Fortschritt-Berichte VDI

VDI

Reihe 10

Informatik/
Kommunikation

Dipl.-Met. Christoph Maget, M.Sc.,
München

Nr. 872

Auf sichere Mobilfunkkommunikation gestütztes Fahrzeugleitsystem

FernUniversität in Hagen
Schriften zur Informations- und Kommunikationstechnik

Der
FernUniversität in Hagen
Fakultät für Mathematik und Informatik
vorgelegte

DISSERTATION

zur Erlangung des akademischen Grades
Doktor-Ingenieur (Dr.-Ing.)

Auf sichere Mobilfunkkommunikation gestütztes Fahrzeugleitsystem

von
CHRISTOPH FRANZ MAGET
aus München

Hagen, 2020

Gutachter:
Prof. Dr. Dr. Wolfgang A. Halang, Hagen
Prof. Dr.-Ing. Linus Schleupner, Köln
Prof. Dr.-Ing. Kyandoghere Kyamakya, Klagenfurt

Tag der mündlichen Prüfung: 11.12.2020

Fortschritt-Berichte VDI

Reihe 10

Informatik/
Kommunikation

Dipl.-Met. Christoph Maget, M.Sc.,
München

Nr. 872

Auf sichere Mobilfunkkommunikation gestütztes Fahrzeugleitsystem

FernUniversität in Hagen
Schriften zur Informations- und Kommunikationstechnik

Maget, Christoph
Auf sichere Mobilfunkkommunikation gestütztes Fahrzeugleitsystem
Fortschr.-Ber. VDI Reihe 10 Nr. 872. Düsseldorf: VDI Verlag 2021.
148 Seiten, 25 Bilder, 23 Tabellen.
ISBN 978-3-18-387210-7, ISSN 0178-9627,
€ 57,00/VDI-Mitgliederpreis € 51,30.

Keywords: Fahrzeugleitsystem – Mobilfunk – Kryptologie – Perfekte Sicherheit – Car2X

Die vorliegende Arbeit richtet sich an Ingenieure und Wissenschaftler in den Bereichen Kryptografie und Mobilkommunikation. Sie stellt ein Fahrzeugleitsystem vor, das mit seiner Kommunikationsarchitektur post-quanten-sichere Kryptografie und Nachrichtenübertragung bei harten Echtzeitbedingungen ermöglicht. Grundlage ist eine genaue Analyse bestehender Standards und die Schlussfolgerung, dass existierende Ansätze diese nicht erfüllen. Die Kommunikationsarchitektur macht sich das Prinzip der perfekt sicheren Einmalverschlüsselung zu Nutze und löst den Schlüsselaustausch durch eine an den Anwendungsfall angepasste Organisationsstruktur. Eine detaillierte Berechnung des benötigten Schlüsselbedarfs beweist die grundsätzliche Eignung der perfekt sicheren Einmalverschlüsselung für die Automatisierungstechnik. Das Fahrzeugleitsystem erfüllt weitestgehend die von der Europäischen Kommission aktuell erarbeiteten Anforderungen an das ethische Verhalten vernetzter und autonomer Systeme.

Bibliographische Information der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind im Internet unter www.dnb.de abrufbar.

Bibliographic information published by the Deutsche Bibliothek
(German National Library)
The Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliographie (German National Bibliography); detailed bibliographic data is available via Internet at www.dnb.de.

Schriften zur Informations- und Kommunikationstechnik
Herausgeber:
Wolfgang A. Halang, Lehrstuhl für Informationstechnik
Herwig Unger, Lehrstuhl für Kommunikationstechnik
FernUniversität in Hagen

ISSN 0178-9627

ISBN 978-3-18-387210-7

Danksagung

Die vorliegende Arbeit entstand parallel zu meiner beruflichen Tätigkeit in den Jahren 2016 bis 2020 und wäre ohne zahlreiche Unterstützer nicht möglich gewesen.

Herrn Prof. Dr. Dr. Wolfgang A. Halang danke ich für die wissenschaftliche Betreuung und Befürwortung der vorliegenden Arbeit. Seine langjährige konstruktive und strukturierende Begleitung hat einen unschätzbaren Beitrag zu meinem akademischen Werdegang geleistet.

Gleichermaßen danke ich Herrn Prof. Dr.-Ing. Linus Schleupner für die Übernahme des zweiten Gutachtens, für die fachlichen Diskussionen und Anregungen und nicht zuletzt für Ermutigung und Zuspruch aus seinem persönlichen Erfahrungsschatz.

Herrn Prof. Dr.-Ing. Kyandoghere Kyamakya danke ich für die Übernahme des dritten Gutachtens und freue mich auf einen weiteren Austausch.

Den Kollegen an der FernUniversität in Hagen danke ich für wertvolle Ideen und Gespräche.

Schließlich danke ich meiner Familie sowie meinen Kollegen und Freunden für Verständnis und Rückhalt.

Christoph Maget, 2020

Die Gefahr, dass der Computer so wird wie der Mensch, ist nicht so groß wie die Gefahr, dass der Mensch so wird wie der Computer.

– Konrad Zuse

Inhaltsverzeichnis

Abkürzungsverzeichnis

AES	Advanced Encryption Standard
ASIL	Automotive Safety Integrity Level
B	Byte
BSI	Bundesamt für Sicherheit in der Informationstechnik
C-V2X	Cellular Vehicle to everything
CAM	Cooperative Awareness Message
CAP	Consistency, Availability and Partition Tolerance
CPOC	Cooperative ITS Point of Contact
CPS	cyberphysisches System
DENM	Decentralized Environment Notification Message
DES	Data Encryption Standard
dID	digitale Identifikation
DIN	Deutsches Institut für Normung
DoS	Denial of Service
EMV	elektromagnetische Verträglichkeit
EN	Europäische Norm
ETSI	European Telecommunications Standards Institute
EU	Europäische Union
GPS	Global Positioning System
GSM	Global System for Mobile Communications
GUID	Globally Unique Identifier
HMI	Human-Machine Interface
HSM	Hardware-Sicherheitsmodul
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICMP	Internet Control Message Protocol
ID	Identifikator
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IKT	Informations- und Kommunikationstechnik
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IP	Internet Protocol

ISM	Industrial, Scientific and Medical
ISMS	Information Security Management System
ISO	International Organization for Standardization
ITS	Intelligent Transport Systems
IVS	Intelligente Verkehrssysteme
JSON	JavaScript Object Notation
KDC	Key Distribution Center
M2M	Machine to Machine
MAC	Media Access Control
MITM	Man in the Middle
OBU	On Board Unit
OSI	Open Systems Interconnection
OTP	One Time Pad
P2P	Peer to Peer
PKI	Public Key Infrastructure
RAMI 4.0	Referenzarchitekturmodell Industrie 4.0
RDS-TMC	Radio Data System – Traffic Message Channel
RFC	Request for Comments
SAE	Society of Automotive Engineers
SCMS	Security Credential Management System
SE	Secure Element
SGAM	Smart Grid Architecture Model
SIKAF	Sichere Kommunikationsarchitektur für Fahrzeugleitsysteme
SIL	Safety Integrity Level
SIM	Subscriber Identity Module
SPOF	Single Point of Failure
SSP	Smart Secure Platform
TCP	Transmission Control Protocol
TPM	Trusted Platform Module
UDP	User Datagram Protocol
UML	Unified Modeling Language
UUID	Universally Unique Identifier
V2X	Vehicle to everything
VANet	Vehicular Ad hoc Network
VDE	Verband der Elektrotechnik, Elektronik und Informationstechnik
VDI	Verein Deutscher Ingenieure
WLAN	Wireless Local Area Network
WWW	World Wide Web

Nomenklatur

Alphabet Ein Alphabet ist eine Menge von Zeichen, aus denen durch Verkettung Klartext, Schlüssel, Maske und Schlüsseltext zusammengesetzt werden.

Chiffriermaske Eine Chiffriermaske (kurz Maske) ist ein Parameter des eingesetzten kryptografischen Verfahrens. Durch *XOR*-Verknüpfung von Klartext und Maske entsteht der Schlüsseltext. Durch *XOR*-Verknüpfung von Schlüsseltext und Maske entsteht der Klartext. Zur Maskierung wird jedes Zeichen des Klartextes mit genau einem Zeichen der Maske verknüpft. Die Maske hat daher dieselbe Länge wie der Klar- bzw. Schlüsseltext und wird aus dem gleichen Alphabet wie der zu verschlüsselnde Klartext gebildet. Um unautorisierte Entschlüsselung zu verhindern, darf die Maske nur berechtigten Nutzern bekannt gemacht werden.

Codebuch In einem Codebuch können häufig übermittelte Informationen tabelliert und mit einem Code verbunden werden. Zur Übermittlung der Information muss dann nicht die vollständige Zeichenkette zur Darstellung der Information übertragen werden, sondern es genügt die Übertragung des Codes. Die Datenmenge kann dadurch reduziert werden.

Maske Kurzform von Chiffriermaske

Maskengröße siehe Schlüsselgröße

Maskenlänge siehe Schlüssellänge

Maskenvorrat siehe Schlüsselvorrat

Maskierung Maskierung ist eine besondere Art der Verschlüsselung. Sie zeichnet sich dadurch aus, dass jedes Zeichen des Klartextes mit genau einem Zeichen der Maske verknüpft wird, um den Schlüsseltext zu erzeugen. Durch Demaskierung wird aus dem Schlüsseltext der Klartext zurückgewonnen. Maskierung ist das Verschlüsselungsverfahren bei der Einmalverschlüsselung (engl. *One Time Pad*).

Nachricht Eine Nachricht ist eine sinnhafte Verkettung von Zeichen, sodass alle zur Übermittlung einer Information notwendigen Angaben vorhanden sind. Die Nachricht kann teilweise verschlüsselt oder maskiert sein.

Nachrichtenlänge Die Nachrichtenlänge ist die Anzahl der Zeichen einer Nachricht. Handelt es sich bei der Nachricht um Binärcode, so kann die Nachrichtenlänge anstatt in Zeichen auch direkt in Bytes angegeben werden.

Prüfsumme Eine Prüfsumme ist eine Zeichenkette fester Länge, die durch einen Algorithmus aus einer Nachricht beliebiger Länge erzeugt wird. Eine

Veränderung der Nachricht oder ihrer Bestandteile führt mit hinreichender Wahrscheinlichkeit zu einer veränderten Prüfsumme. Es wird zwischen technischer und kryptografischer Prüfsumme unterschieden. Eine technische Prüfsumme dient der Entdeckung von Übertragungsfehlern. Eine kryptografische Prüfsumme dient der Entdeckung unautorisierter Änderungen an einer Nachricht und damit der Integritätsprüfung.

Relais Ein Relais ist eine Vermittlungsstelle zwischen zwei Kommunikationsteilnehmern. Alle Nachrichten werden vom Sender zum Relais geschickt und von dort zum Empfänger weitergeleitet.

Schlüssel Ein Schlüssel ist ein Parameter des eingesetzten kryptografischen Verfahrens. Er bestimmt die Zeichenfolge des Schlüsseltextes und ermöglicht die Rückgewinnung des Klartextes aus dem Schlüsseltext. Der Schlüssel wird aus dem gleichen Zeichenvorrat wie der zu verschlüsselnde Klartext gebildet. Um unautorisierte Entschlüsselung zu verhindern, darf der jeweils eingesetzte Schlüssel nur berechtigten Nutzern bekannt gemacht werden. Im Gegensatz zur Maske ist der Schlüssel von geringerer Länge als der zu verschlüsselnde Klartext. Die Menge aller möglichen Schlüssel wird Schlüsselraum genannt.

Schlüsselgröße Die Schlüsselgröße ist die Summe aller Schlüssellängen der Elemente (Schlüssel) eines Schlüsselvorrats. Die Schlüsselgröße ist damit die Anzahl der Zeichen, die bei einem Nutzer vorgehalten wird. Sie kann in Zeichen oder Bytes angegeben werden.

Schlüssellänge Die Schlüssellänge ist die Anzahl der Zeichen eines einzelnen Schlüssels.

Schlüsseltext Ein Schlüsseltext ist die durch Verschlüsselung oder Maskierung eines Klartextes entstandene Zeichenkette. Weitere Bezeichnungen sind Geheimtext, Kryptogramm oder Chiffrat.

Schlüsselvorrat Jedem Nutzer steht eine Teilmenge des Schlüsselraums als Schlüsselvorrat zur Verwendung bei der Ver- und Entschlüsselung zur Verfügung. Die Mächtigkeit dieser Teilmenge wird als Schlüsselvorratsmächtigkeit bezeichnet.

Verschlüsselung Eine Verschlüsselung (auch Chiffrierung genannt) ist eine Funktion (auch Verschlüsselungsverfahren oder Chiffre genannt), die aus Klartext und Schlüssel als Eingangsdaten den Schlüsseltext als Ausgangsdatum erstellt. Aus dem Schlüsseltext kann der Klartext ohne Kenntnis des Schlüssels nicht zurückgewonnen werden. Die in der Nachricht enthaltenen Informationen werden dadurch vor unberechtigten Empfängern verborgen. Die Umkehrung der Verschlüsselung ist die Entschlüsselung.

Zusammenfassung

Automatisierungssysteme spielen in modernen Industriegesellschaften eine zentrale Rolle und durchdringen nahezu alle Lebensbereiche. Der Trend zu verteilten und mobilen Systemen stellt hohe Anforderungen an Sicherheit, Zuverlässigkeit und Echtzeitfähigkeit der Kommunikation zwischen den beteiligten Komponenten. Etablierte Verschlüsselungsverfahren haben sich entweder als unsicher oder als nicht echtzeitfähig beim Einsatz in verteilten Automatisierungssystemen erwiesen. Das einzige, nachweislich sichere Konzept der perfekt sicheren Verschlüsselung wird aufgrund praktischer Hürden bislang kaum in der Automatisierungstechnik eingesetzt. Eine sehr heterogene Systemlandschaft erschwert zudem den übergreifenden Datenaustausch zwischen Systemen unterschiedlicher Hersteller.

In der vorliegenden Arbeit wird eine Kommunikationsarchitektur für Automatisierungssysteme entwickelt und evaluiert, die für drahtlos kommunizierende Komponenten perfekt sichere Verschlüsselung bereitstellt und Echtzeitanforderungen erfüllt. Wesentliche Bestandteile sind eine zentrale Instanz zur Authentifizierung der Teilnehmer, Erzeugung und Verteilung der benötigten Schlüssel sowie eine auf Relaisstationen gestützte Übertragungsinfrastruktur. Die vorgestellte Kommunikationsarchitektur fokussiert auf Automatisierungssysteme im Verkehrsbereich. Die Kommunikationsarchitektur dient dabei dem Datenaustausch in einem Fahrzeugleitsystem, das eine effizientere Ausnutzung vorhandener Verkehrsinfrastruktur ermöglichen soll. In diesem Anwendungsbereich bestehen besonders hohe Anforderungen an Sicherheit und Echtzeitfähigkeit der Datenübertragungen, da der Nachrichtenaustausch zur Abstandsregelung zwischen Fahrzeugen und zur Kollisionsvermeidung dient. Für Konzeption und Evaluierung der Kommunikationsarchitektur werden aus Normen wie der ISO 26262 spezifische Anforderungen an die funktionale sowie an die informations- und kommunikationstechnische Sicherheit abgeleitet. Sicherheitsrelevanten Funktionen wird ein ASIL zugeordnet, um Sicherheitslücken systematisch zu identifizieren und zu schließen.

Es wird nachgewiesen, dass die entwickelte Kommunikationsarchitektur diese spezifischen Anforderungen im Gegensatz zu bestehenden Übertragungssystemen erfüllen kann. Entscheidend dabei ist die Umsetzung als zentralisierte Lösung, da nur so perfekte Datensicherheit möglich ist und gleichzeitig die Komplexität der Gesamtarchitektur auf ein kontrollierbares Maß beschränkt bleibt. Die vorgestellte Kommunikationsarchitektur wird prototypisch auf Basis frei verfügbarer Softwarebibliotheken und Hardwareplattformen implementiert. Dies ermöglicht zum einen die Übertragung der Konzepte auf weite Bereiche der Automatisierungstechnik und zum anderen Geschäftsmodelle, die keine Lizenzierung proprietärer Komponenten voraussetzen.

Abstract

Automation systems are of crucial importance for modern industrial societies and permeate almost any sphere of life. The trend towards distributed and mobile systems imposes high demands on the security, reliability and real-time performance of communication among the components involved. Established encryption methods have proven to be either insecure or to lack real-time capability when used in distributed automation systems. The only provably secure concept – perfectly secure encryption – is rarely used in automation technology due to practical impediments. Different paradigms of system integration impede data exchange between systems from different manufacturers.

In this work a communication architecture for automation systems is developed and evaluated, which features perfectly secure encryption and meets real-time requirements for wireless communication. Essential elements are a central authority to authenticate the participants, and to provide them with the necessary keys as well as a dedicated transmission infrastructure based on relay stations. The main applications of the presented communication architecture are automation systems in the transportation sector. The communication architecture is used to exchange data in a vehicle control system, which is intended to improve safety and capacity of existing transportation infrastructure. Since the message exchange in this application aims at distance control and collision avoidance, all data transmissions impose particularly high demands on security and real-time capability. For conception and evaluation of the communication architecture, specific requirements concerning functional safety as well as information and communication security are derived from standards such as ISO 26262. Consequently, an ASIL is assigned to safety-relevant functions of the communication architecture. No existing concept can meet the identified requirements so far.

It is shown that the developed communication architecture can meet the requirements derived. Implementation with a centralised topology is the only way to allow the use of perfectly secure encryption and, at the same time, to limit the complexity of the overall architecture. The presented communication architecture is implemented as a prototype based on freely available software libraries and hardware platforms. This enables, on one hand, transfer of the concepts to wide areas of automation technology and, on the other, business models that do not require the licensing of proprietary components.

1 Sicherheit im Internet der Dinge

Zunehmende Arbeitsteilung und Spezialisierung erfordern auch in der Automatisierungstechnik, dass die beteiligten Akteure kommunizieren und kooperieren. Für die zunehmende, allgegenwärtige Vernetzung haben sich Begriffe wie *Machine to Machine (M2M)*-Kommunikation, *Ubiquitous Computing*, *Industrie 4.0* oder das *(industrielle) Internet der Dinge* (engl. *Internet of Things [IoT]*) etabliert. In diesem Kapitel werden grundlegende Aspekte und aktuelle Herausforderungen vorgestellt.

1.1 Kommunikation in der Automatisierungstechnik

In von Digitalrechnern geprägten industriellen Umfeldern kommt neben der menschlichen Kommunikation auch der Informationsübertragung zwischen Maschinen eine immer wichtigere Bedeutung zu. Kommunikationsprotokolle spezifizieren die ausgetauschten Nachrichten hinsichtlich der zur Übermittlung einer Information notwendigen Angaben. Information wird für Digitalrechner in Binärcodes dargestellt, die Länge einer Nachricht wird daher in Zeichen oder Bytes angegeben. Ein Gerät, das sowohl über Kommunikationsschnittstellen zu Übertragungsnetzen als auch über Sensoren und Aktoren zur Interaktion mit der physischen Welt verfügt, wird auch *cyberphysisches System (CPS)* genannt. Aktuell werden Komponenten der industriellen Automatisierungstechnik mittels standardisierter Feldbussysteme vernetzt. Unterschiedliche Betriebssysteme, Kommunikationsstandards und Rechenleistungen führen zu einer heterogenen Landschaft zu vernetzender Komponenten. Zwei Aspekte stechen bei der Datenübertragung besonders heraus: Sicherheit und Zeitanforderungen.

Die Sicherheit eines Systems betrifft zwei unterschiedliche Sachverhalte, die in Abbildung 1.1 dargestellt sind. Durch informations- und kommunikationstechnische (IKT) Sicherheit ist das System einerseits vor schädlichen äußeren Einwirkungen zu schützen. Durch funktionale Sicherheit muss andererseits die Gefahrlosigkeit des Systems für die Umwelt gewährleistet sein.

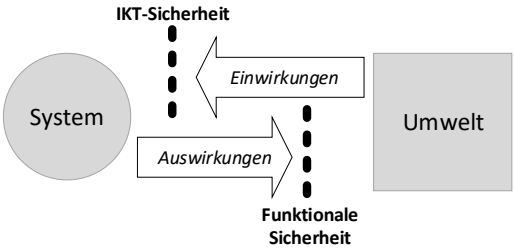


Abbildung 1.1: Funktionale sowie informations- und kommunikationstechnische Sicherheit

Schädlichen äußeren Einwirkungen wird durch physische oder digitale Zugangskontrollen entgegengewirkt. Die Gefahrlosigkeit des Systems für die Umwelt, insbesondere im Fehlerfall, soll durch Begrenzung des Wirkbereichs oder Überführung in einen sicheren Zustand erreicht werden.

Gleichzeitig bestehen häufig Randbedingungen hinsichtlich der zulässigen Dauer eines Kommunikationsprozesses. Solche Echtzeitanforderungen stellen Übertragungssysteme vor besondere Herausforderungen hinsichtlich Übertragungskapazitäten und Latenzen und machen eine effiziente Netzverwaltung notwendig. Bereits in strukturierten Netzen kann die Routenplanung von Datenpaketen komplex sein, was es erschwert, maximale Paketlaufzeiten zu garantieren. Unstrukturierte Vernetzung macht es unmöglich, Übertragungsdauern vorherzusehen.

1.2 Drahtlose Kommunikation beweglicher Objekte

Zur Vernetzung beweglicher Objekte müssen drahtlose Techniken eingesetzt und alle Kommunikationen über die Luftschnittstelle abgewickelt werden. Von Vorteil ist der reduzierte Verkabelungsaufwand, was die flexible Integration weiterer Komponenten in bestehende Netze und damit eine dynamische Skalierung verteilter Automatisierungssysteme begünstigt. Nachteilig sind hohe Anforderungen an die Datensicherheit und -integrität, da die Luftschnittstelle aufgrund der fehlenden physischen Zugangsbeschränkung allgemein zugänglich ist. Alle Kommunikationen können somit auch von unbefugten Dritten empfangen und verändert werden.

