DHBW
Duale Hochschule
Baden-Württemberg
Mannheim

Automotive Security

Studienarbeit

für die Prüfung zum

Bachelor of Science

des Studienganges Informatik / Angewandte Informatik

an der

Dualen Hochschule Baden-Württemberg Karlsruhe

von

Jonas Kölblin

Abgabedatum 22. Mai 2023

Bearbeitungszeitraum	24 Wochen
Matrikelnummer	7150881
Kurs	TINF20B5
Ausbildungsfirma	SICK AG Waldkirch
Gutachter der Studienakademie	Ralf Brune

Erklärung

Ich versichere hiermit, dass ich meine Studienarbeit mit dem Thema: »Automotive Security« selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Ich versichere zudem, dass die eingereichte elektronische Fassung mit der gedruckten Fassung übereinstimmt.

Ort Datum Unterschrift

Abstract

abstract

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

Kapitel 1

Einführung

Autos stellen einen sehr großen Anteil der Infrastruktur heutzutage dar. In einer Umfrage im Jahr 2022 gaben über 70 Prozent der Befragten an, ein eigenes Auto zu besitzen [vgl. Statista 2022]. Unzählige Autos sind täglich auf den Straßen unterwegs. Im Zuge der Digitalisierung werden moderne Autos zunehmend mit neuen Features und Technologien ausgestattet, mit dem Ziel, die Bedienung des Fahrzeugs möglichst komfortabel zu gestalten. Das Auto nimmt der fahrenden Person immer mehr Aufgaben ab, wie zum Beispiel das Abblenden, Einparken oder im Fall von selbst-fahrenden Autos sogar das Steuern des Fahrzeugs an sich. Zudem steigt die Anzahl der Entertainmentfeatures, wie zum Beispiel das Verbinden eines Mobiltelefons mit dem Fahrzeug. Ein Effekt dieser Entwicklung ist, dass zum einen die einzelnen Fahrzeugteile intern zunehmend miteinander vernetzt werden. Zum anderen steigt aber auch die Relevanz der Kommunikation des Fahrzeugs mit externen Systemen. Insgesamt sind die elektronischen Systeme in heutigen Fahrzeugen deutlich komplexer und bieten mehr Schnittstellen als noch vor 20 Jahren. Diese zunehmende Komplexität schafft neue Angriffsflächen für Cyberangriffe. Experimente in der Vergangenheit wie zum Beispiel von Charlie Miller und Chris Valasek [vgl. Greenberg 2015] haben jedoch bereits gezeigt, dass die Sicherheitsmaßnahmen der Automobilhersteller oft nicht ausreichen, um die Fahrzeuge zuverlässig gegen solche Angriffe zu schützen.

1.1 Motivation

Eines der schockierendsten Ereignisse der letzten Jahre im Bereich der Automotive Cyber Security war die oben erwähnte Aktion von Miller und Valasek im Jahr 2015 [vgl. Greenberg 2015]. Den beiden Hackern gelang es, einen Jeep Cherokee über das Internet

zu kompromittieren. Dabei verschafften sie sich nicht nur Zugriff zur grundlegenden Board-Elektronik wie dem Radio oder den Scheibenwischern, sondern es gelang ihnen auch, die Bremsen und den Motor zu deaktivieren. Sie konnten das Fahrzeug fernsteuern und der eingeweihte Fahrer war ihnen hilflos ausgeliefert. Dieses Experiment fand natürlich nur zu Forschungs- und Demonstrationszwecken statt. Aktionen wie diese zeigen jedoch anschaulich, wozu eine Person mit böswilligen Absichten theoretisch in der Lage wäre. Sicherheitslücken wie diese können schlimmstenfalls zum Verlust von Menschenleben führen. Aus diesem Grund ist es wichtig, das dem Thema der Automotive Security noch mehr Aufmerksamkeit gewidmet wird. Hersteller müssen sich intensiver mit den durch die zunehmende Vernetzung der Autos entstandenen Angriffsmöglichkeiten beschäftigen und Sicherheitslücken bestenfalls präventiv, ansonsten so schnell wie möglich, schließen. Daher widmet sich diese Arbeit diesen besagten Angriffsmöglichkeiten.

1.2 Zielsetzung

Diese Arbeit soll einen Überblick über die Angriffsflächen eines Automobils sowie über einige Lösungsansätze für diese Schwachstellen schaffen. Hierzu erfolgt zunächst eine Erläuterung der notwendigen theoretischen Grundlagen wie dem Aufbau des internen Netzwerks eines Automobils sowie notwendigen Grundlagen der Cyber Security. Anschließend sollen die verschiedenen Angriffsmöglichkeiten eines Autos aufgezeigt werden. Darauf folgt die Sammlung und Evaluierung von Schutzmaßnahmen gegen diese Angriffsmöglichkeiten mit Blick auf die Frage, wo die Hersteller ansetzen können oder müssen, um ihre Autos sicherer zu gestalten.

Kapitel 2

Grundlagen

In diesem Kapitel sollen die für das weitere Verständnis notwendigen theoretischen Grundlagen erläutert werden. Dazu gehört zunächst der Aufbau des Netzwerks in einem Fahrzeug. Des Weiteren werden relevante Grundlagen der Cyber Security erklärt.

2.1 Automotive Networking

Im Inneren von Autos befinden sich heutzutage eine Vielzahl elektronischer Systeme, von denen jedes mit benachbarten Komponenten kommunizieren kann. Die einzelnen elektronischen Systeme werden als Electronic Control Units (ECUs) bezeichnet. Moderne Autos enthalten in der Regel über 50 verschiedene ECUs [vgl. Miller und Valasek 2013, S. 6]. Da diese Kontrolleinheiten zum Teil lebensentscheidende Aufgaben übernehmen, muss die Kommunikation zwischen den Einheiten möglichst in Echtzeit erfolgen.

Data-rates supported by the low-latency in-vehicle communication protocols.

In-vehicle Communication Protocol	Maximum Data-rate
Local Interconnect Network (LIN)	20 kbit/s
Controller Area Network (CAN)	1 Mbit/s
CAN-FD (Flexible Data)	5 Mbit/s (data), 1 Mbit/s (arbitration, ack)
CAN XL	10 Mbit/s (data)[a], 1 Mbit/s (arbitration, ack)
FlexRAY	10 Mbit/s
Ethernet with Time-Sensitive Networking	100 Mbit/s to 10 Gbit/s

Abbildung 2.1: Verschiedene Kommunikationsprotokolle in Automobil-Netzwerken
Quelle: [Mohammad Ashjaei u. a. 2021, S. 2]

Für die Vernetzung der ECUs kommen verschiedene Technologien zum Einsatz (siehe Abbildung 2.1). Die relevantesten davon werden im Folgenden genauer erläutert. Die wichtigste davon ist im Automotive-Bereich der sogenannte CAN-Standard.

2.1.1 Controller Area Network

Die elektronischen Kontrolleinheiten eines Autos sind typischerweise über einen oder mehrere Busse, die auf dem Controller Area Network (CAN)-Standard basieren, miteinander verbunden. Hierbei kommunizieren die ECUs über CAN-Pakete. Diese werden an alle Komponenten gesendet, welche dann jeweils basierend auf dem Inhalt entscheiden, ob das Paket für sie bestimmt ist oder nicht. Eine Identifikation der Quelle oder Authentisierung gibt es in diesem Standard nicht. [vgl. Miller und Valasek 2013, S. 7]
Generell wird meistens zwischen High Speed CAN und Low Speed CAN unterschieden. High Speed CAN wird eingesetzt, wenn bei der Übertragung hohe Geschwindigkeit benötigt wird, beispielsweise bei sicherheitskritischen Anwendungsfällen. Außerdem wird bietet sich die Verwendung von High Speed CAN bei der Übertragung von großen Datenmengen an. In Abbildung 2.1.1 ist das CAN-Netzwerk eines 2010 Ford Escape dargestellt. Das abgebildete Netzwerk verfügt über zwei Busse, einen medium speed (MS) und einen high speed (HS) CAN-Bus. Beide Busse enden hier im Data Link Connector (DLC) (siehe Kapitel 2.2.1). In Automotive Netzwerken lassen sich zwei Arten von CAN-Paketen finden: normale CAN-Pakete und diagnostische CAN-Pakete.

