Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

AW1 Ausarbeitung

Philipp Meyer

Informationssicherheit in Fahrzeugnetzen

Fakultät Technik und Informatik
Studiendepartment Informatik

Faculty of Engineering and Computer Science
Department of Computer Science

Philipp Meyer

Informationssicherheit in Fahrzeugnetzen

AW1 Ausarbeitung eingereicht im Rahmen der Anwendungen 1

im Studiengang Master of Science Informatik
am Department Informatik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Eingereicht am: 25. Juli 2014

Inhaltsverzeichnis

1. Einleitung

In modernen Fahrzeugen wird mittlerweile eine Vielzahl an Sensoren und Steuergeräten(ECUs) genutzt um Technologien zu ermöglichen, die die Funktionssicherheit, die Leistung und den Komfort von Fahrzeugen zu verbessern (siehe Abb.A.1). Daraus ergeben sich heutzutage immer komplexere Kommunikationsstrukturen, aus verschiedenen proprietären Bustechnologien, und erhöhte Datenmengen. In Zukunft kann durch den Einsatz von Ethernet die Kommunikation dieser Teilnehmer überschaubarer und leistungsfähiger gestaltet werden. Die Echtzeit Anforderungen in diesem Kontext werden mit Protokollen ermöglicht, die auf das Standard Ethernet IEEE 802.3 aufsetzen und damit deren Funktionalitäten und Zuverlässigkeit erweitern. Die gegenwärtigen Infrastrukturen sind angreifbar (vgl. Koscher u. a. (2010) und Checkoway u. a. (2011) und Bissmeyer u. a. (2013)) und führen zu Manipulationen des Fahrzeugverhaltens die mitunter gefährliche Konsequenzen für Fahrzeug und Mensch haben können. Es ist also ein wichtiges Ziel bei der Entwicklung des Fahrzeug-„Nervensystems“ der nächsten Generation von Anfang an adäquate Sicherheitslösungen bereit zu stellen.

In dieser Arbeit soll ein Überblick des momentanen Forschungsstands in diesem Gebiet vermittelt werden. Aus den herausgearbeiteten Bereichen soll dann weiterführende Arbeit herausgefiltert werden.

In Kapitel 2 werden als erstes die zwei relevanten Begriffe „Informationssicherheit“ und „Fahrzeugnetze“ abgegrenzt. Danach werden im Kapitel 3 die verschiedenen Teilgebiete in der Forschungslandschaft ausgeleuchtet. Am Schluss folgt dann mit Kapitel 4 eine Zusammenfassung und ein Ausblick auf mögliche zukünftige Tätigkeiten und deren Risiko.

2. Grundlagen

In diesem Kapitel werden Grundlagen zu den beiden zentralen Themen Informationssicherheit und Fahrzeugnetze vermittelt.

2.1. Informationssicherheit

Ein funktionssicheres System ist ein System wessen Ist-Funktionalität mit der spezifizierten Soll-Funktionalität übereinstimmt. Dies läuft Korrekt und Zuverlässig. Der Begriff **Informationssicherheit** (Englisch: Security) beschreibt wiederum ein funktionssicheres System, dass keine unautorisierten Informationsveränderung oder -gewinnung zulässt (vgl. Eckert (2013)). Ein solches System muss die folgenden drei Eigenschaften erfüllen damit es geschützt ist:

- **Informationsvertraulichkeit**: Geheimhaltung der Datenobjekte
- **Datenintegrität**: Verhindern von unauthorisierten Modifikationen an den Datenobjekten
- **Systemverfügbarkeit**: Kein Performance-Verlust

Zur Identifizierung und Einordnung von zu schützenden Datenobjekten gibt es Informationen und Richtlinien durch das BSI (vgl. Bundesamt fuer Sicherheit in der Informationstechnik). Die Vorgehensweise zur Entwicklung von informationssicheren Systemen ist durch eine ISO-Norm standartisiert (vgl. ISO 27001 (2013)). Mit diesen beiden und weiteren Mitteln lassen sich gegenwärtig mit einem strukturiert Entwicklungsprozess informationssichere IT-Systeme umsetzten.