Trotz der allgemeinen Verfügbarkeit der Luftschnittstelle haben sich unterschiedliche Verfahren und Standards entwickelt, die sich hinsichtlich der genutzten Frequenzen, der Modulationsverfahren und der Zeichencodierung unterscheiden. Wurde bei der Vernetzung eines Automatisierungssystems die Entscheidung zugunsten eines bestimmten Verfahrens getroffen, ist ein nachträglicher Wechsel in der Regel mit erheblichen Aufwänden verbunden.

Wenn sich die zu vernetzenden Objekte in Bewegung befinden, ändern sich die Längen der Funkstrecken dynamisch mit den Positionen. Im Gegensatz zur kabelgebundenen Übertragung ist die Zeit zur physikalischen Übertragung daher nicht vorherbestimmt und die Dauer der Datenübertragungen nicht vorhersehbar. Drahtlose Datenübertragung zwischen beweglichen, mobilen Teilnehmern kann daher ohne weitere Maßnahmen keine Echtzeitanforderungen erfüllen.

1.3 Angreifbarkeit der Funkschnittstelle

Jedermann kann den Funkkanal stören sowie per Funk übertragene Daten empfangen, senden und damit auch verändern. Unerwünschten Verfälschungen von Nachrichten oder der Verletzung weiterer Schutzziele muss daher mit kryptologischen Verfahren entgegengewirkt werden. In der Vergangenheit wurden alle bis dahin als sicher geltenden kryptografischen Verfahren erfolgreich angegriffen. Daher muss davon ausgegangen werden, dass sich auch aktuell als sicher geltende Maßnahmen künftig als angreifbar erweisen werden. Angreifer können so die Möglichkeit erlagen, ein unerwünschtes oder gefährliches Verhalten eines drahtlos vernetzten Automatisierungssystems herbeizuführen. Die Kommunikation zwi-

schen drahtlos vernetzten Komponenten ist daher besonders abzusichern, um Gefahren für Menschen, Umwelt und Vermögenswerte zu minimieren und im besten Fall auszuschließen. An dieser Stelle setzt die vorliegende Arbeit an.

1.4 Einsatz perfekt sicherer Verschlüsselung

Es existieren Verfahren zur informationstheoretisch perfekt sicheren Verschlüsselung von Nachrichten. Aufgrund praktischer Hürden werden diese Verfahren bislang nicht in der Automatisierungstechnik eingesetzt. Insbesondere die Erzeugung von Schlüsseln mit den benötigten Eigenschaften sowie deren zuverlässige Verteilung über sichere Kanäle ist bisher praktisch nicht zufriedenstellend gelöst und hat deshalb keinen Einzug in die industrielle Automatisierungstechnik gefunden.

In der vorliegenden Arbeit wird eine Architektur zur Datenübertragung zwischen mobilen Kommunikationsteilnehmern vorgestellt, welche als kryptografische Maxime die perfekt sichere Verschlüsselung implementiert. Die benötigten Schlüssel werden durch eine vertrauenswürdige Institution erzeugt und verteilt, die in bestehende administrative Strukturen integriert wird. Nachweislich nicht brechbare Verschlüsselung wird mit dieser Architektur in effizienter Art und Weise umgesetzt.

Die zur perfekt sicheren Verschlüsselung benötigte Zeit verhält sich proportional zur Länge der zu verschlüsselnden Nachricht. Die für den Verschlüsselungsprozess notwendige Zeitspanne kann daher direkt aus den Eigenschaften der Nachrichten abgeleitet werden. Durch Nutzung eines dedizierten Übertragungsnetzes und eines Relais als Vermittlungsstation können zudem die Längen der einzelnen Übertragungsstrecken zwischen Sender und Empfänger vor der Übertragung ermittelt werden. Die Kommunikationen können folglich echtzeitfähig abgewickelt werden, da die Dauern aller für die Datenübertragungen notwendigen Prozesse stets vorhersehbar sind.

1.5 Anwendungsgebiet Fahrzeugleitsystem

Der Mobilitätsbedarf von Menschen und Gütern wird mit Verkehrssystemen (engl. *transport systems*) abgewickelt. Ein Fahrzeugleitsystem ist ein Automatisierungssystem, welches Verkehrssysteme um rechnergestützte Regelungsfunktionen erweitert. Mittels Informations- und Kommunikationstechnik (IKT) werden die notwendigen Steuerinformationen zwischen Fahrzeugen untereinander sowie zwischen Fahrzeugen und Komponenten der Infrastruktur ausgetauscht. In Fahrzeugleitsystemen wird ein großes Potential zur Kapazitätssteigerung bestehender Verkehrssysteme gesehen, da sich Geschwindigkeiten und Abstände rechnergestützt regeln und damit optimieren lassen. Wird das Fahrverhalten eines Fahrzeugs allein durch ein solches Fahrzeugleitsystem und ohne oder mit nur geringen Eingriffen durch einen menschlichen Fahrer geregelt, so wird dieses Fahrzeug als „autonomes Fahrzeug“ bezeichnet [142].

Die automatisierungstechnischen Bestandteile von Verkehrssystemen werden allgemein auch als Verkehrstelematik oder *Intelligent Transport Systems (ITS)* bezeichnet. Sind diese Systeme vernetzt, so spricht man auch von *Cooperative ITS (C-ITS)*. Die (fachlich und sprachlich inkorrekte) Übersetzung ins Deutsche als „Intelligente Verkehrssysteme (IVS)“ hat sich als Begriff in der Forschung und Standardisierung etabliert [19]. Die notwendige

Vereinigung der technisch sehr heterogenen Fahrzeugflotte einerseits und der objektspezifischen Verkehrstechnik andererseits in einer einheitlichen, sicheren und echtzeitfähigen Kommunikationsarchitektur konnte bislang noch nicht erreicht werden. Insbesondere die eingesetzten Verschlüsselungsverfahren basieren bei allen bekannten Ansätzen auf unsicheren Algorithmen.

1.6 Beitrag der Arbeit und weitere Anwendungsgebiete

Die vorliegende Arbeit stellt eine Architektur vor, die durch eine Kombination technischer und organisatorischer Maßnahmen perfekt sichere Verschlüsselung und echtzeitfähige Mobilkommunikation in einem Fahrzeugleitsystem ermöglicht. Technisch werden Fahrzeuge hierzu mit entsprechenden Kommunikationskomponenten ausgerüstet und über einen sicheren Kanal regelmäßig mit aktuellen Schlüsseln versorgt. Zur Kommunikation werden Relaisstationen genutzt, die dedizierte Mobilfunknetze bilden oder bestehende Mobilfunknetze erweitern. Bestehende Institutionen zur Wartung von Kraftfahrzeugen werden organisatorisch erweitert, um als vertrauenswürdige Stellen die für die IKT-Sicherheit benötigten Dienste zu erbringen. Hierzu zählen insbesondere eine digitale Identifizierung der Fahrzeuge sowie Schlüsselerzeugung und -verteilung. Einer zentral ausgerichteten Organisations- und Netzstruktur wird dabei der Vorzug gegenüber einer dezentralen Lösung gegeben, da nur so die Sicherheitsziele nachweisbar erfüllt werden können und die Komplexität des Gesamtsystems auf ein handhabbares Maß limitiert wird.

Im Ergebnis wird erstmals ein Fahrzeugleitsystem vorgestellt, dessen Kommunikationen mit perfekt sicheren Verschlüsselungsverfahren gesichert sind. Die kryptografischen Verfahren zur Gewährleistung von Vertraulichkeit und Integrität ausgetauschter Nachrichten können dadurch nachweislich nicht gebrochen werden. Zur laufenden Versorgung aller Kommunikationsteilnehmer mit den notwendigen Schlüsseln – in der gegenständlichen Anwendung als Masken bezeichnet – werden organisatorische Maßnahmen entwickelt. Das vorgestellte Fahrzeugleitsystem verzichtet auf jegliche Übertragungsprozesse mit stochastischen Einflüssen und ermöglicht damit erstmals vorhersehbare Zeitdauern für alle Verarbeitungsschritte, was die zentrale Voraussetzung zur Erfüllung harter Echtzeitanforderungen ist. Zur Minimierung der Nachrichtenlänge werden die zu übertragenden Nachrichten auf die wesentlichen Inhalte begrenzt. Basierend auf einer detaillierten Herleitung dieser Nachrichtenlänge wird erstmals der Nachweis geführt, dass sich die Schlüssel zum Betrieb perfekt sicherer Verschlüsselung über einen hinreichenden Zeitraum auf Datenträgern handelsüblicher Kapazität bevorraten lassen. Der Bedarf an Schlüsseln lässt sich durch eine speziell entwickelte und in herkömmlichen Fahrzeugleitsystemen bislang nicht berücksichtigte Vorcodierung von Informationen weiter reduzieren.

Verkehrssysteme sind nicht auf die Kraftfahrzeugtechnik beschränkt. Die Automatisierung anderer Verkehrsträger wie des Schienen- und Luftverkehrs lässt sich durch die entwickelte Kommunikationsarchitektur weiter vorantreiben. Weitere Zielgruppen der erarbeiteten Konzepte sind alle Anwender drahtloser Kommunikationsnetze, bevorzugt im Umfeld von Industrie 4.0. Der Fokus auf den industriellen Einsatz ergibt sich aus den vergleichsweise hohen administrativen Anforderungen, die an Implementierungen gestellt werden. Aber auch für die Anlagensteuerung von Einzelanwendern oder die Heimautomatisierung bei Privatanwendern bietet sich der Einsatz der entwickelten Architektur an. Aus Effizienzgründen sollten in diesen Fällen anstelle dedizierter Installationen jedoch Plattformen

genutzt werden. Das Referenzarchitekturmodell Industrie 4.0 (RAMI 4.0) kann einen Rahmen für entsprechende Dienstleistungen (engl. *Platform as a Service [PaaS]*) bilden.

In diesem Kapitel wurden grundsätzliche Aspekte und Anwendungen der allgegenwärtigen digitalen Vernetzung vorgestellt sowie die zentralen Herausforderungen klarer Organisation und sicherer Nachrichtenübertragung erläutert. Darauf aufbauend können im folgenden Kapitel die spezifischen Anforderungen an vernetzte Fahrzeugleitsysteme herausgearbeitet werden.

2 Anforderungen an Fahrzeugleitsysteme

Spezialisierte Digitalrechner sind zur schnelleren Informationsverarbeitung als das menschliche Gehirn in der Lage. Zusammen mit geeigneten Sensoren und Aktoren können Automatisierungssysteme die Reaktionszeiten in technischen Systemen folglich deutlich verringern.

Beim Einsatz von Digitalrechnern ist das Fahrverhalten von Kraftfahrzeugen nicht mehr durch das menschliche Reaktionsvermögen limitiert. Mit Automatisierungssystemen können höhere Geschwindigkeiten und geringere Fahrzeugabstände realisiert werden, was die Kapazität bestehender Strecken erhöht. Zwingende Voraussetzung dafür ist die Kooperationsfähigkeit dieser Digitalrechner. Die zur Kooperation notwendigen Informationen müssen mit Nachrichten ausgetauscht werden, um das Automatisierungssystem zu einem Fahrzeugleitsystem zu erweitern.

Die Entwicklung eines solchen Fahrzeugleitsystems und dessen Integration in bestehende Infrastrukturen erfordert zahlreiche Entwurfsentscheidungen. In diesem Kapitel werden bestehende Standards analysiert sowie ihre Übertragbarkeit auf ein Fahrzeugleitsystem untersucht, um daraus konkrete Anforderungen an ein Fahrzeugleitsystem abzuleiten. Die Standards[1] folgender Institutionen werden bei der Anforderungsanalyse herangezogen:

- Normen
  - Deutsches Institut für Normung (DIN)
  - International Organization for Standardization (ISO)
  - International Electrotechnical Commission (IEC)
  - European Telecommunications Standards Institute (ETSI) (Ratifiziert jede Europäische Norm [EN])
  - Society of Automotive Engineers (SAE)
- Richtlinien
  - Verein Deutscher Ingenieure (VDI)
  - Verband der Elektrotechnik, Elektronik und Informationstechnik (VDE)
  - Institute of Electrical and Electronics Engineers (IEEE)
  - Bundesamt für Sicherheit in der Informationstechnik (BSI)

Es existiert kein Standard, der die notwendigen Eigenschaften eines Fahrzeugleitsystems mit ausschließlich rechnergestützter Steuerung von Fahrzeugen und dessen Einsatz in bestehenden Verkehrssystemen erschöpfend beschreibt.

[1] Standard wird hier als Oberbegriff von Norm und Richtlinie verwendet

2.1 Geometrische Vorbetrachtung

Netze werden allgemein als Graphen (Y) modelliert. Eine Menge von Knoten (W) und eine Menge von Kanten (Z) bilden ein geordnetes Paar (W, Z), sodass für den Graphen des Fahrzeugleitsystems gilt:

$$Y = (W, Z) \tag{2.1}$$

In einem Kommunikationsnetz sind Sender, Empfänger und Zwischenstationen einer übertragenen Nachricht Knoten, die Übertragungsstrecken Kanten. Alle Knoten $w \in W$ haben eine Position im Raum, jede Kante $z \in Z$ stellt eine Verbindung zwischen genau zwei Knoten dar. Die Verbindung von $n(Y)$ Knoten mittels $m(Y)$ Kanten wird Masche genannt. Durch die Art der Vermaschung können Netze und die sie bildenden Knoten typisiert werden [108].

Fahrzeuge können in diesem Anwendungsfall ohne Beschränkung der Allgemeinheit als Punkte $\vec{w_i} \in \mathbb{R}^2$ in einem zweidimensionalen kartesischen Koordinatensystem betrachtet werden. Die Fahrzeuge w bewegen sich mit einer Geschwindigkeit $\vec{v}$ auf einem Verkehrsweg:

$$\vec{v_{w_i}} = \dot{\vec{w}_i} \tag{2.2}$$

Die Bewegungen der hier betrachteten Kraftfahrzeuge sind durch unterschiedliche Randbedingungen eingeschränkt:

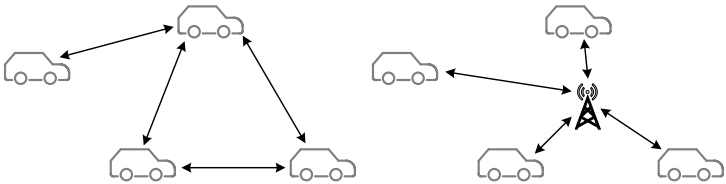
- Die Form der Verkehrswege (hier: Straßen) schränkt die Fahrzeuge auf eine lineare Bewegung im zweidimensionalen Raum ein.
- Geschwindigkeiten können nicht beliebig gewählt werden, sondern sind durch den Verkehrsablauf sowie gesetzliche Grenzen limitiert.
- Abstände zu anderen Fahrzeugen können nicht beliebig verändert werden, sondern müssen zur Kollisionsvermeidung Mindestwerte annehmen.

Diese Randbedingungen wirken sich auf den Abstand zwischen zwei Kommunikationsknoten und damit die Länge der entsprechenden Kante $|z|$ aus. Der Abstand ist eine Funktion g der jeweiligen Orte $\vec{w_i}$ der beteiligten Knoten $w_1, w_2 \in W$ zum Zeitpunkt t:

$$\forall z \in Z : |z(t)| = g(\vec{w_1}(t), \vec{w_2}(t)) \tag{2.3}$$

Entscheidend für die Strukturierung von Kommunikationsnetzen ist die Abwägung, ob alle Kommunikationen durch einen zentralen Zugangspunkt (Relais) vermittelt werden (Infrastrukturmodus) oder ob Direktverbindungen zwischen den Kommunikationsteilnehmern vorgesehen sein sollen (Ad-hoc-Modus). Die beiden Konzepte sind in Abbildung 2.1 skizziert.

Die geometrischen Vorüberlegungen haben entscheidenden Einfluss auf die im Folgenden entwickelten konkreten Anforderungen an ein Fahrzeugleitsystem, da sich aus den Positionen der Fahrzeuge die Längen der Übertragungsstrecken ableiten. Diese Längen wiederum bestimmen die Zeitdauern der Nachrichtenübertragungen und die Position zusätzlich benötigter Infrastruktur.



(a) Ohne Relais: Ad-hoc-Modus **(b)** Mit Relais: Infrastrukturmodus

Abbildung 2.1: Netztopologien zur Fahrzeugvernetzung

2.2 Allgemeine Anforderungen

Standards, die sich den allgemeinen Anforderungen an ein Fahrzeugleitsystem annähern, sind:

SAE 3061:2016-01-14 *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems* [153] betrachtet Fahrzeuge und deren Umfeld als ein CPS und stellt einen Praxisleitfaden für die informationstechnische Absicherung dieses CPS bereit. Der Schwerpunkt liegt auf der Präsentation bewährter Vorgehensweisen zur Gewährleistung der IKT-Sicherheit, durch zahlreiche Verweise auf die ISO 26262 werden jedoch auch Bezüge zur funktionalen Sicherheit hergestellt. Ein Fahrzeugleitsystem muss die Umsetzung dieser Norm bei allen zu integrierenden Fahrzeugen sicherstellen.

VDI 2710:2010-04 *Ganzheitliche Planung von Fahrerlosen Transportsystemen* [173] befasst sich als technische Regel mit dem gesamten Produktlebenszyklus fahrerloser Transportsysteme. Es werden alle Planungsphasen von der Systemfindung und -ausplanung über Beschaffung, Inbetriebnahme, Betrieb und Änderung bis hin zur Außerbetriebsetzung beschrieben. Die Regel sieht neben einer zentralen Leitsteuerung auch Einrichtungen zur Standortbestimmung und Lageerfassung für fahrerlose Transportsysteme vor. Zur weiteren Datenverarbeitung sind Einrichtungen zur Datenübertragung einschließlich peripherer Infrastruktur genannt.

DIN EN ISO 17427 *Intelligente Transportsysteme – Kooperative ITS* [49] sieht als Norm vor, die Verhaltenszuordnungen, Verantwortlichkeiten und Verpflichtungen von IVS in einer organisatorischen Architektur festzulegen. Sie fordert die Kooperation von Akteuren verschiedener Industriezweige. Ein Fahrzeugleitsystem muss daher in der Lage sein, Rechte und Rollen zuzuweisen sowie Fahrzeuge unterschiedlicher Hersteller zu vernetzen.

ISO/SAE 21434 *Straßenfahrzeuge – Cybersecurity engineering* [102] ist ein sich in der Entwicklung befindlicher Normenentwurf zur Informationssicherheit in Fahrzeugen und deren Kommunikationsschnittstellen zu anderen Fahrzeugen oder zur Infrastruktur. Er wird sich bezüglich des Inhalts und des Aufbaus an der ISO 26262 *Straßenfahrzeuge – Funktionale Sicherheit* orientieren und alle Teile und Lebensphasen vernetzter Fahrzeuge abdecken. Ein Fahrzeugleitsystem muss die darin standardisierten Maßnahmen zur Gewährleistung der IKT-Sicherheit umsetzen.

DIN SPEC 91345:2016-04 *Referenzarchitekturmodell Industrie 4.0* [56] ordnet als technische Regel den Konzepten und Komponenten von Industrie 4.0 eine Position in einer Referenzarchitektur zu. Die Position einer Komponente bestimmt sich aus ihrer Hierarchiestufe, ihrem Lebenszyklus und ihrer IT-Repräsentanz. Ein Fahrzeugleitsystem und seine Bestandteile müssen sich in dieses Referenzmodell einordnen lassen.

Aus den Standards zu allgemeinen Anforderungen lässt sich zudem die Forderung nach einer Betriebs- und Änderungsplanung ableiten, um die Funktionen über den gesamten Lebenszyklus zu überwachen und zu gewährleisten. Ein Fahrzeugleitsystem muss skalierbar und in der Lage sein, weitere Fahrzeuge, egal welchen Herstellers, zu integrieren. Das Rechte- und Rollenmodell muss allen Akteuren des Fahrzeugleitsystems bekannt gemacht werden, um Autorisierungen in der digitalen und physischen Welt gleichermaßen zu verwalten.

2.3 Beteiligte Akteure

Als Automatisierungssystem im Internet der Dinge ist ein Fahrzeugleitsystem durch eine große Anzahl mobiler Kommunikationsteilnehmer geprägt, die unterschiedliche Eigenschaften und Fähigkeiten aufweisen. Eine grundsätzliche Unterscheidung besteht zwischen den aktiven, zu vernetzenden Akteuren einerseits und den passiven Akteuren, welche die benötigte Kommunikationsinfrastruktur unterstützen oder bereitstellen, andererseits. In einem Fahrzeugleitsystem sind ferner Akteure zu betrachten, die zwar in der physischen Welt mit den Kommunikationsteilnehmern interagieren, kommunikationstechnisch jedoch nicht mit diesen verbunden sind. Die Anforderungen an die genannten Akteure werden aus einer Analyse einschlägiger Standards abgeleitet.

2.3.1 Fahrer und Passagiere

Ein Fahrzeugleitsystem dient dem Mobilitätsbedürfnis, da Personen und Güter schneller, sicherer und komfortabler bewegt werden können, als es ohne ein Fahrzeugleitsystem der Fall ist. Fahrer und Passagiere sind folglich die Zielgruppe des Fahrzeugleitsystems.

Fahrer müssen in einem Fahrzeugleitsystem besonders betrachtet werden. Die aktuelle Gesetzeslage schreibt insbesondere vor, dass ein Fahrer stets die volle Kontrolle über sein Fahrzeug behalten muss [16]. Das Fahrerverhalten stellt somit eine komplexe Störgröße in den Regelkreisen verbundener Automatisierungssysteme dar.