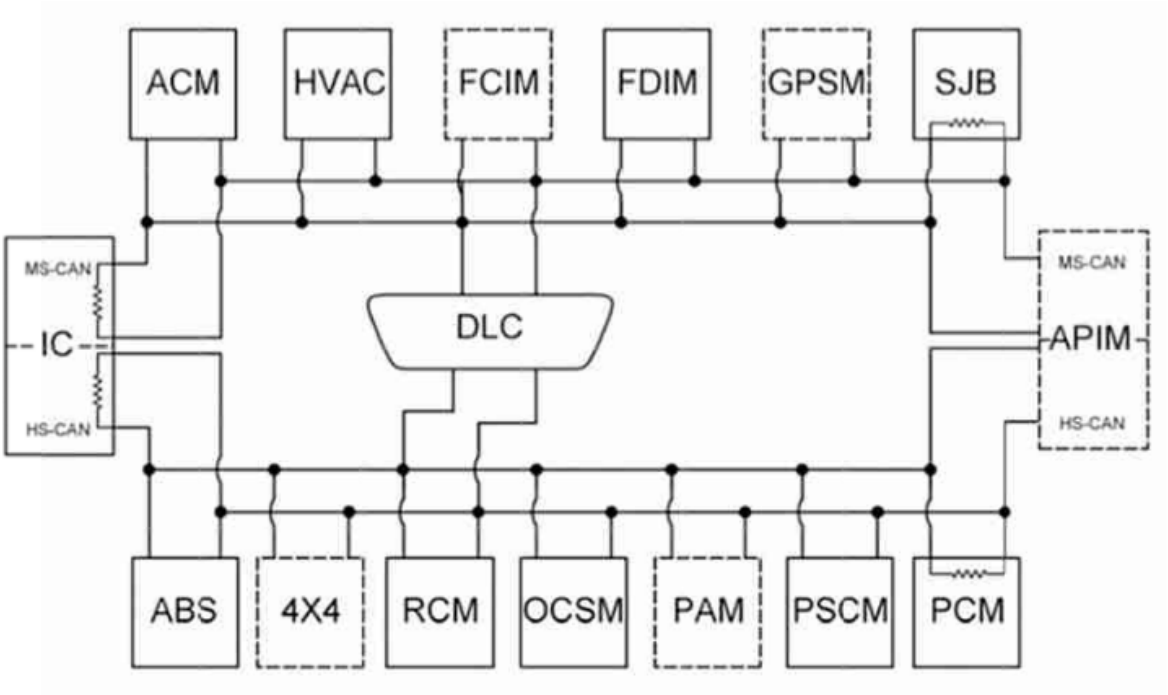

Abbildung 2.2: Beispiel des CAN-Netzwerks eines 2010 Ford Escape
Quelle: [Miller und Valasek 2013, S. 19]

Normale CAN-Pakete

Normale Pakete werden von ECUs gesendet und können entweder Informationen oder Befehle enthalten. Typischerweise werden sie alle Millisekunden gesendet. Auf Anwendungsebene enthalten die CAN-Pakete einen Identifier, die zu übertragenden Daten und manchmal noch eine Prüfsumme, um sicherzustellen, dass das Paket korrekt übertragen wurde. Der Identifier gibt sowohl an, für welche ECUs das Paket bestimmt ist, als auch, welche Priorität das Paket hat. [vgl. Miller und Valasek 2013, S. 9]
Das Format einer CAN-Botschaft ist in Abbildung 2.1.1 dargestellt. Es besteht aus folgenden Bestandteilen:

Header CAN ist ein Broadcast-System, bei dem jeder Sender seine Botschaften mit einem eindeutigen Message Identifier markiert.

Message Identifier Der Message Identifier kennzeichnet eine Botschaft und dient zur eindeutigen Identifizierung. Er kann entweder 11 Bit (CAN 2.0A) oder 29 Bit (CAN 2.0B) lang sein und enthält zusätzlich 1 bis 3 Steuerbits.

Control Bits Die Steuerbits im Control-Feld umfassen den Data Length Code (DLC), der die Anzahl der übertragenen Nutzdatenbytes angibt, sowie eine 15-Bit-Prüfsumme, auch genannt Cyclic Redundancy Check (CRC) zur Fehlererkennung.

Payload Die Nutzdaten (Payload) einer Botschaft können zwischen 0 und 8 Datenbytes umfassen.

Acknowledge und End of Frame Die CAN-Controller der Empfänger senden eine positive Empfangsbestätigung oder eine Fehlermeldung (Error Frame) innerhalb des Acknowledge und End of Frame Felds.

Stuffing Bits Stuffing Bits werden verwendet, um den Bittaktgenerator von Empfängern zu synchronisieren. Sie werden eingefügt, um sicherzustellen, dass nicht mehr als fünf aufeinanderfolgende Bits denselben Wert haben. [Zimmermann und Schmidgall 2014, S. 61 ff.]

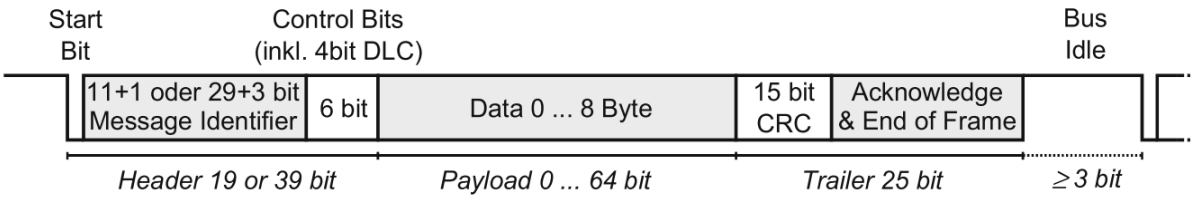

Abbildung 2.3: Format einer CAN-Botschaft
Quelle: [Zimmermann und Schmidgall 2014, S. 61]

Diagnostische CAN-Pakete

Diagnostische Pakete tauchen während des normalen Betriebs des Autos im Normalfall nicht auf. Sie werden von Diagnose-Werkzeugen gesendet, die beispielsweise von Mechanikern genutzt werden um mit den ECUs im Auto zu kommunizieren. So können Mängel und Fehlfunktionen entdeckt oder andere Informationen gewonnen werden. Das Format von diagnostischen CAN-Paketen ähnelt dem von normalen Paketen, erfolgt jedoch meist nach strengeren Konventionen. Standards hierfür sind zum Beispiel ISO-TP, ISO 14229 und ISO 14230. [vgl. Miller und Valasek 2013, S. 10]

2.1.2 Local Interconnect Network

Ein weiteres relevantes Protokoll im Automotive Bereich ist das Local Interconnect Network (LIN) Protokoll. Es wurde 1998 in Zusammenarbeit von Audi, BMW, Daimler-Chrysler, Volvo, Volkswagen, VCT und Motorola entwickelt mit dem Ziel, ein möglichst kosteneffizientes Kommunikationsprotokoll zu schaffen [Fijalkowski 2011, S. 57]. Das LIN-Protokoll basiert auf dem Serial Connections Interface Datenformat und ist in einer Single Master/Multiple Slaves Architektur aufgebaut. Das bedeutet, dass eine elektronische Kontrolleinheit als Masterknoten fungiert und andere elektronische Slave-Einheiten miteinander verbindet.

Aufbau

Nachrichtenpakete bestehen im LIN-Standard aus einem Header und einem Data Frame. Der Header enthält einen Synchronisation Break, ein Synchronisation Byte und einen Message Identifier. Die ersten beiden Bestandteile sind für die Nachrichtensynchronisierung notwendig. Der Identifier wird benötigt, damit Knoten erkennen können, ob eine Nachricht für sie bestimmt ist. Der Data Frame ist nach dem 8N1-Schema aufgebaut. Das bedeutet, dass jedes Paket ein Startbit, acht Datenbits, kein Paritätsbit und ein Stopbit besitzt. [Fijalkowski 2011, S. 58]
Im LIN-Standard sind drei Arten von Kommunikation erlaubt.

1. Master to Slave, beziehungsweise Master to Multiple Slaves
2. Slave to Master
3. Slave to Slave

Die Slaves können somit auch untereinander ohne Beiteiligung des Masters kommunizieren. [Fijalkowski 2011, S. 59]

Anwendung

LIN zeichnet sich wie oben erwähnt vor allem durch seine Kosteneffizienz aus. Allerdings bietet das Protokoll deutlich weniger Bandbreite als CAN. Somit wird es vor allem an Stellen im Fahrzeug eingesetzt, wo nicht viel Bandbreite notwendig ist. Beispielsweise wird LIN häufig für die Steuerung von Türen, Dach, Sitzen und dem Lenkrad verwendet. [Fijalkowski 2011, S. 59]
Für den Aufbau eines Netzwerks mit den zwei Protokollen gibt es zwei gängige Ansätze:

1. Mehrere ECUs werden über LIN mit einer zentralen ECU verbunden. Die Verbindung dieser zentralen ECUs erfolgt mit dem CAN-Standard.

