auswerten von Daten, dem darauf basierenden Erkennen von

[13] https://www.harman.com/

Angriffen auch eine Managementkonsole für weitere Untersuchungen und entsprechenden Reaktionsmöglichkeiten.

Wie auch bei den Anbietern zuvor bietet Harman eine partielle Lösung für einen bestimmten Bereich bei der Fahrzeugsicherheit. Es sind auch hier weitere Lösungen im Zusammenspiel nötig, um ein umfassendes Schutzkonzept zu gewährleisten.

### 4.3.5 Kaspersky Lab

Kaspersky Lab[14] ist ein russisches Securityunternehmen, welches 1997 gegründet wurde. Nachdem es anfänglich nur Securitysoftware für Privatanwender vertrieben hat, ist Kaspersky inzwischen auch im Businesskundenumfeld tätig, unter anderem auch im Bereich Transportation Security. Dabei setzt Kaspersky insbesondere auf zwei Komponenten: Die Secure Communication Unit und das gehärtete Betriebssystem KasperskyOS.

**Secure Communication Unit**

Die Secure Communication Unit ist ein Gateway, welche die In-Car-Systeme vor eingehenden Verbindungen abschirmt. Es dient als Single-Point-of-Contact zwischen Kommunikationskanälen wie der OBD Schnittstelle, WiFi, GPS oder Bluetooth Verbindungen. Die Secure Communication Unit dient dabei auch als Authentifizierungsinstanz sowie für Audit und Loggingzwecke. Durch sie ist kein direkter Zugriff durch Verbindungen von Extern mehr auf fahrzeuginterne Systeme möglich. Die Softwarebasis für die Secure Communication Unit bildet KasperskyOS mit all seinen Funktionen.

**KasperskyOS**

KasperskyOS wurde für Embedded Systeme und deren spezielle Anforderungen entworfen. Es stellt sicher, dass Anwendungen geschützt und in einer vertrauenswürdigen Umgebung ausgeführt werden können, auch wenn diese Anwendungen für sich erst einmal nicht vertrauenswürdig sind oder Fehler enthalten. Das integrierte Kaspersky Security System prüft Anwendungen hinsichtlich deren Konfiguration und Policies und kann diese, insofern sie von einem vorher definierten Sollzustand abweichen, auch korrigieren. Außerdem in KasperskyOS enthalten, ist ein Secure Storage zur Verwaltung von Schlüsseln und wichtigen Konfigurationsparametern (wie den Policies für das Kaspersky Security System). Zusätzlich stellt eine Trusted-Channel-Engine sicher, dass geschützte Übertragungswege zwischen internen Anwendungen und externen Quellen auf

[14] https://www.kaspersky.de/

TLS Basis etabliert werden können. Sie übernimmt dabei auch eine Authentifizierungs- und Validierungsaufgabe.

Auch Kaspersky stellt wichtige, aber nur partielle Security-Komponenten für den Schutz von Fahrzeugen her. Es benötigt weitere Lösungen und Konzepte, um einen umfassenden Schutz zu bieten.

### 4.3.6 Trend Micro

Trend Micro[15] wurde 1988 in den USA gegründet und beschäftigt sich neben den anfänglichen Antivirenprogrammen inzwischen auch mit Cloud-Security, Netzwerksicherheit sowie IoT-Sicherheit. Seit 2018 bietet Trend Micro die Trend Micro IoT Security Lösung TMIS an. Diese Lösung besteht aus zwei Hauptkomponenten: Ein Security Agend im Fahrzeug, welcher mit Fahrzeugsystemen interagieren und diese auch monitoren kann, sowie einer Remote-Komponente im Herstellerbackend oder in der Cloud.

Der Agent bietet zum einen einen Systemschutz durch virtuelle Patche gegen Schwachstellen, durch Whitelist-Regelwerke gegen unerlaubtes Aufführen von Code oder Anwendungen sowie einen Selbstschutz der Agenten. Zum anderen kann die Monitoringkomponente den CAN-Bus, das Netzwerk, Dateisysteme, Prozesse etc. überwachen und nach Angriffen auf bekannte Schwachstellen prüfen.

Die Remote-Komponente dient als Managementplattform, um sicherheitsrelevante Daten von allen Fahrzeugen zu sammeln, zu korrelieren und so Anomalien zu erkennen und darauf reagieren zu können, zum Beispiel durch das Senden von virtuellen Patches an die Fahrzeuge. Dabei werden auch Daten aus der Trend Micro Forschung sowie verifizierte Funde von anderen Plattformnutzern hinzugezogen, um einen Stand nahe Zero-Day zu haben.

Trend Micro bietet damit eine Lösung, die wichtige Bereiche für In-Car Security abdeckt, aber nicht alle. Hier müssen für ein umfassendes Schutzkonzept andere Lösungen hinzugezogen werden.

## 4.4 Darstellung wesentlicher Erkenntnisse von Einzellösungen am Markt

Es ist sichtbar, dass alle vorgestellten Hersteller mit deren angebotenen Lösungen eines erkannt haben: Dass heutige Fahrzeuge bzw. IoT-Geräte ein Sicherheitsrisiko darstellen

[15] https://www.trendmicro.com/

und das dieses Risiko minimiert werden muss. Das für Hersteller von Security-Produkten dort auch eine betriebswirtschaftliche Möglichkeit besteht, sich auf einem noch jungen Markt zu etablieren, ist ebenfalls nicht von der Hand zu weisen.

Hier ist aber auch zu sehen, dass alle Hersteller sich dabei auf ihr jeweiliges Fachgebiet konzentrieren. Während Autotalks zum Beispiel als Chiphersteller sich auf die Produktion von sicheren Chips konzentriert, sind es bei Gemalto Lösungen zur Authentifizierung. Außerdem wird bei allen Herstellern davon ausgegangen, dass alle Fahrzeugarchitekturen mit einer einzigen Lösung kompatibel sind und von dieser abgedeckt werden können. Regionale Unterschiede (wie zwischen Europa, den USA und Japan) oder unterschiedliche Plattformkonzepte der Fahrzeughersteller werden nicht berücksichtigt. Ein weiterer Punkt, der kaum beachtet wird, ist der Prozess, welcher bei der Entwicklung eines neuen Fahrzeugs hinter der Hard- und Software steht, in den viele verschiedene Unternehmen rund um den Globus beteiligt sind. Schon in der klassischen IT-Sicherheit hat sich gezeigt, dass Hard- und Softwaremaßnahmen nur eine reduzierte Wirkung haben, wenn die zugehörigen Prozesse nicht mit angepasst werden.

Das Problem, welches bei dieser Fokussierung entsteht ist, ist dass es so keine ganzheitliche Lösung geben kann. Denn erst das Zusammenspiel von allen genannten Komponenten in verschiedenen Konstellationen unter Berücksichtigung verschiedener Variablen kann ein Defense in Depth Konzept hervorbringen. Außerdem muss ein Prozesskonzept entwickelt werden, welche über den gesamten Lebenszyklus des Fahrzeugs gilt und im gesamten Lebenszyklus des Fahrzeugs, vom ersten Entwurf bis zur Verschrottung, Sicherheitsmaßnahmen beinhaltet.

Mit einem entsprechenden und umfassenden Konzept, sowie des dazugehörigen Prozesses wird sich das nächste Kapitel beschäftigen.

# 5 Konzeption von Defence in Depth Mechanismen für Fahrzeuge

In diesem Kapitel wird ein geeignetes Vorgehensmodell für die Erstellung eines Defense in Depth Ansatzes gewählt. Darauf aufbauend werden Security Bedrohungen und Risiken für Fahrzeuge aufgeführt sowie entsprechende Gegenmaßnahmen für die einzelnen Security Bausteine erläutert. Diese werden am Ende zu einem ganzheitlichen Defense in Depth Modell zusammengeführt.

## 5.1 Vorgehensmodell

Um notwendige Schutzziele zu ermitteln und in einem Defense in Depth Modell zu einem ganzheitlichen Konzept zusammenzuführen, müssen zuerst einmal alle Bedrohungen für das Fahrzeug im IT-Sicherheitskontext identifiziert und klassifiziert werden. Damit dies nicht willkürlich geschieht, bedarf es eines geeigneten Vorgehensmodells. Dieses muss folgende Fragen im Mindestmaß beantworten:

- **Was** ist die Basis? Welche Komponenten müssen abgesichert werden?
- **Wie** können diese Komponenten bedroht werden?
- **Wie hoch** ist das Risiko, dass solch eine Bedrohung eintritt?
- **Was** kann getan werden, um die Risiken zu minimieren?
- **Mit welchen** Mitteln kann das geschehen?
- **Wie** wird es umgesetzt?
- **Wie** wird geprüft, ob die Umsetzung erfolgreich war?

Diese Fragen können im Grundsatz mit dem Plan-Do-Check-Act (PDCA) Zyklus beantwortet und diesem zugeordnet werden. Ein dazu passendes Vorgehensmodell stellt Abbildung 13 dar. Dort sind folgende Schritte für einen Defense-in-Depth-Ansatz definiert:

1. **Assets identifizieren**: Zuerst muss festgestellt werden, welche Systeme und Komponenten hinsichtlich Bedrohungen und Risiken evaluiert werden sollen. Diese Aufstellung dient als Basis für die weiteren Schritte.
2. **Bedrohungen analysieren**: Es wird analysiert, welche Bedrohungen es für die in Schritt eins identifizierten Assets gibt. In diesem Fall wird die Bedrohungsanalyse durch Misuse-Cases abgebildet.

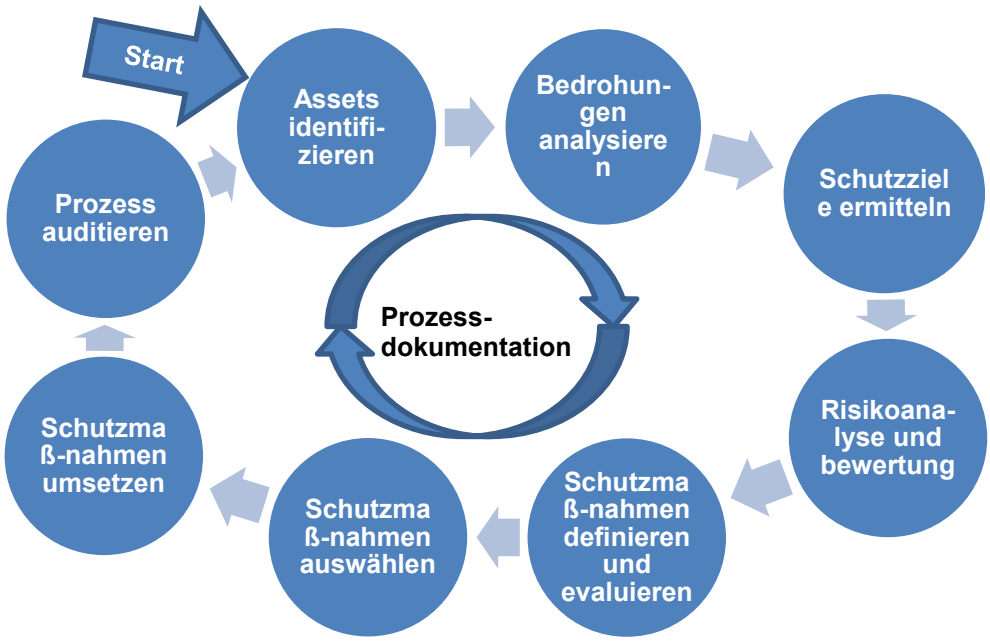


*Abbildung 13: Vorgehensmodell Defense-in-Depth-Konzeption. In Anlehnung an (VDI, 2011)*

3. **Schutzziele ermitteln**: Anhand der Misuse-Cases kann in Schritt drei ermittelt werden, welche Schutzziele es für die Bedrohungsszenarien aus dem zweiten Schritt gibt. Die Schutzziele werden dabei anhand der in Kapitel 2.2 vorgestellten Schutzziele (CIA-Triade) definiert.
4. **Risikoanalyse und -bewertung**: Hier werden die Bedrohungen und die dazu definierten Schutzziele hinsichtlich ihrer Eintrittswahrscheinlichkeit und Kritikalität bewertet. Die Kritikalität beschreibt in diesem Zusammenhang aber nicht den wirtschaftlichen Schaden, sondern den Einfluss auf die Safety des Fahrzeugs, also den möglichen körperlichen Schaden für die Fahrzeuginsassen. Die Risiken werden, wie in der nachfolgenden Tabelle gezeigt, eingestuft. Bei Risiken der Kategorie „Rot“ und „Orange“ wird nach dem Modell von (Larson, et al., 2009) als Maßnahme die Vermeidung des Risikos angestrebt. Bei der Kategorie „Gelb“ wird es Fallabhängig behandelt, bei „Grün“ wird auf Erkennung gesetzt. Risiken, welche nicht unmittelbar das Fahrverhalten des Fahrzeugs beeinflussen (wie zum Beispiel Fahrzeugdiebstahl oder der Diebstahl personenbezogener Daten), werden unter „Keine Verletzungsgefahr“ eingestuft, können aber dennoch die Notwendigkeit von Vermeidungsmaßnahmen mit sich ziehen, wenn durch das Risiko ein hoher Folgeschaden für Fahrer und Unternehmen zu erwarten ist.

| **Kritikalität/ Eintrittswahrscheinlichkeit** | Sehr gering | Gering | Mittel | Hoch |
|---|---|---|---|---|
| Lebensbedrohlich | Vermeidung | Vermeidung | Vermeidung | Vermeidung |
| Verletzungen möglich | Vermeidung | Vermeidung | Vermeidung | Vermeidung |
| Leichte Verletzungen mögl. | Verm./Erk. | Verm./Erk. | Vermeidung | Vermeidung |
| Keine Verletzungsgefahr | Erkennung | Erkennung | Verm./Erk. | Vermeidung |

5. **Schutzmaßnahmen definieren/evaluieren**: Anhand der Risiken sind im fünften Schritt Schutzmaßnahmen definiert und hinsichtlich ihrer Umsetzbarkeit evaluiert worden. Dabei ist zu bewerten, wie gut und wie schnell diese Schutzmaßnahmen umsetzbar sind und inwiefern dadurch Personenschäden vermindert werden können. Eine Wirtschaftlichkeitsbetrachtung spielt hierbei keine Rolle.
6. **Schutzmaßnahmen auswählen**: Auf der Evaluation in Schritt fünf erfolgt in diesem Schritt eine Auswahl von geeigneten Maßnahmen. Dabei werden Maßnahmen mit hoher Kritikalität bevorzugt umgesetzt. Eine Auswahl von Schutzmaßnahmen erfolgt im Rahmen dieser Arbeit nur bedingt, sofern dies für die Arbeit Sinn ergibt.
7. **Schutzmaßnahmen umsetzen**: In diesem Schritt erfolgt die Umsetzung der ausgewählten Schutzmaßnahmen. Da diese Arbeit sich nur theoretisch mit dem Thema beschäftigt, erfolgt keine praktische Umsetzung von Maßnahmen.
8. **Prozess auditieren**: Zum Schluss wird geprüft, ob Schutzmaßnahmen zum einen erfolgreich implementiert wurden, zum anderen, ob diese auch ihre gewünschte Wirkung entfalten. Dies geschieht durch entsprechende Nachprüfungen und Evaluationen der Risiken und durch Penetration Tests. Auch dieser Schritt ist nicht Teil dieser Arbeit.