2.2. Fahrzeugnetze

Ein Fahrzeugnetz ist in dieser Arbeit als das Netzwerk zu verstehen welches innerhalb eines Fahrzeugs verbaut ist um die Kommunikation der Sensoren, Aktoren und Steuergeräten zu gewährleisten. In gegenwärtigen Autos werden vor allem Bustechnologien eingesetzt um diese Kommunikation zu ermöglichen. In Zukunft kann dieses Technologie Schritt für Schritt

durch Ethernet-Netzwerke ersetzt werden (vgl. Bruenglinghaus und Redaktion Springer fuer Professionals). Durch Ethernet sind viel höhere Bandbreiten möglich, die Topologie wird übersichtlicher und es kann Gewicht gespart werden. Des weiteren ist es eine weit verbreitete Technologie. Dies führt zu niedrigen Anschaffungspreisen und hoher Zuverlässigkeit. In Abbildung A.2 sind die beiden Kommunikationstopologien beispielhaft gegenübergestellt. In der AbbildungA.2(a) sind die verschiedenen proprietären Bustechnologien wie CAN, MOST, FlexRay und LIN zu sehen. Kommunikation zwischen Bussen muss hier über ein Zentrales Gateway realisiert werden, welches die als Übersetzter fungiert. In einem reinen Ethernet-Netzwerk ist solch eine Übersetzungsschnittstelle nicht nötig (siehe Abb. A.2(b)).

Um die Funktionssicherheit der Kommunikation zu gewährleisten müssen auf Ethernet aufbauende sogenannte Echtzeitprotokolle eingesetzt werden. In diesem Bereich gibt es verschiedene Kandidaten welche die Problematik zu lösen versuchen. Einer dieser Kandidaten ist Time-Triggered Ethernet (TTE) (vgl. Society of Automotive Engineers - AS-2D Time Triggered Systems and Architecture Committee (2011)). Es enthält drei Nachrichtenklassen welche verschiedene Prioritäten und Eigenschaften vorweisen. Die „Echtzeit“ wird hier durch eine höchst statische Konfiguration erreicht. So sind zu Beispiel für Nachrichten mit höchster Priorität Sende- und Empfangszeitpunkte zur Laufzeit schon genau festgelegt. Ein weiterer Kandidat ist das Audio Video Bridging (AVB) (vgl. Institute of Electrical and Electronics Engineers (2011)). Es versucht eine dynamischere Kommunikation zu ermöglichen, erfüllt aber noch nicht alle Anforderungen. Darum findet hier im Moment eine Weiterentwicklung durch die Time Sensitive Networking Task Group des IEEE statt (vgl. IEEE 802.1 TSN Task Group (a) und IEEE 802.1 TSN Task Group (b)).

Eines dieser oder ein ähnliches Protokoll kann in Zukunft die funktionssichere Kommunikation der Steuergeräte innerhalb des Fahrzeugs ermöglichen.

3. Informationssicherheit in Fahrzeugnetzen

Durch den Einsatz von Ethernet in Fahrzeugen ergeben sich viele Vorteile nicht zuletzt durch zukünftige IP-basierte Dienste. Dies bringt allerdings auch alle Sicherheitsrisiken mit sich die zum Beispiel das Internet seit Jahren beschäftigt. Während die Funktionssicherheit schon im Fokus der Hersteller steht muss nun auch die Informationssicherheit immer mehr ins Visier genommen werden (vgl. Studnia u. a. (2013)). Es gibt einige Projekte die sich dieser Probleme annehmen. Eines der aktivsten ist PRESERVE (vgl. PRESERVE). Es legt das Hauptaugenmerk aber vor allem auf „vehicle-to-vehicle“ und „vehicle-to-infrastructure“ Kommunikation. Das Projekt EVITA (vgl. EVITA) und SEIS (vgl. SEIS) konzentrieren sich aber hauptsächlich auf die sichere Kommunikation innerhalb eines Fahrzeugs. Besondere Herausforderungen in diesem Bereich sind die harte Echtzeitanforderung an Teile der Kommunikation, die begrenzte Rechenleistung der ECUs und die eingeschränkte Möglichkeit von Softwareupdates. In diesem Kapitel werden die verschiedenen Themenschwerpunkte in dieser Forschungslandschaft beschrieben und aufgearbeitet.

3.1. Identifikation von Schwachstellen

Ein wichtiger Teil der Arbeiten in diesem Bereich beschäftigt sich mit der Identifikation und Analyse von Schwachstellen im „Nervensystem“ von Fahrzeugen. Sie versuchen zu ergründen in welchem Umfang ein Angreifer, an den unterschiedlichen Schnittstellen, Kontrolle über die Systeme erlangen kann.

Die Arbeit von Koscher u. a. (2010) zeigt in wie weit sich ein modernes Auto über die Diagnoseschnittstelle (ODB-II) angreifen lässt. Durch auslesen von CAN-Nachrichten der einzelnen Steuergeräte im Labor wurden genug Informationen extrahiert um eine weitreichende Manipulation zu ermöglichen. Durch die physikalische Broadcast-Eigenschaft von CAN-Bussen lassen sich solche Informationen aber auch direkt am Fahrzeug auslesen.Die **Informationsvertraulichkeit** ist schon an dieser stelle nicht mehr gewährleistet. Im nächsten Schritt wird dann ein Laptop an den ODB-II Port angeschlossen. Von diesem lassen sich vor und während der Fahrt