2. Alle ECUs werden über LIN mit einer zentralen ECU verbunden.

Der zweite Ansatz ist skalierbarer, da ohne großen Aufwand neue Knoten hinzugefügt werden können. Der erste Ansatz ermöglicht jedoch eine deutlich höhere Bandbreite bei der Kommunikation zwischen den Einheiten. [Fijalkowski 2011, S. 58]

2.1.3 FlexRay

Der CAN Standard weist neben seinen Stärken auch einige Schwächen auf. Beispielsweise ist die realistisch erreichbare Datenrate beschränkt, zudem lassen sich sehr hohe Datenraten nur mit kurzen Stichverbindungen erreichen. Außerdem verfügt das System nur über einen Kanal und versagt somit bei Ausfall der Busverbindung. Aus diesen Gründen hielten viele Fachleute eine Neuentwicklung für notwendig und sinnvoll [Zimmermann und Schmidgall 2014, S. 96]. Daher wurde FlexRay als Ersatz für CAN entwickelt. In der Praxis wird es allerdings größtenteils mehr als Ergänzung als als vollständiger Ersatz eingesetzt [Zimmermann und Schmidgall 2014, S. 97]. Dies könnte an den höheren Kosten aufgrund größerer Komplexität von FlexRay liegen.s FlexRay ermöglicht Aufbauten in Linien- und Sterntopologien. Diese können einkanalig oder zweikanalig sein.
Der Aufbau einer FlexRay-Botschaft ist in Abbildung 2.1.3 veranschaulicht. Zu Beginn einer FlexRay-Botschaft stehen 5 Steuerbits, in denen Sonderinformationen über die Nachricht angezeigt werden können. Anschließend folgen die Frame ID mit dem Zeitslot der Botschaft, die Nutzdatenlänge, eine Cyclic-Redundancy-Check-Prüfsumme und ein Zykluszähler.

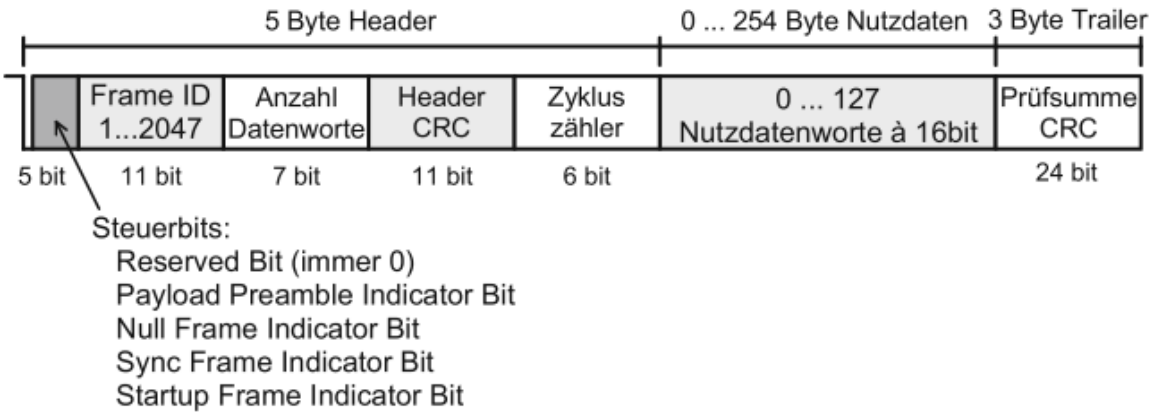

Abbildung 2.4: Aufbau einer FlexRay-Botschaft
Quelle: [Zimmermann und Schmidgall 2014, S. 101]

2.1.4 Media Oriented System Transport

Das Media Oriented Systems Transport (MOST) Protokoll wird vor allem in Infotainment-Systemen von Autos eingesetzt. Anstelle von Kabeln werden hier Lichtwellenleiter verwendet. Somit ist das Signal unempfänglich gegenüber elektromagnetischer Einstrahlung. Es wird unterschieden zwischen MOST25, MOST50 und MOST150, welche sich in Paketgröße und Bandbreite unterscheiden. Ein MOST-Netzwerk ist meist als Ringtopologie aufgebaut (vergleiche Abbildung 2.1.4). Auch im MOST-Protokoll gibt es Master- und Slave-Knoten. Der Master-Knoten ist häufig ein Gateway zu einem CAN-Bus.

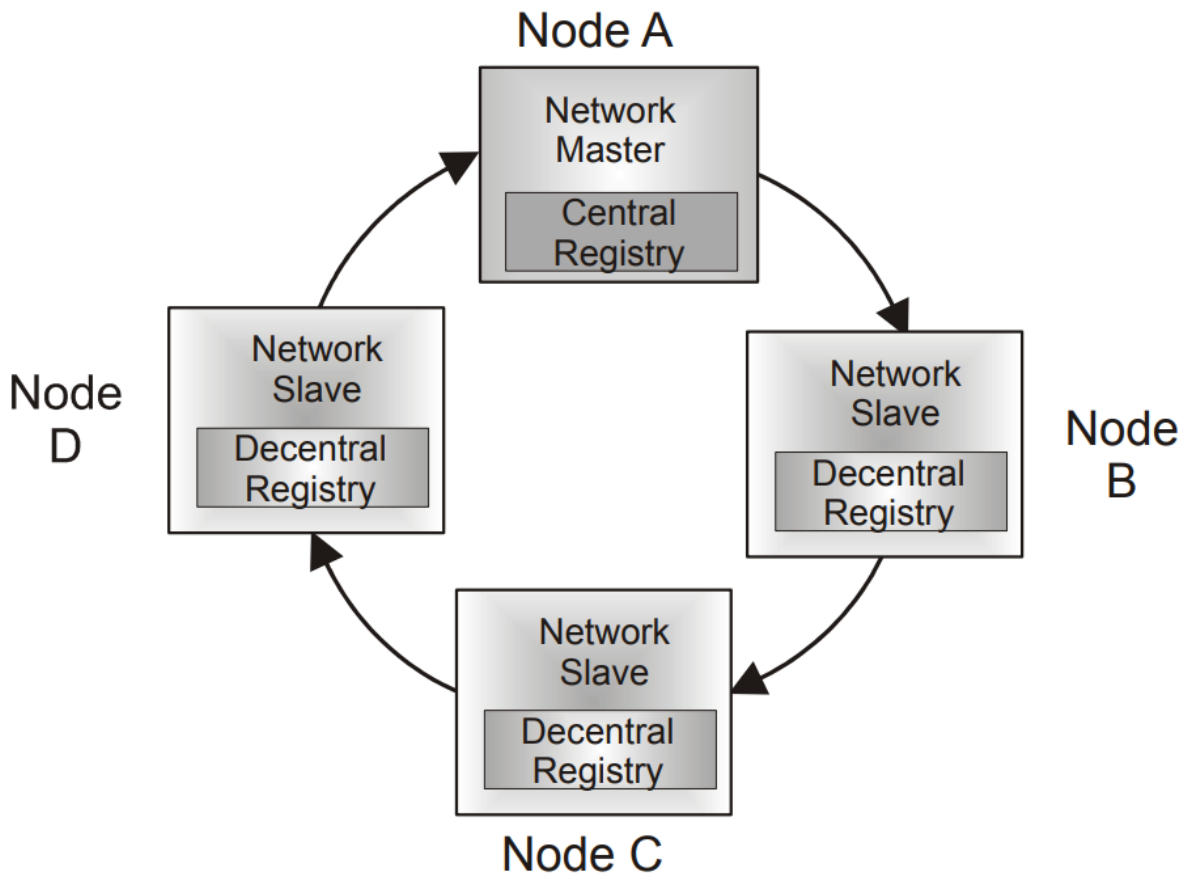

Abbildung 2.5: Ringtopologie eines MOST-Bus
Quelle: [Grzemba 2007, S. 40]

Paketaufbau

Der Aufbau eines MOST25-Pakets ist in Abbildung 2.1.4 dargestellt. Es folgt eine kurze Erklärung der Einzelnen Bestandteile.

Anfangsfeld (Preamble) Das Anfangsfeld wird vom TimingMaster generiert und dient der Synchronisation der Slaves.

Abgrenzungsfeld (Boundary Descriptor) Das Abgrenzungsfeld definiert die in Vier-Byte-Schritten verschiebbare Grenze zwischen Stream- und Paketdaten.

Datenfeld (stream data, packet data) Das Datenfeld besteht aus 60 Bytes die nach Bedarf zwischen Streamdaten und Paketdaten aufgeteilt werden können.

Kontrollbytes (Frame Control) Die Kontrollbytes am Ende dienen der Kontrolle des Frames.

Paritätsfeld (Parity Bit) Das Paritätsfeld ermöglicht das Erkennen von Bit-Fehlern im Frame.