Wie sich aber im bisherigen Forschungsverlauf dieser Arbeit herausgestellt hat, ist es nicht ausreichend, nur ein Modell Schritt für Schritt durchzugehen, um einen Defense-in-Depth-Konzept für Fahrzeuge aufzubauen. Dafür ist die Materie zu umfangreich. Deshalb wird es in der Folgerung mehrere Modelle geben:

1. Das erste Modell wird die verschiedenen Zonen bzw. Schichten voneinander unterscheiden und ihren jeweiligen Anforderungen gerecht werden müssen. Diese

drei Schichten wurden schon in Abbildung 9 vorgestellt: Onboard, Kommunikationsschicht und Offboard bzw. Backend. Jede Zone hat ihre eigenen Anforderungen an IT Sicherheit und muss dementsprechend auch separat behandelt werden.

2. Für die oben genannte Onboard-Zone im Fahrzeug muss ein eigenes Vorgehensmodell entwickelt werden. Hier gibt es so viele unterschiedliche Module, Zonen, Dienste, Kommunikationswege etc., dass dies nicht nur in einem Gesamtmodell behandelt werden kann.
3. Neben den technischen Modellen muss auch der Prozess, der hinter den ganzen Systemen steht, mit angepasst und evaluiert werden. Denn ohne die Prozessabläufe in der Fahrzeug- und Softwareentwicklung, der Produktion, den After Sales usw. ebenfalls sicher zu gestalten, ist auch kein ganzheitlicher Defense in Depth Ansatz im Fahrzeug möglich.

Die Bedrohungs- und Risikoanalyse wird in einem Tabellenformat dargestellt werden. Dabei werden die jeweilige Bedrohung, das Schutzziel und das dazugehörige Risiko in einer kombinierten Tabelle gezeigt. Die Vorlage dazu bietet nachfolgende Tabelle.

| **Identifier: Komponente** | | | |
|---|---|---|---|
| **Usecase** | | **Misuse-Case** | |
| | | | |
| **Schutzziel** | | | |
| | | | |
| **Risiko** | | | |
| Kritikalität: | | | |
| ETW: | | Maßnahmen: | |

In der ersten Zeile werden ein eindeutiger Identifikator und die dazugehörige Komponente und deren Zugehörigkeit (z.B. Backend, Monitoring Service) beschrieben. Der zweite Block beschreibt unter „Usecase“ den angedachten Gebrauch der jeweiligen Komponente. „Misuse-Case“ beschreibt, wie diese Komponente ausgenutzt werden kann. Im dritten Blick wird das dazu passende Schutzziel dargestellt. Der letzte Abschnitt schätzt das Risiko dazu ein, hinsichtlich Kritikalität und Eintrittswahrscheinlichkeit (ETW) und gibt eine Empfehlung, welche Maßnahmen umgesetzt werden sollten.

## 5.2 Vorgehen für den Architekturaufbau und die Bedrohungs- und Risikoanalyse

Wie im Vorgehensmodell beschrieben, ist für eine umfassende Bedrohungs- und Risikoanalyse zuerst eine Aufnahme aller Assets, also aller beteiligten Systeme und Komponenten nötig. Da dies für ein einziges Modell zu umfangreich ist, werden im Folgenden drei Modelle erstellt und hinsichtlich spezifischer Bedrohungen und Risiken bewertet.

### 5.2.1 Gesamtmodell

#### 5.2.1.1 Architektur

Das Gesamtmodell wird auf Basis von der bereits gezeigten Abbildung 9 erstellt. Da das Gesamtmodell einen Überblick geben soll und ein detaillierter Einblick in einem zweiten Modell gegeben wird, wird in diesem Modell auf Details verzichtet. Abbildung 14 zeigt das schematische Gesamtmodell. Dabei gibt es drei Bereiche zu unterscheiden: Das Backend, welches im Rechenzentrum des Fahrzeugherstellers angesiedelt ist, den Onboard-Bereich, welcher Teil des Fahrzeugs ist sowie die Kommunikationsverbindungen zwischen den Bereichen sowie zwischen Drittanbietergeräten (3rd Party Services, Smartphone, Radio…).

Das Backend ist dabei zu einem großen Teil als klassische IT-Architektur zu verstehen, wie sie schon in Abbildung 12 beschrieben wurde. Zwar muss das Backend ebenso abgesichert werden wie die Kommunikationsschicht und der OnBoard-Bereich, um ein ganzheitliches Defense in Depth Konzept zu erreichen. Allerdings gibt es für diese Art von IT-Systemen schon entsprechende Konzepte für deren IT-Sicherheit, sodass hier nicht in der Tiefe auf die Absicherung eines IT-Backend eingegangen werden muss.

Die Kommunikationsschicht zwischen Backend und Fahrzeug basiert zumeist auf dem IP-Protokoll, der Traffic zwischen Backend und Fahrzeug ist also Großteiles http(s)-Traffic. Demnach gibt es hier wenige Besonderheiten gegenüber einer klassischen Absicherung von Kommunikationsstrecken. Die einzigen Punkte, die zusätzlich zu beachten sind, sind die Erreichbarkeit des Fahrzeugs, welche je nach Mobilfunkempfang und Betriebszustand schwanken kann, und das begrenzte Datenvolumen, welches im Gegensatz zu Internetleitungen beim Mobilfunk immer noch eine Rolle spielt.

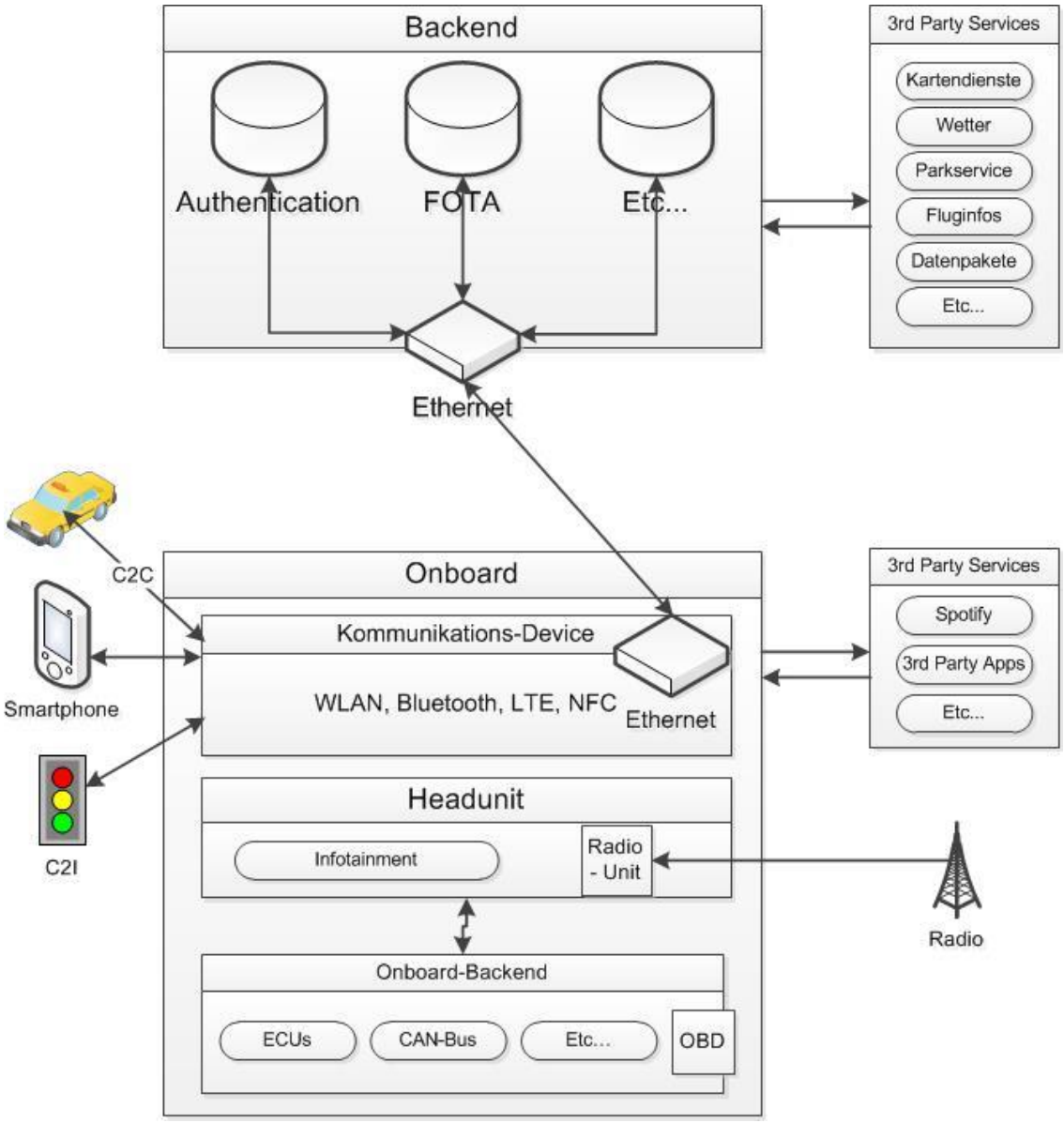


*Abbildung 14: Gesamtmodell, schematisch*

Im OnBoard-Bereich dagegen ist eine neue Architektur anzutreffen, weswegen auch hier der weitere Fokus von Security-Maßnahmen liegen wird. Die hier entstehenden Bedrohungen und Risiken werden deshalb gesondert in Kapitel 5.2.2 behandelt. In diesem Gesamtmodell werden nur die OnBoard-Bedrohungen behandelt, welche im unmittelbaren Zusammenhang mit angrenzenden Systemen entstehen.

#### 5.2.1.2 Bedrohungs- und Risikoanalyse

| **BACK-01: Backendsysteme** | | | |
|---|---|---|---|
| **Usecase** | | **Misuse-Case** | |
| Die Backendsysteme und -applikationen kommunizieren mit dem Fahrzeug um Firewall- und Kartenupdates auszuliefern, Drittanbieterservices bereitzustellen und Monitoringdaten aus dem Fahrzeug zu empfangen. | | Ein Angreifer (von extern oder ein interner Mitarbeiter) greift das Backend an, um über dessen Applikationen Daten an ein Fahrzeug senden zu können oder Daten abzugreifen. Im schlimmsten Fall hat er so Zugriff auf die ganze Flotte. | |
| **Schutzziel** | | | |
| • Vertraulichkeit: Kundendaten im Backend müssen geschützt werden.<br>• Integrität: Es muss sichergestellt werden, dass nur valide Daten an das Fahrzeug gesendet werden. | | | |
| **Risiko** | | | |
| Kritikalität: | Leichte Verletzungsgefahr | | |
| ETW: | Gering | Maßnahmen: | Vermeidungsmaßnahmen |

| **BACK-02: Drittanbieter Services** | | | |
|---|---|---|---|
| **Usecase** | | **Misuse-Case** | |
| Applikationen von Drittanbietern können nach Bedarf in das Fahrzeug geladen werden, um von deren Services zu profitieren. | | Ein Angreifer kann versuchen, über manipulierte Apps Schadcode in das Fahrzeug einzuschleusen und damit Daten abzugreifen oder das Fahrzeug zu manipulieren. | |
| **Schutzziel** | | | |
| • Integrität: Drittanbieter-Services müssen hinsichtlich ihrer Sicherheit und Authentizität überprüft werden, bevor diese ins Fahrzeug geladen werden dürfen. | | | |
| **Risiko** | | | |
| Kritikalität: | Keine Verletzungsgefahr | | |
| ETW: | Gering | Maßnahmen: | Erkennungsmaßnahmen |

| **KOMM-01: Smartphones, USB-Sticks, SD-Karte, CDs** | | | |
|---|---|---|---|
| **Usecase** | | **Misuse-Case** | |
| Applikationen auf Smartphones oder Daten auf USB-Sticks, SD-Karten oder CDs können genutzt werden, um das Infotainment Angebot im Fahrzeug um weitere Services anzureichern. | | Schadcodebehaftete Applikationen auf dem Smartphone können diesen in das Fahrzeug einschleusen und somit einem Angreifer ein Einfallstor bieten. | |
| **Schutzziel** | | | |
| • Integrität: Applikationen von Smartphones und Daten von USB-Sticks, SD-Karten und CDs dürfen nur in einem gesonderten, abgeschlossenen Bereich ausgeführt werden. | | | |
| **Risiko** | | | |
| Kritikalität: | Keine Verletzungsgefahr | | |
| ETW: | Mittel | Maßnahmen: | Vermeidungsmaßnahmen. |

| **KOMM-02: Kommunikation zwischen Backend und Fahrzeug** | | | |
|---|---|---|---|
| **Usecase** | | **Misuse-Case** | |
| Über das IP-Protokoll werden Daten zwischen dem Backend und dem Fahrzeug ausgetauscht. Dies kann unter Umständen unverschlüsselt geschehen. | | Ein Angreifer schaltet sich in den Kommunikationskanal ein und kann so Daten mitlesen oder gesendete Daten manipulieren. Im schlimmsten Fall gelangen so falsche Informationen in das Fahrzeug. | |
| **Schutzziel** | | | |
| • Vertraulichkeit: Daten, welche zwischen Backend und Fahrzeug ausgetauscht werden, müssen geschützt werden.<br>• Integrität: Es muss sichergestellt werden, dass nur valide Daten zwischen Backend und Fahrzeug ausgetauscht werden. | | | |
| **Risiko** | | | |
| Kritikalität: | Keine Verletzungsgefahr | | |
| ETW: | Mittel | Maßnahmen: | Vermeidungsmaßnahmen. |

| **KOMM-03: LTE Modul** | | | |
|---|---|---|---|
| **Usecase** | | **Misuse-Case** | |
| Über das LTE Modul kann das Fahrzeug Daten nahezu jeder Zeit und aus jeder Entfernung empfangen und senden. | | Ein Angreifer kann diese Reichweite ausnutzen, um von jedem Ort auf der Welt das Fahrzeug anzugreifen. Im schlimmsten Fall kann er über diesen Web sicherheitsrelevante Systeme hacken und so Unfälle herbeiführen. | |
| **Schutzziel** | | | |
| Das LTE Modul eines Fahrzeugs muss gegen Angriffe von außen abgesichert werden. Im Falle eines Angriffs muss dieser erkannt und entsprechend behandelt werden. | | | |
| **Risiko** | | | |
| Kritikalität: | Lebensbedrohlich | | |
| ETW: | Hoch | Maßnahmen: | Vermeidungsmaßnahmen |

| **KOMM-04: WLAN Modul** | | | |
|---|---|---|---|
| **Usecase** | | **Misuse-Case** | |
| Über das WLAN Modul kann das Fahrzeug Daten nahezu jeder Zeit und aus einer mittleren Entfernung (~100 Meter) empfangen und senden. | | Ein Angreifer kann innerhalb dieses Radius versuchen, das Fahrzeug anzugreifen. Im schlimmsten Fall kann er sicherheitsrelevante Systeme hacken und so Unfälle herbeiführen. | |
| **Schutzziel** | | | |
| Das WLAN Modul eines Fahrzeugs muss gegen Angriffe von außen abgesichert werden. Im Falle eines Angriffs muss dieser erkannt und entsprechend behandelt werden. | | | |
| **Risiko** | | | |
| Kritikalität: | Lebensbedrohlich | | |
| ETW: | Mittel | Maßnahmen: | Vermeidungsmaßnahmen |