ISO/TR 21959-1:2020-01 *Straßenfahrzeuge – Menschliche Ausführungen und Zustände im Kontext des automatisierten Fahrens* [104] beschreibt als technische Regel die Bedeutung des menschlichen Fahrers und bildet somit eine Grundlage für ein Human-Machine Interface (HMI) in Fahrzeugleitsystemen. Hierzu zählen die Überleitungsphase von der manuellen zur automatischen Lenkung des Fahrzeugs und umgekehrt sowie mögliche Aufgaben des Fahrers, während das Fahrzeug automatisch durch das Fahrzeugleitsystem gelenkt wird. Ein Fahrzeugleitsystem muss stets auf Eingaben des menschlichen Fahrers reagieren können.

DIN EN ISO 17287:2003-10 *Straßenfahrzeuge – Ergonomische Aspekte von Fahrerinformations- und Assistenzsystemen – Verfahren zur Bewertung der Gebrauchstauglichkeit beim Führen eines Kraftfahrzeugs* [47] ist eine Norm zur Bewertung eines

solchen HMI und damit des wechselseitigen Informationsübergangs zwischen Fahrer und automatisiertem Fahrzeug. Die Funktion eines Fahrzeugleitsystems muss sich nach objektiven und nachvollziehbaren Kriterien bewerten lassen.

Zusammengefasst muss das Fahrzeugleitsystem dem Fahrer jederzeit die Kontrolle übertragen können. Es muss dem Fahrer signalisieren, ob es den gegenwärtigen und die prognostizierten Verkehrszustände sicher beherrschen kann. Hierzu ist eine Mensch-Maschine-Schnittstelle (HMI) zum Fahrzeugleitsystem notwendig, die dem Fahrer den Zustand über ein ergonomisch optimiertes Informations- und Kontrollsystem (Transport Information and Control System [TICS]) übermittelt und zugleich die Aktoren des Fahrzeugs stets sicher kontrolliert.

2.3.2 Fahrzeuge

Fahrzeuge transportieren Fahrer und Passagiere und bewegen sich auf den ihnen zugewiesenen Verkehrswegen. Ihre Trajektorien werden durch das Fahrzeugleitsystem beeinflusst. Der Betrieb von Fahrzeugen ist zahlreichen spezifischen Gesetzen und Verordnungen unterworfen.

SAE J 3016:2018-06-15 *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles* [152] ist eine Norm zur Definition und Klassifizierung von automatisiert fahrenden Kraftfahrzeugen anhand deren Eigenschaften. Sie unterteilt den Grad der Automatisierung von Fahrzeugen in sechs Stufen („SAE-Levels“), wobei *0* keine Automatisierung und *5* Vollautomatisierung bedeutet. Ein Fahrzeugleitsystem muss Fahrzeuge aller Stufen integrieren können.

DIN EN ISO 18542-1:2013-04 *Straßenfahrzeuge – Standardisierte Terminologie für Reparatur- und Wartungsinformationen (RMI)* [50] fordert einen normierten Zugriff auf Informationen zum Fahrzeugbetrieb. Neben einheitlichen Schnittstellen zum Auslesen von Wartungsinformationen werden auch standardisierte Prozesse bei der Durchführung von Wartung und Reparatur gefordert. Diese Schnittstellen sind herstellerübergreifend einheitlich zu implementieren.

Ein Fahrzeugleitsystem muss den regelmäßigen Kontakt mit einer befähigten und berechtigten Institution zur technischen Überprüfung von Fahrzeugen vorsehen und hierzu einheitliche Datenschnittstellen bieten.

Neben dieser allgemeinen Analyse der Anforderungen an Fahrzeuge in einem Fahrzeugleitsystem ist es für die weitere Entwicklung zielführend, eine Unterscheidung hinsichtlich kommunikationstechnischer Fähigkeiten der Fahrzeuge vorzunehmen.

Vernetzte Fahrzeuge

Diese Fahrzeugtypen sind mit Komponenten ausgerüstet, die drahtloses Senden und Empfangen von Daten sowie die Verarbeitung dieser Daten ermöglichen. Durch die Kopplung der Datenverarbeitung mit entsprechenden Aktoren und Sensoren bilden sie so die Schnittstelle des Fahrzeugleitsystems zur physischen Welt. Die Ausstattung mit Kommunikationstechnik macht sie zu Quellen und Senken aller ausgetauschten Nachrichten.

Unvernetzte Fahrzeuge

Diese Fahrzeugtypen besitzen keine Komponenten zum Senden und Empfangen von Daten. Dies kann verschiedene Gründe haben, beispielsweise mangelnde technische Voraussetzungen, Fehlfunktionen der Elektronik oder schlicht Verweigerung der Halter. Als Teil des Verkehrssystems interagieren sie dennoch in der physischen Welt untereinander und mit vernetzten Fahrzeugen.

Kompromittierte Fahrzeuge

Diese Fahrzeugtypen sind als vernetzte Fahrzeuge zwar kommunikationstechnisch Bestandteil des Fahrzeugleitsystems, verstoßen jedoch gegen die Vorgaben der Kommunikationsarchitektur. Durch Behauptung falscher Rechte und Rollen versuchen kompromittierte Fahrzeuge, sich unberechtigt Vorteile oder Berechtigungen innerhalb der Kommunikationsarchitektur oder in der physischen Welt anzueignen. Ein kompromittiertes Fahrzeug kann dabei aus eigenem Antrieb – oder dem seines Halters – handeln oder von Dritten ohne eigene Kenntnis manipuliert werden.

Sonstiger Nutzer

Verkehr ist ein komplexes System, in dem zahlreiche unterschiedliche Nutzer auf einer teilweise gemeinsamen Verkehrsfläche interagieren. Ein Fahrzeugleitsystem muss daher auch solche Beteiligte berücksichtigen, die zwar in der physikalischen Welt miteinander interagieren, kommunikationstechnisch jedoch nicht vernetzt sind. Bei solchen Beteiligten kann es sich um Fußgänger, Fahrradfahrer oder auch Gegenstände handeln.

Ein Fahrzeugleitsystem muss folglich die Möglichkeit zum Mischbetrieb aus vernetzten und nicht vernetzten Fahrzeugen bieten und Nicht-Teilnehmer adäquat berücksichtigen. Trotz fehlender Kommunikation sind aus diesem Mischbetrieb resultierende Konflikte in der physischen Welt zu vermeiden.

DIN CEN/TS 17380:2019-12 *Intelligente Verkehrssysteme – Urbane ITS – Steuerung in einer „kontrollierten Zone“ unter Verwendung von C-ITS* [34] beschreibt als technische Regel die administrativen Vorgaben zum Betrieb abgegrenzter Bereiche, in denen Verkehrstelematik implementiert werden kann. Bestandteile dieser Verkehrstelematik sind Leitsysteme, die Fahrzeuge teilweise oder vollständig steuern. Das Fahrzeugleitsystem muss sich in bestehende Verkehrsinfrastrukturen integrieren lassen.

Die korrekte Funktion eines Fahrzeugleitsystems darf nicht von einem minimalen Anteil vernetzter Fahrzeuge an der gesamten Fahrzeugflotte abhängig sein. Es muss robust gegenüber kompromittierten Teilnehmern und damit in der Lage sein, Angriffsversuche kompromittierter Teilnehmer abzuwehren. Dies bezieht sich auf aktiv und passiv an der Kommunikation beteiligte Angreifer.

2.3.3 Vermittlungstechnik

Falls die Knoten eines Netzes ausschließlich durch Fahrzeuge gebildet werden, kann die Zuverlässigkeit bestehender Netzmaschen aufgrund der komplexen und schwer vorhersehbaren Fahrzeugbewegungen nicht garantiert werden: Zum einen können Entfernungen zwischen Fahrzeugen zu groß für eine Funkübertragung werden. Zum anderen fehlt in diesem

Fall eine übergeordnete Instanz zur Steuerung des Nachrichtenflusses. Letzteres macht das gesamte Netz anfällig für unerwünschte Nachrichten sowie Überlastungsangriffe. Ein Fahrzeugleitsystem benötigt daher Relaisstationen als zusätzliche Netzknoten: Einerseits können damit zuverlässige Verbindungen zwischen Sendern und Empfängern garantiert werden. Andererseits kann mit dem Relais ein Moderator eingerichtet werden, der bei Überlastungen zielgerichtet in den Netzverkehr eingreift.

Relais

Beim Relais handelt es sich um eine technische Einrichtung, die wie vernetzte Fahrzeuge zum drahtlosen Senden und Empfangen von Daten sowie zur Datenverarbeitung in der Lage ist. Das Relais interagiert jedoch nicht in der physischen Welt mit den Fahrzeugen, sondern befindet sich stationär außerhalb des Verkehrsraums. Das Relais muss in einem Fahrzeugleitsystem die folgenden Komponenten umfassen:

- Funkmasten zum Empfang und zum Senden von Nachrichten,
- lokale Kommunikationsrechner zur Vermittlung der Nachrichten,
- eine zentrale Recheneinheit zur
  - globalen Optimierung des Verkehrssystems und zur
  - Durchführung der kryptografischen Maßnahmen auf Seiten des Relais sowie
- eine Datenbank zur Verwaltung aller relevanten Informationen über die Kommunikationsteilnehmer.

Notwendige Rechte müssen durch eine entsprechend autorisierte Instanz verwaltet und vergeben werden.

DIN CEN/TS 17182:2019-03 *Intelligente Verkehrssysteme – eSicherheit – eCall über eine ITS-Station* [33] beschreibt als technische Regel ein Notrufsystem („eCall“ genannt), welches bei einem Unfall automatisch einen Notruf unter Angabe der Koordinaten der beteiligten Fahrzeuge an eine Zentrale übermittelt. Die Regel schreibt eine „ITS-Stations- und Kommunikationsarchitektur [vor], die den Betrieb von ITS-Anwendungen auf verwaltete, sichere und priorisierte Art ermöglicht“. Ein solches Notrufsystem nach EN 16072, EN 15722 und EN 16545 ist gesetzlich für Neufahrzeuge vorgeschrieben.

DIN CEN/TS 17395:2020-04 *Intelligente Verkehrssysteme – eSicherheit – eCall für automatisierte und autonome Fahrzeuge* [35] stellt aktuell eine Vornorm dar und beschreibt die Übertragung der zuvor genannten Norm auf automatisierte und autonome Fahrzeuge. Die Vornorm verwendet den Begriff der *ITS-Station* als notwendige Komponente eines intelligenten Verkehrssystems, die eine zentrale Verarbeitung der Notrufe ermöglicht.

DIN EN ISO 18750:2018-09 *Intelligente Verkehrssysteme – Kooperative ITS – Lokale dynamische Karten* [51] ist eine Norm zur Beschreibung der einheitlichen Datennutzung durch alle Teilsysteme intelligenter Verkehrssysteme. Dies betrifft insbesondere

digitale Karten. Auch digitale Karten, die für lokale und isolierte Anwendungen erstellt werden, sollen nach einer Prüfung allen Teilnehmern eines IVS zur Verfügung gestellt werden.

DIN CEN ISO/TS 17426 *Intelligente Transportsysteme (ITS) – Kooperative Systeme – Kontextuelle Geschwindigkeiten* [52] ist eine technische Regel zur Beschreibung, wie die aktuelle Geschwindigkeitsempfehlung bestimmt und deren Übertragung in Fahrzeuge mittels Verkehrstelematik erreicht werden soll. Sie sieht die Ermittlung von Verkehrs- und Umwelteinflüssen im Verantwortungsbereich des Infrastrukturbetreibers.

Aus der Analyse der Standards ergeben sich mehrere Aspekte hinsichtlich der Notwendigkeit und des Leistungsumfangs eines Relais in einem Fahrzeugleitsystem. Ein Fahrzeugleitsystem muss zumindest einen Teil der Kommunikationen über eine zentrale Stelle abwickeln und zur zentralen Verwaltung und Verteilung von Informationen, hier digitaler Karten, ausgelegt sein. Technisch muss ein Fahrzeugleitsystem über einen Kommunikationskanal zu einer zentralen Stelle verfügen, um von dort die aktuellen Vorgaben zur globalen Optimierung des Verkehrssystems erhalten zu können.

2.3.4 Administration

Zur Bereitstellung und Verwaltung der technischen Betriebsmittel für ein Fahrzeugleitsystem ist eine administrative Struktur notwendig.

DIN EN 419241-1:2018-09 *Vertrauenswürdige Systeme, die Serversignaturen unterstützen* [38] sieht vor, dass zentrale IKT-Systeme wie Server stets von vertrauenswürdigen Stellen zertifiziert werden müssen. Sie gibt zudem Anforderungen an die Vertrauenswürdigkeit der Stellen vor, die solche Zertifikate ausstellen. Hierzu zählen die alleinige Kontrolle über die Signaturerstellungseinheit durch die vertrauenswürdige Stelle sowie die Nutzung sicherer Kommunikationskanäle zur Verteilung der Zertifikate.

Als Bestandteil der Mobilität stellt ein Fahrzeugleitsystem eine Form der Daseinsvorsorge dar. Vertrauenswürdig gemäß den einschlägigen Standards können daher nur solche Institutionen sein, die allgemein autorisiert und legitimiert sind, hoheitliche Aufgaben zu erbringen. Für ein Fahrzeugleitsystem kommt als solche Institution nur eine hoheitliche Behörde in Betracht. Diese Instanz muss sich als Zertifizierungsstelle der Identität und Authentizität von Teilnehmern versichern und kann diese durch Ausstellen digitaler Zertifikate bestätigen.

2.4 Anforderungen an die Netztechnik

Die Netztechnik muss die zuverlässige Verbindung zwischen Netzteilnehmern und die sichere Zustellung von Nachrichten zu avisierten Empfängern über diese Verbindungen gewährleisten. Unterschiedliche Standards beschäftigen sich mit der Netztechnik für verschiedene Anwendungsfälle. In Fahrzeugleitsystemen kommen sowohl drahtlose als auch kabelgebundene Netze zur Anwendung.

2.4.1 Funktechnik

Alle Daten von und zu Fahrzeugen müssen drahtlos übertragen werden, da es sich bei Fahrzeugen um bewegliche Objekte handelt. Die genutzten Frequenzen müssen sich regelkonform in das elektromagnetische Spektrum einfügen.

VDI/VDE 2185 Blatt 1:2020-08 *Funkgestützte Kommunikation in der Automatisierungstechnik – Anforderungen und Grundlagen* [175] erörtert mögliche Vorgehensweisen, um einen störungsfreien Betrieb von Funkkommunikationssystemen in Mess- und Automatisierungsanwendungen zu ermöglichen. Die technische Regel geht dabei insbesondere auf die zeitkritische Nachrichtenübertragung in industriellen Anwendungen ein. Sie beschreibt ein mögliches Management zur Koexistenz von Funklösungen.

DIN EN 62657-1:2018-05 *Industrielle Kommunikationsnetze – Funk-Kommunikationsnetze* [43] ist eine Norm zur Beschreibung von Rechten sowie Limitierungen bei der Anwendung von Funktechnik. Hierzu zählen insbesondere die Regeln zur Nutzung bestimmter Frequenzbänder in der industriellen Automatisierung.

DIN EN 303613:2020-03 *Intelligente Verkehrssysteme (IVS) – Spezifikation der LTE-V2X-Zugriffsschicht für Intelligente Verkehrssysteme zum Betrieb im 5-GHz-Frequenzband* [37] ist eine Norm zur Spezifikation der für die Nutzung durch IVS zugelassenen Frequenzbänder. Insbesondere definiert sie den Betrieb eines IVS im dedizierten Frequenzband bei 5 GHz. Die Kommunikationsvorgänge zwischen Fahrzeugen untereinander sowie zwischen Fahrzeugen und der Infrastruktur werden in der Norm als „Vehicle to everything (V2X)“ bezeichnet.

Ein Fahrzeugleitsystem muss sich in das bestehende Funkspektrum integrieren, beispielsweise durch Nutzung des Industrial, Scientific and Medical (ISM)-Frequenzbandes oder des für IVS reservierten G5-Bandes bei 5 GHz. Es muss alle Anforderungen an die elektromagnetische Verträglichkeit (EMV) erfüllen und robust gegen Interferenzen mit anderen funkgestützten Anwendungen sein. Die eingesetzte Funktechnik muss zudem in der Lage sein, die aufmodulierten Informationen echtzeitfähig zu übertragen. Topologisch sind hierzu die Anzahl benötigter Zwischenstationen zwischen Sendern und Empfängern sowie die jeweiligen Entfernungen der Zwischenstationen zu evaluieren.

2.4.2 Topologie und Routing

Bestehende Standards zu Topologie und Routing in Automatisierungsnetzen des Verkehrsbereichs beschränken sich zumeist auf kabelgebundene Feldbussysteme. In einem Fahrzeugleitsystem wird kabelgebundene Übertragung zur Vernetzung aller stationären Komponenten eingesetzt.

DIN EN 62591:2017-02 *Industrielle Kommunikationsnetze – Drahtlose Kommunikationsnetze und Kommunikationsprofile* [42] liefert eine Norm zur Nutzung des Highway Addressable Remote Transducer (HART)-Protokolls durch drahtlose Übertragungsnetze. WirelessHART sieht wie das herkömmliche, kabelgebundene HART-Protokoll ein Kontrollsystem für die Netzverwaltung vor.

ETSI TR 102 962 *Intelligent Transport Systems (ITS); Framework for Public Mobile Networks in Cooperative ITS (C-ITS)* [65] sieht vor, dass IVS-Anwendungen in bestehende zellenbasierte Kommunikationsnetze integrierbar sein müssen. Ein Fahrzeugleitsystem muss daher in der Lage sein, eine zellenbasierte Topologie zu bilden oder existierende, zellenbasierte Kommunikationsnetze zu nutzen.

Das Routen von Datenpaketen durch ein Netz zum Empfänger ist umso effizienter möglich, je strukturierter das Netz aufgebaut ist. In unstrukturierten Netzen, die zudem über keine zentrale Verwaltung verfügen, kann zunächst nur ein Flooding-Algorithmus verwendet werden. Dieser erzeugt jedoch viel unnötigen Datenverkehr im Netz und kann daher zu einer Überlastung des Netzes führen.

2.4.3 Identifikatoren und Adressen

Jeder mögliche Empfänger und damit jeder Knoten im Netz muss mit einer eindeutigen Adresse (Rufzeichen) ausgestattet sein, um seine Identifizierung zu ermöglichen und Nachrichten eindeutig zuzustellen. Die Verwendung einer spezifischen Adresse ist eng mit der sicheren Authentifizierung verknüpft, um die Beanspruchung einer beliebigen Adresse zu unterbinden. Die missbräuchliche Behauptung einer fremden Adresse wird auch Identitätsdiebstahl genannt.

DIN EN 302636-1:2014-09 *Intelligente Verkehrssysteme (IVS) – Fahrzeugkommunikation – GeoNetworking* [36] schreibt eindeutige Adressen für alle Teilnehmer eines Fahrzeugnetzes vor. Indem die Netzadresse teilweise aus der geografischen Position abgeleitet und so die geografische Position eines Knotens zum Bestandteil von Routingtabellen wird, können Datenpakete effizient zum jeweils geografisch nächsten Knoten geleitet werden. Wird die Netzadresse vollständig aus der geografischen Position abgeleitet, kann die Adresse dezentral und ohne Beteiligung einer weiteren Instanz erzeugt werden. Ein Fahrzeugleitsystem muss dann ein positionsbasiertes Routing ermöglichen, um Nachrichten auf dem räumlich (und bei ansonsten gleichen Parametern auch zeitlich) kürzesten Weg zum Empfänger zu leiten.

Bestehende Standards fordern eine eindeutige digitale Identifizierung vernetzter Fahrzeuge. Das Fahrzeugleitsystem muss die Übertragung sowohl an einen einzelnen Empfänger (Unicast) als auch an einen definierten Empfängerkreis (Multicast oder Broadcast) ermöglichen. Andere als die berechtigten, avisierten Empfänger dürfen nicht in der Lage sein, den Nachrichteninhalt zu lesen.

2.5 Anforderungen an die funktionale Sicherheit

Funktionale Sicherheit ist ein Bestandteil der Sicherheit (im Sinne von Gefahrlosigkeit für die Umwelt) eines Systems. Ein Fahrzeugleitsystem umfasst sowohl Kraftfahrzeuge als auch sicherheitsbezogene programmierbare, elektronische Systeme, sodass mehrere Bereiche der funktionalen Sicherheit betroffen sind.

DIN EN 61508-1:2011-02 *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme* [39] stellt eine übergeordnete

Norm zur funktionalen Sicherheit von elektrischen, elektronischen und programmierbaren elektronischen (E/E/PE) Systemen dar. Ein Fahrzeugleitsystem muss als programmierbares Automatisierungssystem den Anforderungen an die funktionale Sicherheit gemäß dieser Norm genügen.

ISO 26262-1:2018-12 *Straßenfahrzeuge – Funktionale Sicherheit* [100] ist eine Weiterentwicklung der IEC 61508 für die Anforderungen an die funktionale Sicherheit in Anwendungsfällen mit Beteiligung straßengebundener Kraftfahrzeuge. Sie verwendet den Begriff „Item“ als Bezeichnung für das nach funktionalen Sicherheitsaspekten zu bewertende System auf Fahrzeugebene oder für ein System von Systemen. Es werden notwendige Schritte vorgegeben, um die Erfüllung der Anforderungen nachzuweisen. Die funktionale Sicherheit ist nach diesen Schritten zu konzipieren und nachzuweisen, wenn das gesamte Fahrzeugleitsystem als das Item angesehen wird.