angriffe auf das Fahrzeugnetz durchführen. Die folge ist ein nahezu Vollzugriff auf die Systeme des Autos. Eins der harmlosesten Beispiele ist die Kontrolle über das Radio. Es lässt sich einfach lauter drehen. Der Fahrzeugführer hat nicht einmal die Möglichkeit manuell gegenzusteuern. Schon in diesem Bereich kann dies im Verkehr zu einer gefährlichen Situation kommen. Noch viel Gefährlicher wird es durch den Zugriff auf den Tacho, einzelne Bremsen, die Verriegelung und teile der Motorsteuerung. In einem immens großen Bereich der Kommunikation ist die **Datenintegrität** verloren gegangen. Durch „Denial of Service"-Attacken lässt sich zusätzlich die Kommunikation von CAN-Komponenten verhindern. Damit ist auch, spätestens an dieser Stelle, die **Systemverfügbarkeit** nicht mehr gewährleistet.

Checkoway u. a. (2011) untersuchen in ihrer Arbeit vor allem über welche Schnittstellen ein Fahrzeug Angegriffen werden kann. Dafür werden die unterschiedlichen I/Os in drei Kategorien unterteilt:

- indirekter physikalischer Zugriff: Hierzu gehören zum Beispiel die ODB-II Diagnoseschnittstelle und die Eingänge des Unterhaltungssystems (CD, USB, iPod).
- kabelloser Zugriff über kurze Distanzen: Beispiele hierfür sind Bluetooth, WiFi, Remote-Keyless-Entry und die kabellose Überwachung des Reifendrucks.
- kabelloser Zugriff über weite Distanzen: GPS, Digital Radio, Traffic Message Channel (TMC) sind in diesem Bereich Beispiele für Informationen welche an alle Fahrzeuge verteilt werden. Zusätzlich besitzen moderne Autos aber auch adressierbare Zugriffsmöglichkeiten über Mobilfunk.

Unter Zuhilfenahme von Reverse-Engineering und Debugging gelingt es ihnen in allen drei Bereichen Zugriff auf das Fahrzeugnetz zu erhalten und über dieses zu Kommunizieren. Dies geschieht entweder über eine CD mit einer speziellen WMA-Datei, Lücken im Bluetooth-Stack der Freisprechanlage oder eine Mobilfunkverbindung. Mit dem Wissen welche Manipulationen getätigt werden können muss klar sein, dass eine Kontrolle über ein bestimmtes Fahrzeug aus beliebiger Entfernung möglich sein kann.

Durch die Einführung immer neuer Technologien zur Verbesserung von Komfort und Funktionssicherheit entstehen immer neue Schnittstellen. Beispiele sind die Kommunikation zwischen Fahrzeugen und zwischen Fahrzeugen und Infrastruktur. Daraus werden auch immer mehr Schwachstellen entstehen. Die Komplexität moderner Fahrzeugnetze führt zu einer gesteigerten Gefahr im Bereich der Informationssicherheit. Zukünftige Netze müssen die Verletzlichkeit durch Angriffe von Außen verhindern können.

3.2. Schutzkonzepte

Der Fokus bei Konzepten zum Schutz vor Angriffen wie denen aus Kapitel 3.1 liegt auf Netzen der nächsten Generation. Diese sind Ethernet-basiert und haben den Vorteil, dass es erprobte Technologien aus der IT-Sicherheit gibt. Diese können zu Rate gezogen werden um viele Risiken eliminieren.

In der Arbeit von Kleberger u. a. (2011) wird aber erst einmal der momentane Stand diskutiert. Nachdem klar ist, dass ein Fahrzeug massiv anfällig für Angriffe ist wird hier die Basis möglicher Lösungen erarbeitet. Die besonderen Herausforderungen in diesem Feld sind unabhängig von der Netztechnologie. Denn ECUs haben eine begrenzte Leistung, sollen weiterhin so günstig wie möglich sein und regelmäßige Softwareupdates können nicht durchgeführt werden. Daraus resultiert, dass Lösungen über einen sehr langen Zeitraum gültig bleiben müssen. Das Hauptziel ist die Daten innerhalb des Fahrzeugnetzes verschlüsselt zu übertragen um es zu Schützen. Aber auch das Zuverlässige erkennen von Teilen des Systems die kompromittiert wurden kann viele Gefahren für Mensch und Maschine abwenden. Im Ethernet-Netzwerk werden zumindest die Bandbreiten des Mediums massiv vergrößert und viele Technologien aus dem Werkzeugkasten IT-Sicherheit einfacher einsetzbar.