| **KOMM-05: Bluetooth Modul** | | | |
|---|---|---|---|
| **Usecase** | | **Misuse-Case** | |
| Über das Bluetooth Modul kann das Fahrzeug Daten nahezu jeder Zeit und aus einer kurzen Entfernung (~10 Meter) empfangen und senden. | | Ein Angreifer kann innerhalb dieses Radius versuchen, das Fahrzeug anzugreifen. Im schlimmsten Fall kann er sicherheitsrelevante Systeme hacken und so Unfälle herbeiführen. | |
| **Schutzziel** | | | |
| Das Bluetooth Modul eines Fahrzeugs muss gegen Angriffe von außen abgesichert werden. Im Falle eines Angriffs muss dieser erkannt und entsprechend behandelt werden. | | | |
| **Risiko** | | | |
| Kritikalität: | Lebensbedrohlich | | |
| ETW: | Mittel | Maßnahmen: | Vermeidungsmaßnahmen |

| **KOMM-06: Radio Modul** | | | |
|---|---|---|---|
| **Usecase** | | **Misuse-Case** | |
| Über das Radio Modul (FM, AM und DAB) kann ein Fahrzeug Radiosender und weitere dazugehörige Daten (Verkehrsinformationen, Senderinfos etc.) empfangen. | | Ein Hacker kann versuchen, über die Radiofrequenzen falsche Informationen an das Fahrzeug zu senden. Ein Personenschaden dadurch ist aber unwahrscheinlich. | |
| **Schutzziel** | | | |
| Das Radio Modul muss Möglichkeiten bieten, Angriffe von außen zu erkennen. | | | |
| **Risiko** | | | |
| Kritikalität: | Keine Verletzungsgefahr | | |
| ETW: | Gering | Maßnahmen: | Erkennungsmaßnahmen |

| **KOMM-07: NFC-Modul** | | | |
|---|---|---|---|
| **Usecase** | | **Misuse-Case** | |
| NFC kann dafür verwendet werden, um<br>1. ein Mobiltelefon mit dem Fahrzeug zu verbinden.<br>2. ein Mobiltelefon dazu zu benutzen, um das Fahrzeug zu entriegeln. | | Ein Angreifer kann sich als Smartphone des Fahrers auszugeben, um<br>1. So an dessen Daten zu kommen<br>2. So das Fahrzeug zu entriegeln und zu stehlen. | |
| **Schutzziel** | | | |
| • Vertraulichkeit: Daten des Fahrers müssen so geschützt sein, dass ein unbefugter Dritter diese nicht auslesen kann.<br>• Integrität: Es muss sichergestellt sein, dass nur berechtigte Smartphones das Fahrzeug entriegeln können. | | | |
| **Risiko** | | | |
| Kritikalität: | Keine Verletzungsgefahr | | |
| ETW: | Mittel | Maßnahmen: | Erkennungsmaßnahmen |

| **KOMM-08: Car2Car-Kommunikation** | | | |
|---|---|---|---|
| **Usecase** | | **Misuse-Case** | |
| Sondereinsatzfahrzeuge (wie Feuerwehr, Krankenwagen, Polizei) können Car2Car mit anderen Fahrzeugen kommunizieren, um diese aufzufordern, Platz zu machen. | | Ein Angreifer kann sich als Sonderfahrzeug ausgeben, um sich Platz und einen Vorteil auf der Straße zu verschaffen. Damit könnte er den Verkehr auch stören. | |
| **Schutzziel** | | | |
| • Integrität: Es muss geprüft werden, ob es sich tatsächlich um ein Sondereinsatzfahrzeug handelt.<br>• Verfügbarkeit: Es muss eine Backup-Lösung geben, wenn ein Angreifer den Kommunikationskanal für Sondereinsatzfahrzeuge blockiert. | | | |
| **Risiko** | | | |
| Kritikalität: | Keine Verletzungsgefahr | | |
| ETW: | Mittel | Maßnahmen: | Vermeidungsmaßnahmen |

<table>
<tr><th colspan="4">KOMM-09: Car2Infrastruktur-Kommunikation</th></tr>
<tr><th colspan="2">Usecase</th><th colspan="2">Misuse-Case</th></tr>
<tr><td colspan="2">Verkehrsinfrastruktur (wie Ampeln, Leitsysteme, Parkhäuser) können mit Fahrzeugen kommunizieren und so Signale (wie Ampelstatus oder freie Parkplätze) übermitteln.</td><td colspan="2">Ein Angreifer kann dies ausnutzen, in dem er sich selber einen Vorteil verschafft (nur grüne Ampeln auf seiner Route) oder für ein Verkehrschaos sorgt (alle Ampeln auf Rot).</td></tr>
<tr><th colspan="4">Schutzziel</th></tr>
<tr><td colspan="4">• Integrität: Die Integrität der betreffenden Infrastruktur muss gewährleistet sein.<br>• Verfügbarkeit: Es muss eine Backup-Lösung geben, wenn die Car2Infrastruktur-Kommunikation nicht wie vorgesehen funktioniert.</td></tr>
<tr><th colspan="4">Risiko</th></tr>
<tr><td>Kritikalität:</td><td colspan="3">Leichte Verletzungsgefahr</td></tr>
<tr><td>ETW:</td><td>Gering</td><td>Maßnahmen:</td><td>Vermeidungsmaßnahmen</td></tr>
</table>

Weitere Bedrohungen und Risiken, welche unmittelbar mit den OnBoard-Systemen im Fahrzeug zusammenhängen, werden im Folgekapitel beschrieben.

### 5.2.2 OnBoard-Modell

#### 5.2.2.1 Architektur

Das OnBoard-Modell ist aus IT-Security-Sicht deutlich komplexer. Dies liegt vor allem an den vielen unterschiedlichen Komponenten und Schnittstellen. Abbildung 15 zeigt den möglichen Aufbau eines OnBoard-Modells. Da die Fahrzeugausstattung und damit auch die verbauten Komponenten sich von Fahrzeug zu Fahrzeug unterscheiden, werden in diesem generischen Modell neben den obligatorischen Modulen (wie zum Beispiel Motor, Getriebe, Bremsen) nur einige, meistverbaute Komponenten angegeben. Das OnBoard-Netz besteht aus drei Hauptbereichen: Dem Kommunikationsmodul (oder auch TCU), der Head-Unit und dem CAN-Bus oder auch mehreren CAN-Bus Systemen, je nach Systemarchitektur.

Das Kommunikationsmodul ist zum einen für die Kommunikation mit externen Quellen (wie dem Smartphone oder dem Internet) zuständig und leitet ein- und ausgehende

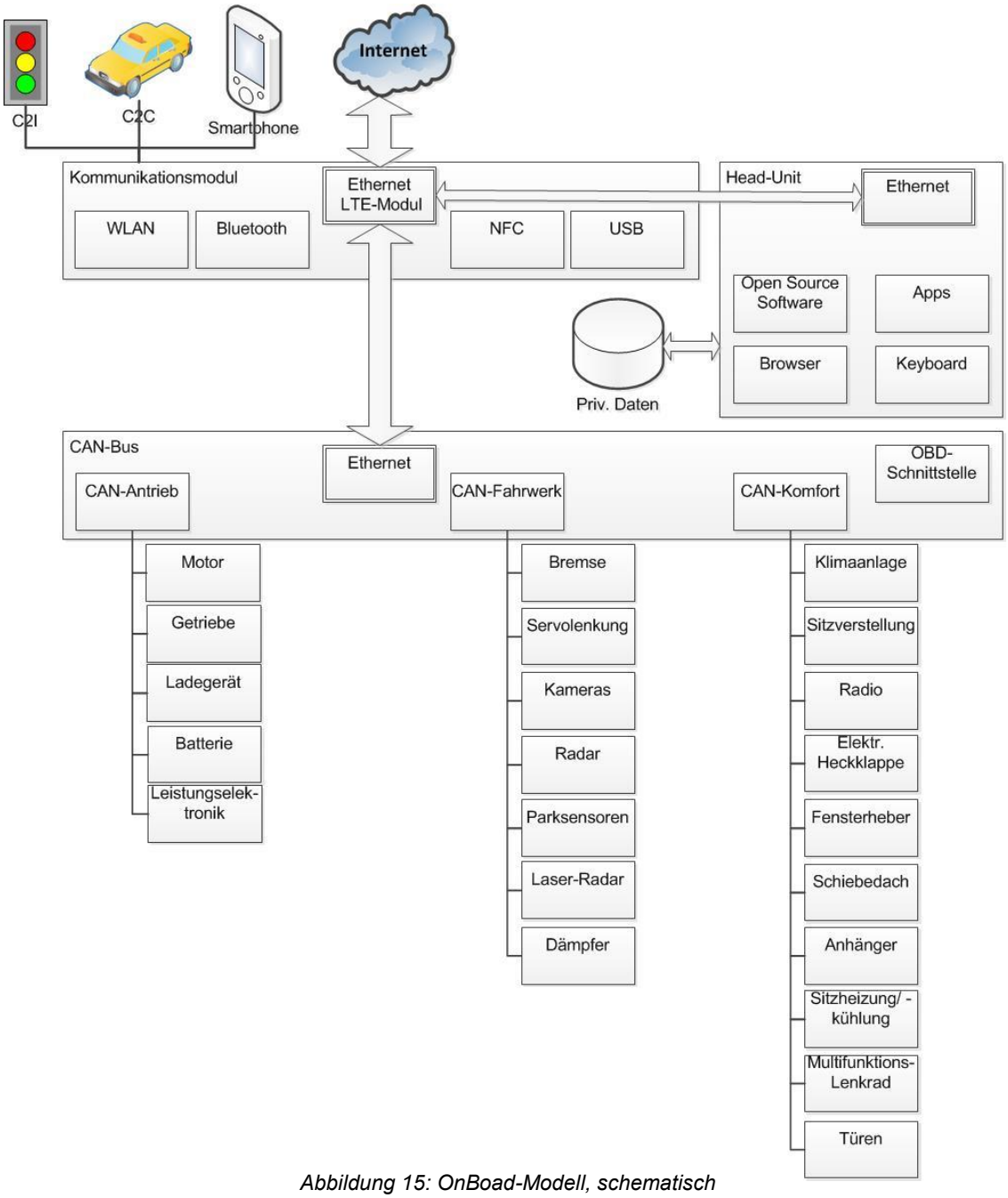


*Abbildung 15: OnBoad-Modell, schematisch*

Kommunikationsanfragen weiter. Das Kommunikationsmodul ist demnach auch das Model, welches für Angriffe von außen die größte Angriffsfläche bietet.

Die Head-Unit ist das Infotainment-Herzstück des Fahrzeugs. In ihr sind alle Komponenten verbaut, die zur visuellen Kommunikation mit dem Fahrer dienen. Der Fahrer kann die Head-Unit teilweise selbst anpassen, in dem er zum Beispiel Apps für diese herunterlädt. Diese können aber ebenfalls ein Einfallstor für Angreifer sein.

Der CAN-Bus ist der Teil in der OnBoard-Architektur, welcher die eigentlichen Fahrzeugsysteme (ECUs, Sensoren und Aktoren) beinhaltet. Es kann dabei einen oder auch mehrere CAN-Bus-Systeme geben, welche gegebenenfalls nochmals segmentiert oder nach

Funktionen unterteilt sind, wie zum Beispiel in der Abbildung in „Antrieb“, „Fahrwerk“ und „Komfort“. Über Komponenten im CAN-Bus werden unter anderem auch die Bremsen, die Lenkung und der Motor gesteuert. Daraus lässt sich ableiten, dass der CAN-Bus der sicherheitskritischste Bereich im Fahrzeug ist. Ein Angriff auf eine Komponente des Antriebs oder des Fahrwerks kann immer eine lebensbedrohliche Situation auslösen.

Da im Fahrzeug alle drei Bereiche miteinander verbunden sind, kann ein Angriff auf einen der drei Bereiche unmittelbare Auswirkungen auf die anderen beiden haben.

#### 5.2.2.2 Bedrohungs- und Risikoanalyse

Angriffe auf das Kommunikationsmodul wurden bereits im vorhergehenden Kapitel beleuchtet. Demnach werden sich Bedrohungen und Risiken in diesem Abschnitt auf solche beziehen, welche gegen die Head-Uni und den CAN-Bus gerichtet sind.

<table>
<tr><th colspan="4">HEAD-01: Open Source</th></tr>
<tr><th>Usecase</th><th colspan="3">Misuse-Case</th></tr>
<tr><td>Open Source Software kann im Fahrzeug verwendet werden, um entweder als Betriebssystem auf der Head-Unit zu dienen oder um verschiedene Applikationen (wie einen Browser) bereitzustellen.</td><td colspan="3">Ein Angreifer kann versuchen, Open Source Exploits auszunutzen, um so in das Fahrzeug einzudringen und Daten auszulesen oder Systeme zu manipulieren.</td></tr>
<tr><th colspan="4">Schutzziel</th></tr>
<tr><td colspan="4">• Open Source Software muss Schutz gegen Exploits bieten.<br>• Es dürfen nur geprüfte Softwarepakete/-patches eingespielt werden.</td></tr>
<tr><th colspan="4">Risiko</th></tr>
<tr><td>Kritikalität:</td><td colspan="3">Verletzungen möglich</td></tr>
<tr><td>ETW:</td><td>Mittel</td><td>Maßnahmen:</td><td>Vermeidungsmaßnahmen</td></tr>
</table>

| **HEAD-02: Keyboard** | | | |
|---|---|---|---|
| **Usecase** | | **Misuse-Case** | |
| Das Keyboard (physisch oder virtuell) ermöglicht es dem Fahrer, Eingaben an das Fahrzeug zu übermitteln. | | Ein Angreifer kann versuchen, diese Eingaben mitzulesen (Sniffing), um so an private Daten des Fahrers zu gelangen. | |
| **Schutzziel** | | | |
| • Vertraulichkeit: Eingegebene Daten müssen vor unbefugtem Mitlesen geschützt werden. | | | |
| **Risiko** | | | |
| Kritikalität: | Keine Verletzungsgefahr | | |
| ETW: | Gering | Maßnahmen: | Erkennungsmaßnahmen |

| **HEAD-03: Privater Datenspeicher** | | | |
|---|---|---|---|
| **Usecase** | | **Misuse-Case** | |
| In der Head-Unit sind private Daten des Fahrers (Navigationsziele, Kontakte, Einstellungen von Klimaanlage etc…) gespeichert. | | Ein Angreifer kann versuchen, an diese Daten zu gelangen, um diese zu missbrauchen (weiterzuverkaufen). | |
| **Schutzziel** | | | |
| • Vertraulichkeit: Gespeicherte Daten müssen vor unbefugtem Lesen geschützt werden (Privacy). | | | |
| **Risiko** | | | |
| Kritikalität: | Keine Verletzungsgefahr | | |
| ETW: | Mittel | Maßnahmen: | Vermeidungsmaßnahmen |