ISO 13849-1:2015-12 *Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen* [97] besteht aus insgesamt zwei Teilen und spezifiziert allgemeine Vorgaben für Steuerungen hinsichtlich Leistung, Überwachung und Zuverlässigkeit. Es werden Entwurfsempfehlungen zur Berücksichtigung während der Umsetzung gegeben, die unter anderem die Einstufung der Funktionen in Sicherheitsniveaus und deren anschließende Validierung beinhalten.

Die Standards zur funktionalen Sicherheit fordern von einem Fahrzeugleitsystem, seine einzelnen Funktionen hinsichtlich ihrer Bedeutung für die Sicherheit vorab zu analysieren. Ausgehend von dieser Funktionsanalyse ist eine Gefahren- und Risikoanalyse durchzuführen, die eine Einordnung der Funktionen in entsprechende Sicherheitsstufen ermöglicht. Darauf aufbauend muss mit der Entwicklung funktionaler und technischer Sicherheitskonzepte aufgezeigt werden, wie den identifizierten Gefahren und Risiken begegnet wird. Die erforderlichen Schritte zur Umsetzung dieser Konzepte in einem Fahrzeugleitsystem werden im Folgenden dargestellt.

2.5.1 Funktionsanalyse

Die von jedem technischen System zu erfüllenden übergeordneten funktionalen Sicherheitsanforderungen sind korrekte, sichere Funktion sowie im Fehlerfall kontrolliertes Überführen in einen sicheren Zustand. Hierzu sind Funktionsanalyse, Fehleranalyse und Maßnahmenanalyse notwendig [87].

Funktionsdekomposition Der erste Teil der Funktionsanalyse, die Unterteilung in Einzelfunktionen, kann bereits zu Beginn der Produktentwicklung erarbeitet werden. Mit der folgenden Auflistung wird dies für ein Fahrzeugleitsystem getrennt nach den Anforderungen an die Fahrzeuglenkung und den Anforderungen an die Kommunikationen, jeweils in absteigender Abstraktionsebene, geleistet. Die so entstehende Funktionsdekomposition ist auch in Abbildung 2.2 dargestellt.

1. Anforderungen an die Fahrzeuglenkung
   - Optimierung des Verkehrsablaufs: Die zentrale Aufgabe eines Fahrzeugleitsystems und damit die Funktion auf der höchsten Abstraktionsebene ist die Optimierung des Verkehrsablaufs anhand einer Zielfunktion. Durch optimale Aus-

nutzung der vorhandenen Verkehrsinfrastruktur wird die Reisezeit für alle Verkehrsteilnehmer minimiert. Das Fahrzeugleitsystem analysiert dazu alle möglichen Routen für alle in das Fahrzeugleitsystem integrierten Fahrzeuge. Alle Fahrzeuge werden über die optimale Route geleitet. Die Zielfunktion zur Bestimmung der optimalen Route berücksichtigt neben der Reisezeit noch weitere Parameter wie den Kraftstoffverbrauch.

- Regelung von Abständen und Geschwindigkeiten: Abstände und Geschwindigkeiten der Fahrzeuge werden durch den Einsatz des Fahrzeugleitsystems optimiert, um Fahrzeuge sicher und situationsangepasst zu steuern sowie Streckenkapazitäten effizient auszunutzen. Dadurch können in der gleichen Zeiteinheit mehr Fahrzeuge einen gewissen Streckenabschnitt passieren, als es ohne Fahrzeugleitsystem der Fall wäre. Das Fahrzeugleitsystem muss daher die Positionen, Trajektorien und Randbedingungen aller Fahrzeuge bestimmen können, um eine entsprechende Regelung der Abstände vorzunehmen. Hierzu zählt auch die Funktion, die Geschwindigkeit auf $\vec{v} = 0$ zu stellen, beispielsweise bei Annäherung an ein Haltesignal.
- Abbildung abweichender Streckenführung: Das Fahrzeugleitsystem muss Fahrzeuge durch eine temporär geänderte Streckenführung leiten können. Die Streckenführung kann sich lokal durch Verschwenkung der Fahrstreifen oder Verringerung ihrer Anzahl sowie durch Sperrung von Fahrstreifen und daraus resultierender Umleitung ändern. In beiden Fällen muss dem Fahrzeugleitsystem die geänderte Route bekannt gemacht werden. Das Fahrzeugleitsystem muss alle betroffenen Fahrzeuge durch Nachrichten informieren und wenn möglich direkt durch die geänderte Streckenführung steuern.

2. Anforderungen an die Kommunikationen
   - Einheitliche Kommunikationsarchitektur: Für die Vernetzung der Fahrzeuge verschiedener Hersteller wird eine einheitliche Kommunikationsarchitektur benötigt. Diese muss in der Lage sein, die Fahrzeuge verschiedener Hersteller zu integrieren. Ihre Funktion besteht somit in der Bereitstellung einheitlicher Kommunikationsschnittstellen für den Nachrichtenaustausch und die Nachrichtenverarbeitung. Informationen über nicht vernetzte Fahrzeuge müssen verteilt werden können.
   - Sichere und rechtzeitige Datenübertragung: Für alle Funktionen muss das Fahrzeugleitsystem die Voraussetzungen für sichere und rechtzeitige Datenübertragungen zwischen den Fahrzeugen schaffen. Alle notwendigen Nachrichten müssen korrekt und rechtzeitig übertragen werden, um gefährliche Situationen durch falsche oder zu späte Übertragungen zu vermeiden.

Nachdem die Funktionen und deren Wechselwirkungen analysiert wurden, muss im zweiten Teil der Funktionsanalyse das Systemverhalten bei Fehlfunktionen untersucht werden.

Sicherheitsanalyse Das Fahrzeugleitsystem muss zu ausfallsicherheitsgerichtetem Systemverhalten (engl. *fail-safe*) in der Lage sein, da Hardware nur mit endlicher Fertigungsgenauigkeit und komplexe Software nicht fehlerfrei erstellt werden können. Für ein Fahr-

zeugleitsystem müssen gemäß ISO 26262 zunächst verschiedene Ausfallraten λ ($[\lambda] = \mathrm{h}^{-1}$) ermittelt werden [100]:

- Ausfallrate für Einzelfehler der Hardwareelemente: *Single-point faults* λ_{SPF}
- Ausfallrate für Restfehler der Hardwareelemente: *Residual faults* λ_{RF}
- Ausfallrate für Mehrfachfehler der Hardwareelemente: *Multiple-point faults* λ_{MPF}
  - wahrgenommene oder beherrschte Mehrfachfehler: *Perceived or detected MPF* $\lambda_{MPF\,PD}$
  - durch keine Maßnahme abgedeckte Mehrfachfehler: *Latent MPF* $\lambda_{MPF\,L}$
- Ausfallrate für Fehler der Hardwareelemente ohne Verletzung eines Sicherheitsziels: *Safe faults* λ_S

Diese Ausfallraten sind Berechnungsgrundlagen für die *Probability of dangerous Failure per Hour (PFH)* ($[PFH] = \mathrm{h}^{-1}$) sowie die *Latent Fault Metric (LFM)* und die *Single Point Fault Metric (SPFM)*, wobei letztere Metriken in Prozent angegeben werden.

Sicherer Zustand Für den Ausfall ist mindestens ein sicherer Zustand zu definieren, in den das Fahrzeugleitsystem (oder jedes betroffene Teil davon) überführt werden kann, bevor ein durch den Ausfall verursachtes Schadensereignis eintritt. Der sichere Zustand eines Fahrzeugleitsystems könnte grundsätzlich das kontrollierte Anhalten aller Fahrzeuge darstellen. Hierbei ist jedoch zu beachten, dass ein Haltesignal nicht alle Fahrzeuge erreichen, einzelne Fahrzeuge nicht in das Fahrzeugleitsystem integriert sein oder das Haltesignal mutwillig missachtet werden könnte. Sich weiterbewegende Fahrzeuge wären dann plötzlich mit zahlreichen Hindernissen auf ihren Fahrwegen konfrontiert, was ein zusätzliches Risiko bedeutet.

Dieses Beispiel bestätigt, dass die Betrachtung ausfallsicherheitsgerichteten Systemverhaltens in einem frühen Stadium der Produktentwicklung nur bedingt möglich ist. Die Entwicklung ausfallsicherheitsgerichteten Systemverhaltens erfordert vielmehr einen iterativen Prozess, da sich mögliche Risiken erst im Laufe der Produktentwicklung zeigen. Die Funktionsdekomposition und die Sicherheitsanalyse sind Voraussetzungen für die im

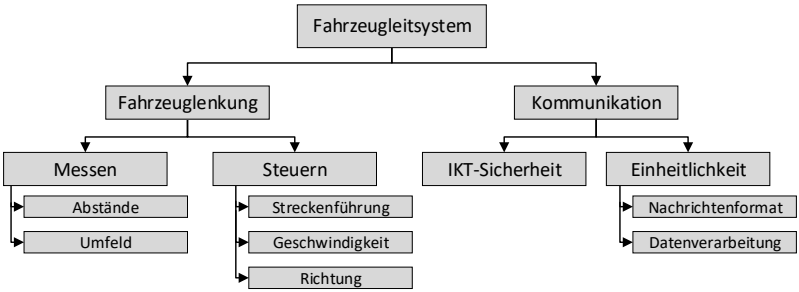


Abbildung 2.2: Funktionsdekomposition für ein Fahrzeugleitsystem

Folgenden durchgeführten Gefahren- und Risikoanalysen, mit der jede Teilfunktion entsprechend bewertet wird.

2.5.2 Gefahren- und Risikoanalyse

Die Gefahren- und Risikoanalyse ist eine zentrale Anforderung bei der Produktentwicklung nach ISO 26262 und wird im Folgenden für ein Fahrzeugleitsystem geleistet. Zur Bewertung des Risikos gilt vereinfachend:

$$Risiko = Eintrittswahrscheinlichkeit\ (E) \times Schaden\ (S) \tag{2.4}$$

Zur Klassifizierung des Schadensausmaßes werden drei Klassen unterschieden, die in die zuvor genannte Formel eingehen [87]:

- S1: Leichte bis mittlere Verletzungen
- S2: Schwere Verletzungen, Überleben wahrscheinlich
- S3: Lebensgefährliche Verletzungen, Überleben unwahrscheinlich

Entsprechend wird mit der Eintrittswahrscheinlichkeit verfahren, die in fünf Klassen eingeteilt wird [87]:

- E0: Unvorstellbar
- E1: Sehr niedrige Eintrittswahrscheinlichkeit
- E2: Niedrige Eintrittswahrscheinlichkeit
- E3: Mittlere Eintrittswahrscheinlichkeit
- E4: Hohe Eintrittswahrscheinlichkeit

Diese Einstufungen müssen bei der Konzeption eines Fahrzeugleitsystems zur zielgerichteten Bewertung von Risiken und anschließender Integration von Sicherheitsfunktionen beachtet werden.

Die Eintrittswahrscheinlichkeit kann nur auf Basis bekannter Teilsysteme bewertet werden, da für integrierte Fahrzeugleitsysteme noch keine praktischen Erfahrungswerte vorliegen. Das Schadensausmaß wird dann auf die möglichen Auswirkungen in einem Fahrzeugleitsystem übertragen und das Risiko bewertet.

Die ISO 26262 sieht als weiteren Faktor bei der Risikobewertung die Kontrollierbarkeit (C) von Fehlern durch den Fahrer vor, die mit vier Klassen bewertet wird [87]:

- C0: Im Allgemeinen kontrollierbar
- C1: Einfach kontrollierbar
- C2: Normalerweise kontrollierbar
- C3: Schwierig kontrollierbar oder nicht kontrollierbar

Mit diesem Faktor wird eine Aussage darüber getroffen, in welchem Maße eine Fehlfunktion durch den Fahrer eines Fahrzeugs beherrschbar ist.

Ziel der Gefahren- und Risikoanalysen ist die Zuordnung jeder Funktion zu einem Automotive Safety Integrity Level (ASIL). Der ASIL beschreibt eine Stufe für das tolerierbare Restrisiko und verlangt die Unterschreitung einer maximalen *Probability of dangerous Failure per Hour (PFH)* sowie Mindestwerte für eine *Latent Fault Metric (LFM)* und eine *Single Point Fault Metric (SPFM)*. ASIL D fordert die strengsten, ASIL A die geringsten Anforderungen. In Tabelle 2.1 ist die Ableitung des ASIL aus den Faktoren S, E und C dargestellt. Nicht mit einem ASIL belegte Zellen bezeichnen Risiken, denen allein mit Maßnahmen des Qualitätsmanagements (QM) begegnet werden kann.

Tabelle 2.1: Bestimmung des ASIL nach ISO 26262 [100]

		C1	**C2**	**C3**
S1	**E1**	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	**E1**	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	**E1**	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Im vorliegenden Anwendungsfall wird ein Fahrzeugleitsystem bewertet, das im Regelbetrieb ausschließlich von Digitalrechnern gesteuert wird. Diese Digitalrechner sind zu einem definierten Verhalten programmiert und zusammen mit den verbundenen Aktoren zu einer definierten Reaktionszeit in der Lage. Eine weitere Abstufung, die zudem individuelle Eigenschaften wie fahrerisches Können berücksichtigt, ist somit nicht sinnvoll. In Fahrzeugleitsystemen kann die Kontrollierbarkeit C von Fehlfunktionen daher binär unterteilt werden in solche, die mit den vorhandenen Rechenkapazitäten beherrschbar sind, und solche, die es nicht sind.

2.5.3 Sicherheitsziele und Automotive Safety Integrity Levels

Sicherheitsziele werden definiert, um gefährliche Situationen auch bei möglichen Fehlfunktionen eines Fahrzeugleitsystems zu erkennen und zu vermeiden. Eine Gefahren- und Risikoanalyse der Funktionen liefert als Anforderungen an ein Fahrzeugleitsystem die folgenden Sicherheitsziele:

1. Vermeide Inkompatibilitäten bei der Nachrichtenverarbeitung.
2. Vermeide eine Fehldetektion nicht vernetzter Objekte.
3. Vermeide falsches oder verzögertes Übermitteln von Nachrichten.

4. Vermeide falsches oder verzögertes Einstellen geänderter Streckenführungen.
5. Vermeide falsches oder verzögertes Messen von Abständen.
6. Vermeide falsches oder verzögertes Einstellen von Geschwindigkeiten oder Richtungen.

Die Punkte 3 bis 6 beziehen sich auf unterschiedliche Aspekte der geforderten Echtzeitfähigkeit. Entsprechend der ISO 26262 werden die Sicherheitsziele einem ASIL zugeordnet. Tabelle 2.2 zeigt diese qualitative Risikobewertung für die definierten Sicherheitsziele.

Tabelle 2.2: Bestimmung des ASIL in Fahrzeugleitsystemen

	S1	S2	S3
E4	–	Falsches oder verzögertes Einstellen geänderter Streckenführung	Fehldetektion nicht vernetzter Objekte
E3	Inkompatibilität bei der Nachrichtenverarbeitung	Falsches oder verzögertes Übermitteln von Nachrichten	Falsches oder verzögertes Messen von Abständen
E2	–	–	Falsches oder verzögertes Einstellen von Geschwindigkeiten oder Richtungen
E1	–	–	–

Mit dieser Zuordnung zu einem ASIL können konkrete Anforderungen an die Sicherheitsziele formuliert werden.

ASIL A fordert eine PFH unter $10^{-6}\,\mathrm{h}^{-1}$ [109]. Diesem ASIL wird das folgende Sicherheitsziel zugeordnet:

- Vermeide Inkompatibilitäten bei der Nachrichtenverarbeitung.

ASIL B fordert eine PFH unter $10^{-7}\,\mathrm{h}^{-1}$, eine LFM von mindestens 60 % und eine SPFM von mindestens 90 % [109]. Diesem ASIL werden die folgenden Sicherheitsziele zugeordnet:

- Vermeide falsches oder verzögertes Übermitteln von Nachrichten.
- Vermeide falsches oder verzögertes Einstellen von Geschwindigkeiten oder Richtungen.

ASIL C fordert eine PFH unter $10^{-7}\,\mathrm{h}^{-1}$, eine LFM von mindestens 80 % und eine SPFM von mindestens 97 % [109]. Diesem ASIL werden die folgenden Sicherheitsziele zugeordnet:

- Vermeide falsches oder verzögertes Einstellen geänderter Streckenführungen.
- Vermeide falsches oder verzögertes Messen von Abständen.

ASIL D fordert eine PFH unter $10^{-8}\,\mathrm{h}^{-1}$, eine LFM von mindestens 90 % und eine SPFM von mindestens 99 % [109]. Diesem ASIL wird das folgende Sicherheitsziel zugeordnet:

- Vermeide eine Fehldetektion nicht vernetzter Objekte.

Mit der Definition der Sicherheitsziele und deren Zuordnung zu einem ASIL wurden die Anforderungen an die funktionale Sicherheit in einem Fahrzeugleitsystem analysiert. Konkrete technische Lösungen sind kein Bestandteil dieser Anforderungsanalyse, sondern werden als Maßnahmen bei der Entwicklung eines Fahrzeugleitsystems vorgesehen.

2.5.4 Funktionales Sicherheitskonzept

Aus jedem Sicherheitsziel müssen Sicherheitsanforderungen abgeleitet werden. Die Umsetzung dieser Anforderungen in konkrete Maßnahmen stellt das funktionale Sicherheitskonzept dar. Dieses muss mindestens die folgenden Gesichtspunkte umfassen [100]:

- Fehlerentdeckung und -vermeidung
- Überführen in den sicheren Zustand
- Mechanismen zur Fehlertoleranz
- Fehlerwarnungen
- Priorisierung von Steuer- oder Regelinformationen bei Mehrfachanforderungen

Die Sicherungsmaßnahmen müssen bezogen auf die zugehörigen Funktionen in das Fahrzeugleitsystem integriert werden.

2.5.5 Technisches Sicherheitskonzept

Das technische Sicherheitskonzept für ein Fahrzeugleitsystem verlangt, dass der Ausfall eines Systems nicht zum Ausfall weiterer Systeme führen darf. Aus den dargestellten Abstrahierungsebenen ergibt sich, dass sich Fehler bei Funktionen mit hohem Abstrahierungsgrad nicht negativ auf Funktionen mit niedrigem Abstrahierungsgrad auswirken dürfen und umgekehrt. Die Umsetzung eines technischen Sicherheitskonzepts fordert somit eine technische und organisatorische Trennung der einzelnen Funktionen, sofern dies möglich ist. Die Funktionen müssen hierzu über Schnittstellen gegeneinander abgegrenzt und in der Lage sein, einen Ausfall zu registrieren.

Zur Berücksichtigung nicht vernetzter Fahrzeuge muss ein Fahrzeugleitsystem zusätzliche Sensoren in der Infrastruktur implementieren, um ein ganzheitliches Bild der umgebenden Situation zu erfassen.

2.6 Anforderungen an die Informations- und Kommunikationssicherheit

In einem Fahrzeugleitsystem können alle drahtlosen Übertragungen abgehört und verändert werden. Der Informations- und Kommunikationssicherheit (IKT-Sicherheit) kommt daher eine zentrale Bedeutung zu, was sich auch aus entsprechenden Standards ableiten lässt.

DIN EN ISO/IEC 27000:2020-06 *Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme* [54] bildet die zentrale Normenreihe für informations- und kommunikationstechnische Sicherheit. Die Reihe spezifiziert Steuerung, Kontrolle, Aufrechterhaltung und Verbesserung eines Managementsystems für Informationssicherheit (Information Security Management System [ISMS]), um die IKT-Sicherheit eines Produkts in allen Phasen der Wertschöpfung zu gewährleisten und zu verbessern. In einem Fahrzeugleitsystem ist daher ein angepasstes ISMS vorzusehen, welches die Bereiche Planung, Implementierung und Überwachung umfasst.

VDI/VDE 2182 Blatt 1:2020-01 *Informationssicherheit in der industriellen Automatisierung – Allgemeines Vorgehensmodell* [174] überträgt in Form einer technischen Regel die Anforderungen aus der ISO 27000 auf automatisierte Maschinen und Anlagen und schlägt die Umsetzung konkreter Schutzmaßnahmen vor. Sie legt einen Schwerpunkt auf die Abstimmung zwischen Hersteller und Nutzer, was die enge Verflechtung von Mensch und Automatisierungssystem in einem Fahrzeugleitsystem unterstreicht.

DIN EN ISO/IEC 15408-1:2020-06 *Informationstechnik – IT-Sicherheitsverfahren – Evaluationskriterien für IT-Sicherheit* [53] ist ein aktueller Normenentwurf, der ein konkretes Bewertungsmodell für die umgesetzten Konzepte und Prinzipien zur Gewährleistung der IKT-Sicherheit zur Verfügung stellt. Hierzu werden den einzelnen Funktions- und Sicherheitskomponenten sogenannte Schutzprofile zugewiesen. Ein Fahrzeugleitsystem muss daher eine Unterteilung in voneinander abgegrenzte Komponenten vorsehen und diese Komponenten mit einem Rechte- und Rollenmodell sowie Schutzprofilen ausstatten.

DIN EN 61907:2010-09 *Zuverlässigkeit von Kommunikationsnetzen* [40] ist die Norm zur Bewertung der Netzzuverlässigkeit und stellt einen Prozess zu ihrer Realisierung bereit. Zudem trifft die Norm Aussagen zur Gestaltung von Netzen und der anschließenden Leistungsbeurteilung. Diese wird durch eine Sicherheitsbetrachtung und Messung der Dienstgüte durchgeführt. An ein Fahrzeugleitsystem ergibt sich daraus die Anforderung, Zuverlässigkeit und Leistungsfähigkeit des Übertragungskanals laufend zentral zu überwachen.