Skopik u. a. (2012) setzen direkt an einer speziellen Echtzeit-Ethernet-Protokoll-Familie an. Dieses heißen „Time-Triggered“(TT) und der Repräsentant TTE wurde bereits kurz in Kapitel 2.2 vorgestellt. Für diese Protokolle wird eine Konzept vorgestellt um die Informationssicherheit zu gewährleisten. Diese TT-Protokolle basieren auf einer globalen Uhr welche zwischen allen teilnehmenden Geräten synchronisiert sein muss. Nachrichten höchster Priorität werden nur zu den statisch konfigurierten Zeiten versendet und empfangen. Ein große Schwachstelle ist also die Uhrensynchronisation, welche zu jeder Zeit stimmen muss. Ein Vorteil ist aber das ein Switch nur vorher Konfigurierte Pakete zu den definierten Zeiten durchlässt. Der erste vorgestellte Schritt zum Schutz der Kommunikation ist, dass sich die Geräte eines Netzwerks gegenseitig Authentifizieren um den von ihnen versendeten Nachrichten zu Vertrauen. Im Schritt zwei muss die Synchronisation der Zeit abgesichert sein. Der Switch ist nun des Kernelement für die Informationssicherheit im Netzwerk und kann neben der Überprüfung des Timings der Pakete auch deren Integrität prüfen. Damit ist die **Datenintegrität** und die **Systemverfügbarkeit** erfüllt. Die Anwendungen auf den Endknoten setzten Ende-zu-Ende Authentifizierung und Verschlüsselung darauf auf. Auf diese weise wird auch **Informationsvertraulichkeit** erreicht.Dieses Gesamtkonzept kann also in einem reinen Time-Triggered-Netzwerk eine informationssichere Kommunikation umsetzen.

Ein konkreter Ansatz von Bouard u. a. (2012) wird sogar eine mögliche Middleware-Unabhängige Erweiterung vorgestellt, welches die Sicherheit von rein IP-basierter Kommunikation im Auto umsetzen soll.

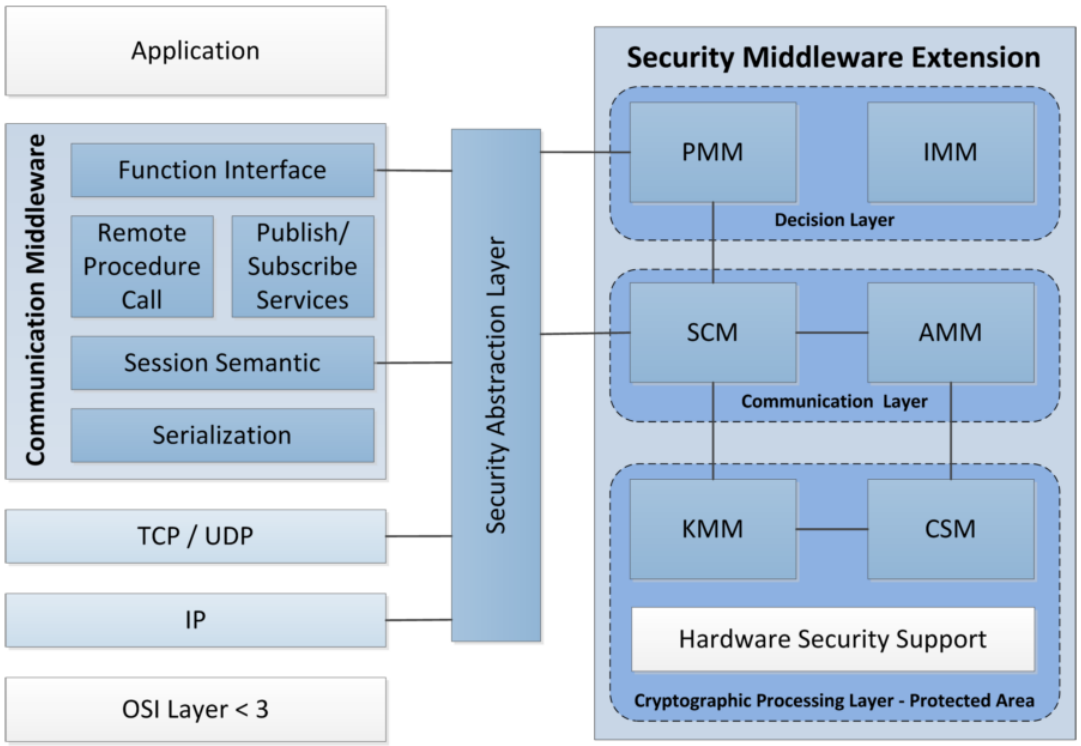


Abbildung 3.1.: Middleware-Erweiterung(Bouard u. a. (2012))