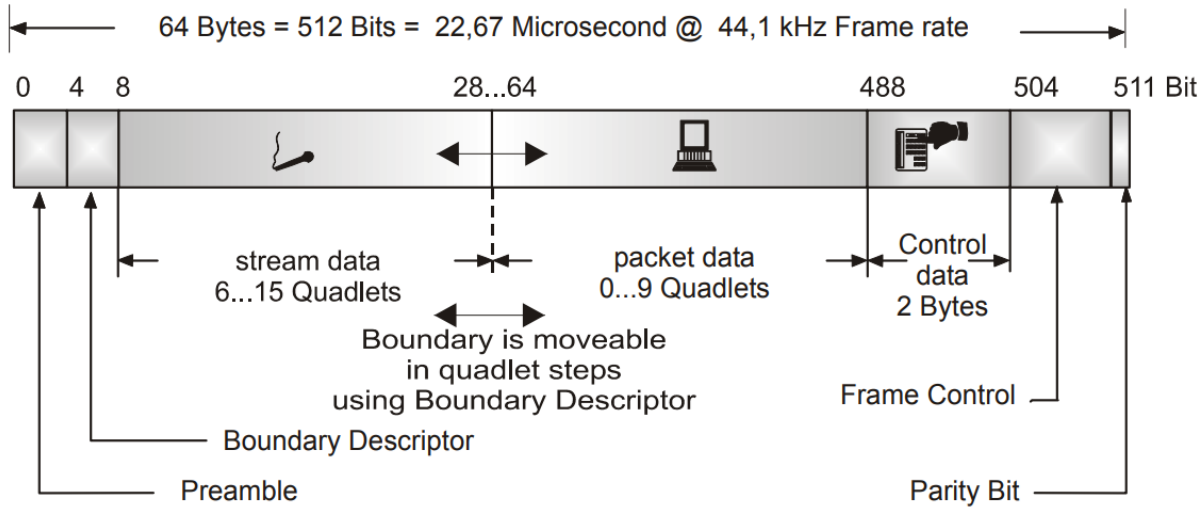

Abbildung 2.6: Aufbau eines MOST25-Pakets
Quelle: [Grzemba 2007, S. 88]

2.1.5 Automotive Ethernet

Die Vielzahl inkompatibler und nur in der Automobilindustrie verwendeter Lösungen resultierte in hohen Kosten und kontinuierlichem Weiterentwicklungsaufwand. Zudem steigt der Bandbreitenbedarf. Daher wird das im Bürobereich etablierte Konzept Ethernet/IP relevanter für den Automobilbereich. [Zimmermann und Schmidgall 2014, S. 138]
Die in diesem Standard verwendeten Protokolle Internet Protocol (IP), Transmission Control Protocol (TCP) und User Datagram Protocol (UDP) werden außerdem bereits von den meisten computerähnlichen Geräten unterstützt. Das ermöglicht eine transparente Kommunikation und vereinfacht die Integration von Consumergeräten erheblich

[Zimmermann und Schmidgall 2014]. Ethernet war ursprünglich ein Linienbussystem, wird heutzutage aber meistens als Sterntopologie mit Switches an Kopplungspunkten umgesetzt.
In Abbildung 2.1.5 ist der Aufbau eines Ethernet-Pakets dargestellt. Die Präambel und der Start Frame Delimiter spielen eine Rolle bei der Taktsynchronisation bei manchen Physical Layern. Die Ziel- und Quell-MAC-Adresse dienen der Geräteadressierung. Das VLAN-Tag erlaubt die Bildung von Unternetzen. Das Typfeld kennzeichnet den Typ des Inhalts des darauf folgenden Datenfelds. Das Datenfeld enthält den eigentlichen Nachrichteninhalt. Am Ende jedes Pakets befindet sich noch die Frame Check Sequence zur Detektion von Übertragungsfehlern. Beim Eintritt eines Übertragungsfehlers wird die Botschaft automatisch vom Empfänger verworfen. [Zimmermann und Schmidgall 2014, S. 140]

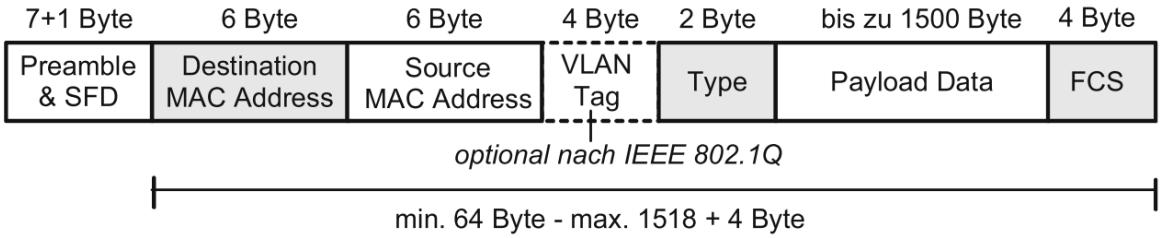

Abbildung 2.7: Aufbau eines Ethernet-Pakets
Quelle: [Zimmermann und Schmidgall 2014, S. 140]

2.2 Schnittstellen

Moderne Autos verfügen über eine Vielzahl von Schnittstellen, um eine Verbindung mit dem Fahrzeug herzustellen, sei es, um ein Multimediagerät zu verbinden oder zu Diagnosezwecken. Diese Schnittstellen können aber auch eventuell einem potentiellen Angreifer den Zugriff auf das Fahrzeugnetzwerk ermöglichen. Diese möglichen Angriffsvektoren können nach Checkoway et al [Checkoway u. a. 2011, S. 1] in drei Kategorien eingeteilt werden. Diese drei Kategorien sind „indirect physical access“, „short-range physical access“ und „long-range physical access“. Es folgt eine Beschreibung der Kategorien mit einer Übersicht der typischsten Schnittstellen eines modernen Autos.

2.2.1 Indirect Physical Access

Zu dieser Kategorie zählen sämtliche physische Schnittstellen, die direkt oder indirekt auf die internen Netzwerke des Autos zugreifen. Bei diesen Schnittstellen müsste ein Angreifer, um darauf zuzugreifen, mindestens einmalig physischen Zugang zum Fahrzeug haben oder über einen Vermittler arbeiten.

OBD-II Port

Der On-Board-Diagnose (OBD)-II Port ist eine für Fachleute gedachte Schnittstelle auf den CAN-Bus zu Diagnosezwecken. Er befindet sich meist im Fußraum auf der Fahrerseite. Der Port umfasst 16 Pins, obwohl durch den Standard nur die Belegung von neun Pins vorgeschrieben ist. Die zusätzlichen Pins werden je nach Anbieter teilweise für den Zugriff auf zusätzliche Bussysteme verwendet. [Klinedinst und King 2016, S. 2]
Üblicherweise wird an diesen Port ein Diagnosegerät des Herstellers oder einer Werkstatt angeschlossen. Das Diagnosegerät wird entweder von meist Windows-basierten Personal Computern programmiert oder fungieren als Mittler, um direkt mittels Laptop auf Port zuzugreifen [Checkoway u. a. 2011, S. 3]. In beiden Fällen hat ein Windows-basierter PC direkt oder indirekt Zugriff auf das Netzwerk des Fahrzeugs. Der Hauptzweck dieses Gerätes ist es, Daten aus den ECUs des Fahrzeugs zu sammeln. Das erfolgt über das Senden von diagnostischen CAN-Paketen. Die betroffenen ECUs senden anschließend die angefragten Daten. Diese Daten können dann beispielsweise zur Behandlung von Problemen verwendet werden.
Verbrauchermarktanbieter konnten allerdings die Kommunikationsarchitektur durch Reverse-Engineering verstehen und für andere Zwecke nutzen, zum Beispiel Pay-By-Mile-Versicherungen, Fahrzeuggebrauchstracking und kommerzielles Flottenmanagement [Klinedinst und King 2016, S. 3].

Ladeanschluss eines Elektro-Autos

Elektronische Fahrzeuge tanken nicht an Tankstellen wie ihre kraftstoffbetriebenen Pendants, sondern können an einer Steckdose oder speziellen, teilweise öffentlichen Ladestationen aufgeladen werden. Beim Ladevorgang an Ladestationen werden allerdings nicht nur elektrischer Strom sondern auch Daten ausgetauscht [Checkoway u. a. 2011, S. 3]. Beispiele dafür können die Steuerung des Ladevorgangs, Authentifizierung und Autorisierung und Informationen über Ladezeit, Ladeleistung, Energieverbrauch und Batteriezustand

sein. Dieser Datenaustausch ermöglicht einen effizienten und sicheren Ladevorgang, eine Abrechnung des bereitgestellten Stroms und eine Überwachung der Ladeinfrastruktur. Zudem können eine unautorisierte Nutzung der Ladestation oder eine Überlastung des Stromnetzes verhindert werden.

Entertainment

Eine Vielzahl der physischen Schnittstellen eines Autos ist außerdem der Unterhaltung des Benutzers gewidmet. Beispielsweise bieten die meisten Autos mindestens einen USB- und einen Aux-Anschluss, damit Musik von externen Geräten abgespielt werden kann. Außerdem sind viele Autos mit einem CD-Laufwerk ausgestattet. Meist werden mehrere Audioformate unterstützt. Häufig sind die Entertainment-Systeme mit einem CAN-Bus verbunden [Checkoway u. a. 2011, S. 4], um beispielsweise ganzheitliche Firmwareupdates zu ermöglichen. Außerdem kann das Infotainment-System Informationen von anderen Fahrzeugsystemen abrufen, um dem Fahrer relevante Daten anzuzeigen. Dazu gehören Informationen wie Fahrzeuggeschwindigkeit, Motordrehzahl oder Kraftstoffverbrauch, die dann auf dem Display angezeigt werden können.