DIN CEN ISO/TS 21177:2020-01 *Intelligente Verkehrssysteme – Sicherheitsdienste für eine ITS-Station zum sicheren Aufbau von Sitzungen und zur Authentisierung zwischen vertrauenswürdigen Geräten* [32] ist eine Norm für Sicherheitsanforderungen und -dienste zur sicheren Kommunikation in intelligenten Verkehrssystemen. Diese soll durch eine „ITS-Station“ erreicht werden. Neben den IKT-Schutzzielen soll diese Station Authentizität und Vertrauenswürdigkeit der sendenden Quelle gewährleisten. In einem Fahrzeugleitsystem führt dies zu der Anforderung, alle Teilnehmer durch eine zentrale Instanz eindeutig zu identifizieren und sicher zu authentifizieren.

DIN EN ISO 24534-3:2016-08 *Intelligente Verkehrssysteme – Automatische Identifizierung von Fahrzeugen und Ausrüstungen – Elektronische Identifizierung für die Registrierung (ERI) von Fahrzeugen* [52] ist eine Norm für die Festlegung einheitlicher digitaler Identifikationsmerkmale für Fahrzeuge einschließlich einer elektronischen Registrierung. Der darin erwähnte Anwendungsfall der elektronischen Gebührenerhebung erfordert eine zentrale Verwaltung zur Abrechnung der beanspruchten Leistungen

und Dienste. Durch zentrale Verwaltung wird einer doppelten Vergabe von Identifikatoren entgegengewirkt. Die individuellen Identifikationsmerkmale eines Fahrzeugs müssen als digitale Identifikation (dID) in einem Fahrzeugleitsystem hinterlegt sein.

Neben diesen spezifischen Anforderungen muss ein Fahrzeugleitsystem auch die allgemeinen Schutzziele der Informationstechnik erfüllen. Die IKT-Schutzziele für industrielle Automatisierungssysteme sind in der Normenreihe IEC 62443 [45] definiert und müssen auf ein Fahrzeugleitsystem übertragen werden.

2.6.1 Allgemeine Schutzziele

Die allgemeinen Schutzziele werden als besonders wichtig eingestuft und daher herausgestellt. Wegen der Anfangsbuchstaben der englischen Begriffe *Confidentiality*, *Integrity* und *Availability* werden die allgemeinen Schutzziele auch als „CIA-Schutzziele“ bezeichnet.

Vertraulichkeit

Nur die berechtigten Empfänger dürfen Zugang zu avisierten Informationen erhalten. In einem Fahrzeugleitsystem müssen alle Kommunikationen mit kryptografischen Verfahren abgesichert werden, da Funksignale prinzipiell von jedem empfangen, gesendet und somit auch verändert werden können. Zwischen Sendern und Empfängern dürfen keine oder nur vertrauenswürdige Dritte stehen, die Zugriff auf die Informationen haben. Für die hohen Sicherheitsanforderungen in einem Fahrzeugleitsystem muss ein perfekt sicheres Verfahren zum Einsatz kommen.

Wegen der strikten Zeitanforderungen in einem Fahrzeugleitsystem muss jeder Teilschritt einer Kommunikation innerhalb einer vorhersehbaren Zeitspanne ablaufen. Folglich kommen nur kryptografische Verfahren mit vorhersehbarer Verarbeitungsdauer in Betracht.

Verfügbarkeit

Es werden hohe Anforderungen an die Verfügbarkeit der Kommunikationsinfrastruktur gestellt, da ein Ausfall eines Fahrzeugleitsystems zu gefährlichen Situationen wie Kollisionskursen führen kann. Es ist daher von großer Bedeutung, dass stets ein Kommunikationskanal zwischen kommunizierenden Fahrzeugen zur rechtzeitigen Nachrichtenübertragung zur Verfügung steht.

Zur Verfügbarkeit zählt ferner, dass für die kryptografischen Verfahren stets ein adäquater Schlüssel zur Verschlüsselung und zur Entschlüsselung verfügbar ist. Ein Fahrzeugleitsystem muss somit die Schlüsselverteilung und den Schlüsselnachschub über einen sicheren Kanal sicherstellen.

Integrität

Im Zusammenhang mit der IKT-Sicherheit in Fahrzeugleitsystemen bedeutet Integrität die Freiheit von unautorisierten Modifikationen an Nachrichten. Veränderungen der Nachrichten und Störungen des Übertragungskanals müssen erkannt werden, da die Luftschnittstelle allgemein zugänglich ist. Vorsätzliche Veränderung der Daten kann zu gefährlichen Situationen führen, beispielsweise zum Unterschreiten von Mindestabständen zwischen Fahrzeugen. Zufällige Störungen des Funkkanals können den Zeitpunkt oder die korrekte

Reihenfolge der empfangenen Nachrichten beeinträchtigen. Ein Fahrzeugleitsystem muss daher über kryptografisch abgesicherte Maßnahmen zur Integritätsprüfung verfügen.

2.6.2 Weitere Schutzziele

Andere als die allgemeinen Schutzziele werden den weiteren Schutzzielen zugeordnet.

Authentizität Authentizität ist die überprüfbare Echtheit eines Objekts und dessen Eigenschaften. In einem Fahrzeugleitsystem ist die Authentizität von Nachrichten, von Relais und von Fahrzeugen bedeutend. Bei Fahrzeugen ist bei allen Interaktionen sicherzustellen, dass nicht missbräuchlich die dID eines anderen Fahrzeugs vorgegeben wird.

Nichtabstreitbarkeit und Zurechenbarkeit Jede Aktion in einem Netz muss eindeutig einem Teilnehmer zugeordnet werden und dieser darf nicht vorgeben können, ein anderer Teilnehmer hätte die Aktion durchgeführt oder veranlasst. In einem Fahrzeugleitsystem müssen sich aus einer missbräuchlichen Verbreitung von Nachrichten unmittelbar Konsequenzen für den störenden Teilnehmer ziehen lassen, ohne dass eine langwierige Suche nach dem Verursacher erforderlich ist.

Netzneutralität Netzneutralität bedeutet die gleichberechtigte Durchleitung von Daten durch ein Netz, unabhängig insbesondere von Anwendung, Sender und Empfänger. In einem Fahrzeugleitsystem ist die rechtzeitige und zuverlässige Weiterleitung sicherheitsrelevanter Informationen von größtem Interesse. Eine Priorisierung sicherheitsrelevanter Daten gegenüber Komfortfunktionen dienenden Daten ist daher vorstellbar.

Datenschutz Datenschutz wird primär im Zusammenhang mit der Verarbeitung personenbezogener oder -beziehbarer Informationen gesehen und soll deren missbräuchliche Verwendung verhindern. In Fahrzeugleitsystemen werden Daten zwischen technischen Systemen und ohne Bezug zu Personen ausgetauscht, weshalb keine personenbezogenen oder -beziehbaren Informationen vorliegen. Dennoch sind Daten zu schützen und das Gebot der Datensparsamkeit zu beachten.

2.6.3 Schlüsselerzeugung und -verteilung

Zueinander passende Schlüssel sind die zur verschlüsselten Kommunikation notwendigen Parameter und müssen vorab an die Kommunikationsteilnehmer übermittelt werden. Eine wichtige Eigenschaft von Schlüsseln ist die Schlüssellänge, also die Anzahl Zeichen, aus denen sich ein einzelner Schlüssel zusammensetzt. Als Parameter zur perfekt sicheren Einmalverschlüsselung eingesetzte Schlüssel werden als Masken bezeichnet. Kryptografisch sichere Schlüssel k müssen einige Voraussetzungen erfüllen, die sich je nach eingesetztem Verfahren unterscheiden können [15, 146, 163]. Zur Gewährleistung hinreichender Schlüsselsicherheit in einem Fahrzeugleitsystem müssen folgende Voraussetzungen erfüllt sein:

- Die Schlüssellänge $|k|$ muss einen Mindestwert aufweisen, um Brute-Force-Angriffen zu widerstehen.

- Die Maskenlänge muss gleich oder größer der Länge des zu maskierenden Klartextes sein.
- Schlüssel und Masken müssen mit einem kryptografisch sicheren, echten Zufallsprozess generiert werden.
- Schlüssel und Masken müssen über einen sicheren Kanal verteilt werden.
- Schlüssel und Masken müssen sicher gelagert und vor unbefugtem Zugriff geschützt werden. Unbefugter Zugriff muss erkannt werden.
- Masken müssen nach einmaliger Verwendung vernichtet werden.

Schlüssel und Masken mit diesen Eigenschaften müssen durch geeignete Verfahren erzeugt und verteilt werden.

Schlüsselerzeugung Die Menge aller kombinatorisch möglichen Schlüssel, die bei gegebener Schlüssellänge $|k|$ generiert werden können, wird als Schlüsselraum M bezeichnet. Handelt es sich beim Schlüssel um eine Bitfolge, wird der Zusammenhang zwischen Schlüssellänge $|k|$ und Mächtigkeit des Schlüsselraums $|M|$ durch

$$|k| = \log_2 |M| \tag{2.5}$$

beschrieben. Teilmengen K von M werden als Schlüsselvorrat bezeichnet ($K \subseteq M$) und haben ihrerseits eine Mächtigkeit, die Schlüsselvorratsmächtigkeit $|K|$. Die Schlüsselgröße G_K ist die Summe aller Schlüssellängen eines Schlüsselvorrats:

$$G_K = \sum_{k \in K} |k| \tag{2.6}$$

Wird von den Verschlüsselungsalgorithmen eines Fahrzeugleitsystems perfekte Sicherheit gefordert, müssen die eingesetzten Masken mindestens so lange wie die Nachrichten selbst sein. Bei der Erzeugung von Schlüsseln großer Länge muss gleichzeitig die Zeitspanne zur Schlüsselerzeugung vorhersehbar sein, um Echtzeitanforderungen zu erfüllen. Bei einem Fahrzeugleitsystem ist somit eine Instanz notwendig, die über hierzu ausreichende Ressourcen verfügt.

Schlüsselverteilung Zur symmetrischen Ver- und Entschlüsselung benötigt jeder Teilnehmer w_i einen Schlüsselvorrat K_i mit entsprechend aufeinander abgestimmten Schlüsseln. Bei Fahrzeugleitsystemen müssen bei der Schlüsselverteilung zwei Einheiten berücksichtigt werden: Die Fahrzeuge einerseits und die infrastrukturseitigen Installationen (Relais) andererseits. Zu beiden Einheiten muss für jede Verteilung symmetrischer Schlüssel ein sicherer Kanal etabliert werden. Beim Einsatz symmetrischer Schlüssel muss darauf geachtet werden, dass jeder Schlüssel mit einem eindeutigen Index gekennzeichnet ist, damit sich Sender und Empfänger einer verschlüsselten Nachricht über den einzusetzenden Schlüssel verständigen können.

2.6.4 Authentisierung und Authentifizierung

Vor jeder Datenübertragung muss ein Fahrzeug seine Identität überprüfbar nachweisen, um entscheiden zu können, ob es zur Teilnahme am Kommunikationsvorgang berechtigt ist. Dabei beschreibt die Authentisierung die Vorgabe einer Identität, die Authentifizierung deren anschließende Überprüfung und die Autorisierung die Erteilung von Genehmigungen (Abbildung 2.3). Für die Vorgänge Authentisierung, Authentifizierung und Autorisierung sind einige Standards bekannt:

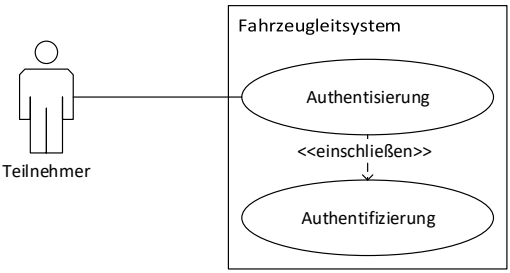


Abbildung 2.3: Anwendungsfall für Authentisierung und Authentifizierung

DIN EN ISO 17419:2018-09 *Intelligente Verkehrssysteme – Kooperative Systeme – Global eindeutige Identifikation* [48] ist eine Norm für Klassifikation und Management von Teilnehmern in ITS-Anwendungen. Sie fordert einen global eindeutigen ITS-Anwendungsbezeichner (ITS-AID) für Objekte wie Fahrzeuge oder stationäre Installationen („ITS-Anwendungsobjekte“). Damit ist es möglich, Absender von Nachrichten global eindeutig zu identifizieren, was die Grundlage zur Authentifizierung darstellt. Ein Fahrzeugleitsystem muss Funktionalitäten zur eindeutigen Kennzeichnung durch eine zentrale Instanz implementieren.

BSI TR-03159 *Mobile Identities* [13] ist eine technische Richtlinie, die europaweit gültige Rahmenbedingungen zur Vereinheitlichung und Zuweisung von Identitäten im digitalen Kontext enthält. Sie stellt Anforderungen an die Authentifizierung in Form eines „Level of Assurance“, das abhängig vom möglichen Gefahrenpotential des jeweiligen Gerätes ist. Im allgemeinen Fall sieht sie eine zentrale Zertifizierungsstelle zur technischen Ausstellung dieser Identitäten vor, die bei einer hoheitlichen Behörde des jeweiligen Staates angesiedelt ist. Eine Erweiterung der Richtlinie sieht die Nutzung bestehender Techniken wie die der Fast IDentity Online (FIDO)-Allianz oder die der Extended Access Control (EAC) vor.

Die Standards fordern von einem Fahrzeugleitsystem eine einheitliche Datenbank zur zentralen Verwaltung von Identitäten, um doppelte Zuweisungen von Identitäten zu vermeiden und Missbrauch vorzubeugen. Für konsistente Rechte und Rollen in der digitalen wie in der physischen Welt muss diese einheitliche Datenbank hoheitlich überwacht werden.

Der Nachweis über seine Identität kann von einem Teilnehmer im Allgemeinen durch eine der folgenden Möglichkeiten erbracht werden [13]:

- Wissen des Teilnehmers, zum Beispiel ein Passwort
- Besitz des Teilnehmers, zum Beispiel ein Schlüssel
- Eigenschaft des Teilnehmers, zum Beispiel ein biometrisches Merkmal

Aufgabe eines Fahrzeugleitsystems muss es sein, die vorgegebene Berechtigung automatisiert zu prüfen und die Freigabe zur Teilnahme an der Kommunikation zu erteilen. Zudem sind unterschiedliche Berechtigungsstufen (Rechte) zu implementieren, die der jeweils zugewiesenen Rolle des Teilnehmers entsprechen.

2.6.5 Autorisierung

Autorisierung ist die Erteilung der Berechtigung zur Nutzung einer Ressource in einem Fahrzeugleitsystem. Basierend auf der Authentifizierung muss ein Fahrzeugleitsystem die Autorisierung einzelner Fahrzeuge umsetzen, was technisch durch ein Rechte- und Rollenkonzept implementiert wird. Berechtigungen können nach Art und Umfang abgestuft werden. Dadurch wird auch vermieden, dass einem Fahrzeug eine Berechtigungsstufe zugeteilt wird, für die es nicht die entsprechende Rolle besitzt. Durch die Autorisierung zur Datenübertragung wird der Teilnehmer zum Bestandteil der Kommunikationsarchitektur innerhalb des Fahrzeugleitsystems und darf Übertragungsressourcen nutzen.

2.6.6 Ver- und Entschlüsselung

An die Verschlüsselung werden sowohl zeitliche als auch kryptografische Anforderungen gestellt. Bei der Entschlüsselung handelt es sich um die Umkehrung der Verschlüsselung.

Zeitliche Anforderungen Die zur Ver- und Entschlüsselung einer Nachricht benötigte Dauer muss innerhalb einer vorhersehbaren Zeitspanne liegen, damit für den gesamten Kommunikationsprozess Echtzeitbedingungen erfüllt werden können. Diese Zeitspannen müssen stets zuverlässig vorhersehbar sein.

Kryptografische Anforderungen Die Verschlüsselung muss robust gegenüber aktuellen und künftigen Angriffsvektoren sein. Zwar sind Fahrzeuge einer regelmäßigen Wartung zu unterziehen, die auch zur Aktualisierung der Verschlüsselungsalgorithmen genutzt werden könnte. Jedoch können die Wartungsintervalle im Vergleich zu Innovationszyklen in der Rechner- und Softwaretechnik lang sein, was eine große Anfälligkeit insbesondere für *Zero-Day-Exploits* darstellt. Jede Verschlüsselung muss daher gemäß dem Konzept *secure by design* bereits beim Entwurf auf Widerstandsfähigkeit gegen mögliche aktuelle und zukünftige Angriffe hin ausgelegt werden.

2.6.7 Nachrichtenübertragung

Zur Vermeidung von Informationsverlust müssen Nachrichten vollständig und rechtzeitig übertragen werden. Die zentrale Anforderung an die Nachrichtenübertragung ist daher, Nachrichten durch Einsatz geeigneter Routingverfahren zuverlässig an die Empfänger zu vermitteln. Eine erfolgreiche Übertragung muss vom Empfänger an den Sender auf geeignete Weise bestätigt werden. Kann die Nachrichtenübertragung nicht innerhalb einer

vorhersehbaren Zeitspanne ablaufen, muss das Fahrzeugleitsystem den kompletten Prozess zuverlässig und rechtzeitig abbrechen und betroffene Fahrzeuge in einem sicheren Zustand belassen oder in einen solchen überführen können. Dies betrifft sowohl die Übertragung der Nachricht selbst als auch die Übertragung einer Empfangsbestätigung. Der zusammengefasste Ablauf einer den Anforderungen entsprechenden Nachrichtenübertragung ist in Abbildung 2.4 zusammengefasst.

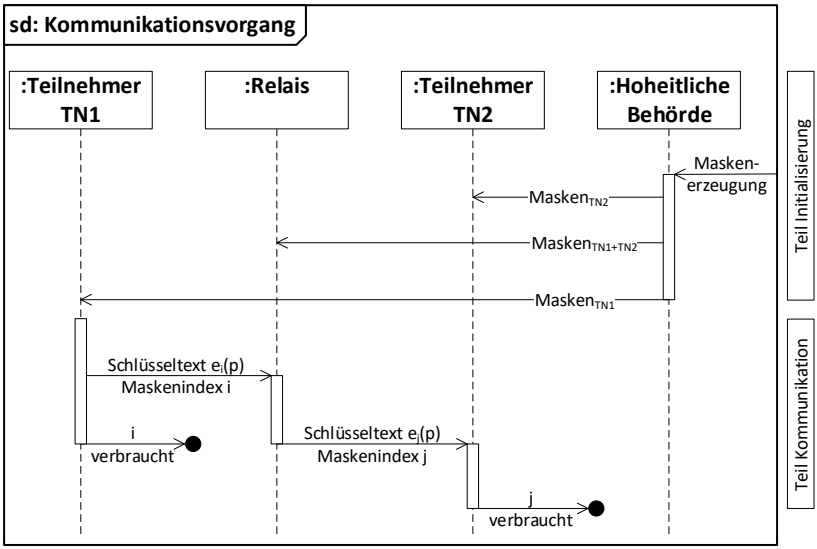


Abbildung 2.4: UML-Sequenzdiagramm einer Nachrichtenübertragung

Im Teil *Initialisierung* werden die Voraussetzungen zur sicheren Kommunikation geschaffen. Aus Erzeugung und Verteilung der Masken folgt, dass das Relais über alle notwendigen Masken zur verschlüsselten Kommunikation mit jedem Teilnehmer verfügt. Im Teil *Kommunikation* ist das Relais somit zur Entschlüsselung empfangener Nachrichten, zur Auswertung von Klartexten und zur weiteren Vermittlung befähigt. Zentraler Aspekt bei der Ver- und Entschlüsselung ist Kennzeichnung und Vernichtung der verwendeten Schlüssel oder Masken k_i und k_j, in der Abbildung nur mit i und j indiziert.

2.7 Anforderungen an die Informationsverarbeitung

Neben Anforderungen an die Informationsübertragung bestehen in einem Fahrzeugleitsystem auch Anforderungen an die vor- und nachbereitende Informationsverarbeitung. Durch die Informationsverarbeitung müssen die folgenden Zustände des Fahrzeugleitsystems abbildbar sein:

- Der aktuelle Systemzustand (Ist-Fall),

- der angestrebte Systemzustand (Soll-Fall) sowie
- die Randbedingungen (Rechte und Rollen der beteiligten Fahrzeuge in der physischen wie auch in der digitalen Welt).

Die zum Erreichen des angestrebten Systemzustandes notwendigen ETL-Prozesse (Extraktion, Transformation, Laden) erfordern eine Kombination aus zentralen und dezentralen Datenspeichern und Datenverarbeitungsgeräten.

2.7.1 Datenspeicher

In Fahrzeugleitsystemen sind Datenbanksysteme einzusetzen, um Informationen aus verschiedenen Quellen technisch zusammenzuführen.

ISO 17572-1:2015-01 *Intelligente Verkehrssysteme (ITS) – Positionsreferenzierung für geografische Datenbanken* [99] ist eine Norm für die Verwaltung von Geoinformationen in IVS. Sie beinhaltet Beispiele für Datenbankinhalte, insbesondere zur Verortung der Infrastrukturobjekte in Verkehrssystemen. Ein Fahrzeugleitsystem muss in der Lage sein, die Positionen von Fahrzeugen und von Infrastrukturobjekten in einer Datenbank zusammenzuführen.

ISO 14296:2016-02 *Intelligente Verkehrssysteme – Erweiterung von Karten-Datenbankspezifikationen für Anwendungen von kooperativer ITS* [98] ist eine weiterführende Norm zur Spezifikation der Datenbankinhalte in Form konkreter Datenmodelle. Ihr Schwerpunkt liegt auf der Datenbereitstellung an alle Teilnehmer eines kooperativen IVS. Ein Fahrzeugleitsystem muss das Sammeln, Prüfen und Verteilen von Geoinformationen an die beteiligten Fahrzeuge ermöglichen.

ISO/TR 21718 *Intelligente Verkehrssysteme – Räumliches und zeitliches Datenwörterbuch für kooperative ITS und automatisisierte* [sic] *Fahrsysteme 2.0* [103] ist ebenfalls eine technische Regel zur digitalen Speicherung und Verteilung von Informationen über physische Objekte, sieht jedoch zusätzlich die Angabe von Zeitstempeln vor. Ein Fahrzeugleitsystem muss daher dynamische Verkehrsinformationen über beispielsweise Staus oder Unfälle ermitteln, zeitlich einordnen und die Informationen verteilen können.