Die Abbildung 3.1 zeigt den in der Arbeit vorgestellten Aufbau. Wie zu sehen setzt die Erweiterung ab der IP-Schicht an. Dadurch ist das Konzept mit unterschiedlichen Ethernet-Protokollen realisierbar. Die „Communication Middleware“-, „TCP/UDP“- und die „IP“-Schicht kommunizieren über das „Security Abstraction Layer“ mit der „Security Middleware Extension“. Bei Letzterer wird der untersten Schicht(“Cryptographic Processing Layer“) vertraut. Das bedeutet, dass die Hardware als Sicher angenommen werden muss. Hier befindet sich das Modul zur Verwaltung von Schlüsseln(KMM) und zur Ver- und Entschlüsselung(CSM). Damit ist die **Informationsvertraulichkeit** sicher gestellt. Darüber befindet sich das „Communication Layer“. Dieses Organisiert die sicheren Kommunikationskanäle(SCM) und die Authentifizierung(AMM). Auf diese weise kann die **Datenintegrität** erfüllt werden. Die oberste Schicht (“Decision Layer“) besitzt die Rechteverwaltung(PMM) und Erkennung von Sicherheitsverletzungen(IMM). Die **Systemverfügbarkeit** hängt stark davon ab welches Protokoll unterhalb

von IP für die Kommunikation eingesetzt wird. Durch die Modularität lassen sich verschiedene Steuergeräte mit unterschiedlichen Anforderungen realisieren.

Die Konzepte zum Schutz der Informationssicherheit sind in den meisten Fällen nicht umgesetzt. Darum kann die Zuverlässigkeit nicht endgültig festgestellt werden. Des weiteren sind sie teilweise sehr wage formuliert und geben keine Auskunft über konkrete Umsetzungsvorschläge. Dazu kommt noch das sie meistens nur Lösungen für Homogene Netze anbieten. Die Einführung von Ethernet im Auto kann aber nur schrittweise erfolgen. Erste Gehversuche werden sehr wahrscheinlich mit Ethernet als „Backbone“ für Verschiedene Busse gewagt. Des weiteren müssen in Zukunft solche Lösungen den echten Anforderungen einer Fahrzeugumgebung standhalten können. Dies muss natürlich anhand von konkreten Umsetzungen getestet werden.

3.3. Datenschutz

Der Datenschutz ist, obwohl in einem geschütztem System einfach zu realisieren, ein Kernthema in allen Bereichen der Informationssicherheit. Allein die Erfüllung der **Informationsvertraulichkeit** eines solchen Systems würde den Datenschutz implizieren. Aber hier ist vor allem die Frage welche Daten geschützt werden müssen. Es ist zusätzlich nicht immer klar vor wem diese Daten geschützt werden sollen und wer ein Recht auf Zugriff hat.

In einem Fahrzeug mit vielen, miteinander kommunizierenden, ECUs fallen auch viele Informationen über das Fahrverhalten oder den Fahrzeugzustand an. Eine Frage ist ob diese Informationen gespeichert werden dürfen (zB. in einer Art Blackbox). Wer darf oder hat dann das Recht auf Zugriff? Polizei, Versicherung, Werkstatt oder nur der Besitzer? Diese Fragen lassen sich Heute noch nicht beantworten. Zumindest ist die Diskussion in der Politik gestartet (vgl. Stern). Hier muss geklärt werden welche Daten privat sind und welche unter was für Umständen von wem gelesen werden dürfen. Ansonsten wird es keinen wirklichen Datenschutz im Fahrzeug geben.

In der Umfrage von Pell u. a. (2012) wird Untersucht in wie weit das Sammeln von Daten im Auto von den Benutzer akzeptiert wird. Im Ergebnis würden 58% dies bei einem Firmenwagen in Ordnung finden. Bei privaten Fahrzeugen sind es nur noch 45%. Weiterhin sind 70% der Befragten dafür, dass die Daten durch staatliche Institutionen gesammelt werden dürfen. Darauf folgt mit 66% die Polizei, mit 40% eine private Firma und mit nur 24% der Autohersteller. Diese Zahlen zeigen das komplexe Zusammenspiel, dass bei der Entwicklung von neuen Technologien beachtet werden muss um die Akzeptanz und damit den Erfolg solcher zu garantieren.

Der Datenschutz, im Kontext von in Fahrzeugnetzen anfallenden Daten, ist also weniger eine technologische als viel mehr eine Frage der Definition. Der Gesetzgeber muss einen Rahmen schaffen um festzulegen welche dieser anfallenden Informationen von privater Natur sind. Des weiteren müssen auch die Fahrzeughersteller auf einen verantwortungsvollen Umgang mit diesen Daten achten um die Akzeptanz ihrer Kunden zu behalten.