| **CANB-01: Funkschlüssel/Keyless Go** | | | |
|---|---|---|---|
| **Usecase** | | **Misuse-Case** | |
| Über Funkschlüssel und Keyless Go kann ein Fahrzeug entriegelt werden, ohne dass dafür der Schlüssel ins Schloss gesteckt werden muss. | | Ein Angreifer kann das Funksignal abgreifen und nutzen, um das Fahrzeug zu stehlen. | |
| **Schutzziel** | | | |
| • Integrität: Es muss sichergestellt sein, dass nur berechtigte Smartphones das Fahrzeug entriegeln können. | | | |
| **Risiko** | | | |
| Kritikalität: | Keine Verletzungsgefahr | | |
| ETW: | Mittel | Maßnahmen: | Erkennungsmaßnahmen |

| **CANB-02: Fehlerhafte Flashware** | | | |
|---|---|---|---|
| **Usecase** | | **Misuse-Case** | |
| Das Einspielen von Flashware dient dazu, ECUs zu programmieren, neue Funktionen auf ECUs zu bringen oder fehlerhafte Flashware zu verbessern. | | Eine Flashware mit Fehlern kann dazu führen, dass ECUs nicht mehr korrekt arbeiten und dass sich Einfallstore für Angreifer in der ECU öffnen. | |
| **Schutzziel** | | | |
| • Flashware muss durch einen definierten Prozess vor dem Einspielen auf Fehler und Lücken geprüft werden. | | | |
| **Risiko** | | | |
| Kritikalität: | Lebensbedrohlich | | |
| ETW: | Mittel | Maßnahmen: | Vermeidungsmaßnahmen |

| **CANB-03: Manipulierte Flashware** | | | |
|---|---|---|---|
| **Usecase** | | **Misuse-Case** | |
| Flashware ist auf ECUs für deren Programmierung nötig. Sie bestimmt, wie eine ECU auf eingehende Signale reagiert, diese interpretiert und wieder Befehle nach außen gibt. | | Ein Angreifer kann versuchen, manipulierte Flashware einzuspielen, die dann nicht mehr ordnungsgemäß arbeitet. | |
| **Schutzziel** | | | |
| • Es muss sichergestellt sein, dass nur autorisierte Flashware auf der ECU ausgeführt werden darf. | | | |
| **Risiko** | | | |
| Kritikalität: | Lebensbedrohlich | | |
| ETW: | Mittel | Maßnahmen: | Vermeidungsmaßnahmen |

| **CANB-04: CAN-Injection** | | | |
|---|---|---|---|
| **Usecase** | | **Misuse-Case** | |
| Über den CAN-Bus werden Signale zwischen ECUs und Sensoren, Aktoren und anderen ECUs hin- und hergeschickt. | | Ein Angreifer kann sich in diesen Signalfluss einhacken und übertragene Signale abfangen und manipulieren. | |
| **Schutzziel** | | | |
| • Der CAN-Bus muss vor dem Einbringen von unerwünschten Signalen Dritter geschützt werden.<br>• Es muss sichergestellt werden, dass nur authentisierte Signale in den ECUs, Sensoren und Aktoren angenommen werden. | | | |
| **Risiko** | | | |
| Kritikalität: | Lebensbedrohlich | | |
| ETW: | Hoch | Maßnahmen: | Vermeidungsmaßnahmen |

| **CANB-05: Ladesäule** | | | |
|---|---|---|---|
| **Usecase** | | **Misuse-Case** | |
| Über eine Ladesäule kann ein Elektro- oder Hybridfahrzeug mit Strom betankt werden. Außerdem kann das Fahrzeug mit der Ladesäule Informationen austauschen (z.B. Ladezustand) | | Ein Angreifer kann versuchen, entweder über die Ladesäule oder das Ladekabel auf Fahrzeugsysteme (wie die Batterie) zu gelangen und sich von dort zu sicherheitsrelevanten Komponenten vorzuarbeiten und zum Beispiel das Fahrzeug zu entriegeln. | |
| **Schutzziel** | | | |
| • Ladesäulen und der Ladevorgang müssen abgesichert werden. | | | |
| **Risiko** | | | |
| Kritikalität: | Keine Verletzungsgefahr | | |
| ETW: | Mittel | Maßnahmen: | Vermeidungsmaßnahmen |

| **CANB-06: OBD Schnittstelle** | | | |
|---|---|---|---|
| **Usecase** | | **Misuse-Case** | |
| Die OBD-Schnittstelle dient dazu, Konfigurations- und Fehlerdaten aus dem Fahrzeug auszulesen, Fehler zurückzusetzen und Konfigurationsänderungen durchzuführen. | | Ein Angreifer kann die OBD Schnittstelle nutzen, um manipulierte Konfigurationen in ein Fahrzeug einzuspielen, welche im schlimmsten Fall zu Unfällen führen können. Dazu ist aber ein physischer Zugang zum Fahrzeug nötig. | |
| **Schutzziel** | | | |
| Die OBD-Schnittstelle muss gegen unbefugte Nutzung abgesichert werden. Unbefugte Schreib- und Leseversuche müssen erkannt und unterbunden werden. | | | |
| **Risiko** | | | |
| Kritikalität: | Lebensbedrohlich | | |
| ETW: | Mittel | Maßnahmen: | Vermeidungsmaßnahmen |

| CANB-07: Leicht zugängliche ECUs, Sensoren, Aktoren | | | |
|---|---|---|---|
| **Usecase** | | **Misuse-Case** | |
| Manche ECUs, Sensoren oder Aktoren sind unweigerlich so verbaut, dass ein leichter Zugang möglich ist, ohne dass man dafür das Fahrzeug oder den Motorraum öffnen müsste (wie Komponenten in den Außenspiegeln oder an den Reifen). | | Ein Angreifer kann sich leicht Zugang zu diesen Komponenten verschaffen und so im schlimmsten Fall direkt auf den CAN-Bus und andere Komponenten zugreifen und diese manipulieren. | |
| **Schutzziel** | | | |
| ECUs, Sensoren und Aktoren, insbesondere jene, welche leicht zugänglich sind, müssen vor unerlaubten Zugriffen und Manipulation geschützt werden. | | | |
| **Risiko** | | | |
| Kritikalität | Lebensbedrohlich | | |
| ETW | Mittel | Maßnahmen: | Vermeidungsmaßnahmen |

### 5.2.3 Prozessmodell

Während seiner Betriebsdauer durchläuft ein Fahrzeug viele verschiedene Stationen – von der Idee bis zur Verschrottung. Die Absicherung dieses Prozesses ist ebenfalls essentiell für die IT-Sicherheit im Fahrzeug. Im Folgenden wird zunächst der Prozess dargestellt und erläutert und anschließend Bedrohungen und Risiken im Prozess identifiziert.

#### 5.2.3.1 Prozessablauf

Ein Fahrzeug hat in seinem Lebenszyklus verschiedene Stationen, welche in Abbildung 16 aufgezeigt werden. Die meisten Phasen haben dabei eine vorher festgelegte Dauer, außer die Betriebsphase, da diese nicht in der Entscheidungsgewalt des Herstellers, sondern beim Kunden liegt.

Während der Spezifikation wird vom Hersteller ein Anforderungskatalog erstellt, mit allen möglichen Ausstattungen und Ausstattungsvarianten. Auf dessen Basis wird dann auch


*Abbildung 16: Lebenszyklus eines Fahrzeugs*

die E/E/PE-Architektur entworfen, sowie Anforderungen an neue Bauteile an potentielle Zulieferer gesendet.

In der Entwicklung werden neue Systeme, Software und Komponenten designt, welche es bisher noch nicht gegeben hat und welche in einem spezifischen Fahrzeug das erste Mal in Serie gehen. Im Prototyping werden dann die ersten Vor-Fahrzeuge erstellt, um hier früh noch Anpassungen vornehmen zu können, wenn nötig. Auch wird während des Prototyping die für das Fahrzeug benötigte Software erstellt und auf die verschiedenen Bauteile aufgespielt.

In der Testphase wird das Fahrzeug hinsichtlich des Zusammenspiels aller Komponenten, der Software und neuer Systeme ausführlich getestet. Die meisten Tests umfassen dabei heutzutage zertifizierungsrelevante Tests. Diese sind zum Beispiel Emissionstests, Safety-Tests (Crashtests) oder das Testen der Fahreigenschaften auf speziellen Teststrecken. Die meisten dieser Tests sind relevant für die am Ende der Testphase anstehende Typzulassung, ohne die Fahrzeuge nicht produziert oder zumindest nicht verkauft werden dürfen.

In der Produktion werden die Fahrzeuge hergestellt, mit Software konfiguriert und ausgeliefert. Dabei ist auch zu beachten, dass viele Schritte in der Vorproduktion und Vormontage in der Verantwortung von Zulieferern und wiederum deren Lieferanten liegen.

Während der Betriebsphase hat der Hersteller nur noch eine beschränkte Verfügbarkeit über das Fahrzeug, nämlich wenn dieses gerade zum Service oder zu einer Reparatur in der Werkstatt ist. Internetfähige Fahrzeuge können auch während des Betriebs ohne Werkstatt in einem abgesteckten Umfang von Hersteller erreicht werden (zum Beispiel durch Karten- oder Flashwareupdates). Ansonsten liegt die Hoheit über das Fahrzeug beim jeweiligen Besitzer.

Am Ende des Lebenszyklus steht entweder die „Auschlachtung“, also die Zerlegung und der Weiterverkauf in Einzelteilen, oder die endgültige Verschrottung. Auch hier hat der Hersteller nur einen bedingten Einfluss auf den Prozess.

Dabei können in allen Phasen des Prozesses Sicherheitslücken auftreten, während alle in den Kapiteln 5.2.1 und 5.2.2 beschrieben Bedrohungen und Risiken sich auf die Betriebsphase beziehen. Auf diese wird in diesem Abschnitt demnach auch nur noch aus Prozesssicht eingegangen.

#### 5.2.3.2 Bedrohungs- und Risikoanalyse

<table>
<tr><th colspan="4">PROZ-01: Spezifikation</th></tr>
<tr><th colspan="2">Usecase</th><th colspan="2">Misuse-Case</th></tr>
<tr><td colspan="2">In der Spezifikationsphase werden alle für das Fahrzeug notwendigen Anforderungen festgelegt.</td><td colspan="2">Es wurden in der Spezifikationsphase nur safetybezogene und keine securitybezogenen Anforderungen definiert.</td></tr>
<tr><th colspan="4">Schutzziel</th></tr>
<tr><td colspan="4">Security-Anforderungen müssen schon frühestmöglich im Prozess mitberücksichtigt werden. Zulieferer müssen diese ebenfalls von Anfang an kennen.</td></tr>
<tr><th colspan="4">Risiko</th></tr>
<tr><td>Kritikalität:</td><td colspan="3">Keine Verletzungsgefahr</td></tr>
<tr><td>ETW:</td><td>Mittel</td><td>Maßnahmen:</td><td>Vermeidungsmaßnahmen</td></tr>
</table>

| **PROZ-02: Prototyping und Entwicklung** | | | |
|---|---|---|---|
| **Usecase** | | **Misuse-Case** | |
| Im Prototyping und in der Entwicklung werden Bauteile und Software für das spätere Fahrzeug und die Testphase bereitgestellt. | | Es werden in der Prototyping-Phase Bauteile nicht auf Security geprüft. Es wird keine Codeanalyse der entwickelten Software gemacht. | |
| **Schutzziel** | | | |
| Bauteile und Software müssen schon so früh wie möglich im Gesamtprozess auf Security-Schwachstellen geprüft werden. | | | |
| **Risiko** | | | |
| Kritikalität: | Keine Verletzungsgefahr | | |
| ETW: | Mittel | Maßnahmen: | Vermeidungsmaßnahmen |

| **PROZ-03: Testing** | | | |
|---|---|---|---|
| **Usecase** | | **Misuse-Case** | |
| In der Testphase werden verschiedene Tests gemacht, um ein neues Fahrzeug auf Safety und Security zu prüfen. | | Es werden nur Safety-Tests gemacht. Security-Tests und Penetration-Tests werden ausgelassen, weil diese noch nicht zertifizierungsrelevant sind. | |
| **Schutzziel** | | | |
| Es müssen auch entsprechende Security- und Penetration-Tests in der Testphase mit einzuplanen und durchzuführen. Es muss darauf hingearbeitet werden, kommende Zertifizierungen für Security-Tests mit zu integrieren. | | | |
| **Risiko** | | | |
| Kritikalität: | Keine Verletzungsgefahr | | |
| ETW: | Mittel | Maßnahmen: | Vermeidungsmaßnahmen |

| **PROZ-04: Produktion Fremdbauteile** | | | |
|---|---|---|---|
| **Usecase** | | **Misuse-Case** | |
| Zulieferer liefern Bauteile für das Fahrzeug, welche schon Flashware oder Software enthalten. | | Die Bauteile werden vor dem Einbau nicht auf securityrelevante Aspekte hin überprüft. Enthaltene Parameter, Passwörter oder Schlüssel könnten hart kodiert sein. | |
| **Schutzziel** | | | |
| Bauteile und deren Soft/Flashware müssen auf ihre Integrität geprüft werden. Es muss ein Verfahren zum sicheren Einspielen von Schlüsseln geben. | | | |
| **Risiko** | | | |
| Kritikalität: | Keine Verletzungsgefahr | | |
| ETW: | Mittel | Maßnahmen: | Vermeidungsmaßnahmen |

| **PROZ-05: Produktion Endmontage** | | | |
|---|---|---|---|
| **Usecase** | | **Misuse-Case** | |
| Fahrzeuge werden während der Produktion mit benötigter Software und Zugangsdaten, Schlüsseln etc. bespielt. | | Das Aufspielen dieser Daten geschieht in einem nicht sicheren Umfeld, wo Manipulationen nicht ausgeschlossen werden können. | |
| **Schutzziel** | | | |
| Software, Flashware, Parameter, Schlüssel etc. müssen in einem nachweisbar abgesicherten Umfeld aufgespielt werden. | | | |
| **Risiko** | | | |
| Kritikalität: | Keine Verletzungsgefahr | | |
| ETW: | Mittel | Maßnahmen: | Vermeidungsmaßnahmen |

| **PROZ-06: Betrieb – Wartung und Reparatur** | | | |
|---|---|---|---|
| **Usecase** | | **Misuse-Case** | |
| Während der Inspektion oder einer Reparatur werden Änderungen an Bauteilen oder an Flashware und Software vorgenommen. | | Werkstätten könnten sowohl mutwillig als auch aus Versehen die falsche oder eine Flashware oder Software mit Fehlern aufspielen. Es könnten Teile verbaut werden, welche eine falsche oder manipulierte Flashware enthalten. | |
| **Schutzziel** | | | |
| Bei Wartungen und Reparaturen muss sichergestellt werden, dass nur verifizierte Teile und Software verwendet wird. Die OBD Schnittstelle muss Schutz vor unerlaubtem Aufspielen bieten. | | | |
| **Risiko** | | | |
| Kritikalität: | Keine Verletzungsgefahr | | |
| ETW: | Mittel | Maßnahmen: | Vermeidungsmaßnahmen |

| **PROZ-07: Stilllegung** | | | |
|---|---|---|---|
| **Usecase** | | **Misuse-Case** | |
| Nach der Stilllegung eines Fahrzeugs werden noch brauchbare Komponenten weiterverkauft. | | Diese Komponenten können noch personenbezogene Daten des Vorbesitzers oder Passwörter und Schlüssel enthalten, die der Käufer ausnutzen könnte. | |
| **Schutzziel** | | | |
| Bei der Stilllegung eines Fahrzeugs muss vorher sichergestellt werden, dass Security-kritische Teile und Daten so gelöscht werden, dass diese Daten im Nachhinein nicht ausgenutzt werden können. | | | |
| **Risiko** | | | |
| Kritikalität: | Keine Verletzungsgefahr | | |
| ETW: | Mittel | Maßnahmen: | Vermeidungsmaßnahmen |

## 5.3 Konzeption einzelner Security Bausteine

Für ein ganzheitliches Defense-in-Depth-Konzept ist es notwendig, dass in allen Bereichen in und um das Fahrzeug Security-Maßnahmen getroffen werden. Demnach sind verschiedene Security-Bausteine in den Bereichen nötig, welche alle zusammen zu einem sicheren Gesamtkonzept beitragen. Die verschiedenen Bereiche werden in Abbildung 17 dargestellt.