2.2.2 Short-Range Wireless Access

Diese Kategorie umfasst Schnittstellen, deren Nutzung zwar drahtlos erfolgt, aber dennoch eine geringe physische Distanz zum Fahrzeug erfordert. Ein potenzieller Angreifer müsste sich für die Nutzung dieser Schnittstellen entweder in der Nähe befinden oder einen Transmitter in der Umgebung platzieren.

Bluetooth

Um Features wie eine Freisprecheinrichtung oder das Hören eigener Musik vom Smartphone zu realisieren, bieten die Infotainment-Systeme der meisten modernen Autos eine Bluetooth-Schnittstelle. Bluetooth ermöglicht die drahtlose Kommunikation zwischen dem Fahrzeug und externen Geräten wie Smartphones. Durch die Verbindung des Infotainment-Systems mit dem Controller Area Network des Fahrzeugs kann es mit anderen elektronischen Steuergeräten (ECUs) kommunizieren. Diese Integration ermöglicht eine nahtlose Interaktion zwischen dem Infotainment-System und anderen Fahrzeugsystemen. Die Bluetooth-Verbindung eröffnet Möglichkeiten für die Nutzung von verschiedenen Funktionen und Diensten. Eine der häufigsten Anwendungen ist die Freisprecheinrichtung, die es

dem Fahrer ermöglicht, Anrufe über das Infotainment-System zu tätigen und entgegenzunehmen, ohne das Telefon in die Hand nehmen zu müssen. Das Infotainment-System wird über Bluetooth mit dem Telefon gekoppelt und kann auf die Telefonkontakte zugreifen, Anrufe initiieren und Anrufinformationen auf dem Display anzeigen. Darüber hinaus ermöglicht die Bluetooth-Schnittstelle auch die drahtlose Übertragung von Audiodateien vom Smartphone zum Infotainment-System. Fahrer und Insassen können ihre eigenen Musikbibliotheken, Streaming-Dienste oder Podcasts über das Fahrzeuglautsprechersystem abspielen. Das Infotainment-System fungiert als Empfänger für das Audiosignal, das vom Smartphone gesendet wird.

Remote Keyless Entry

Remote Keyless Entry (RKE) Systeme, auch als Funkfernbedienung oder Keyless-Entry-Systeme bekannt, sind Technologien, die es Fahrzeugbesitzern ermöglichen, ihr Fahrzeug aus der Ferne zu verriegeln und zu entriegeln, ohne einen physischen Schlüssel verwenden zu müssen. Diese Systeme bieten eine bequeme und sichere Möglichkeit, auf das Fahrzeug zuzugreifen. Ein typisches RKE-System besteht aus zwei Hauptkomponenten: einem Funksender (Fernbedienung) und einem Empfänger, der im Fahrzeug eingebaut ist. Die Fernbedienung ist normalerweise eine kleine tragbare Vorrichtung, die über eine oder mehrere Tasten verfügt. Durch Betätigen der Tasten sendet die Fernbedienung ein verschlüsseltes Funksignal mit einer bestimmten Reichweite an den Empfänger im Fahrzeug. Der Empfänger im Fahrzeug erkennt das Signal der Fernbedienung und interpretiert es. Wenn das empfangene Signal korrekt und authentifiziert ist, führt das RKE-System die gewünschte Aktion aus. Das kann das Entriegeln oder Verriegeln der Türen, das Aktivieren oder Deaktivieren der Diebstahlalarmanlage oder das Öffnen der Kofferraumklappe sein. In einigen Fahrzeugen können auch weitere Funktionen über die Fernbedienung gesteuert werden, wie das Starten des Motors oder das Ein- und Ausschalten der Fahrzeugbeleuchtung.
Des Weiteren sind viele moderne Automobile mit sogenannten Passive Keyless Entry and Start Systemen ausgestattet. Diese basieren auf einem bidirektionalen Challenge-Response-Schema. Das Auto sendet eine Challenge, woraufhin der Autoschlüssel mit einer kryptographischen Antwort (Response) reagiert. Bei einer gültigen Antwort werden die Türen entriegelt, das Alarmsystem deaktiviert und das Starten des Motors ermöglicht. Eine Benutzerinteraktion ist nicht notwendig, der Schlüssel muss sich lediglich in einem Umkreis von in der Regel etwa einem Meter zum Fahrzeug befinden. [Garcia u. a. 2016, S. 930]

RKE-Systeme nutzen verschiedene drahtlose Kommunikationstechnologien wie Radiofrequenz (RF) oder Infrarot (IR), um die Signale zwischen der Fernbedienung und dem Fahrzeug zu übertragen [Checkoway u. a. 2011, S. 4]. RF-basierte Systeme sind am weitesten verbreitet, da sie eine größere Reichweite bieten und nicht auf Sichtverbindung angewiesen sind.

Reifendruck-Kontrollsystem

Ein weiteres drahtloses Netzwerk in Fahrzeugen stellt das Reifendruck-Kontrollsystem (RDKS) oder auf englisch Tire Pressure Monitoring System (TPMS) dar. Die Integration eines solchen Systems ist in vielen Ländern gesetzlich vorgeschrieben. Neben der Vermeidung von Reifenpannen verspricht die Warnung vor falschem Reifendruck eine Steigerung der Verkehrssicherheit und Kraftstoffeffizienz, da der richtige Reifendruck die Traktion, den Bremsweg und den Rollwiderstand verbessert. Das Reifendrucküberwachungssystem misst kontinuierlich den Luftdruck in allen Reifen von Personenkraftwagen, Lastwagen und Mehrzweckfahrzeugen und warnt den Fahrer, wenn ein Reifen signifikant zu wenig aufgepumpt ist. Es gibt sowohl direkte als auch indirekte Messverfahren. Bei einem direkten Messsystem werden batteriebetriebene Drucksensoren in jedem Reifen verwendet, um den Reifendruck zu messen, und die Daten werden über einen Funkfrequenz (RF)-Sender übertragen, da eine Verkabelung von einem rotierenden Reifen zur elektronischen Steuereinheit des Fahrzeugs schwierig umzusetzen ist. Die empfangende Reifendrucksteuereinheit analysiert die Daten und kann über das CAN Ergebnisse oder Befehle an den zentralen Bordcomputer senden, um beispielsweise eine Warnmeldung auf dem Fahrzeugdashboard auszulösen. Indirekte Messsysteme leiten den Druckunterschied zwischen den Reifen aus den Unterschieden in der Rotationsgeschwindigkeit ab, die mithilfe der Antiblockiersystem (ABS)-Sensoren gemessen werden können. Ein Reifen mit niedrigerem Druck muss schneller rotieren, um die gleiche Strecke wie ein Reifen mit höherem Druck zurückzulegen. Die Nachteile dieses Verfahrens sind jedoch eine geringere Genauigkeit, die Kalibrierung durch den Fahrer und die Unfähigkeit, den gleichzeitigen Druckverlust in allen Reifen zu erkennen. Daher werden primär direkte Reifenkontrollsysteme verwendet. [Rouf u. a. 2010, S. 1]

Wireless LAN

Viele Hersteller statten ihre modernen Autos heutzutage mit einer Wireless Local Area Network (WLAN)-Schnittstelle aus [Checkoway u. a. 2011, S. 4]. Die Technologie wird

für verschiedene Anwendungsfälle eingesetzt. Viele moderne Autos sind mit Infotainment-Systemen ausgestattet, die WLAN verwenden, um eine drahtlose Verbindung zum Internet herzustellen. Dadurch können Insassen auf Streaming-Dienste, Musik, Online-Radio, und andere Online-Inhalte zugreifen. WLAN ermöglicht auch Over-the-Air-Updates für das Infotainment-System, um Softwareaktualisierungen und neue Funktionen bereitzustellen. Auch für den Rest des Fahrzeugs lassen sich je nach Modell teilweise Softwareupdates über WLAN herunterladen. Zum Beispiel die Autos von Tesla bieten dieses Feature. Darüber hinaus ermöglicht WLAN den Passagieren im Auto in manchen Fahrzeugen die drahtlose Verbindung ihrer mobilen Geräte wie Smartphones, Tablets und Laptops mit dem Internet. Schließlich werden WLAN-basierte Standards ebenfalls in der Fahrzeug-zu-Fahrzeug-Kommunikation eingesetzt. Diese Art der Kommunikation wird auch Dedicated Short-Range Communications (DSRC) genannt [Checkoway u. a. 2011, S. 4]. Durch den Datenaustausch zwischen Fahrzeugen sollen beispielsweise Kollisionen frühzeitig erkannt und verhindert werden.
Um die genannten Features umsetzen zu können, ist größtenteils eine Verbindung der ECU mit der WLAN-Schnittstelle zum Controller Area Network notwendig. Somit kann in vielen Fahrzeugen auch über WLAN theoretisch indirekt auf den CAN-Bus zugegriffen werden.