4. Zusammenfassung & Ausblick

Stand der Technik im Auto sind Netzwerke aus verschiedenen heterogenen Bussen. Diese werden durch immer neue Technologien immer komplexer. Komplexe Netze führen in modernen Fahrzeugen zwar zu funktionssicheren aber immer weniger informationssicheren Systemen. Gegenwärtige Autos sind massiv Angreifbar und unauthorisiert Kontrollierbar. Es gibt aber Konzepte um diesen Stand zu überwinden. Viele davon setzen schon auf Ethernet-Netzwerke auf. Denn damit können die Anforderungen an ein Fahrzeugnetz der Zukunft erfüllt werden. Die Konzepte müssen aber konkretisiert, umgesetzt und untersucht werden um deren umfassende Sicherheit garantieren zu können. Im Rahmen des Datenschutzes fehlt es vor allem an klaren Definitionen die festlegen welche Informationen genau Geschützt werden müssen.

In Zukunft werde ich mich vor allem weiter in das Thema Schutzkonzepte und Umsetzungen einarbeiten. Denn es sind viele genau Analysen von Schwachstellen vorhanden und der Datenschutz ist wie bereits erwähnt vor allem eine Frage der Definition. Im Bereich von konkreten Konzepten und Umsetzungen ist dafür aber noch viel Arbeit gefordert.Ein fortschritt wäre zum Beispiel eine Kombination von Sicherheitskonzept und Netzwerkprotokoll untersuchen. Ein großes Risiko bei der Entwicklung von Lösungen ist es gefährliche Angriffsszenarien zu übersehen oder die Komplexität zu unterschätzen. Im ersten Schritt muss dafür vor allem eine strukturierte Vorgehensweise festgelegt werden.

A. Anhang

A.1. Kommunikationstopologien im Fahrzeug

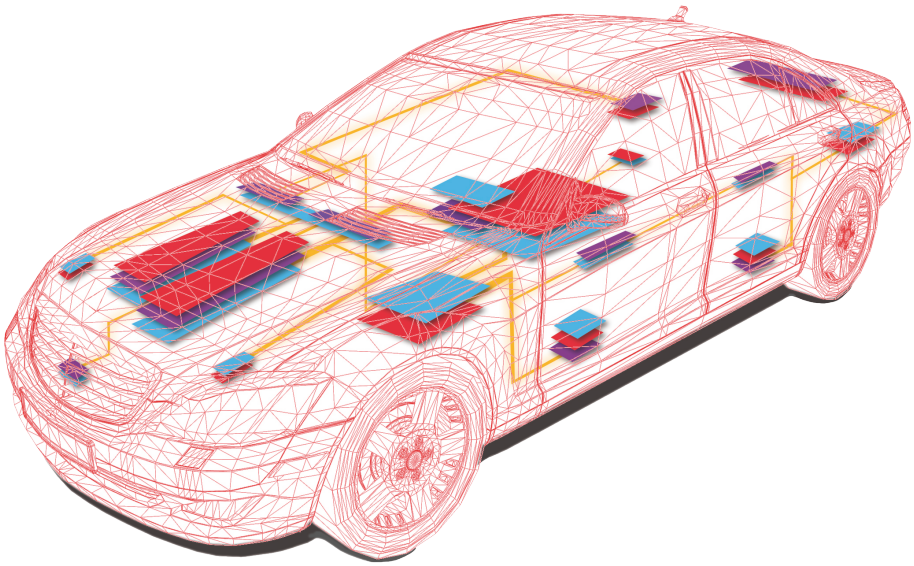
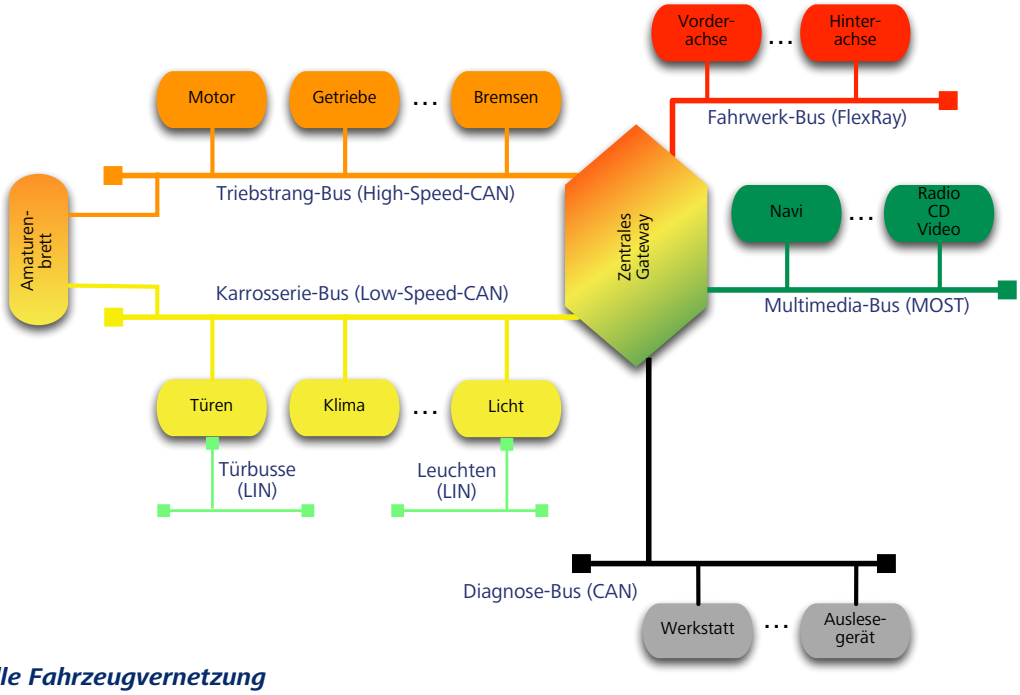
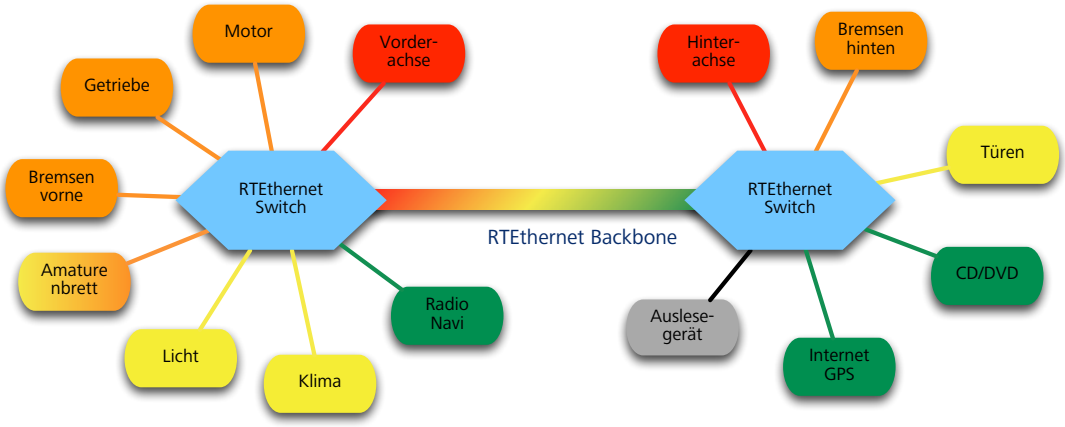