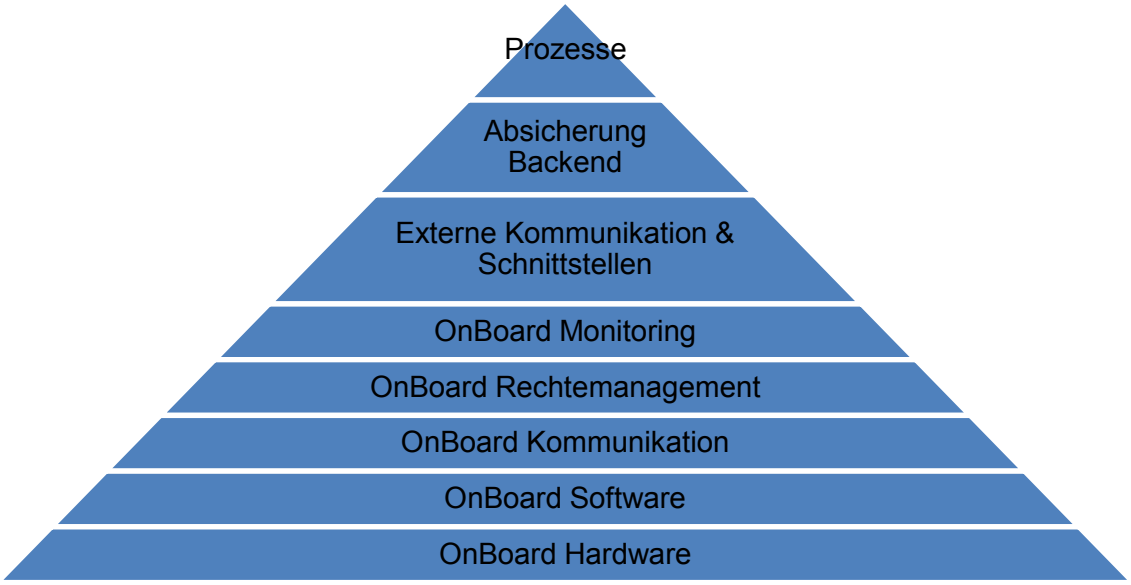


*Abbildung 17: Schichtenmodell Security-Bausteine*

Im Folgenden werden Security-Bausteine entlang der dargestellten Pyramide aufsteigend beschrieben. Dabei werden den einzelnen Bausteinen auch in Kapitel 5.2 beschriebene Schutzziele zugeordnet.

### 5.3.1 OnBoard Hardware

#### Hardware Secure Module

HSMs sind spezielle Krypto-Prozessoren, welche dafür entwickelt wurden, um kryptografische Schlüssel zu schützen und die Ausführung von kryptografischen Applikationen (wie zum Beispiel die Schlüssel- oder Zufallszahlenerzeugung) manipulationsgeschützt sicherzustellen. HSMs können dabei als Teil in ein bestehendes System eingebettet werden, auch Integrated System on Chip (SoC) genannt. Oder sie werden außerhalb eines Systems mit einer dedizierten Anbindung betrieben. In diesem Fall ist noch ein zusätzlicher Schutz dieser Anbindung erforderlich. In einem Fahrzeug werden HSMs überall dort gebraucht, wo Krypto-Schlüssel oder Zufallszahlen erzeugt werden müssen.

Bietet Schutzmaßnahmen für: CANB-03, CANB-07

**Secure SIM Element**

Secure Elements in Form einer SIM Karte sind dafür gemacht, dass kritische Daten an einem sicheren Ort gespeichert werden können und nur autorisierte Zugriffe darauf erfolgen können. Auf einer SIM Karte werden in der Regel eine Besitzer-ID und ein dazugehöriger Schlüssel gespeichert. Mit diesen beiden Werten ist es einer authentifizierten Person oder Applikation möglich, sich gegenüber einem anderen Device zu authentifizieren, wie zum Beispiel gegenüber einem Mobilfunk-Provider. Im Fahrzeug kann eine in eine TCU oder ECU integrierte SIM Karte dazu dienen, sich an einem Remote Server, einer PKI, dem Herstellerbackend etc. sicher und verschlüsselt zu authentifizieren. Durch ihre geringe Größe sowie die niedrigen Produktionskosten ist sie gut für einen flächendeckenden Einsatz im Fahrzeug geeignet.

Bietet Schutzmaßnahmen für: KOMM-02, KOMM-08, KOMM-09

**Secure Boot**

Mit Secure Boot wird sichergestellt, dass die Authentizität und Integrität einer Firmware zu jedem Zeitpunkt des Boot-Vorgangs sichergestellt ist. Dabei wird zuerst ein initialer Boot-Code geladen, welcher in einem speziellen On-Chip-Bereich gespeichert ist, der nicht verändert werden kann. Dabei wird auch das Root-Zertifikat geladen, welches die nächste Boot-Stufe verifiziert. In der folgenden Stufe wird der eigentliche Bootloader, welcher die Firmware ausführt, geladen. Dieser wird über das Root-Zertifikat verifiziert. Wenn im nachfolgenden Schritt die digital signierte Firmware geladen wird, wird anhand des Zertifikats deren Authentizität und Integrität geprüft. Es wird also eine Trust-Chain vom initialen Bootloader bis zur Firmware aufgebaut. Nur wenn alle Stufen richtig verifiziert sind, kann die Firmware auch geladen werden. Im Fahrzeug kann diese Methode auf jedem Chip ausgeführt werden, welcher Secure Boot unterstützt. Dies sind in erster Linie solche, die auch über ein HSM oder ein Secure Element verfügen.

Bietet Schutzmaßnahmen für: KOMM-03, KOMM-04, KOMM-05, KOMM-07, CANB-03

**Hardware-Virtualisierung (Secure Storage)**

Um schützenswerte Systemdaten von Anwendungsdaten sicher zu trennen, empfiehlt sich der Einsatz eines Hypervisors auf einem SoC mit HSM. Dabei werden durch den Hypervisor zwei voneinander getrennte Partitionen auf dem Chip erstellt, welche durch eine Firewall getrennt sind: Eine Partition beinhaltet Systemdaten wie das Betriebssystem oder sicherheitsrelevante Daten (Secure Storage). Auf der anderen Partition werden dagegen solche Daten gespeichert, die aus nicht vertrauenswürdigen Quellen kommen oder welche nicht geschützt werden müssen. Das können zum Beispiel Apps von

Drittanbietern oder die Wiedergabe von Medien sein. Die Firewall trennt die beiden Partitionen und dient als Filter für den Datenaustausch zwischen ihnen. Dieser Aufbau macht im Fahrzeug insbesondere dort Sinn, wo sicherheitskritische Systemdaten auf nicht vertrauenswürdige Daten treffen, wie es zum Beispiel in einer Head-Unit und deren Infotainment-Funktionen der Fall ist.

Bietet Schutzmaßnahmen für: KOMM-01, KOMM-03 bis KOMM-07, HEAD-03

### 5.3.2 OnBoard Software

#### Härtung von Betriebssystemen und Anwendungen

Betriebssysteme und Applikationen im Fahrzeug sollten gehärtet sein. Härtung bedeutet in diesem Fall, dass Parameter und Einstellungen in diesen so gesetzt werden, dass ein Angriff schwieriger ist. Ein klassisches Beispiel für eine Härtung ist die Abschaltung von unsicheren Ports und Protokollen (wie Telnet). Auch in Fahrzeugen sollten diese Maßnahmen getroffen werden, insbesondere dort, wo Software von Fremdanbietern eingesetzt wird, wie es in der Head-Unit (Unix Betriebssystem) häufig der Fall ist. Zusätzlich sollte die Software auch regelmäßig auditiert werden, ob alle Parameter noch den Soll-Zustand haben oder ob es Anomalien und unerwünschte Änderungen gibt.

Bietet Schutzmaßnahmen für: HEAD-01, KOMM-03 bis KOMM-07, CANB-03

#### Signieren und Hashen von Software

Mit der Signierung von Software und Softwareupdates im Fahrzeug wird sichergestellt, dass nur solche Software ausgeführt werden kann, die auch von einem autorisierten Absender (Hersteller, Zulieferer, Werkstatt) kommt. Außerdem ist nur mit einer entsprechend signierten Software ein Secure-Boot Prozess möglich. Die Signatur ist einem Inhaber eineindeutig zugeordnet und bietet damit Schutz vor dem Ausführen von Software von unautorisierten Absendern. Zusätzlich empfiehlt es sich, an das Fahrzeug gesendete Software-Updates mit einem Hash zu versehen. Dieser Hash dient dazu, um sicherzustellen, dass die Software, welche vielleicht zwar von einem autorisierten Absender kommt, nicht auf dem Übertragungsweg manipuliert wurde.

Bietet Schutzmaßnahmen für: KOMM-02, HEAD-01, CANB-03

### 5.3.3 OnBoard Kommunikation

#### Verifizierung Kommunikation

Um Nachrichten im Fahrzeug zu authentifizieren, bietet sich die Message Authentication Code (MAC) Nachrichtenauthentifizierung an. Dabei teilen sich Sender und Empfänger einen vereinbarten Schlüssel. Dieser wird mit jeder Nachricht beim Sender berechnet

und an diese angehängt. Der Empfänger berechnet seinerseits den zur Nachricht gehörenden MAC-Schlüssel und prüft, ob dieser zur empfangenen Nachricht passt. Ist dem so, so gilt die empfangene Nachricht als verifiziert. Zusätzlich gibt es eine sogenannte „freshness Value“, um Schutz gegen Replay-Attacken zu bieten. Das MAC-Authentifizierung sehr einfach zu implementieren ist, bietet sie sich im Fahrzeug für eine verifizierte Kommunikation zwischen einzelnen ECUs, Sensoren und Aktoren an. MAC alleine bietet dabei aber keine Verschlüsselung, so dass ein Dritter die Nachrichten zwar nicht mehr manipulieren, aber dennoch mitlesen kann. Für Fahrzeuge eignet sich insbesondere die AutoSAR SecOC Spezifikation mit CAN FD (Flexible Datarate) in diesem Bereich.

Bietet Schutzmaßnahmen für: CANB-04

**Verschlüsselung Kommunikation**

Eine Verschlüsselung der Kommunikation im Fahrzeug gegen unbefugtes Mitlesen ist nur unter bestimmten Voraussetzungen möglich. Es bedarf für die Verschlüsselung entsprechender Elemente, welche die Verschlüsselung schnell (in Echtzeit) und vertrauenswürdig vornehmen können. Diese Funktionalitäten bieten HSMs und Secure Elements. Um eine flächendeckende Verschlüsselung zu gewährleisten wären entsprechende Module damit in jedem Sender und Empfänger notwendig, was einen hohen Aufwand und hohe Kosten darstellen würde. Derzeit wird deshalb selten über eine Verschlüsselung auf CAN-Ebene nachgedacht. Mit der nach und nach stattfindenden Ablösung von CAN durch IP ist eine Verschlüsselung der OnBoard Kommunikation wahrscheinlicher.

Bietet Schutzmaßnahmen für: HEAD-02, CANB-04., CANB-07

**Segmentierung Netzwerk**

Netzwerksegmentierung im OnBoard-Netzwerk isoliert einzelne Domänen mit unterschiedlicher Kritikalität und schützt so vor unerlaubten Zugriffen zwischen verschiedenen Bereichen im Fahrzeug. Dabei werden sicherheitsrelevante und sicherheitskritische Systeme (wie CAN-Antrieb und CAN-Fahrwerk) von solchen getrennt, die mit externen Quellen Kommunizieren (CAN-Komfort) oder aus ihrer Funktion heraus ein niedrigeres Sicherheitslevel haben (wie die Infotainment-Systeme). Zwischen den einzelnen Domänen gibt es Security-Gateways, die alle durchgehenden Verbindungen überwachten. Als Basis für Fahrzeuge eignet sich der bereits vorgestellte Ansatz nach IEC62443 durch Zonen und Conduits.

Bietet Schutzmaßnahmen für: KOMM-03, KOMM-04, KOMM-05, CANB-04, CANB-05, CANB-07.

**OnBoard Firewalls**

OnBoad Firewalls bzw. Security-Gateways trennen die verschiedenen Netzwerksegmente voneinander. In ihnen wird entschieden, welche Nachrichten passieren dürfen und welche nicht. Teilweise können Security-Gateways auch Nachrichten hinsichtlich ihres Inhalts prüfen (Datenvalidierung, Virenscanning etc.). Dies ist aber nur bei solchen Gateways sinnvoll, wo keine Echtzeitanforderungen gegeben sind. Dabei gibt es auch einen Master-Slave Ansatz: sicherheitsrelevante Domänen dürfen Daten an weniger sicherheitsrelevante senden, umgekehrt jedoch nicht. Die Security-Gateways müssen dabei zusätzlich durch bereits vorgestellte Hardware-Maßnahmen vor Manipulation geschützt werden.

Bietet Schutzmaßnahmen für: KOMM-03, KOMM-04, KOMM-05, CANB-04, CANB-05, CANB-07.

### 5.3.4 OnBoard Rechtemanagement

**Zertifikate und Token**

Zertifikate im Fahrzeug bieten mehrere Vorteile: Zum einen können sie genutzt werden, um eine Authentifizierung zwischen zwei Parteien zu ermöglichen, zum anderen, um über diese Zertifikate den Nachrichtenverkehr zwischen diesen Parteien zu verschlüsseln. Dabei wird unterschieden zwischen Langzeitzertifikaten und Kurzzeit- bzw. Pseudonym-Zertifikaten. Langzeitzertifikate sind fest mit einem Fahrzeug verknüpft und bleiben für dessen gesamten Lebenszyklus erhalten. Diese können zum Beispiel zur Kommunikation und Authentifizierung gegenüber dem Herstellerbackend, einer Werkstatt oder zwischen Fahrzeug und Schlüssel verwendet werden. Pseudonym-Zertifikate werden nur für einen kurzen Zeitraum ausgestellt und verfallen, sobald sie nicht mehr gebraucht werden. Außerdem ist hier der Zertifikatsbesitzer gegenüber dem Empfänger pseudonymisiert. Diese Zertifikate eignen sich zum Beispiel für die Car2Infrastruktur- oder Car2Car-Kommunikation. Zertifikate können entweder initial in der Produktion oder während des Betriebs von einer PKI erstellt werden.