Die untersuchten Standards lassen zur Erfüllung der Anforderungen an ein Fahrzeugleitsystem nur die Kombination aus zentralen und verteilten Datenbanken zu.

Zentrale Datenbank In einer zentralen Datenbank müssen Informationen über Rechte und Rollen aller an einem Fahrzeugleitsystem beteiligten Fahrzeuge gespeichert und mit einer dID verbunden werden. Eine zentrale Zuteilung dieser Rechte und Rollen sowie deren Verwaltung ist notwendig, um falsche oder missbräuchliche Behauptungen von Identitäten oder Rechten zu verhindern. Die zentrale Datenbank muss zudem die von den Fahrzeugen eintreffenden Informationen zusammenführen, bereinigen und plausibilisieren. Nur durch Zusammenführen der Daten in einer zentralen Datenbank kann eine vollständige Lage des Verkehrssystems erstellt werden. Fahrzeugen, die räumlich und zeitlich betroffen sind, kann diese Lage gezielt übermittelt werden.

Dezentrale Datenbank Zur Informationsverwaltung an Bord von Fahrzeugen muss eine dezentrale Datenbank vorgesehen werden. Zunächst dient diese der Verwaltung und Vorverarbeitung aller durch bordeigene Sensorik generierten Daten. Zudem müssen Rechte und Rollen anderer Fahrzeuge, mit denen Interaktionen in der physischen oder digitalen Welt stattfinden, hinterlegt und abgeglichen werden. Die dezentrale Datenbank muss Informationen zum Zustand des Verkehrssystems aufnehmen, von dem das jeweilige Fahrzeug aktuell oder im Laufe der weiteren Fahrt betroffen ist. So kann rechtzeitig eine adäquate Fahrzeugsteuerung antizipiert werden. Nicht zuletzt nimmt die dezentrale Datenbank die dID sowie die Schlüssel zur Ver- und Entschlüsselung von Nachrichten auf.

2.7.2 Datenverarbeitungsgeräte

Digitalrechner an Bord der Fahrzeuge müssen die verfügbaren Informationen verarbeiten und die Fahrzeuge entsprechend steuern. Die Datenverarbeitungssysteme zur Steuerung der Fahrzeuge müssen grundsätzlich nicht Bestandteil des Fahrzeugleitsystems sein, sondern können weiterhin im Hoheitsbereich der Fahrzeughersteller liegen. Das Fahrzeugleitsystem muss jedoch Schnittstellen zu diesen Datenverarbeitungssystemen vorgeben, um den Nachrichtenfluss zwischen dem Fahrzeugleitsystem und den Fahrzeugaktoren zu ermöglichen. Die Fahrzeugaktoren setzen die vom Fahrzeugleitsystem gelieferten Nachrichten in Fahrverhalten um. Zur Spezifikation der Nachrichten muss eine formale Sprache verwendet werden, um eine eindeutige und widerspruchsfreie Übertragung von Informationen zu gewährleisten. Die formale Sprache muss sich in effizienter Weise von Digitalrechnern in Steuergeräten verarbeiten lassen und soll optional menschenlesbar sein. Zur Minimierung der benötigten Schlüsselgröße muss die Anzahl der zu verschlüsselnden und zu übertragenden Zeichen möglichst gering gehalten werden.

Durch dieses Konzept bleibt die Interoperabilität von Fahrzeugen verschiedener Hersteller gewahrt, ohne dass dem Fahrzeugleitsystem die genauen Spezifikationen einzelner Fahrzeugtypen bekannt sein müssen.

2.7.3 Skalierung

Die Informationsverarbeitung in einem Fahrzeugleitsystem muss sowohl horizontal als auch vertikal skalierbar sein: horizontal, um zusätzliche Fahrzeuge in das Fahrzeugleitsystem integrieren zu können; vertikal, um die benötigten Ressourcen zur Verarbeitung zusätzlicher Daten bereitstellen zu können. Alle Akteure des Fahrzeugleitsystems müssen gleichermaßen für diese Skalierung ausgelegt sein.

2.8 Zusammenfassung der Anforderungen

In diesem Kapitel wurden die Anforderungen an ein Fahrzeugleitsystem anhand bestehender Standards erarbeitet. Hierzu mussten verschiedene Standards, die jeweils einzelne Aspekte eines Fahrzeugleitsystems behandeln, zusammengeführt werden. Zur weiteren Entwicklung müssen aus den identifizierten Anforderungen konkrete Entwurfsentscheidungen abgeleitet werden. Die für die Entwicklung eines Fahrzeugleitsystems wesentlichen Entwurfsentscheidungen hinsichtlich Netztechnik, Informationssicherheit und Nachrichtenformat werden wie folgt zusammengefasst.

2.8.1 Infrastrukturmodus anstatt Ad-hoc-Netz

Die Netztopologie in einem Fahrzeugleitsystem muss zusammengefasst folgende Anforderungen erfüllen:

- Die Datenübertragung zwischen Fahrzeugen muss über einen zentralen Zugangspunkt abgewickelt werden.
- Die Netzadressen der einzelnen Fahrzeuge müssen von einer zentralen Instanz erzeugt, verteilt und verwaltet werden.
- Es muss ein Moderator für die Nachrichtenübertragung vorhanden sein.

Diese geforderten Eigenschaften lassen nur eine Netztopologie im Infrastrukturmodus zu. Allein diese Topologie ist in der Lage, die Gesamtheit der Anforderungen mit einem vertretbaren Maß an Komplexität zu erfüllen.

Nur der Infrastrukturmodus kann durch ein dediziertes Netz die Aufrechterhaltung vollständiger Maschen zwischen Sendern und Empfängern stets gewährleisten. Netze im Ad-hoc-Modus weisen zwar prinzipiell die vorteilhafte Fähigkeit auf, sich dynamisch neu zu strukturieren und damit auf Ausfälle einzelner Routen zu reagieren. Ihr entscheidender Nachteil ist jedoch, dass die Verfügbarkeit von Routen von den Positionen der Fahrzeuge abhängt und diese nicht zuverlässig prognostizierbar sind. Die permanente Verfügbarkeit der benötigten Verbindungen im Netz kann somit nicht garantiert werden. Ad-hoc-Netze benötigen zudem einen Mindestanteil und eine räumliche Mindestdichte an vernetzten Fahrzeugen, um vollständige Maschen zwischen Sendern und Empfängern zu bilden. Würde dieser Mindestanteil auch nur lokal unterschritten, so könnten sich die Abstände zwischen den Fahrzeugen derart vergrößern, dass keine zuverlässige Nachrichtenübertragung mehr möglich ist.

Ein weiterer Aspekt betrifft die Signallaufzeit, also die zur Übertragung einer Nachricht benötigte Zeitspanne. Netze im Ad-hoc-Modus bestehen aus einer dynamisch veränderlichen Menge von Zwischenstationen, welche die Nachricht vom Sender zum Empfänger weiterleiten. Die logische Länge der Übertragungsstrecke ist dadurch einerseits dynamischen Änderungen unterworfen, was die Vorhersehbarkeit einschränkt. Andererseits kann jede Zwischenstation das Weiterleiten der Nachricht bewusst oder fahrlässig verzögern. Insgesamt führen diese Eigenschaften von Ad-hoc-Netzen zu einem nicht vorhersehbaren Zeitverhalten des Kommunikationskanals.

Netze im Infrastrukturmodus benötigen zur Nachrichtenübertragung von Sender zu Empfänger stets genau zwei logische Übertragungsstrecken: vom Sender zum Relais und vom Relais zum Empfänger. Das Relais kann als vertrauenswürdige und zuverlässige Zwischenstation angenommen werden. Gleichzeitig ist die Ausbreitungsgeschwindigkeit elektromagnetischer Wellen bekannt: Sie entspricht im Vakuum der Lichtgeschwindigkeit, in Materie (auch in Luft) ist sie geringer. Aus dem Abstand eines Fahrzeugs zum nächsten Relaiszugangspunkt und den Parametern des eingesetzten Übertragungsprotokolls kann somit stets die Dauer der Nachrichtenübertragung berechnet werden. Als Randbedingung muss sich der Zugangspunkt zum Relais innerhalb einer maximal möglichen Übertragungsreichweite befinden. Diese Reichweite ist zum einen durch die Länge der Strecke limitiert, auf der das gesendete Signal nicht unter einen Pegel gedämpft wird, der vom Empfänger noch vom Grundrauschen unterschieden werden kann. Zum anderen müssen neben dieser

physikalischen Grenze auch limitierende Parameter der eingesetzten Kommunikationsprotokolle beachtet werden. So sieht der Standard IEEE 802.11 vor, ein Paket als verloren zu werten und erneut an den Empfänger zu senden, wenn der Sender nicht innerhalb einer festgelegten Zeitspanne eine Quittierung (ACK) des Pakets erhält.

Für Netze im Infrastrukturmodus kann eine maximale Entfernung zum Netz durch eine entsprechend hohe Dichte an Zugangspunkten (Funkmasten) gewährleistet werden. Eine höhere Dichte an Zugangspunkten ermöglicht dabei geringere Sendeleistungen und geringere Latenzen. Gegen eine alternativ denkbare Erhöhung der Sendeleistung sprechen neben limitierter Verfügbarkeit elektrischer Leistung bei mobilen Transceivern auch gesetzliche Grenzwerte. Netze im Infrastrukturmodus benötigen somit zwar zusätzliche Infrastruktur in nicht unerheblichem Umfang, die je nach Ausgestaltung zudem einen einzelnen Ausfallpunkt (engl. *Single Point of Failure [SPOF]*) darstellen kann. Jedoch kann die Abdeckung mit Zugangspunkten des betroffenen Verkehrsbereichs geplant und damit auch garantiert werden. Beim Infrastrukturmodus können zwar höhere Latenzzeiten als beim Ad-hoc-Modus auftreten, wenn die direkte Strecke zwischen Sender und Empfänger bei einer Ad-hoc-Übertragung kürzer ist als über ein Relais. Dies ist jedoch kein Nachteil, da die Übertragungszeiten stets vorhersehbar sind. Die dadurch mögliche echtzeitfähige Kommunikation stellt das wichtigere Merkmal eines Fahrzeugleitsystems dar. Bei der Kommunikation im Infrastrukturmodus sind insgesamt alle Netzparameter kontrollierbar und das Zeitverhalten somit vorhersehbar.

Eindeutige Identitäten müssen an zentraler Stelle erzeugt und in einem Register verwaltet werden. Bei der dezentralen Vergabe von Identifikatoren kann es leicht zu Uneindeutigkeiten durch doppelte Verwendung von Identitäten kommen, da keine Abstimmung zwischen allen Beteiligten gewährleistet ist. Zudem kann missbräuchliche Vergabe falscher Identitäten in dezentralen Umgebungen nur mit komplexen Verfahren verhindert werden, die, da hierzu asymmetrische Kryptografie notwendig ist, zudem unsicher sind. Bei Netzen im Infrastrukturmodus befindet sich außer dem Relais kein weiterer Teilnehmer als Vermittler zwischen Sender und Empfänger. Das Relais und seine Komponenten können bei korrekter Implementierung als vertrauenswürdig eingestuft werden. Angriffe durch fingierte Zwischenstationen (*Man in the Middle*-Angriffe) können durch Authentifizierung und Verschlüsselung von Nachrichten auf der Funkstrecke verhindert werden. Bei Netzen im Ad-hoc-Modus besteht hingegen die Gefahr, dass die zur Weiterleitung dienenden Fahrzeuge die durchgeleiteten Nachrichten mutwillig oder fahrlässig verändern, verzögern oder verwerfen.

Eine zentral ausgelegte Architektur macht ein Fahrzeugleitsystem insgesamt einfach in der Verwaltung und sicher in der Anwendung. Mischformen, wie die gezielte Verdichtung von Ad-hoc-Netzen durch sogenannte roadside units, sollten zur Reduzierung der Komplexität sowie zur Vermeidung von Brüchen in der Übertragungskette vermieden werden. In vielen Anwendungen des Internets ist allgemein ein Trend zu cloudbasierten Lösungen zu beobachten, bei denen neben den eigentlichen Inhalten auch die Merkmale zur Identifikation durch den jeweiligen Anbieter zugeteilt und verwaltet werden. Sind sensible, personenbezogene Daten betroffen, muss diesem Anbieter viel Vertrauen entgegengebracht werden. Auch im Automobilbereich ist mittelfristig davon auszugehen, dass sensible Daten wie Versicherungsinformationen, Halterdaten und eben die für die Kryptografie notwendige Parametrierung an zentrale Stellen ausgelagert werden müssen. Ab einer gewissen Stufe der Datensensibilität kann ausreichendes Vertrauen nur bei demokratisch legitimierten In-

stitutionen erwartet werden. Zwar bestehen allgemein aktuell noch gewisse Vorbehalte gegenüber staatlichen Stellen hinsichtlich der zuverlässigen Umsetzung digitaler Prozesse. Dennoch sollte hoheitlichen Stellen größeres Vertrauen als multinationalen Konzernen mit kommerziellen Interessen entgegengebracht werden. Diese Entwicklung unterstreicht die Entwurfsentscheidung bei einem Fahrzeugleitsystem zugunsten einer Netztopologie im Infrastrukturmodus mit zentraler Verwaltung.

2.8.2 Symmetrische anstatt asymmetrischer Verschlüsselung

Die in einem Fahrzeugleitsystem eingesetzte Verschlüsselung muss folgende Anforderungen erfüllen:

- Die Verschlüsselung muss allen aktuellen und künftigen Angriffen standhalten können.
- Die Schlüssel müssen von einer vertrauenswürdigen Stelle erzeugt werden.
- Für die Schlüsselverteilung muss ein vom Kommunikationskanal unabhängiger, sicherer Kanal zum Fahrzeug hergestellt werden.
- Authentisierung und Authentifizierung müssen dem gleichen Sicherheitsniveau genügen wie die Nachrichtenverschlüsselung.

Diese Anforderungen an die Kommunikationssicherheit erlauben in einem Fahrzeugleitsystem nur den Einsatz symmetrischer, perfekt sicherer Verschlüsselungsverfahren. Es werden hierzu Schlüssel von der Länge der Nachrichten selbst benötigt.

Die Notwendigkeit symmetrischer Verschlüsselung ergibt sich ferner aus den Zeitanforderungen. Asymmetrische Verschlüsselung benötigt verhältnismäßig viel Rechenzeit und wird auch aktuell nur für die Verteilung symmetrischer (Sitzungs-)Schlüssel eingesetzt. Für Echtzeitanwendungen, wie sie in Fahrzeugleitsystemen vorliegen, müssen daher Verfahren mit auch auf leistungsschwachen Digitalrechnern ausreichendem und vorhersehbarem Zeitverhalten eingesetzt werden. Diese Anforderungen sind nur bei symmetrischer Verschlüsselung gegeben. Praktische Hürden perfekt sicherer Verschlüsselung wie Schlüsselverteilung und -nachschub müssen durch eine geeignete Implementierung gelöst werden.

2.8.3 Formale Sprache anstatt Freitext

Inhalt und Struktur der in einem Fahrzeugleitsystem ausgetauschten Nachrichten müssen folgende Anforderungen erfüllen:

- Jede Nachricht muss eine eindeutige Information transportieren.
- Nachrichten müssen in einer auf den Bedarf dieses Anwendungsgebiets beschränkten formalen Sprache abgefasst sein.
- Die zu übertragende Zeichenanzahl muss minimiert werden.

Aufgrund der endlichen Übertragungskapazität und der benötigten Schlüsselgröße muss die verschlüsselt übertragene Datenmenge auf ein Minimum reduziert und folglich die Informationsdichte maximiert werden. Dazu muss eine formale Sprache verwendet werden,

die auf die Anforderungen eines Fahrzeugleitsystems zugeschnitten ist. Zentrale Bestandteile einer solchen Sprache sind die Verwendung von Schlüsselwörtern oder Codes mit einer minimalen Anzahl Zeichen, eine reduzierte Grammatik und die Vermeidung von Doppeldeutigkeiten. Die notwendigen Definitionen zur Verwendung dieser Sprache müssen laufend aktualisierbar sein.

3 Stand der Technik in Wissenschaft und Praxis

In Fahrzeugleitsystemen müssen verschiedene Techniken zusammenwirken. Es werden daher mehrere Gebiete der Forschung und Entwicklung berührt, die im Wesentlichen sind:

- Elektronische Datenverarbeitung
- Kommunikationsnetze
- Kryptologie und Informationssicherheit
- Systemintegration und funktionale Sicherheit

Der Stand der Technik in den einzelnen Gebieten wird in diesem Kapitel dargestellt und hinsichtlich seiner Bedeutung für Fahrzeugleitsysteme erörtert. Manche Gebiete sind durch etablierte Techniken gekennzeichnet, was sich in Patenten niederschlägt, andere sind bislang nur fragmentiert erforscht.

3.1 Sicherheit mechatronischer Systeme

Unter Sicherheit in der Automatisierungstechnik wird allgemein ein Zustand verstanden, in dem ein System seine Funktion erfüllt und dabei keine Gefahr bewirkt oder zulässt [84]. Durch die Fähigkeit zu ausfallsicherheitsgerichtetem Systemverhalten soll dieser Zustand auch bei einem (Teil-)Ausfall einzelner Funktionen beibehalten werden. Diese Fähigkeit wird durch redundante Auslegung der beteiligten Komponenten erreicht. Zur Umsetzung auf Mikrorechnerebene stehen Systeme wie LOGISIRE [118] oder LOGISAFE [9] zur Verfügung, die für konkrete Anwendungen angepasst werden können.

Bei der Gesamtbetrachtung mechatronischer Systeme muss zwischen informations- und kommunikationstechnischer Sicherheit einerseits und funktionaler Sicherheit andererseits unterschieden werden.

3.1.1 Informations- und kommunikationstechnische Sicherheit

Sicherheit in der Informations- und Kommunikationstechnik (IKT) zählt zu den zentralen Bedürfnissen moderner Industriegesellschaften. Entsprechend zahlreich sind die Veröffentlichungen von Institutionen, Forschungseinrichtungen und Interessenverbänden zu diesem Thema. Zu den wichtigsten Institutionen zählen das Bundesamt für Sicherheit in der Informationstechnik (BSI), das Institute of Electrical and Electronics Engineers (IEEE) sowie das European Telecommunications Standards Institute (ETSI).

Das BSI sieht den Schwerpunkt von Cyberangriffen im Bereich Ransomware und Trojaner wie „Emotet“ [14]. Als Gegenmaßnahme wird Authentifizierung von Anwendern und Programmen durch kryptografische Verfahren mit Mindestschlüssellängen empfohlen [15].

Das IEEE widmet sich dem Thema Sicherheit in Fahrzeugleitsystemen durch Veranstaltung zahlreicher Fachkonferenzen und liefert regelmäßig einen Überblick zur aktuellen Sicherheitslage vernetzter Fahrzeuge [155]. Demnach resultieren Sicherheitslücken vordringlich aus dem Einsatz herkömmlicher Kommunikationsprotokolle in Fahrzeugleitsystemen, obwohl sie dafür nicht entwickelt wurden. Sicherheitslücken sollen dann durch eine systematische Identifizierung und Absicherung geschlossen werden.

Das ETSI versucht sich bereits an konkreten Sicherheitsstandards für die zukünftige Nachrichtenübertragung zwischen Fahrzeugen in Fahrzeugleitsystemen. Als zentraler Beitrag werden Architekturen und Nachrichtenformate spezifiziert, die einen sicheren Betrieb von Fahrzeugleitsystemen ermöglichen sollen [64].

Trotz dieser Bemühungen um IKT-Sicherheit kommt es immer wieder zu erfolgreichen Angriffen auf kritische Infrastrukturen, beispielsweise mit „Stuxnet“ [70] oder „Duqu“ [6]. Dabei sind nicht hackbare Rechner und perfekt sichere kryptografische Verfahren bekannt, die immun gegen Angriffe mit derartigen Werkzeugen sind [82]. Aktuell verbreitete Rechnerarchitekturen und kryptografische Paradigmen erfüllen jedoch nicht die notwendigen Voraussetzungen zum Einsatz dieser Verfahren.

IKT-Sicherheit wird manchmal (nicht ganz korrekt) mit dem englischen Begriff „security“ bezeichnet.

3.1.2 Funktionale Sicherheit

Unter funktionaler Sicherheit von elektrischen/elektronischen (E/E) Systemen wird „Freiheit von unakzeptablen Risiken basierend auf Gefahren, die durch Fehlfunktionen von E/E-Systemen verursacht werden“, verstanden [149]. Fahrzeugleitsysteme zählen zu programmierbaren elektronischen Systemen, deren Fehlfunktion zu schweren Schäden oder sogar zur Gefährdung von Menschenleben führen kann und die somit hohe Sicherheitsanforderungen erfüllen müssen. Der Versuch, diese Sicherheitsanforderungen zu quantifizieren, hat zur Einführung der Sicherheitsintegritätsstufen *Safety Integrity Level (SIL)* 1 bis SIL 4 in der Norm IEC 61508 geführt [39], welche die funktionale Sicherheit elektrischer/elektronischer/programmierbarer Systeme beschreibt. Die ISO 26262 bildet eine daraus abgeleitete, eigene Normenreihe für Kraftfahrzeuge [100]. Sie kann damit als konkrete Implementierung der IEC 61508 mit spezifischen Anpassungen für das Anwendungsgebiet eines Fahrzeugleitsystems betrachtet werden.