2.2.3 Long-Range Wireless Access

Zu dieser letzten Kategorie zählen alle Zugriffskanäle, die aus großer Entfernung, nämlich mehr als einem Kilometer, zugegriffen werden kann. Immer mehr Autos bieten auch derartige Schnittstellen. Diese lassen sich in zwei Kategorien einteilen: Broadcast Kanäle und Adressierbare Kanäle. [Checkoway u. a. 2011, S. 4]

Broadcast Kanäle

Broadcast Kanäle sind Kanäle, die nicht speziell auf ein bestimmtes Fahrzeug ausgerichtet sind, sondern von Empfängern nach Bedarf empfangen werden können. Neben der externen Angriffsfläche können weitreichende Broadcastmedien als Steuerungskanäle attraktiv sein (z. B. zum Auslösen von Angriffen), da sie schwer zuzuordnen sind, mehrere Empfänger gleichzeitig steuern können und Angreifer keine genaue Adressierung ihrer Opfer benötigen. Das moderne Automobil umfasst eine Vielzahl von Empfängern für weitreichende Signale: Global Positioning System (GPS), Satellitenradio, Digitalradio und das Radio Data System (RDS) und der Traffic Message Channel (TMC), die als digitale Unterträger

auf vorhandenen FM-Bändern übertragen werden. Die Reichweite solcher Signale hängt von der Sendeleistung, Modulation, Gelände und Störungen ab. Im Allgemeinen werden diese Kanäle in das Mediasystem eines Autos (Radio, CD-Player, Satellitenempfänger) implementiert, das, wie bereits erwähnt, häufig über interne Automobilnetzwerke Zugriff auf andere wichtige Automotive-ECUs ermöglicht. [Checkoway u. a. 2011, S. 4 f.]

Adressierbare Kanäle

Über adressierbare Kanäle lassen sich individuelle Fahrzeuge direkt ansteuern. Die Verbindung erfolgt in der Regel über das Mobilfunknetz.
Durch diese Kanäle können viele Funktionen bereitgestellt werden. Dazu gehören die Unterstützung von Sicherheit (Unfallberichterstattung), Diagnose (frühzeitige Warnung bei mechanischen Problemen), Diebstahlschutz (Fernverfolgung und Deaktivierung) und Komfort (Zugriff auf Daten wie Fahrtrichtungen oder Wetterinformationen). [Checkoway u. a. 2011, S. 5]
Da diese Kanäle meist eine hohe Bandbreite bieten, über große Distanzen und in beide Richtungen funktionieren und das direkte Ansteuern von individuellen Fahrzeugen ermöglichen, sind diese Schnittstellen für potenzielle Angreifer besonders interessant [Checkoway u. a. 2011, S. 5].

2.3 Cyber Security

Als nächstes werden die Grundlagen der Cyber Security und IT Sicherheit erläutert, die im Bereich der Automotive Security relevant sind. Die IT Security befasst sich eher mit der Sicherheit von elektronisch gespeicherten Daten während die Cyber Security diese Sicherheit auf ganze Systeme, Netzwerke und Kommunikation ausweitet. Die Begriffe Cyber- und IT Security sind jedoch eng miteinander verwandt und werden oft als Synonym verwendet.

2.3.1 Security und Safety

Der deutsche Begriff „Sicherheit“ ist mehrdeutig, was ihn für eine genaue, technische Definition ungeeignet macht. In der IT-Sicherheit wird zwischen den beiden englischen Begriffen „Safety“ und „Security“ unterschieden.

Safety „Der Begriff Safety bezeichnet die funktionale Sicherheit, bzw. die Betriebssicherheit eines Systems. Ein System darf seine Umgebung etwa durch undefiniertes, unzulässiges Verhalten oder Zustände nicht gefährden. Safety schützt somit Mensch und Umwelt vor negativen Einflüssen des Systems, etwa durch Fehlverhalten und Ausfälle." [Wurm 2022, S. 2]

Security „Der Begriff Security bezeichnet die Informations- und Datensicherheit bzw. die Angriffssicherheit eines Systems. Security umfasst alle Eigenschaften und Maßnahmen, die das System vor absichtlichen und unabsichtlichen Bedrohungen von außen schützen. Security schützt somit das System vor negativen Einflüssen von Mensch und Umwelt, wie etwa Bedrohungen und Angriffe. Während sich die sog. klassische IT-Security auf die Absicherung der informationstechnischen Systeme eines Unternehmens wie etwa Computer, Server, Netzwerke und Internetanbindungen konzentriert, zielt die Cybersecurity im Kontext des Automotive Bereichs auf die Absicherung deren Produkte ab." [Wurm 2022, S. 2 f.]

Safety bezieht sich somit mehr auf die Sicherheit des Nutzers während sich die Security eines Systems mehr auf die Sicherheit von Daten, Informationen und des Systems an sich fokussiert. Im Automotive-Kontext ist Security in vielen Fällen eine Voraussetzung für die Safety von Fahrzeugen, da durch Security-Maßnahmen verhindert werden soll, dass das Fahrzeug in einen Safety-kritischen Zustand gebracht wird. In anderen Fällen stehen sich Safety- und Security-Ziele aber auch teilweise gegenseitig im Weg. Zum Beispiel kann durch erhöhte Security-Maßnahmen die Latenz der Fahrzeugsysteme ansteigen, was sich wiederum negativ auf die Safety auswirkt. Daher kann es eine Herausforderung sein, beide Disziplinen gemeinsam ausreichend zu behandeln.

2.3.2 Sicherheitsziele

Die Sicherheitsziele beschreiben Eigenschaften von Informationen und anderen schützenswerten Ressourcen, die gewünscht sind, um Sicherheit zu gewährleisten. Security-Maßnahmen sollten darauf ausgelegt sein, diese Ziele zu erreichen. Faktoren, die das Erreichen der Sicherheitsziele gefährden, können als Bedrohung identifiziert werden. Die klassischen Sicherheitsziele in der IT Security sind Vertraulichkeit, Integrität und Verfügbarkeit (siehe Abbildung 2.3.2). Diese Ziele werden manchmal auch als CIA-Ziele bezeichnet. CIA entspricht hierbei der Abkürzung der englischen Begriffe Confidentiality, Integrity und Availability. Im Automotive Bereich werden allerdings oft zusätzlich die Ziele Authentizität, Zurechenbarkeit und Schutz der Privatsphäre genannt [Wurm 2022, S. 6].

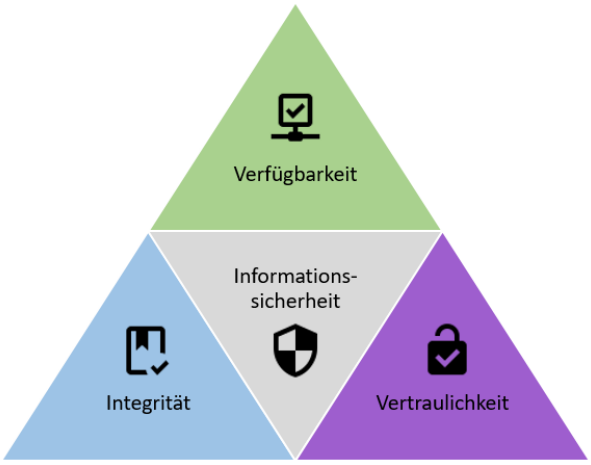

Abbildung 2.8: Die drei klassischen Sicherheitsziele der IT Security
Quelle: [Pukies 2020]

Vertraulichkeit

„Vertraulichkeit beschreibt die Eigenschaft, dass ausschließlich berechtigte Personen bzw. Entitäten auf die zu schützenden Informationen zugreifen können. “ [Wurm 2022, S. 7]
Dieses Sicherheitsziel kann durch unterschiedliche Maßnahmen erreicht werden, die sich teilweise gegenseitig ergänzen. Dazu gehören zum Beispiel Zugriffskontrollen, Verschlüsselung und Verstecken der Informationen.
Es kann verschiedene Gründe geben, warum manche Informationen vertraulich bleiben sollen. So kann durch das Bekanntwerden gewisser Informationen zum Beispiel ein wirtschaftlicher Schaden entstehen. Das kann der Fall sein bei geistigem Eigentum oder auch Firmengeheimnissen. Außerdem schützenswert sind personenbezogene Daten.

Integrität

„Integrität beschreibt den Schutz von Informationen vor unbeabsichtigten oder böswilligen Veränderungen. “ [Wurm 2022, S. 7]
Das Wort Veränderungen schließt hierbei auch das Entfernen oder Hinzufügen von Daten ein, somit gelten diese Aktionen ebenfalls als Verletzung der Integrität. Um die Integrität schützenswerter Informationen zu gewährleisten, werden technische Maßnahmen wie kryptographische Checksummen eingesetzt. Dadurch kann zwar ein Verlust der Integrität nicht verhindert werden, jedoch kann er zweifelsfrei und nicht kompromittierbar erkannt werden.