Abbildung A.1.: Beispiel des Innenlebens eines Autos(CoRE RG)



(a) Heterogene Bustopologie



(b) Ethernet Netzwerktopologie

Abbildung A.2.: Kommunikationstopologien von Fahrzeugen im Vergleich(CoRE RG)

Literaturverzeichnis

[Bissmeyer u. a. 2013] Bissmeyer, N. ; Schroder, K.H. ; Petit, J. ; Mauthofer, S. ; Bayarou, K.M.: Short paper: Experimental analysis of misbehavior detection and prevention in VANETs. In: *Vehicular Networking Conference (VNC), 2013 IEEE*, December 2013, S. 198–201

[Bouard u. a. 2012] Bouard, Alexandre ; Glas, Benjamin ; Jentzsch, Anke ; Kiening, Alexander ; Kittel, Thomas ; Stadler, Franz ; Weyl, Benjamin: Driving Automotive Middleware Towards a Secure IP-based Future. In: *10th conference for Embedded Security in Cars (Escar'12)*. Berlin, Germany, November 2012. – URL https://www.sec.in.tum.de/assets/staff/alexandre/Escar_Paper_final.pdf

[Bruenglinghaus und Redaktion Springer fuer Professionals] Bruenglinghaus, Christiane ; Redaktion Springer fuer Professionals: *Am Ethernet im Auto fuehrt kein Weg vorbei.* – URL http://www.springerprofessional.de/am-ethernet-im-auto-fuehrt-kein-weg-vorbei/4979586.html. – Zugriffsdatum: 2014-07-22

[Bundesamt fuer Sicherheit in der Informationstechnik] Bundesamt fuer Sicherheit in der Informationstechnik: *IT-Grundschutz-Kataloge.* – URL www.bsi.de/gshb. – Zugriffsdatum: 2014-07-21

[Checkoway u. a. 2011] Checkoway, Stephen ; Mccoy, Damon ; Kantor, Brian ; Anderson, Danny ; Shacham, Hovav ; Savage, Stefan ; Koscher, Karl ; Czeskis, Alexei ; Roesner, Franziska ; Kohno, Tadayoshi: Comprehensive Experimental Analyses of Automotive Attack Surfaces. In: *USENIX Security* (2011). – URL http://static.usenix.org/events/sec11/tech/full_papers/Checkoway.pdf

[CoRE RG] CoRE RG: *Communication over Real-time Ethernet.* – URL http://core.informatik.haw-hamburg.de