Bei programmierbaren elektronischen Systemen stellt sich das Problem, dass verbreitete Programmiersprachen nicht auf funktionale Sicherheit hin ausgelegt sind. Obwohl PEARL dahingehend weiterentwickelt wurde [31], muss aktuell auf Instrumente zurückgegriffen werden, um herkömmlich entwickelte Software auf Konformität mit einschlägigen Standards funktionaler Sicherheit hin zu prüfen [77].

Funktionale Sicherheit wird manchmal (nicht ganz korrekt) mit dem englischen Begriff „safety“ bezeichnet.

3.1.3 Echtzeit in der Automatisierungstechnik

Zeitanforderungen sind ein wichtiger Baustein zur sicheren Funktion von Systemen. In der Automatisierungstechnik treten Zeitanforderungen insbesondere in Form von Latenz- und Reaktionszeiten auf. Daten- und Prozessverarbeitung in Echtzeit zeichnen sich durch „Rechtzeitigkeit der Reaktionen innerhalb vorgegebener und vorhersehbarer Zeitschranken“ aus, so „dass die funktionale Korrektheit eines Systems nicht nur vom Resultat [und der Schnelligkeit] einer Berechnung, sondern auch von der Zeit abhängt, wann dieses Resultat produziert wird“ [84]. Sind einzelne Überschreitungen der vorgegebenen Zeitschranken tolerierbar, da „es genügt, die Zeitbedingungen für den überwiegenden Teil der Fälle zu erfüllen, oder sich geringfügige Überschreitungen der Zeitbedingungen ergeben“ dürfen, spricht man auch von *weichen* Echtzeitanforderungen [188]. Die konkret zulässige Toleranz muss jedoch einzelfallbezogen festgelegt werden.

Am Beispiel Fernwartungssysteme konnte eine echtzeitfähige Kommunikation über eine latenzbehaftete drahtlose Kommunikationsverbindung bereits realisiert werden [177]. Ein vielversprechender Übertragungsstandard zur drahtlosen Vernetzung in der Automatisierungstechnik, mit dem eine hohe Übertragungszuverlässigkeit bei geringen Latenzen erreicht werden kann, ist IEEE 802.15.4 [91]. Für eine Industrie 4.0-Anwendung im Verkehrsbereich wurde auf Basis kostengünstiger *Android*-CE-Geräte ein Modul zur Geschwindigkeitsregelung im Automobil entwickelt. Aufgrund experimenteller Untersuchungen wird vermutet, dass sich ein solches Modul nach weiterer Entwicklung zum Einsatz unter weichen Echtzeitbedingungen eignen könnte [90].

Besondere Anforderungen werden auch an die eingesetzten Datenbankmanagementsysteme (DBMS) gestellt, da diese nicht nur statische und fertig verarbeitete Daten aufnehmen, sondern kontinuierliche Datenströme behandeln müssen. Zu diesem Zweck werden *Data Stream Management Systeme (DSMS)* entwickelt, die laufend aktuelle Zeit-Werte-Paare aufnehmen und darauf bezogene Abfragen verarbeiten können [124].

3.1.4 Systemintegration von Fahrzeugleitsystemen

Die wichtigsten Fähigkeiten eines mobilen autonomen Systems sind Informationserfassung, Informationsverarbeitung und Aktorik (engl. *sensing*, *reasoning* und *acting*) [186]. Zur Entwicklung von Fahrzeugleitsystemen müssen daher die Steuer- und Regelaufgaben, die aktuell der Mensch durchführt, auf Digitalrechner übertragen werden. Zu jedem der genannten Teilbereiche sowie der übergreifenden Systemintegration existieren Forschungsansätze, die ihrerseits in eigenen Kompendien zusammengestellt sind [131].

Automatische Informationserfassung (*sensing*) reicht von der automatisierten Verkehrsdatenanalyse [145] über spezialisierte Anwendungen wie der Fusion von Fahrzeugsensordaten für die Wettererkennung im Straßenverkehr [26] bis hin zur Gefahrenerkennung, -weiterleitung und -warnung der Fahrer durch Datenfusion vorhandener Sensoren, die in Serienfahrzeugen verbaut sind [168]. Zur automatischen Informationserfassung kommen zunehmend Kamerasysteme mit Bilderkennungssoftware zum Einsatz [7].

Zur Informationsverarbeitung vernetzter Fahrzeuge (*reasoning*) wird, insbesondere in der Einführungsphase von Fahrzeugleitsystemen, eine Kombination aus dedizierten Kommunikationsknoten („roadside units“) und einem Backend zur Ausführung der notwendigen Sicherheitsanwendungen, jeweils getrennt für Inner- und Außerortsbereich, als zielführend erachtet [2]. Für die entstehenden Automatisierungsnetze werden passende Architektur-

komponenten und Schnittstellen benötigt, um Komponenten aus anderen Industriebereichen für den Einsatz in Automobilen zu ertüchtigen [96]. Zur Entwicklung eines verteilten, eingebetteten Echtzeitsystems existieren hierzu erste Ansätze für eine offene Rahmenarchitektur, die die im Automobilbereich notwendige Skalierung erlaubt [133].

Als Aktorik (*acting*) werden zumeist existierende Fahrerassistenzsysteme genutzt. Hierzu zählen Techniken zur Regelung der Maximalgeschwindigkeit oder zur Fahrerunterstützung bei Fahrmanövern in komplexen Situationen [115]. Eine automatisierte Analyse und die Interpretation von Fahrzeugtrajektorien erlauben selbst die Steuerung von Gelenkfahrzeugen [189].

Die Entwicklung von Fahrzeugleitsystemen betrifft nicht zuletzt die Analyse wirtschaftlicher Potentiale und notwendiger Rahmenbedingungen für autonomes Fahren [22]. Hierzu fördert die Politik die Entwicklung von Fahrzeugleitsystemen durch entsprechende Rahmenbedingungen und Förderprogramme [17, 19, 20].

3.2 Struktur informationsverarbeitender Systeme

Informationsverarbeitende Systeme werden in Module oder Schichten unterteilt, um ihre Komplexität durch klare Abgrenzung von Aufgaben zu reduzieren. Die Automatisierungspyramide und das Referenzarchitekturmodell Industrie 4.0 (RAMI 4.0) bilden organisatorische Rahmen, das Open Systems Interconnection (OSI)- und das TCP/IP-Modell eine technische Struktur für kommunikationsfähige, informationsverarbeitende Systeme.

3.2.1 Automatisierungspyramide

Die Automatisierungspyramide ist das grundlegende Konzept der industriellen Datenerfassung, -speicherung und -verarbeitung mit dem „Ziel, die Komplexität der industriellen Fertigung durch die Unterteilung der anfallenden Prozesse zur Datenerhebung und -verarbeitung in einzelne Ebenen zu verringern und in eine leicht verständliche, visuelle Darstellung der industriellen Fertigung zu überführen“ [112]. Die Automatisierungspyramide nach IEC 62264 umfasst die folgenden Ebenen [41]:

- Unternehmensebene
- Betriebsleitebene
- (Prozess-)Leitebene
- Steuerungsebene
- Feldebene

Wegen dieser grundlegenden Bedeutung werden ihre Konzepte fortlaufend auf die Anforderungen für Industrie 4.0 übertragen [117].

3.2.2 Referenzarchitekturmodell Industrie 4.0

Das Referenzarchitekturmodell Industrie 4.0 (RAMI 4.0) [56] bildet eine Erweiterung der Automatisierungspyramide um die speziellen Anforderungen von Industrie 4.0. Diese Erweiterung wird durch Strukturierung der technischen und organisatorischen Anforderungen

für Industrie 4.0 erreicht. Zuständigkeiten, Abhängigkeiten und Schnittstellen zwischen Systemen werden mittels der drei Achsen *Hierarchy Levels*, *Life Cycle & Value Stream* sowie *Layers* strukturiert, die alle wesentlichen Aspekte von Industrie 4.0 abbilden [57]. Das RAMI 4.0 ist in Abbildung 3.1 dargestellt. Mit dieser auf dem *Smart Grid Architecture Model (SGAM)* beruhenden Struktur lässt sich ein reales Element der physischen Welt hinsichtlich Hierarchiestufe, Abschnitt in der Wertschöpfungskette und Aufgabe in der Automatisierungspyramide beschreiben. Die Zuweisung einer Verwaltungsschale erweitert dieses Element zu einem „Asset“, indem sie Informationen über das Asset speichert, pflegt und bereitstellt. Damit ist das Asset zur Interaktion mit anderen Assets im Sinne von Industrie 4.0 befähigt.

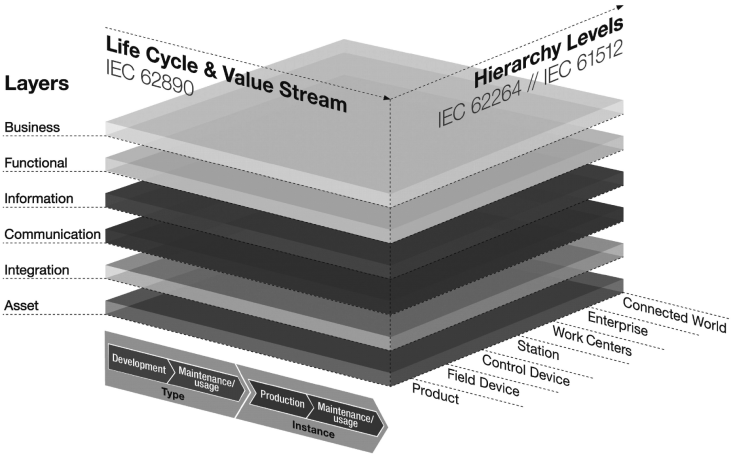


Abbildung 3.1: Referenzarchitekturmodell Industrie 4.0 [57]

Das RAMI 4.0 bietet damit einen Rahmen, um bestehende physische Systeme durch technische und organisatorische Ertüchtigung zu einer Kommunikationsarchitektur zu vereinen [130]. Dieser Rahmen ermöglicht die Entwicklung von Geschäftsmodellen und soll damit betriebs- und volkswirtschaftliches Potential von Industrie 4.0 für verschiedene Branchen erschließen [5]. Ansätze, die das RAMI 4.0 als Grundlage für kommerzielle Plattformen zur Vernetzung von Assets nutzen und damit standardisierte Schnittstellen für Hard- und Software bieten, sind:

- *MindSphere* von Siemens
- *Predix* von General Electric
- *Azure IoT Platform* von Microsoft
- *Watson IoT Platform* von IBM
- *IoT Suite* von Bosch

Die Verwaltungsschale ist ein zentraler Bestandteil jedes Assets. Sie macht ein Asset zur Komponente von Industrie 4.0 und bildet die „informationstechnische Repräsentanz“ [57] eines Assets in einem entsprechenden System. Über seine Verwaltungsschale werden die Eigenschaften eines Assets sowie dessen Schnittstellen zu anderen Komponenten von Industrie 4.0 verwaltet. Zu den Eigenschaften zählen insbesondere Zugriffsschutz, Identitäts- und Rechtemanagement, Vertraulichkeit und Integrität.

3.2.3 Open Systems Interconnection-Modell

Das Open Systems Interconnection (OSI)-Modell ist eine genormte [101] Struktur als Referenz für Netzprotokolle, um Kommunikationsmöglichkeiten und Weiterentwicklungspotentiale unterschiedlicher technischer Systeme zu ermöglichen [169]. Hierzu werden die zur Kommunikation notwendigen Abläufe in sieben unterschiedliche Ebenen unterteilt, von denen jede eine spezifische Aufgabe des Kommunikationsvorgangs erfüllt.

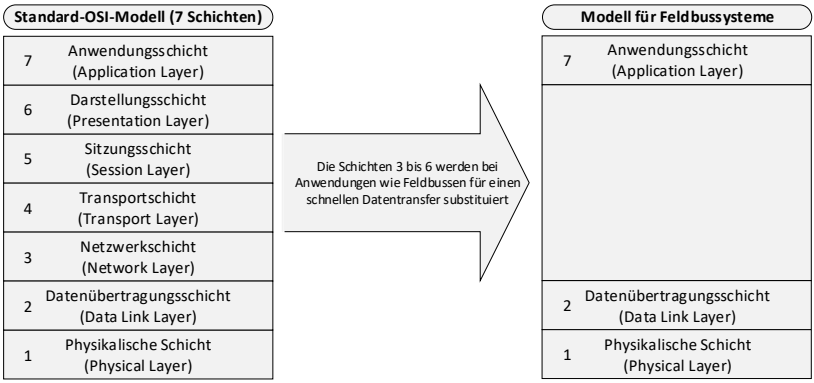


Abbildung 3.2: Kommunikation im OSI-Modell [84]

Für konkrete Implementierungen wie Ethernet oder Bluetooth können die sieben Schichten des OSI-Modells teilweise zusammengefasst werden. Eine solche Substitution ist in Abbildung 3.2 für das Beispiel Feldbussysteme dargestellt. Auf dem OSI-Modell bauen bereits Spezialprotokolle für die Vernetzung von Industrieanwendungen mit Echtzeitanforderungen auf [95], weshalb es auch als ein Referenzmodell für Kommunikationsprotokolle in Fahrzeugleitsystemen dienen kann.

3.2.4 Internetprotokollfamilie und TCP/IP-Referenzmodell

Für die Datenübertragung im Internet hat sich eine große Anzahl spezieller Protokolle herausgebildet. Zu den wichtigsten zählen das Internet Protocol (IP), das Transmission Control Protocol (TCP), das User Datagram Protocol (UDP) und das Internet Control Message Protocol (ICMP), von denen die Bezeichnung *TCP/IP-Referenzmodell* abgeleitet ist. Damit werden die sieben Schichten des OSI-Modells auf vier Schichten aggregiert [167] und für die Anforderungen des Internets optimiert. Aufgrund der Popularität des Internets

und insbesondere des World Wide Web (WWW) hat die TCP/IP-Protokollfamilie große Popularität erreicht, was zu einer entsprechenden Entwicklergemeinschaft mit zahlreichen, offenen Implementierungen in Form von Programmbibliotheken geführt hat.

Daher ist der Versuch naheliegend, die Bestandteile der TCP/IP-Protokollfamilie auch in Anwendungen des Internet of Things als Kommunikationsprotokolle zu verwenden [21, 78]. Dies führt jedoch zu Problemen bei Echtzeitanwendungen: So wird das TCP zwar beispielsweise unter weichen Echtzeitanforderungen wie bei der IP-Telefonie eingesetzt. TCP kann jedoch prinzipbedingt nicht für die Kommunikation unter harten Echtzeitbedingungen eingesetzt werden, da das Zeitverhalten des TCP probabilistisch ist [161]. In Fahrzeugleitsystemen kann TCP daher nur bei Anwendungen zum Einsatz kommen, für die keine harten Echtzeitbedingungen gelten.

3.3 Informationsübertragung durch drahtlose Kommunikationsnetze

Drahtlose Datenübertragung bietet die Möglichkeit, Informationen unabhängig von Kabeln zu übertragen. Aus dem Fehlen einer physischen Kommunikationsinfrastruktur ergeben sich jedoch auch zusätzliche Herausforderungen: Verwaltung und Strukturierung der Netze müssen auf rein logischer Ebene umgesetzt und auch beim Kanalzugriff müssen spezielle Verfahren zur Kollisionsvermeidung vorgesehen werden.

3.3.1 Physikalische Möglichkeiten und Grenzen

Zur drahtlosen Datenübertragung wird eine Trägerfrequenz aus dem elektromagnetischen Spektrum genutzt, der die zu übertragenden Zeichen aufmoduliert werden.

Modulation Der Sender verändert gezielt Frequenz, Amplitude oder Phase der Trägerfrequenz, um die gewünschte Nachricht in Form einer Zeichenfolge aufzumodulieren. Die verschiedenen Modulationsarten Amplituden-, Frequenz- und Phasenmodulation für ein Digitalsignal sind in Abbildung 3.3 dargestellt. Zur Vermeidung ungewollter elektrischer oder elektromagnetischer Wechselwirkungen kann die Trägerfrequenz nicht beliebig gewählt werden, sondern muss sich im Sinne der EMV in das existierende elektromagnetische Spektrum einfügen.

Der Empfänger registriert diese Änderungen von Frequenz, Amplitude oder Phase und extrahiert daraus wiederum die Information (hier die Binärziffern 1 und 0). Der Beginn eines Datenpakets ist durch eine spezifische Bitfolge gekennzeichnet. Wie in Abbildung 3.4 dargestellt ist, besteht diese aus einer Präambel (engl. *preamble*) und einem *Start Frame Delimiter (SFD)* zur Kennzeichnung des Beginns des Datenpakets. Dadurch wird dem Empfänger signalisiert, an welcher Stelle er die Nutzdaten aus dem Signal extrahieren kann. Bei der Wahl von Präambel und SFD darf es nicht zu Doppeldeutigkeiten mit einer Bitfolge des Nachrichteninhalts kommen.

Frequenzen Da eine Vielzahl von Anwendungen gleiche oder überlappende Frequenzbänder wie ISM nutzt [80], müssen Maßnahmen zur Vermeidung gegenseitiger Störungen gefunden werden. Die Grundvoraussetzung für den Einsatz drahtloser Kommunikation in

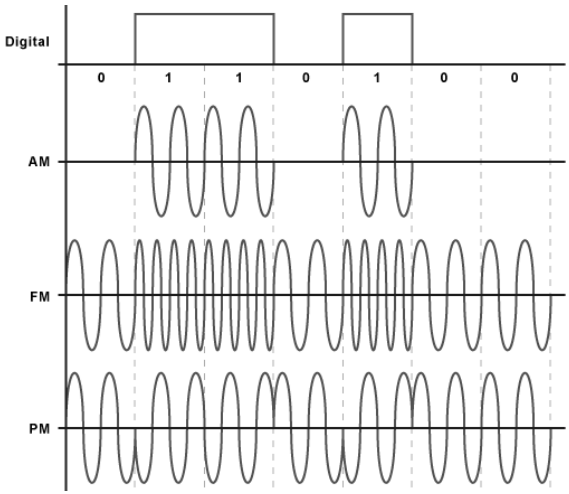


Abbildung 3.3: Amplituden (AM)-, Frequenz (FM)- und Phasenmodulation (PM) von Binärwerten eines Digitalsignals [160]

sicherheitskritischen Industrieanwendungen ist daher die sorgfältige Auswertung möglicher Störeinflüsse zur Gewährleistung der EMV [23]. Ein Ansatz dazu ist, das verfügbare Funkspektrum durch dynamische Anpassung der Datenübertragung an die jeweils aktuelle Auslastung möglichst effizient auszunutzen [86].

Die Substitution speziell für echtzeitfähige Datenübertragung ausgelegter Datenbusse wie PROFIBUS durch Ethernet- und Wireless Local Area Network (WLAN)-Netze wurde modellhaft untersucht [157], ist in der Praxis bislang aber nur ansatzweise gelungen [28, 180]. Dies verdeutlicht, dass der Einsatz dieser bewährten Echtzeitkommunikationssysteme in einem drahtlos kommunizierenden Fahrzeugleitsystem nicht in einfacher Weise möglich ist.

Vor einem Einsatz von Funksystemen im industriellen Umfeld muss neben der technischen Machbarkeit auch die wirtschaftliche Perspektive, beispielsweise in Form einer Kosten-Nutzen-Betrachtung, untersucht werden [10].

3.3.2 Topologie

Zur Vernetzung frei beweglicher Objekte kann keine Verkabelung eingesetzt werden, weshalb eine Netzstrukturierung auf physikalischer Ebene nicht möglich ist. Topologie, In-

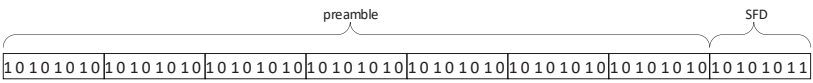


Abbildung 3.4: Präambel und SFD eines Ethernet-Frames [93]

formationsfluss und Vermittlung müssen daher auf einer rein logischen Ebene festgelegt werden. Es existieren zahlreiche Topologien zur Strukturierung eines Netzes [21].

Ad-hoc-Modus Im Ad-hoc-Modus werden die Kommunikationsteilnehmer direkt miteinander verbunden. Es wird keine zusätzliche Infrastruktur benötigt und die Nachrichten können entweder direkt zwischen den Teilnehmern oder indirekt mit Teilnehmern als Zwischenstationen übertragen werden. Ein Vorteil des Ad-hoc-Modus in Fahrzeugleitsystemen ist Unabhängigkeit von zusätzlicher Infrastruktur. Dies erhöht auch die Ausfallsicherheit einzelner Routen durch mögliche Redundanzen [79]. Jedoch ist der Schutz der übertragenen Daten aufwändig und erfordert komplexe Maßnahmen zur Absicherung von Dateninhalten und Privatsphäre [8, 156]. Zudem können sich Anzahl und Länge der Verbindungen zwischen Sender und Empfänger laufend ändern oder Verbindungen abbrechen [125]. Die resultierende nicht-deterministische Netzstruktur erfüllt keine Echtzeitbedingungen, wie sie von Fahrzeugleitsystemen gefordert werden. Auch in Ad-hoc-Netzen wird stets eine zentrale Instanz zur Zuweisung und Überwachung der von den Teilnehmern verwendeten Adressen benötigt [182]. Betrachtet man Ad-hoc-Netze als verteilte Peer to Peer (P2P)-Netze, die auf darunterliegende physikalische Netze aufbauen [74], können die Hardwareadressen diese Funktion zwar übernehmen. Dies bietet jedoch keinen Schutz gegen mutwillig veränderte oder unberechtigt behauptete Adressen [187]. Ad-hoc-Netze werden teilweise auch als (unstrukturierte) P2P-Netze bezeichnet [123]. Zur Beschreibung bewegter Kommunikationsobjekte in Verkehrssystemen werden spezielle Datenmodelle benötigt [183]. Ein Ad-hoc-Funknetz zur Vernetzung von Kraftfahrzeugen wird auch „Fahrzeug-Ad-hoc-Netz“ (engl. *Vehicular Ad hoc Network [VANet]*) genannt. Für VANets auf Basis des Standards IEEE 802.11 wurde ein Bereich im Frequenzband von 5,85 GHz bis 5,925 GHz reserviert und als IEEE 802.11p standardisiert [106].