Der Schutz der Integrität spielt eine entscheidende Rolle für die korrekte Funktionsweise der gesamten ECU-Software und insbesondere für sicherheitsrelevante Informationen.

Verfügbarkeit

„Verfügbarkeit (engl. availability) definiert die Anforderung an das System, seine Dienste und Funktionen innerhalb einer gewissen Zeitspanne (Echtzeitfähigkeit) nach Aufforderung zur Verfügung stellen zu können. “ [Wurm 2022, S. 7]
Um einen reibungslosen und sofortigen, teilweise sogar Echtzeit-, Betrieb zu gewährleisten, müssen Hardware-, Software- und Kommunikationsressourcen verfügbar sein. Häufig ist das Ziel eines Angreifers, den Dienst einzuschränken oder vollständig zu verweigern. Eine gängige technische Lösung zur Aufrechterhaltung der Verfügbarkeit ist zum Beispiel die Implementierung redundanter Pfade. Wenn ein Primärsystem ausfällt, kann ein redundantes (Teil-)System die Aufgabe übernehmen und so die Verfügbarkeit sicherstellen.

Authentizität

„Authentizität bedingt, dass die Echtheit einer Information bzw. eines Absenders sichergestellt ist. Die Authentizität einer Information ist gegeben, falls dessen Urheber eindeutig identifizierbar und dessen Urheberschaft kryptographisch sicher überprüfbar ist. “ [Wurm 2022, S. 7]
Die Authentizität von Informationen ist eng mit der Integrität von Informationen verwandt. Technisch kann Authentizität durch digitale Signatur oder Zertifikate umgesetzt werden.

Zurechenbarkeit

„Zurechenbarkeit bzw. Verbindlichkeit (engl. accountability) ist eine Eigenschaft, die dafür garantiert, dass die entsprechende Person oder Entität die Urheberschaft einer bestimmten Information bzw. eine bestimmte Aktion nicht von sich weisen kann. “ [Wurm 2022, S. 8]
Der Begriff Nichtabstreitbarkeit wird oft ähnlich verwendet, spielt jedoch insbesondere in rechtlichen Angelegenheiten wie Haftung und Gewährleistung eine Rolle. Es wurde festgestellt, dass die Abstreitbarkeit eine potenzielle Schwachstelle darstellt. Wenn zum Beispiel der Empfang oder das Senden bestimmter kritischer Nachrichten, wie Warnungen vor Stauenden oder Geschwindigkeitsbegrenzungen, bestritten werden kann, ist eine rechtssichere Zuordnung nicht möglich und eine mögliche Strafverfolgung wird erschwert. Ohne das Schutzziel der Nichtabstreitbarkeit könnte jeder Teilnehmer bestreiten, eine bestimmte Nachricht gesendet oder empfangen zu haben. Die technische Umsetzung kann durch

manipulationssichere Log-Speicher erfolgen, die den Empfang bestimmter Nachrichten protokollieren und nachweisen können. Die Nichtabstreitbarkeit der Urheberschaft einer gesendeten Nachricht wird durch das digitale Signaturverfahren in Verbindung mit einer vertrauenswürdigen Public-Key-Infrastruktur gewährleistet. [Wurm 2022, S. 8]

Schutz der Privatsphäre

Moderne Fahrzeuge und Hersteller erheben, verarbeiten und speichern personenbezogene Daten. Beispielsweise wird die Position des Autos im Rahmen der Vehicle-to-Everything (V2X)-Kommunikation zyklisch veröffentlicht. Hierbei ist es zum einen im Interesse der betroffenen Person, des Fahrers, dass sich diese Daten sich nicht zu den betroffenen Personen zuordnen lassen. Außerdem ist es aber auch durch die Datenschutzgrundverordnung, die im Jahr 2018 in Kraft trat. Technisch lässt sich der Schutz der Privatsphäre zum Beispiel mit einer Tarnidentität umsetzen.

2.3.3 Risikomanagement

Der systematische Umgang mit Gefahren und Risiken ist ein wichtiger Bestandteil des Cybersecurity-Engineering-Prozesses. Im Kontext von Cybersecurity-Angriffen beziehen sich Bedrohungen, Schwachstellen und Risiken auf verschiedene Aspekte. Die schützenswerten Güter eines Systems, auch genannt Assets, können sowohl materieller als auch immaterieller Natur sein, wie zum Beispiel sensible Informationen, Fahrzeugfunktionen, Softwarekomponenten, Hardwarekomponenten, Infrastrukturkomponenten und Kommunikationsverbindungen. Risikobewertungsmodelle definieren die Sicherheitseigenschaften der Assets, wie Vertraulichkeit, Integrität und Verfügbarkeit (vergleiche Kapitel 2.3.2), und legen ihren Schutzbedarf fest. [Wurm 2022, S. 5]
Bedrohungen können absichtliche oder unabsichtliche Ereignisse sein, die die Schutzziele der Assets beeinträchtigen können, sei es durch bösartige Aktivitäten von Angreifern oder unvorhersehbare Ereignisse wie Ausfälle oder physische Beschädigungen.
Angreifer nutzen vorhandene Schwachstellen aus, um Angriffe durchzuführen und die Assets eines Systems zu bedrohen. Passive Angriffe zielen hierbei auf die Informationsbeschaffung ab, während aktive Angriffe darauf abzielen, die Integrität, Authentizität und Verfügbarkeit des Systems zu beeinträchtigen.
Risiken werden im Rahmen einer Risikoanalyse bewertet und sind definiert durch Eintrittswahrscheinlichkeit und potenzielles Schadensausmaß. Schwachstellen erhöhen das Risiko, während Gegenmaßnahmen und Schutzkonzepte das Risiko reduzieren. Gegenmaßnahmen,

auch als Sicherheitskontrollen bezeichnet, sollen potenzielle Bedrohungen verhindern und die Wahrscheinlichkeit von Angriffen auf ein akzeptables Niveau reduzieren. Angreifer können aus verschiedenen Personengruppen stammen, von Hobby-Hackern bis hin zu staatlichen Organisationen wie Geheimdiensten. Es ist jedoch auch möglich, dass Angriffe von aktuellen Fahrzeugbesitzern selbst durchgeführt werden, beispielsweise durch das Manipulieren des Kilometerstandes zur Erhöhung des Wiederverkaufswerts eines Fahrzeugs. [Wurm 2022, S. 5 f.]

Risikomatrix

Ein sehr verbreitetes Werkzeug der Risikoanalyse ist die Risikomatrix (siehe Abbildung 2.3.3). Sie dient der Einschätzung und Berechnung von Risiken. Mithilfe einer Risikomatrix kann die Bedeutung und das Ausmaß eines Risikos einfach bestimmt und anschaulich visualisiert werden. In der Regel hat eine Risikomatrix die zwei Dimensionen Eintrittswahrscheinlichkeit und Schadensausmaß. Diese verfügen meist über eine vorher zu definierende, künstliche, ordinale Skalierung. Die Risiken werden dann auf einer Skala von niedrig bis hoch in Bezug auf ihre Wahrscheinlichkeit und Auswirkung eingestuft. Die Wahrscheinlichkeit kann beispielsweise in Kategorien wie selten, gelegentlich, häufig oder sehr häufig unterteilt werden, während die Auswirkung auf Kategorien wie gering, moderat, hoch oder katastrophal abgestuft werden kann. Die einzelnen Felder der Matrix sind meist in verschiedenen Farben eingefärbt. Die genaue Farbverteilung der Felder innerhalb der Matrix ist individuell und kann sich je nach Anwendungsfall unterscheiden. In der Regel sind geringe Risiken grün, mittlere Risiken gelb und große Risiken rot eingefärbt. Wo genau die Grenze gezogen wird ist jedoch dem Ersteller überlassen. Die Risikobewertung erfolgt durch das Zuweisen eines Wertes oder einer Farbe zu jedem Risiko, abhängig von seiner Position in der Risikomatrix. Für die Berechnung eines Wertes wird meist der Wert der Eintrittswahrscheinlichkeit mit dem Wert des Schadensausmaßes multipliziert. Abhängig von der Klassifikation eines Risikos kann anschließend entschieden werden, wie es zu behandeln ist.