Token sind Schlüssel, welche Zugriff auf Ressourcen ermöglichen und dabei eine Autorisierung gegenüber der Ressource ermöglichen. Token sind meist zeitlich begrenzt und verfallen nach dem Zugriff wieder. Der Einsatz von Token empfiehlt sich daher besonders bei Einmal-Autorisierungen wie dem Herunterladen einer neuen Flashware, einer App oder eines Karten-Updates.

Bietet Schutzmaßnahmen für: KOMM-02, KOMM-08, KOMM-09, CANB-01, CANB-05, CANB-06

**PKI und Identity Management**

Die PKI und das Identity Management sind für die Verwaltung von Rechten und Zertifikaten zuständig. Die PKI kann sowohl Zertifikate erstellen und das Fahrzeug damit gegenüber Dritten authentifizieren als auch Rechte, Zertifikate und Berechtigungen rund um das Fahrzeug verwalten und prüfen. Dabei gibt es verschiedene Arten von Rechten und Zertifikaten:

- Interne Zertifikate: Diese werden Fahrzeugintern verwendet, um eine verschlüsselte Verbindung zwischen internen Komponenten aufzubauen (z.B. zwischen TCU und Head-Unit). Wird aber eher selten verwendet.
- Herstellerzertifikate: Werden verwendet, um sich am Herstellerbackend zu authentifizieren und zu kommunizieren.
- Zertifikate von Dritten für interne Berechtigungen: Zertifikate von Dritten können verwendet werden, um diesen im Fahrzeug entsprechend definierte Berechtigungen einzuräumen. So kann sich zum Beispiel eine Werkstatt per Zertifikat am Fahrzeug anmelden, um bestimmte Funktionen der OBD-Schnittstelle nutzen zu dürfen, oder ein Kartenanbieter, um dem Fahrzeug Karten-Updates zu senden.
- Zertifikate für kurzzeitige, verschlüsselte Kommunikation: Diese können zum Beispiel im Bereich Car2Car Kommunikation genutzt werden, um diese zu verschlüsseln.

Bietet Schutzmaßnahmen für: BACK-02, KOMM-02, KOMM-08, KOMM-09, CANB-01, CANB-05, CANB-06

### 5.3.5 OnBoard Monitoring

**IDS/IPS**

Ein Intrusion Detection System (IDS) trägt zum Erkennen von Angriffen bei. Das Intrusion Prevention System (IPS) wiederum kann erkannte Angriffe abwehren.

Das IDS kann Log-Dateien, Netzwerkverkehr, Prozesse und nach bekannten Schwachstellen scannen und im Falle einer Anomalie oder eines Angriffs diesen melden. Das IDS sollte dabei an den Punkten im Netzwerk eingesetzt werden, wo zum einen der Übergang zwischen einer sicherheitskritischen und einer unkritischen Zone ist (wie am Schnittpunkt zwischen CAN-Antrieb, CAN-Fahrwerk und CAN-Komfort) und an Punkten, an denen Daten in das Fahrzeug kommen oder dieses verlassen (wie an der TCU und deren Schnittstellen nach außen). Ein IDS kann in der Regel auch aggregierte Daten an das Backend senden und dort eine tiefere Auswertung auf Flottenebene ermöglichen.

Ein IPS dient nach dem Erkennen eines Angriffs der Vermeidung von Folgeschäden. Wenn das IDS einen Angriff meldet, kann das IPS darauf reagieren und zum Beispiel eine Netzwerkverbindung trennen oder auch Funktionen im Fahrzeug abschalten. Dieses Vorgehen ist teils aber auch als hochkritisch angesehen, da es Verbindungen und Funktionen gibt, welche unter allen Umständen funktionieren müssen (wie das Senden eines Signals vom Bremspedal an das Bremssystem).

Bietet Schutzmaßnahmen für: Alle OnBoard Bereiche und angrenzende Schnittstellen.

### 5.3.6 Externe Kommunikation & Schnittstellen

Um die Kommunikation nach Extern abzusichern, benötigt es Schutzmechanismen an den Schnittstellen. Im Idealfall nutzt man die Komponenten, welche auch für OnBoard-Security schon genutzt werden, und zwar IDS und IPS, zertifikatsbasierte Anmeldung und eine entsprechende Firewall bzw. ein Security-Gateway. Hier gilt es allerdings zu beachten, dass der Datenverkehr nach Extern in der Regel nicht auf CAN, sondern auf IP-Ebene abläuft und die Produkte dies entsprechend unterstützen müssen. Eine zertifikatsbasierte Anmeldung ist insbesondere bei der Kommunikation mit einem Backend, ob Hersteller oder Drittanbieter, von Vorteil und einfach über Client-Server-Zertifikate zu implementieren. Für die Kommunikation mit anderen Geräten über WLAN und Bluetooth könnte sich das schwieriger Darstellen. Hier kann aber auch auf Mechanismen im externen Gerät (Fingerabdruck, Webanmeldung über O-Auth, Anmeldung über SIM Karte etc.) zurückgegriffen werden.

Bietet Schutzmaßnahmen für: KOMM-02, KOMM-03, KOMM-04, KOMM-05, KOMM-07, KOMM-08, KOMM-09.

### 5.3.7 Absicherung Backend

Da es sich beim Herstellerbackend um großteils klassische IT-Technologie handelt, kann diese auch mit bekannten Maßnahmen abgesichert werden. Diese sollten unter anderen beinhalten:

- Netzwerksegmentierung mit DMZ-Bereichen
- (Web)Firewalls, Proxy-Server, Load-Balancer
- IDS/IPS, Logging/Monitoring-System, SIEM-System
- Virenschutz, Datenfilterung
- System und Applikations-Härtung
- Secure Hosting

Bietet Schutzmaßnahmen für: BACK-01

### 5.3.8 Prozesse

**Spezifikationsphase**

Security-Anforderungen müssen schon im Anforderungskatalog mit spezifiziert werden. Dazu muss es auch ein dediziertes Security-Konzept geben, wo Bedrohungen und Risiken für das Fahrzeug aufgelistet sind. Außerdem sollte entsprechende Ressourcen bereits hier mit eingeplant werden. Zulieferer sind vertraglich auf verbindliche Security-Richtlinien zu verpflichten.

Bietet Schutzmaßnahmen für: PROZ-01

**Prototyping & Entwicklungsphase**

Hier müssen Bauteile hinsichtlich Schwachstellen geprüft werden. Dafür eignen sich Tools zur Prüfung von Common Vulnerabilities and Exposures (CVE) und Common Weakness Enumeration (CWE). Die in dieser Phase erstellte Software muss nach definierten Secure Desing und Coding Standards erstellt und geprüft werden. Für diese Software muss es auch Code Reviews geben. Über den gesamten Lebenssyklus des Fahrzeugs und die damit verbundene Software ist ein Secure Software Developement Lifecycle (SSDLC) zu definieren.

Bietet Schutzmaßnahmen für: PROZ-02

**Test & Zertifizierungsphase**

In der Testphase müssen auch Security-Tests durchgeführt werden. Dabei sind umfangreiche Penetration-Tests aller sicherheitsrelevanten Bauteile sowie des Gesamtfahrzeugs durchzuführen. In Integrationstests muss auch das Zusammenspiel aller Komponenten getestet werden. Es sollte sich an einem Standard orientiert werden (AutoSAR, IEC62443, UN TF CS/OTA…).

Bietet Schutzmaßnahmen für: PROZ-03

**Produktion**

In der Produktion werden Sicherheitsmerkmale in dem Produkt verbaut. Das kann sowohl Hardware (HSMs, Secure Elements, Secure Storage) also auch Software sein (Bootloader, Firmware, Krypto-Schlüssel). Dabei muss beachtet werden, dass diese Elemente in einer nachweisbar sicheren Umgebung verbaut werden, welche jegliche Manipulation ausschließt. Dies gilt insbesondere für die initialen Krypto-Schlüssel. Hier gilt eine besondere Vorsicht, da viele Krypto-Schlüssel schon bei Zulieferern auf Bauteile aufgespielt werden und bei der Lieferung an den Fahrzeughersteller in irgendeiner

Weise übergeben werden müssen. Dabei wird meist ein Dummy-Schlüssel genutzt, welcher dann beim Fahrzeughersteller wieder ausgetauscht wird. Demnach sind die Sicherheitsmodule und -schlüssel zwischen Zulieferer und Fahrzeughersteller ungeschützt. Idealerweise würden Krypto-Schlüssel von Anfang an in der Hoheit des Fahrzeugherstellers liegen. Dazu muss eine abgesicherte Verbindung zwischen dem Schlüssel-Server des Herstellers und der Produktion des Zulieferers bestehen. Über diese wird der richtige Schlüssel gleich bei der Produktion eingespielt und das Bauteil kommt somit abgesichert zum Hersteller.

Bietet Schutzmaßnahmen für: PROZ-04. PROZ-05

**Betrieb**

Während des Betriebs muss zum einen die Wartung des Fahrzeugs, also das Bereitstellen von Sicherheitsupdates oder dem Austausch von Schlüsseln, zum anderen das Monitoring nach Schwachstellen und Angriffen im Fokus stehen. Auch muss der Hersteller sicherstellen, dass in seinen Werkstätten nur verifizierte Soft- und Flashware an Fahrzeuge ausgeliefert wird und, wenn ein sicherheitsrelevantes Teil getauscht werden muss, dies auch unter Einhaltung von Sicherheitsregeln nachweisbar geschieht.

Bietet Schutzmaßnahmen für: PROZ-06

**Stilllegung**

Der Hersteller muss Möglichkeiten haben, ausgegebene Schlüssel auch wieder zurückzunehmen und Komponenten des Fahrzeugs zu deaktivieren. Der Hersteller muss also prüfen, welche Schlüssel für die Anmeldung am Backend verwendet werden und ob diese noch einem registrierten Fahrzeug zuzuordnen sind. Das gilt auch für Komponenten im Fahrzeug, die in ein neues Fahrzeug umgebaut wurden und von diesem versuchen, sich wieder anzumelden. Der Hersteller muss demnach ein Inventar pflegen, in dem alle Fahrzeuge mit allen relevanten Komponenten und Schlüsseln gelistet sind und dieses den gesamten Lebenszyklus lang pflegen.

Bietet Schutzmaßnahmen für: PROZ-07

## 5.4 Erstellung ganzheitlicher Sicherheitsmodelle

### 5.4.1 Gesamtmodell

Anhand der vorgestellten Schutzmaßnahmen wurden letztendlich die Architektur-Modelle so verändert, dass alle Maßnahmen in diese übertragen wurden. Abbildung 18 zeigt das überarbeitete Gesamtmodell. Dabei wird angenommen, dass alle empfohlenen

Security-Maßnahmen, welche das Backend betreffen, umgesetzt sind. Zusätzlich gibt es Firewalls, die den ein- und ausgehenden Datenverkehr überwachen. Außerdem wurde das Backend um eine PKI erweitert, welche dafür zuständig ist, während der Produktion initiale Krypto-Schlüssel an die Fahrzeuge auszuliefern und im Betriebs des Fahrzeugs eine sichere Kommunikation mit diesem aufbauen zu können. OnBoard wurde auch eine entsprechende Firewall aufgebaut, um eine direkte, aber gefilterte Kommunikation mit Drittanbietern zu ermöglichen. Außerdem wurden, wie vorgesehen, auch externe Geräte wie Smartphones oder die Car2Car Kommunikation mit entsprechenden Krypto-Schlüsseln ausgestattet, um auch hier den Kommunikationskanal absichern zu können. Damit wurden die wichtigsten Security-Maßnahmen außerhalb des Fahrzeugs umgesetzt.

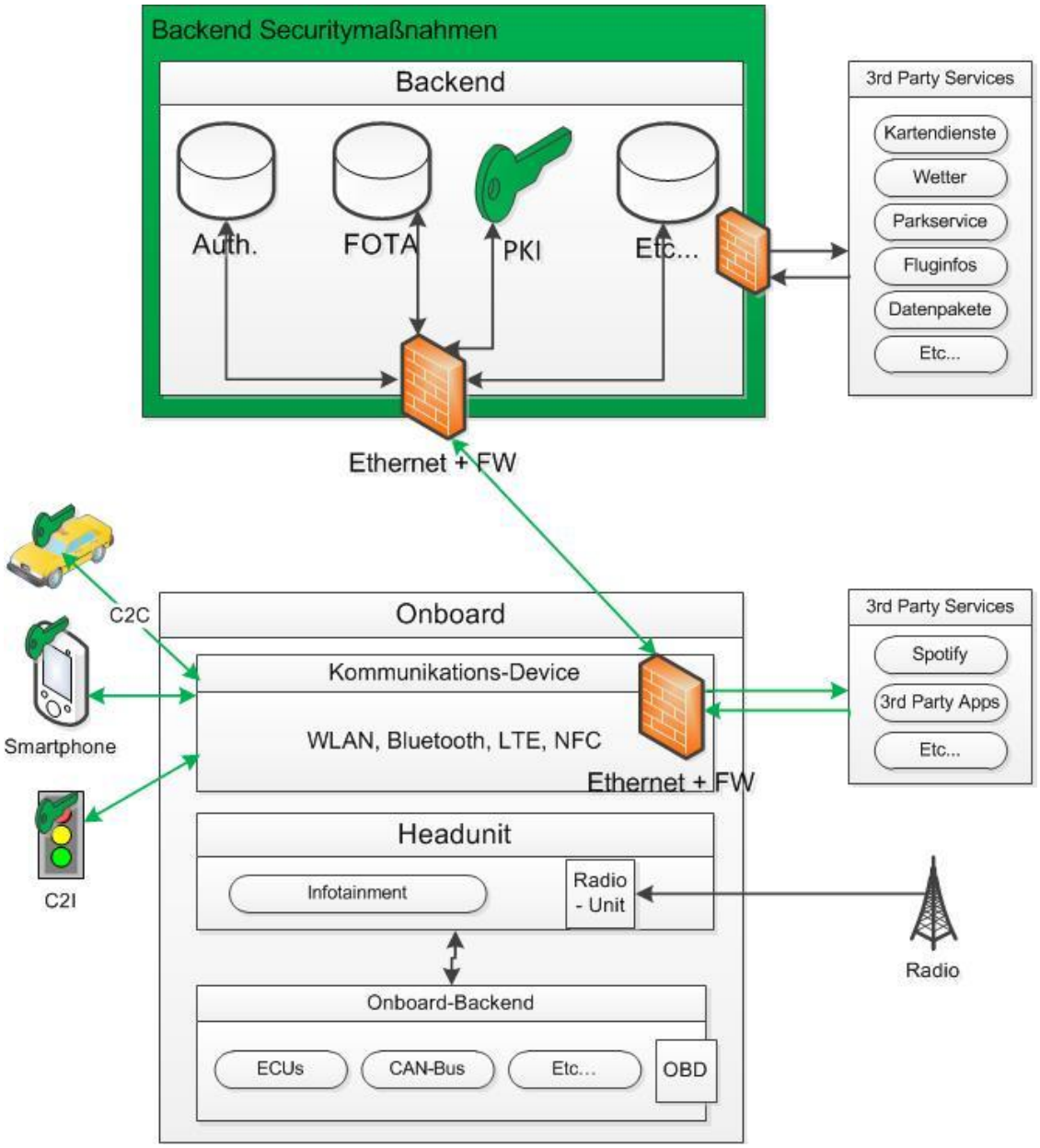


*Abbildung 18: Abgesichertes Gesamtmodell*

### 5.4.2 OnBoard Modell

Das OnBoard Modell beschreibt die Security-Maßnahmen im Fahrzeug. Dieses ist in Abbildung 19 dargestellt. Dabei wurden im Modell, neben den bereits vorgestellten Krypto-Schlüsseln in externen Geräten, folgende Maßnahmen implementiert:

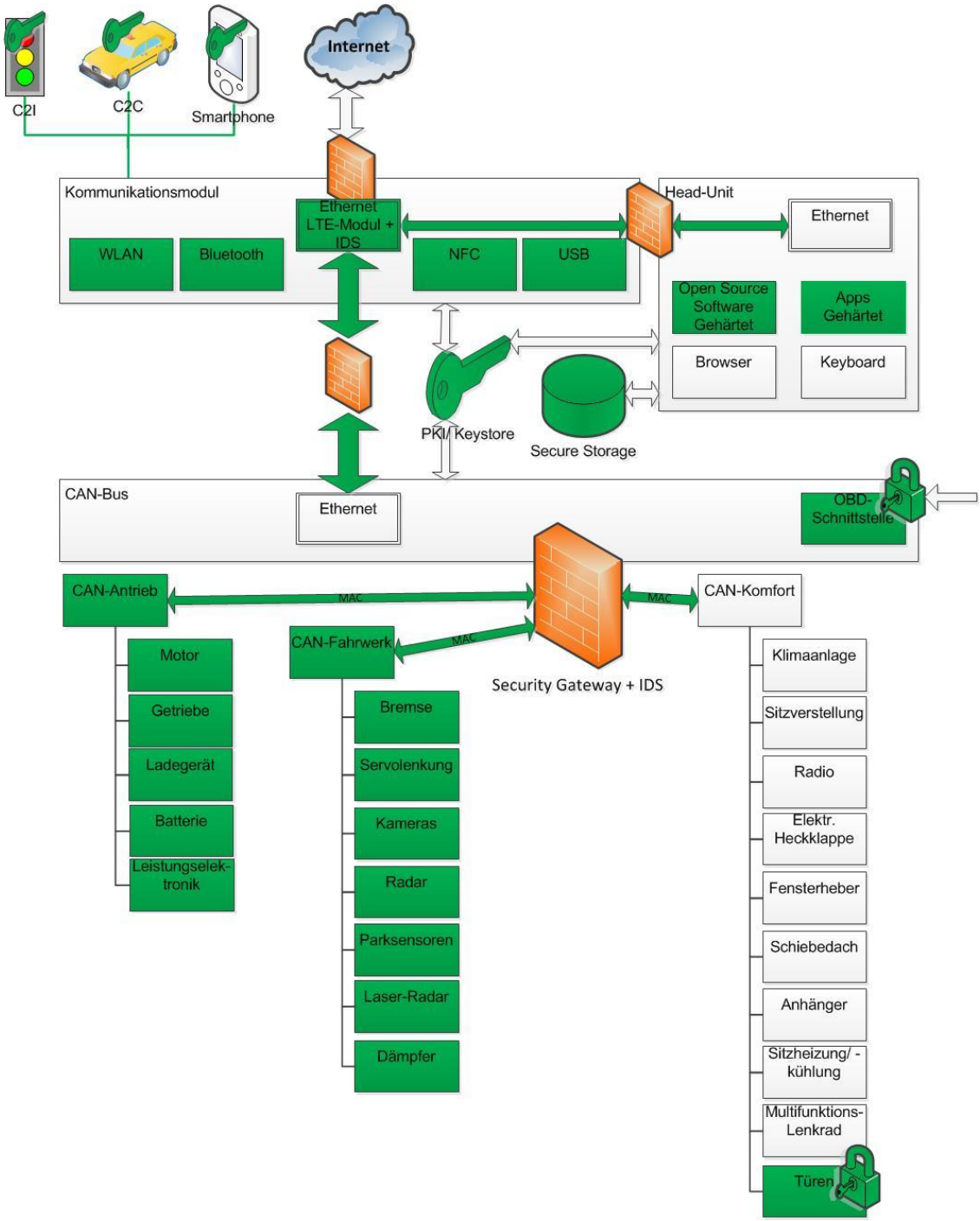


*Abbildung 19: Abgesichertes OnBoard Modell*

- Im Kommunikationsmodul wurde das Ethernet/LTE-Modul um Firewall-Funktionen sowie ein IDS erweitert. Das Resultat daraus ist, dass nur ausgewählte Verbindungen von außen in das Kommunikationsmodul gelangen können. Das IDS prüft zudem, ob es sich bei den Verbindungen um einen Angriffsversuch handelt.
- Auch die andren Komponenten des Komm-Moduls WLAN, Bluetooth, NFC und USB nutzen die Funktionen des IDS und sind zusätzlich gegen Angriffe gehärtet.
- Die Head-Unit kann nur noch durch eine Firewall erreicht werden. Damit werden auch hier ein- und ausgehende Verbindungen gefiltert.
- Open Source Software sowie Applikationen auf der Head-Unit ist gehärtet.
- Private Daten liegen geschützt in einem Secure Storage
- Es wurde eine PKI implementiert, welche die Schlüsselerzeugung sowie das Berechtigungsmanagement übernimmt. Die PKI ist entsprechend gehärtet, durch Secure Hardware und ein abgesichertes Betriebssystem.
- Auch der CAN-Bus kann nur noch über eine Firewall erreicht werden, welche Verbindungen filtert.
- Die OBD-Schnittstelle wurde abgesichert, dass nur noch autorisierte Personen mit einem entsprechenden Zertifikat und den entsprechenden Rechten auf Funktionen des CAN-Bus zugreifen können.
- Der CAN-Bus wurde in verschiedene Netzwerksegmente unterteilt.
- Das zentrale Security Gateway, welches die Netzwerksegmente verbindet, verwaltet die Verbindungen und prüft auf deren Berechtigung. Gleichzeitig ist hier auch ein IDS integriert, um Angriffe zu erkennen.
- Der Datenverkehr auf dem CAN-Bus und zwischen den Bereichen und ECUs ist mit MAC Authentifizierung abgesichert.
- Die Türsteuerung zum Öffnen des Fahrzeugs ist, wie die OBD-Schnittstelle, über ein entsprechendes Rechtemanagement abgesichert.
- Die sicherheitskritischen ECUs im Bereich CAN-Antrieb und CAN-Fahrwerk sind allesamt gehärtet und mit Secure-Boot, abgesicherter Firmware, HSM oder Secure Element ausgestattet.

Das Endergebnis ist eine OnBoard-Architektur, welche durch verschiedene Security-Maßnahmen abgesichert wurde. Dabei wurde sowohl auf präventive Maßnahmen zur Angriffsvermeidung gesetzt, als auch auf solche zur Erkennung von Angriffen und zur Reaktion darauf. In das Modell lassen sich auch die in 4.3 vorgestellten Lösungen der verschiedenen Security-Hersteller implementieren, je nachdem welche davon für einen Fahrzeughersteller in seine spezifische Architektur passen.

### 5.4.3 Prozess-Modell

Neben den Architektur-Modellen wurden auch für das Prozessmodell Security-Bausteine vorgestellt, die nun in das Prozessmodell eingearbeitet werden.

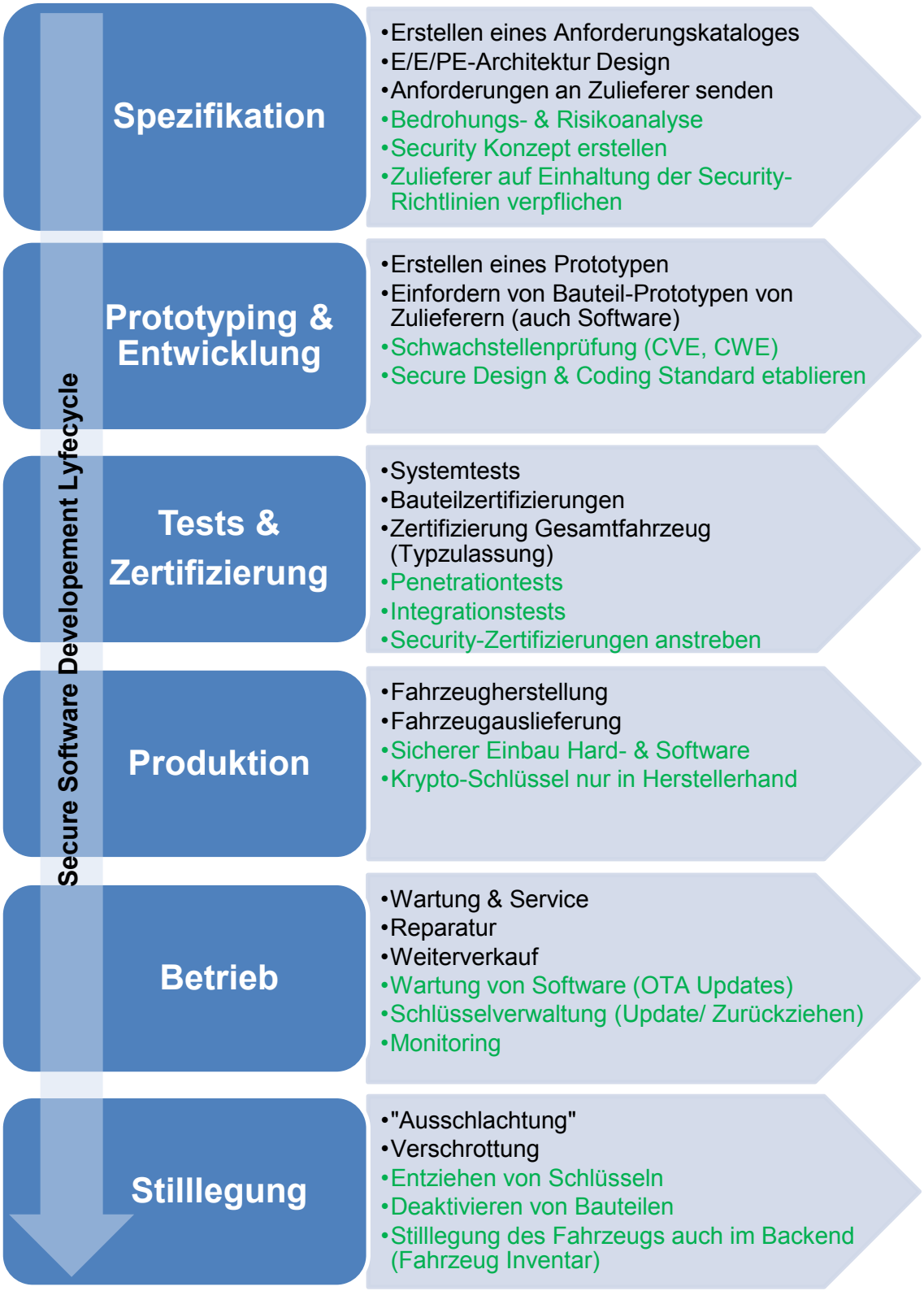


*Abbildung 20: Abgesichertes Prozessmodell*

Abbildung 20 zeigt das überarbeitete Prozessmodell. In dieses wurden alle Schutzmaßnahmen, die zuvor vorgestellt wurden, eingearbeitet. Dabei ist insbesondere zu beachten, dass über den Gesamtprozess ein SSDLC gelegt wurde, welchen es einzuhalten gilt. Dieser ist nicht fahrzeugspezifisch, sondern sollte über die Gesamtorganisation hin abgestimmt sein. Es ist demnach also durchaus sinnvoll, einen solchen Prozess unternehmensweit zu erstellen und einzuführen – unabhängig von der Softwareentwicklung für Fahrzeuge. Für diese müssen dann nur noch solche Elemente hinzugefügt werden, welche spezifisch für die Softwareentwicklung für Fahrzeuge gelten.

Da es neben dem Prozess für Security bei den meisten Fahrzeugherstellern bereits einen gut definierten Prozess für die Einhaltung von Safety-Maßnahmen gibt, sollten diese beiden Prozessen zudem in Einklang gebracht werden. Dies ist insbesondere notwendig, weil sich die beiden Prozesse teilweise gegenseitig bedingen. Ein nach ASIL eingestuftes, sicherheitsbezogenes System hat auch immer Auswirkungen auf die Security in einem Fahrzeug, weil dieses System besonders vor Angriffen geschützt werden muss.

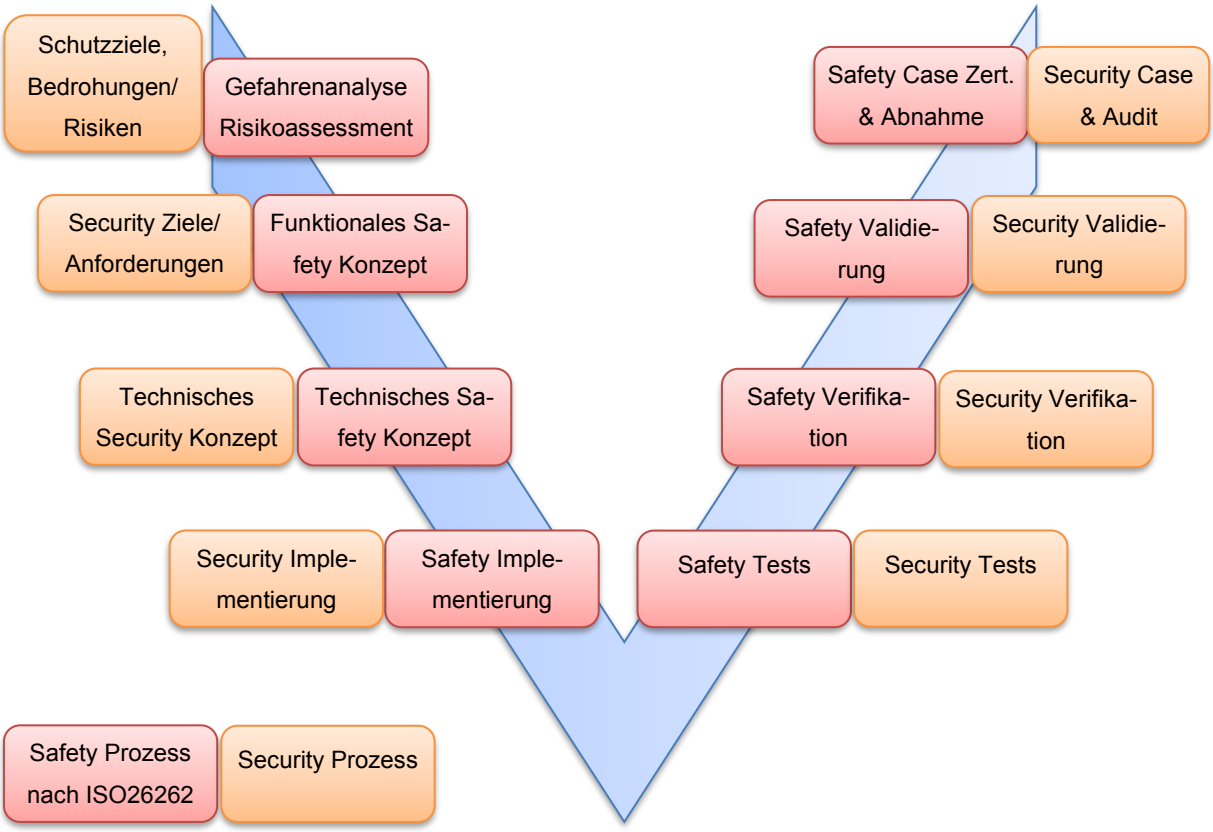


*Abbildung 21: Safety und Security Prozess*

Umgekehrt ist es genauso: Wenn ein sicherheitsrelevantes System eine Fehlfunktion hat (wie es durch einen Angriff der Fall sein kann), entsteht dadurch eine Gefahr welche unmittelbare Auswirkung auf die Safety eines Fahrzeugs hat. Nach ISO26262 gibt es

bereits einen für Fahrzeuge definierten Prozess, um die Einhaltung von Safety-Maßnahmen sicherzustellen. An diesen kann auch der Security-Prozess für das Fahrzeug anknüpfen, wie Abbildung 21 zeigt. Es muss also für jeden definierten Safety-Schritt auch ein Security-Gegenstück geben. Diese beiden Prozess-Bausteine sollten dabei Hand in Hand arbeiten und eine enge Abstimmung zueinander haben. So können schon frühzeitig Abhängigkeiten erkannt und im Projekt berücksichtigt werden.