[Eckert 2013] Eckert, Claudia: *IT-Sicherheit Konzepte - Verfahren - Protokolle.* 8., aktualisierte und korr. Aufl. Muenchen : Oldenbourg, 2013

[EVITA] EVITA: *E-safety vehicle intrusion protected applications*. – URL http://www.evita-project.org. – Zugriffsdatum: 2014-05-05

[IEEE 802.1 TSN Task Group a] IEEE 802.1 TSN Task Group: *IEEE 802.1Qbu - Frame Preemption*. – URL http://www.ieee802.org/1/pages/802.1bu.html

[IEEE 802.1 TSN Task Group b] IEEE 802.1 TSN Task Group: *IEEE 802.1Qbv - Enhancements for Scheduled Traffic*. – URL http://www.ieee802.org/1/pages/802.1bv.html

[Institute of Electrical and Electronics Engineers 2011] Institute of Electrical and Electronics Engineers: IEEE 802.1BA - IEEE Standard for Local and metropolitan area networks - Audio Video Bridging (AVB) Systems / IEEE. September 2011 (IEEE 802.1BA-2011). – Standard. – ISBN 987-0-7381-7639-8

[ISO 27001 2013] : *Information technology – Security techniques – Information security management systems – Requirements*. 2013

[Kleberger u. a. 2011] Kleberger, P. ; Olovsson, T. ; Jonsson, E.: Security aspects of the in-vehicle network in the connected car. In: *Intelligent Vehicles Symposium (IV), 2011 IEEE*, June 2011, S. 528–533. – ISSN 1931-0587

[Koscher u. a. 2010] Koscher, K. ; Czeskis, A. ; Roesner, F. ; Patel, S. ; Kohno, T. ; Checkoway, S. ; McCoy, D. ; Kantor, B. ; Anderson, D. ; Shacham, H. ; Savage, S.: Experimental Security Analysis of a Modern Automobile. In: *2010 IEEE Symposium on Security and Privacy (SP)*, May 2010, S. 447–462. – ISSN 1081-6011

[Pell u. a. 2012] Pell, A ; Starkl, F. ; Menrad, M.: A field study on the acceptance of extended floating car data for real-time monitoring traffic conditions. In: *Sustainable Systems and Technology (ISSST), 2012 IEEE International Symposium on*, May 2012, S. 1–4. – ISSN 2157-524X

[PRESERVE] PRESERVE: *Preparing Secure Vehicle-to-X Communication Systems*. – URL http://www.preserve-project.eu. – Zugriffsdatum: 2014-05-05

[SEIS] SEIS: *Sicherheit in Eingebetteten IP-basierten Systemen*. – URL http://strategiekreis-elektromobilitaet.de/public/projekte/seis. – Zugriffsdatum: 2014-05-05

[Skopik u. a. 2012] Skopik, Florian ; Treytl, Albert ; Geven, Arjan ; Hirschler, Bernd ; Bleier, Thomas ; Eckel, Andreas ; El-Salloum, Christian ; Wasicek, Armin: Towards Secure Time-Triggered Systems. In: Ortmeier, Frank (Hrsg.) ; Daniel, Peter (Hrsg.): *Computer Safety, Reliability, and Security* Bd. 7613. Springer Berlin Heidelberg, 2012, S. 365–372. – URL http://dx.doi.org/10.1007/978-3-642-33675-1_33. – ISBN 978-3-642-33674-4

[Society of Automotive Engineers - AS-2D Time Triggered Systems and Architecture Committee 2011] Society of Automotive Engineers - AS-2D Time Triggered Systems and Architecture Committee: *Time-Triggered Ethernet AS6802.* SAE Aerospace. November 2011. – URL http://standards.sae.org/as6802/

[Stern] Stern: *Maas will glaeserne Autofahrer vermeiden.* – URL http://www.stern.de/politik/deutschland/datenschutz-im-auto-maas-will-glaeserne-autofahrer-vermeiden-2122048.html. – Zugriffsdatum: 2014-07-22

[Studnia u. a. 2013] Studnia, I. ; Nicomette, V. ; Alata, E. ; Deswarte, Y. ; Kaaniche, M. ; Laarouchi, Y.: Security of embedded automotive networks: state of the art and a research proposal. In: *SAFECOMP 2013 - Workshop CARS (2nd Workshop on Critical Automotive applications : Robustness and Safety) of the 32nd International Conference on Computer Safety, Reliability and Security*, URL http://hal.archives-ouvertes.fr/hal-00848234, September 2013

Hiermit versichere ich, dass ich die vorliegende Arbeit ohne fremde Hilfe selbständig verfasst und nur die angegebenen Hilfsmittel benutzt habe.

Hamburg, 25. Juli 2014 Philipp Meyer