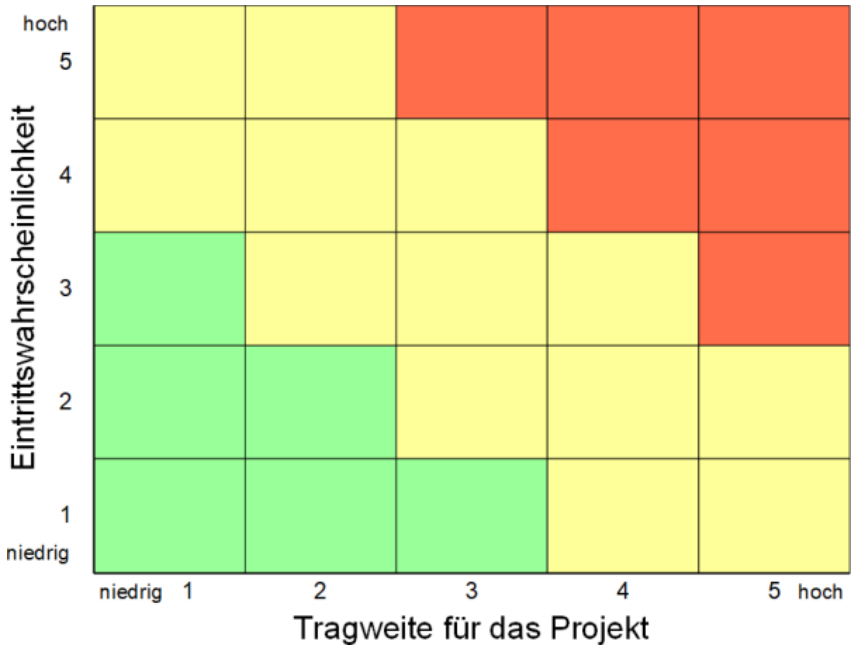

Abbildung 2.9: Beispiel für eine Risikomatrix
Quelle: [**Peterjohann.2014**]

2.3.4 Kryptographie

„Der Begriff Kryptographie stammt vom griechischen kryptos (verborgen) und graphein (schreiben) ab und bezeichnet die Wissenschaft der Geheimschriften oder der Verschlüsselung von Informationen. “ [Wurm 2022, S. 9]
Die Kryptographie beschäftigt sich also hauptsächlich damit, Informationen in anderer Form darzustellen. Dies kann Zwecken der Geheimhaltung, Datenübertragung oder Komprimierung dienen. Außerdem können kryptographische Verfahren wie zum Beispiel RSA auch zur Authentifizierung durch Signaturen eingesetzt werden.
Kryptographie im Zusammenhang mit der Sicherheit von Kraftfahrzeugen bezieht sich auf den Einsatz von Ver- und Entschlüsselungstechniken zur Gewährleistung der Vertraulichkeit, Integrität und Authentizität von Daten und Kommunikationssystemen in Fahrzeugen. Durch den Einsatz kryptografischer Techniken werden Informationen vor unbefugtem Zugriff und Manipulationen geschützt, um die Sicherheit und Privatsphäre der Fahrzeuginsassen zu gewährleisten.
Hierbei gilt wie in der allgemeinen IT Security das Auguste Kerkhoff Prinzip. Dieses besagt, dass in einem guten Kryptographiesystem lediglich der Schlüssel geheim gehalten werden muss. Das System muss auch dann Sicherheit bieten, wenn seine genaue Funktionsweise

bekannt ist. Das Prinzip „Security by Obscurity“, also Sicherheit durch Verschleierung der Funktionsweise des Kryptographiesystems, sollte nicht zum Einsatz kommen. Daher beruhen viele Kryptographieverfahren auf sehr schwer berechenbaren, mathematischen Problemen. Im Fall von RSA wäre das die Faktorisierung sehr großer Zahlen.
Im Automobilbereich umfasst die Kryptographie verschiedene Anwendungsfälle, wie die sichere Übertragung von Daten zwischen Fahrzeugkomponenten, die Verschlüsselung von drahtlosen Kommunikationskanälen (z. B. V2X-Kommunikation) und die Absicherung von Fahrzeugfunktionen gegen potenzielle Angriffe. Verschiedene kryptografische Verfahren wie symmetrische und asymmetrische Verschlüsselung, digitale Signaturen und Hash-Funktionen werden eingesetzt, um die Vertraulichkeit von Daten zu gewährleisten, die Integrität von Nachrichten zu garantieren und die Authentizität der Kommunikationsteilnehmer zu überprüfen. Außerdem werden sichere Schlüsselverwaltungssysteme und -protokolle verwendet, um den sicheren Austausch von Verschlüsselungs- und Authentifizierungsschlüsseln zu ermöglichen. Die Kryptographie spielt im Zusammenhang mit der Sicherheit von Kraftfahrzeugen eine wichtige Rolle, da sie dazu beiträgt, die Risiken von Cyberangriffen auf Fahrzeuge zu verringern und die Sicherheit von Fahrzeugelektronik und Kommunikationssystemen zu erhöhen. Durch den Einsatz kryptografischer Verfahren können vertrauliche Informationen geschützt und die Integrität von Fahrzeugdaten gewährleistet werden, was letztlich zu einer sicheren und zuverlässigen Fahrzeugkommunikation und -funktionalität führt.

Kapitel 3

Angriffsflächen

3.1 Vorgehensweise

[Wurm 2022, S. 35]

3.2 Bootvorgang

[Wurm 2022, S. 82]

3.2.1 Remote Keyless Entry

[Garcia u. a. 2016]

Kapitel 4

Schutzmaßnahmen

[Wurm 2022, S. 42] und generell Kapitel 2 + 4 + 5

4.1 Herausforderungen der Automotive Security

[Wurm 2022, S. 36] + 233 (AM-Devices)

4.1.1 SecureBoot

[Wurm 2022][84]

Literatur

Checkoway, Stephen u. a. [2011]. »Comprehensive Experimental Analyses of Automotive Attack Surfaces«. In: *20th USENIX Security Symposium (USENIX Security 11)*. San Francisco, CA: USENIX Association. URL: https://www.usenix.org/conference/usenix-security-11/comprehensive-experimental-analyses-automotive-attack-surfaces [siehe S. 12–14, 16–18].

Fijalkowski, B. T. [2011]. »Local Interconnect Networking«. In: *Automotive Mechatronics: Operational and Practical Issues: Volume I*. Dordrecht: Springer Netherlands, S. 57–59. ISBN: 978-94-007-0409-1. DOI: 10.1007/978-94-007-0409-1{\textunderscore}5 [siehe S. 7, 8].

Garcia, Flavio u. a. [2016]. »Lock It and Still Lose It—On the (In)Security of Automotive Remote Keyless Entry Systems«. In: *SEC'16: Proceedings of the 25th USENIX Conference on Security Symposium*. Hrsg. von Thorsten Holz und Stefan Savage. USA: USENIX Association. ISBN: 9781931971324 [siehe S. 15, 26].

Greenberg, Andy [2015]. *Hackers Remotely Kill a Jeep on the Highway - With Me in It*. URL: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ [besucht am 04. 01. 2023] [siehe S. 1].

Grzemba, Andreas, Hrsg. [2007]. *MOST: das Multimedia-Bussystem für den Einsatz im Automobil*. Bd. Bd. 2. Elektronik- & Elektrotechnik-Bibliothek. Poing: Franzis. ISBN: 978-3772341496 [siehe S. 10, 11].

Klinedinst, Dan und Christopher King [2016]. »On Board Diagnostics: Risks and Vulnerabilities of the Connected Vehicle«. Diss. Carnegie Mellon University [siehe S. 13].

Miller, Charlie und Chris Valasek [2013]. »Adventures in automotive networks and control units«. In: *Def Con* 21.260-264, S. 15–31 [siehe S. 3–6].

Mohammad Ashjaei u. a. [2021]. »Time-Sensitive Networking in automotive embedded systems: State of the art and research opportunities«. In: *Journal of Systems Architecture* 117, S. 102137. ISSN: 1383-7621. DOI: 10.1016/j.sysarc.2021.102137. URL: https://www.sciencedirect.com/science/article/pii/S1383762121001028 [siehe S. 3].

Pukies, Gaston [2020]. *Sicherheit in IT-Systemen*. URL: https://safe-ur-chain.de/security [besucht am 21. 05. 2023] [siehe S. 20].

Rouf, Ishtiaq u. a. [2010]. *Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study*. URL: https://www.usenix.org/legacy/event/sec10/tech/full_papers/Rouf.pdf [siehe S. 16].

Statista [2022]. *Besitz eines Pkw in Deutschland im Jahr 2022*. URL: https://de.statista.com/prognosen/999770/deutschland-besitz-eines-pkw [besucht am 04. 01. 2023] [siehe S. 1].

Wurm, Manuel [2022]. *Automotive Cybersecurity*. Springer Berlin Heidelberg. ISBN: 978-3-662-64227-6 [siehe S. 19–24, 26, 27].

Zimmermann, Werner und Ralf Schmidgall [2014]. *Bussysteme in der Fahrzeugtechnik: Protokolle, Standards und Softwarearchitektur ; mit 103 Tabellen*. 5., aktualisierte und erw. Aufl. ATZ/MTZ-Fachbuch. Wiesbaden: Springer Vieweg. ISBN: 978-3-658-02418-5. DOI: 10.1007/978-3-658-02419-2 [siehe S. 6, 8, 9, 11, 12].