## 5.5 Evaluierung der Lösungen und weiterer Forschungsbedarf

Die in diesem Kapitel vorgestellten Bedrohungs- und Risikoanalysen, sowie die dargestellten Modelle sind als ein generischer Ansatz zur Absicherung von Fahrzeugen erstellt worden. Dies impliziert, dass ein Fahrzeughersteller diese mit hoher Wahrscheinlichkeit nicht eins zu eins auf seine Fahrzeugarchitektur übernehmen kann. Zum einen werden Anpassungen hinsichtlich der CAN-Architektur notwendig sein, da dort jeder Hersteller seine eigene und unterschiedliche Vernetzung hat, zum anderen sind die aufgezeigten ECUs im CAN-Komfort nur eine beispielhafte Auswahl der ECUs, die am häufigsten in Fahrzeugen zu finden sind. Je nach Hersteller und Ausstattungsniveau des Fahrzeugs können hier Abweichungen entstehen. Außerdem betrachten die Modelle keinen Reifegrad von einem spezifischen Hersteller, sondern gehen von einem allgemeinen und eher niedrigen Reifegrad aus. Hier müssen die Fahrzeughersteller selber evaluieren, an welchem Punkt sie sich hinsichtlich Architektur- und Prozesssicherheit sehen und an welcher Stelle sie anknüpfen müssten.

Weiterer Forschungsbedarf hinsichtlich der Architektur-Modelle wird insbesondere in den Bereichen gesehen, wo es gerade große architektonische Veränderungen gibt. Dies gilt bei der Einführung von 5G und LTE-V, wo Anforderungen hinsichtlich Verfügbarkeit (Echtzeitfähigkeit), Integrität und Vertraulichkeit (Datenverschlüsselung und der Schutz personenbezogener Daten) im Fokus stehen sowie bei der Umstellung der internen Fahrzeugkommunikation von CAN auf IP-Protokolle. Mit diesen Änderungen werden manche Schutzmaßnahmen obsolet (wie MAC-Nachrichtenauthentifizierung) und neue kommen dazu (Absicherung IP-Kommunikation im Fahrzeug)

Im Bereich Prozesssicherheit werden in naher Zukunft viele neue Richtlinien und Standards veröffentlicht werden (vgl. Kapitel 3.3.3), welche neue Anforderungen an die Security-Prozesse rund um das Fahrzeug sowie die Notwendigkeit von entsprechenden Nachweisen und Zertifizierungen stellen. An dieser Stelle gilt es dann, den vorgestellten Prozess aus dieser Perspektive neu zu evaluieren und noch einmal nachzuschärfen.

# 6 Fazit und Ausblick

Im Laufe dieser Arbeit wurde herausgearbeitet, was Defense in Depth bedeutet und wieso ein Defense-in-Depth-Konzept für Fahrzeug-IT nicht dasselbe Konzept wie für klassische IT sein kann. Es wurde ein Überblick über Studien zu diesem Thema gegeben und evaluiert, wo diese noch nicht den Anforderungen an ein ganzheitliches Defense-in-Depth-Konzept für Fahrzeuge entsprechen. Im Anschluss wurden Hersteller-Lösungen für Security im Fahrzeug betrachtet und auf ihre Reife für ein Defense in Depth Konzept hin betrachtet. Aufbauend auf den Erkenntnissen aus den Vorkapiteln wurde zum Schluss eine Bedrohungs- und Risikoanalyse durchgeführt, Schutzmaßnahmen für Security im Fahrzeug erarbeitet und in einem ganzheitlichen Konzept umgesetzt.

Es ist im Laufe der Auseinandersetzung mit diesem Thema deutlich geworden, dass es nicht einen, universell gültigen Weg gibt, um Fahrzeuge abzusichern. Vielmehr ist der Weg zu einem aus IT-Sicht sicheren Fahrzeug einer aus vielen einzelnen Komponenten und Prozessschritten, welche alle zusammenpassen müssen, um ein stimmiges Gesamtkonzept zu ergeben. Bevor viele der vorgestellten Schutzmaßnahmen im Fahrzeug umgesetzt werden können, bedarf es noch viel Vorarbeit, auf prozessualer wie auf systemseitiger Ebene. Bisher scheint aber auch der Bedarf von OEMs nach einem ganzheitlichen Sicherheitsmodell noch gering zu sein, da vorhandene Security-Lösungen noch nicht so gefragt zu sein scheinen. Dies kann sich in naher Zukunft ändern, indem Richtlinien von Regierungen oder staatlichen Organisationen erlassen werden, welche Fahrzeughersteller zu einer Einhaltung eines Mindeststandards an Sicherheit im Fahrzeug zwingen. Dabei ist aber auch zu sehen, dass es zwar globale Richtlinien geben wird, aber in manchen Ländern auch regionale Standards, welche für eine zusätzliche Hürde bei der Einhaltung und Implementierung von Security sorgen werden.

Es wäre demnach ratsam, wenn sich Automobilhersteller und deren Zulieferer in baldiger Zukunft Gedanken über die Umsetzung von Security machen, bevor der Druck eines Gesetzes sie dazu zwingt. So kann erstens ein Vorteil gegenüber Wettbewerbern erreicht, als auch einem Vertrauensverlust der Kunden (durch einen Angriff) vorgebeugt werden. Als Basis, um den eigenen Reifegrad zu ermitteln und entsprechende Maßnahmen zu planen, kann diese Arbeit dienen.

Als Ausblick kann man sagen, dass Security im Fahrzeug mit dem zunehmenden Reifegrad des autonomen Fahrens noch stärker in den Fokus der Öffentlichkeit und damit auch der Fahrzeughersteller sowie der Security-Anbieter rücken wird. Der kommende Ausbau von LTE-V, 5G, Car2Infrastruktur und Car2Car-Kommunikation wird zudem

neue Security-Themen auf die Agenda bringen, mit denen sich alle Beteiligten, ob Fahrzeughersteller, Regierungs- und Nichtregierungsorganisationen oder Security-Anbieter, beschäftigen müssen. Insbesondere die Politik ist gefragt, hier die notwendigen Rahmenbedingungen so schnell wie möglich zu schaffen, um erstens die Entwicklung im Bereich autonomen Fahren und Fahrzeug-Security weiter voranzutreiben und zweitens diese auch sicher zu gestalten.

Nicht zuletzt zeigt aber auch „Diesel-Gate“, dass dringend Transparenz und Sicherheit für Kunden geschaffen werden muss, indem es entsprechende Vorgaben für den Bereich Softwareentwicklung im Fahrzeug, FOTA und Monitoring von Fahrzeugparametern gibt. Es sind also viele verschiedene Themen, die auf die IT-Security im Bereich Fahrzeug-Security in den nächsten Jahren zukommen werden.

# Quellenverzeichnis

**ADAC. 2014.** ADAC. [Online] 2014. [Zitat vom: 29. 05 2018.] https://www.adac.de/infotestrat/adac-im-einsatz/motorwelt/bmw-luecke.aspx.

**Bedner, Mark und Ackermann, Tobias. 2010.** Schutzziele der IT-Sicherheit. *Datenschutz und Datensicherheit - DuD.* 2010, 34.

**Benz, Stefan. 2004.** Eine Entwicklungsmethodik für sicherheitsrelevante Elektroniksysteme im Automobil. [Dissertation]. Karlsruhe : Universität Karlsruhe, 2004.

**Birkhölzer, Thomas und Vaupel, Jürgen. 2003.** *IT-Architekturen : Planung, Integration, Wartung.* Berlin : VDE-Verlag, 2003.

**British Department for Transport. 2017.** Gov.uk. *Principles of cyber security for connected and automated vehicles.* [Online] 2017. [Zitat vom: 30. 06 2018.] https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles.

**Broy, Manfred. 2010.** *Cyber-Physical Systems - Innovation durch softwareintensive eingebettete Systeme.* Berlin : Springer, 2010.

*Defense-in-depth and Role Authentication for Microservice Systems.* **Jander, Kai, Braunbach, Lars und Pokahr, Alexander. 2018.** 9th International Conference on Ambient Systems, Networks and Technologies, ANT-2018 and the 8th International Conference on Sustainable Energy Information Technology, SEIT 2018 : Procedia Computer Science, 2018.

**Dégardins, Pascal, et al. 2009.** Funktionsstandardisierung und deren Integration in die E/E-Fahrzeugarchitektur. *ATZelektronik.* 2009, 4.

**Dierstein, Rüdiger. 2014.** Sicherheit in der Informationstechnik - der Begriff IT-Sicherheit. *Informatik-Spektrum.* 2014, 27.

**Dr. Löffler, M und Prof. Dr. Decker, R. 2017.** „Connected Car“ und Customer Experience Management – Unlösbare Herausforderung oder gemeinsame Chance für Hersteller und Händler? [Buchverf.] Heike Proff und Thomas Fojcik. *Innovative Produkte und Dienstleistungen in der Mobilität.* Wiesbaden : Gabler Verlag, 2017.

**Durst, Michael. 2007.** Wertorientiertes Management von IT-Architekturen. Wiesbaden : Deutscher Universitäts-Verlag, 2007.

**European Union Agency for Network and Information Security. 2017.** Publications/Cyber Security and Resilience of smart cars. [Online] 2017. [Zitat vom: 30. 06 2018.] https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars.

**Greenberg, Andy. 2015.** Wired. [Online] 21. 07 2015. [Zitat vom: 29. 05 2018.] https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

**International Organization for Standardization. 2011.** ISO 26262-1:2011. [Online] 2011. [Zitat vom: 30. 06 2018.] https://www.iso.org/standard/43464.html.

**intersoft consulting. 2018.** Datenschutz-Grundverordnung. [Online] 2018. [Zitat vom: 30. 06 2018.] https://dsgvo-gesetz.de/.

**Kästner, J. 2007.** Umfassendes Security-Konzept für Prozessleitsysteme (defense in depth). *atp–Automatisierungstechnische Praxis.* 2007, 49. Jg., S. 70-75.

**Kerschenlohr, Roland. 2015.** Die Funktionsintegration. *ATZextra.* 2015, 15.

**Kersten, Heinrich und Klett, Gerhard. 2008.** Infrastruktursicherheit. *Der IT Security Manager.* 2008.

**Lass, Sander und Kotarski, David. 2014.** IT-Sicherheit als besondere Herausforderung von Industrie 4.0. [Buchverf.] Wolfgang Kersten, Hans Koller und Hermann (Hrsg.) Lödding. *Industrie 4.0 Wie intelligente Vernetzung und kognitive Systeme unsere Arbeit verändern.* Berlin : GITO mbH Verlag, 2014, S. 425.

**Ministry of Internal Affairs and Communications . 2014.** CYBER SECURITY POLICY IN JAPAN. [Online] 2014. [Zitat vom: 30. 06 2018.] http://crc.gov.mn/file/newfile/PRF-14-INP-07-MIC-JP-Cybersecurity.pdf.

**Müller, Klaus-Rainer. 2008.** *IT-Sicherheit mit System.* Wiesbaden : Friedrich Vieweg & Sohn GmbH Verlag, 2008.

**NTT Data Deutschland GmbH. 2018.** Autonomous Driving. *Autonomous Driving - A Holistic Perspective on a Leading Megatrend in the Automotive Industry.* [Internes Dokument]. München : s.n., 2018.

**NTT Security (Germany) GmbH. 2018.** Securing Connected Cars. [Internes Dokument]. 2018.

**Prof. Dr. Eckert, Claudia. 2013.** *IT-Sicherheit, Konzepte - Verfahren - Protokolle.* München : Oldenbourg Verlag, 2013.

**Reißmann, Ole. 2013.** Spiegel Online. [Online] Spiegel, 07. 08 2013. [Zitat vom: 29. 05 2018.] http://www.spiegel.de/auto/aktuell/computerexperten-hacken-auto-software-a-914783.html.

**SAE International. 2012.** Standards/J3061. [Online] 2012. [Zitat vom: 30. 06 2018.] https://www.sae.org/standards/content/j3061/.

**Schwarz, Robert. 2018.** *Geprüfte Schutz- und Sicherheitskraft (IHK).* Wiesbaden : Springer Gabler, 2018. S. 230.

**Shen, Kelei. 2015.** Connected Safety – eine Herausforderung für die IT-Sicherheit. *ATZ - Automobiltechnische Zeitschrift.* 2015, 4.

**UN ECE. 2016.** UN Task Force on Cyber security and OTA issues. [Online] 2016. [Zitat vom: 08. 07 2018.] https://wiki.unece.org/pages/viewpage.action?pageId=40829521.

**United States Department of Transportation. 2017.** National Highway Traffic Safety Administration. *Vehicle Cybersecurity.* [Online] 2017. [Zitat vom: 30. 06 2018.] https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity.

**US Kongress. 2015.** Legislation/114th Congress/ H.R.3876. *Autonomous Vehicle Privacy Protection Act of 2015.* [Online] 2015. [Zitat vom: 30. 06 2018.] https://www.congress.gov/bill/114th-congress/house-bill/3876/text.

**—. 2017.** Legislation/115th Congress/ S.680. *SPY Car Act of 2017.* [Online] 2017. [Zitat vom: 30. 06 2018.] https://www.congress.gov/bill/115th-congress/senate-bill/680/text?q=%7B%22search%22%3A%5B%22spy+car+act%22%5D%7D&r=1.

**Weyl, Benjamin, Graf, Maximilian und Bouard, Alexandre. 2012.** Smart Apps in einem vernetzten (auto)mobilen Umfeld: IT-Security und Privacy. [Buchverf.] S Verclas und C Linnhoff-Popien. *Smart Mobile Apps.* Berlin : Springer Verlag, 2012.