Infrastrukturmodus Im Infrastrukturmodus werden alle Kommunikationen über einen zentralen Zugangspunkt abgewickelt. Diese Struktur ist aus Rechnernetzen bekannt, die als WLAN mit zentralem Zugangspunkt (engl. *access point*) aufgebaut sind. Der Zugangspunkt wird auch als *Relais* bezeichnet. Im Infrastrukturmodus können wichtige Parameter wie die Entfernungen zwischen den Teilnehmern und den Relais, die Auslastungen der einzelnen Relais und die Signallaufzeiten bestimmt werden [154]. Damit sind zentrale Bedingungen für die Echtzeitkommunikation erfüllt. Der Infrastrukturmodus wird bereits erfolgreich in Netzen für Sprach- und Datenkommunikation zwischen mobilen Teilnehmern eingesetzt (Global System for Mobile Communications [GSM]), wo allerdings nur weiche Echtzeitanforderungen gestellt werden. Die Identifikatoren der Teilnehmer werden zentral mittels Subscriber Identity Module (SIM), Universally Unique Identifier (UUID) oder Globally Unique Identifier (GUID) zugeteilt und verwaltet. In der Erweiterung des GSM-Standards um *5G* wird großes Potential für Fahrzeugnetze, insbesondere für echtzeitfähige Kommunikation, gesehen [135]. Hierzu sollen bestehende Netze durch sogenannte *cloudlets* um die benötigten Funktionen erweitert werden [165]. Die Vernetzung von Fahrzeugen im Infrastrukturmodus wird auch „Cellular Vehicle to everything (C-V2X)“ genannt. C-V2X konnte sich durch den Einsatz als Notrufsystem („eCall“) bereits in einer sicherheitsrelevanten verkehrstechnischen Anwendung mit Echtzeitanforderungen bewähren [3].

Gegenüberstellung Funkgestützte Kommunikation in der Automatisierungstechnik wird in der technischen Regel VDI/VDE 2185 behandelt [175], die als Entscheidungshilfe bei der Auswahl eines geeigneten Übertragungskonzepts in Automatisierungsanwendungen dienen soll. Auf dieser Grundlage sind in Tabelle 3.1 die wesentlichen Eigenschaften der jeweiligen Topologie hinsichtlich des Einsatzes in einem Fahrzeugleitsystem bewertet. Dabei wird davon ausgegangen, dass ein Kollektiv von $|W| = n$ Fahrzeugen um m Fahrzeuge erweitert wird und das entstehende Kollektiv entsprechend der Folgerungen aus Unterabschnitt 2.8.2 zur symmetrischen Verschlüsselung befähigt sein soll.

Tabelle 3.1: Bewertung verschiedener Netztopologien für Fahrzeugleitsysteme

	Mit Relais (Infrastruktur)		Ohne Relais (Ad-hoc)	
Kosten Infrastruktur	−	dediziertes Netz	+	kaum benötigt
Skalierbarkeit				
Schlüsselverteilung	+	$\mathcal{O}(1)$	−	$\mathcal{O}(n)$
Schlüsselvorratsmächtigkeit	+	$\mathcal{O}(m)$	−	$\mathcal{O}((n+m)^2)$
Schlüsselgröße	+	$\mathcal{O}(m)$	−	$\mathcal{O}((n+m)^2)$
Übertragungsstrecke	+	2 Abschnitte	−	nicht vorhersehbar

Für die Vernetzung im Infrastrukturmodus muss das gesamten Netzgebiet mit Relais abgedeckt sein, was zusätzliche Infrastruktur und damit verbundene Investitionskosten notwendig macht. Der Ad-hoc-Modus kann mit Kommunikationskomponenten der Fahrzeuge betrieben werden.

Die Skalierbarkeit der jeweiligen Topologie betrifft drei Aspekte: Schlüsselverteilung (Zeitkomplexität), Schlüsselvorratsmächtigkeit und Schlüsselgröße (jeweils Platzkomplexität). Die Skalierung der Schlüsselverteilung bezieht sich auf den sicheren Kanal zur Versorgung aller Beteiligten mit Schlüsseln. Im Infrastrukturmodus wird ein sicherer Kanal zum Relais und ein sicherer Kanal zur Stelle der Erstzulassung benötigt, um sowohl Fahrzeuge als auch Relais mit Schlüsseln zu versorgen. Die Komplexitätsklasse zur Integration von m Fahrzeugen ist daher im Infrastrukturmodus konstant. Im Ad-hoc-Modus wird zusätzlich ein sicherer Kanal zu allen bestehenden n Fahrzeugen benötigt, um diesen die Schlüssel der neu hinzugefügten m Fahrzeuge bekannt zu machen. Die Komplexitätsklasse zur Integration von m Fahrzeugen ist daher im Ad-hoc-Modus linear. Ein sicherer Kanal würde auch beim Einsatz asymmetrischer Kryptosysteme benötigt, um *Man in the Middle (MITM)*-Angriffe zu verhindern.

Die Skalierung der Schlüsselvorratsmächtigkeit bezieht sich auf die Anzahl der Schlüsselpaare, die zur Integration von m Fahrzeugen erzeugt werden müssen. Im Infrastrukturmodus ist jeweils ein Schlüsselpaar für die Übertragungen zwischen Fahrzeug und Relais notwendig, die Komplexitätsklasse ist daher linear. Im Ad-hoc-Modus ist ein individuelles Schlüsselpaar für jede mögliche Kombination von Teilnehmern notwendig, die Komplexitätsklasse ist daher quadratisch.

Die Schlüsselgröße und damit die zu erzeugende und vorzuhaltende Datenmenge ist nach Gleichung 2.6 proportional zur Schlüsselvorratsmächtigkeit. Die jeweiligen Komplexitätsklassen verhalten sich daher entsprechend.

Wie in Unterabschnitt 2.8.1 bereits dargestellt wurde, ist die logische Länge einer Übertragungsstrecke im Ad-hoc-Modus nicht vorhersehbar, da sich die Netzmaschen abhängig

von den Fahrzeugbewegungen dynamisch bilden und auflösen. Im Infrastrukturmodus erstreckt sich die Übertragungsstrecke stets über genau zwei Abschnitte.

3.3.3 Identifizierung und Routing

Jedes Kommunikationssystem muss den Empfänger einer Information mit einer Adresse eindeutig kennzeichnen und Nachrichten durch das Kommunikationsnetz zu diesem Empfänger leiten können. Der Prozess, einen bestimmten Weg durch das Kommunikationssystem zu finden, wird Routing genannt.

In der Automatisierungstechnik werden Feldbusse zur seriellen Kommunikation zwischen Sensoren, Aktoren und Reglern eingesetzt [84], die hohen Standards hinsichtlich der Sicherheit genügen müssen [44]. Bei der Planung einer Industrieanlage wird in der Regel einem bestimmten System der Vorzug gegeben, um redundante Pflege- und Wartungsaufwände zu vermeiden. Dies ermöglicht einerseits die initiale Festlegung von Adressen und Routen auf einfache Weise, andererseits ist eine nachträgliche Erweiterung oder Kopplung verschiedener Feldbusse trotz Standardisierungsversuchen wie *Open Platform Communications (OPC)* nicht oder nur mit hohem Aufwand möglich.

Unter der Bezeichnung „Echtzeit-Ethernet“ rückt Ethernet in den Fokus [116], um diesen Nachteil bei der Skalierung zu beseitigen. Optimierte Zugriffsverfahren und das Vorhalten von Alternativpfaden sind vielversprechende Voraussetzungen für eine weitere Verbreitung von Ethernet als Feldbus [132].

Die Substitution von Ethernet durch WLAN, wie es in Anwendersystemen weite Verbreitung gefunden hat, wird folglich auch für Feldbussysteme untersucht. Konzeptuelle Schwächen von WLAN im Bereich der Echtzeitkommunikation hinsichtlich Zugriffsverfahren, Zuverlässigkeit und Hidden-Terminal-Problem lassen sich mit bestehenden Verfahren nur mindern, jedoch nicht beseitigen [111, 170]. Darüber hinaus sind in VANets die Sicherstellung der benötigten Mindestdichte an Vermittlungspunkten [181] und die Anfälligkeit für den Diebstahl digitaler Identifikatoren [30, 121] ungelöst.

3.3.4 Synchronisierung und Konsens

Drahtlose Netze sind aufgrund fehlender Abschirmung des Übertragungsmediums anfälliger für natürliche oder künstliche Störungen als kabelgebundene Übertragungsstrecken. Die Teilnehmer müssen daher zu autarkem Verhalten befähigt sein, da zumindest mit vereinzelten Verbindungsabbrüchen gerechnet werden muss. Dies betrifft besonders den Konsens über die Rechte anderer Teilnehmer sowie die Kenntnis über das aktuelle Umfeld.

Das *Internet of Things* stellt die verbreitete Client-Server-Architektur zur Verwaltung von Berechtigungsstufen vor neue Herausforderungen, da stets eine Verbindung zum Server benötigt wird. In Fahrzeugleitsystemen muss auch ohne diese Verbindung die Überprüfung von Berechtigungsstufen möglich und zudem robust gegenüber fehlerhaftem oder böswilligem Verhalten einzelner Teilnehmer sein. Theoretisch wird dieser Sachverhalt durch das Consistency, Availability and Partition Tolerance (CAP)-Theorem beschrieben [75], welches besagt, dass in einem verteilten System die Anforderungen *Consistency* (Konsistenz), *Availability* (Verfügbarkeit) und *Partition Tolerance* (Ausfalltoleranz) nicht gleichzeitig auf einem beliebig hohen Niveau gewährleistet werden können.

Herausragende Bedeutung in Fahrzeugleitsystemen hat der Identifikator (ID) für jeden Teilnehmer, der durch geeignete Protokolle nur in Ansätzen dezentral vergeben werden

kann [107]; denn die Probleme Authentifizierung und Identitätsdiebstahl sind für Ad-hoc-Netze trotz intensiver Forschung nur unzureichend gelöst [88]. Aus diesem Grund ist es sicher kein Zufall, dass etablierte Kommunikationsnetze letztendlich durch zentrale Instanzen verwaltet werden:

- Internet: Die Internet Corporation for Assigned Names and Numbers (ICANN) und ihre Unterabteilung Internet Assigned Numbers Authority (IANA) bilden zentral organisierte Organisationen, die auf der obersten Hierarchiestufe die zum Betrieb des Internets benötigten Nummern und Namen verwalten. Sie stellen authentifizierten Teilnehmern IP-Adressbereiche sowie Top-Level-Domains zur Verfügung und vermeiden somit Adresskonflikte durch entsprechende Organisation.
- Rechnernetze: Zur Vergabe einer Media Access Control (MAC)-Adresse an Netzschnittstellen definiert und verwaltet das IEEE eindeutige Herstellerkennungen und stellt diese in einer zentralen Datenbank zur Einsicht bereit.
- Global System for Mobile Communications: Subscriber Identity Module (SIM), International Mobile Equipment Identity (IMEI) und International Mobile Subscriber Identity (IMSI) werden von einem Telekommunikationsunternehmen zentral verwaltet und den mobilen Teilnehmern zugewiesen.
- Mauterfassung auf deutschen Autobahnen: Die Fahrten mautpflichtiger Lkw werden auf einem zentralen Server erfasst, um den Spediteuren die Gebühren berechnen zu können [188].
- Elektronische Bankgeschäfte: Die Society for Worldwide Interbank Financial Telecommunication (SWIFT) betreibt ein dediziertes, zentral verwaltetes Telekommunikationsnetz (SWIFTNet) für die standardisierte Datenübertragung zwischen Finanzinstituten. Kontoinformationen werden zentral bei den angeschlossenen Banken verwaltet. Zugriffsberechtigungen für die Konten werden mit Schlüsselkarten (Chipkarte oder Zahlungskarte) an die Kunden verteilt, die sich damit authentisieren und eine *Transaction Authentication Number* (TAN) zur Autorisierung von Finanztransaktionen generieren können. Eine TAN hat häufig eine Länge von sechs Ziffern.

Durch zentrale Verwaltung wird vermieden, dass ein ID doppelt vergeben wird. Komplexe Verfahren zur dezentralen Konsensfindung sind bei zentraler Verwaltung nicht erforderlich. Dort sind jedoch besondere Vorkehrungen zur Gewährleistung von Sicherheit und Zuverlässigkeit erforderlich, da es sich bei jeder der zentralen Stellen um einen SPOF handelt.

3.3.5 Nachrichtenübertragung in Verkehrssystemen

Bestehende Konzepte für die Nachrichtenübertragung in Verkehrssystemen lassen sich in die Übertragung von Informationen zur Strecke und Informationen zu einzelnen Fahrzeugen unterteilen.

Streckenbezogene Informationen Als streckenbezogene Informationen werden temporäre Änderungen bekannter Streckeneigenschaften wie erhöhte Reisezeiten aufgrund von Stauungen oder Sperrungen übermittelt. Hierzu werden dem zentral ausgestrahlten Rundfunk Verkehrs- und Reiseinformationen im nicht hörbaren Bereich des UKW-Signals in

Form von Codes hinzugefügt (Radio Data System – Traffic Message Channel [RDS-TMC]). Diese Codes sind mit inhaltlich und geografisch vorab codierten Verkehrsmeldungen verknüpft, die als Volltext in einer Datenbank an Bord des Fahrzeugs hinterlegt sind. Ein übertragenes und entsprechend verarbeitetes Codewort löst beim Empfänger die Darstellung einer ausführlichen Meldung aus, deren Bestandteile sich aus den Inhalten der hinterlegten Datenbank speisen. Der Fahrer kann so in seiner jeweils eingestellten Landessprache über Ort und Art einer Verkehrsbeeinträchtigung informiert werden, ohne dass die spezifischen Meldungsinhalte vollständig mit dem Rundfunksignal übertragen werden müssten [46]. Es handelt sich bei RDS-TMC um einen unidirektionalen Broadcast, ein Rückkanal vom Fahrzeug zum Sender ist nicht vorgesehen.

Fahrzeugbezogene Informationen Als fahrzeugbezogene Informationen sendet jedes Fahrzeug Parameter zu seinem aktuellen Zustand. Datenformate sind mit der *Cooperative Awareness Message (CAM)* [61] und der *Decentralized Environment Notification Message (DENM)* [62] spezifiziert. Die Länge einer Nachricht variiert mit den modular und in Form von Containern festzulegenden Nachrichteninhalten. Nachrichten können entweder mit einer festen Frequenz (CAM) oder ereignisgesteuert (DENM) gesendet werden. Die Generierungs- und Übertragungsfrequenz f_{cam} einer CAM liegt dabei im Bereich $1\,\mathrm{Hz} \leq f_{cam} \leq 10\,\mathrm{Hz}$ [61]. Zum Vergleich: Die menschliche Verarbeitungszeit setzt sich aus der „Schrecksekunde“ und der Reaktionszeit zusammen. Sie dauert von der Ereigniswahrnehmung bis zur Aktion insgesamt rund eine Sekunde [73]. Nachrichten im Format CAM oder DENM können sowohl empfangen als auch gesendet werden.

Ein Fahrzeugleitsystem kann mit diesen Informationen den Verkehrsfluss optimieren und die Verkehrssicherheit verbessern. Zur Optimierung des Verkehrsflusses werden ein aktueller und ein prognostizierter Verkehrszustand mit Modellen beschrieben, um geeignete Optimierungsmaßnahmen zu entwickeln und vorab zu bewerten. Für dynamische Anwendungen wie ein Fahrzeugleitsystem müssen diese Modelle speziell kalibriert werden [1].

Zur Verbesserung der Verkehrssicherheit muss diese zunächst anhand geeigneter Parameter bewertet werden [119], um bei Bedarf passende Maßnahmen zu ergreifen.

Im Gegensatz zu RDS-TMC gibt es noch keine Implementierung eines Dienstes, der auf Nachrichten vom Typ CAM oder DENM basiert. Auch die Standards des ETSI sind noch unvollständig und verweisen auf weitere Spezifikationen in der Zukunft.

3.4 Informationssicherheit durch angewandte Kryptologie

Funksignale können grundsätzlich von jedem gesendet und empfangen werden, der über geeignete Ausrüstung und Fähigkeiten verfügt. Drahtlos übertragene Nachrichten können somit abgehört und mit verändertem Inhalt erneut gesendet werden. Als Gegenmaßnahme haben sich zahlreiche kryptografische Methoden herausgebildet, um die in Abschnitt 2.6 vorgestellten Schutzziele zu erreichen. Diese Methoden werden zur Absicherung einer Nachricht selbst, aber auch zur Authentifizierung von Sender und Empfänger benötigt. Die allgemeine Form eines kryptologischen Systems ist in Abbildung 3.5 dargestellt.

Regeln zur Informationssicherheit in der industriellen Automatisierung wurden von der ISO und dem VDE festgelegt [54, 174]. Empfehlungen zu deren praktischer Umsetzung

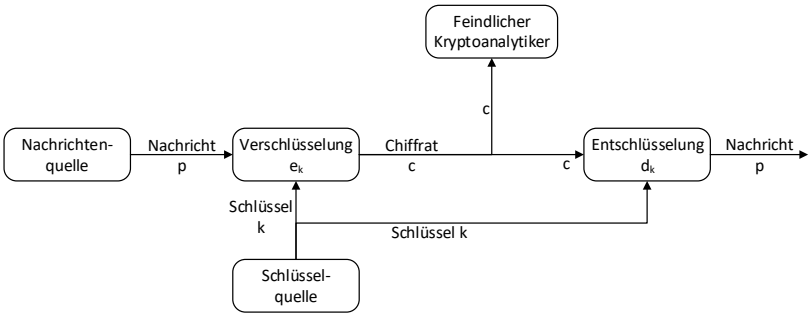


Abbildung 3.5: Schematische Darstellung eines kryptologischen Systems [163]

wurden bereits in Unterabschnitt 3.1.1 vorgestellt [12–14, 138].

3.4.1 Paradigmen und kryptografische Sicherheit

Die Kryptologie besteht aus den Teilbereichen *Kryptografie* als Wissenschaft der Ver- und Entschlüsselung von Informationen sowie der *Kryptoanalyse*, die sich mit dem Gewinnen von Informationen aus verschlüsselten Daten beschäftigt. Die Geschichte der Kryptologie erstreckt sich über viele Jahrhunderte und hat zu zahlreichen Erkenntnissen und Erfahrungen geführt [4]. Als übergeordneter Grundsatz hat sich das *kerckhoffssche Prinzip* herausgebildet, nach dem die Sicherheit eines kryptografischen Verfahrens nicht von der Geheimhaltung des zugrunde liegenden Algorithmus, sondern nur von der Geheimhaltung der Schlüssel abhängen darf [143].

Symmetrische Kryptografie Bei der symmetrischen Kryptografie wird zur Ver- und Entschlüsselung der gleiche Schlüssel eingesetzt. Bekannte Verfahren sind Blockchiffren wie der Advanced Encryption Standard (AES) und der Data Encryption Standard (DES) sowie Stromchiffren wie A5. Die Verfahren zeichnen sich durch ihre Schnelligkeit und die im Vergleich zur Nachricht geringe Schlüssellänge aus. Obwohl die drei genannten Verfahren im Rahmen der Entwicklung vielfach evaluiert wurden und eine weite Verbreitung gefunden haben, gelten der DES und A5 bereits als gebrochen [58, 110].

Ein weiteres symmetrisches Verfahren ist *perfekt sichere Einmalverschlüsselung*, welches nachweislich nicht gebrochen werden kann [163]. Hierzu betrachtet man die Menge aller Klartexte P und die Menge aller Schlüsseltexte C. Mit der Wahrscheinlichkeit $Pr(p)$ erhält man einen beliebigen Klartext $p \in P$, mit der Wahrscheinlichkeit $Pr(c)$ einen beliebigen Schlüsseltext $c \in C$. Die bedingte Wahrscheinlichkeit, den Klartext p zu erhalten, wenn der Schlüsseltext c gewählt wurde, ist $Pr(p|c)$. Ein Verschlüsselungsverfahren ist *perfekt sicher*, wenn für alle Klartexte $p \in P$ und für alle Schlüsseltexte $c \in C$ gilt:

$$Pr(p|c) = Pr(p) \tag{3.1}$$

Eine notwendige und hinreichende Bedingung für perfekte Sicherheit ist, dass $Pr(c|p)$ stochastisch unabhängig ist von p [163]:

$$Pr(c|p) = Pr(c) \quad \forall c \in C \wedge \forall p \in P \tag{3.2}$$

Wird ein Schlüsseltext empfangen, so kann ein Angreifer nur auf die Tatsache schließen, *dass* eine Nachrichtenübertragung stattfindet. Es ist ihm jedoch nicht möglich, Rückschlüsse auf den Inhalt der Nachricht zu ziehen, die über bloßes Raten hinausgehen. Dabei ist es unerheblich, über welche Ressourcen der Angreifer verfügt. Insbesondere widersteht die perfekt sichere Einmalverschlüsselung auch denkbaren Angriffen mittels Quantencomputern.

Praktische Voraussetzung ist eine korrekte Implementierung des Verfahrens im jeweiligen Anwendungsfall [146]. Insbesondere sind Schlüssel $k \in K$ notwendig, die mindestens so lang sind wie die Nachricht selbst ($|k| \geq |p|$) und mit einem echten Zufallsprozess erzeugt wurden. Im einfachsten Fall wird ein Schlüsselstrom bitweise mit einer Nachricht *XOR*-verknüpft [176]. Zur Vermittlung zwischen Feldgerät und Kommunikationsbus in automatisierungstechnischen Systemen setzen spezielle Module die Schlüsselversorgung praktisch um [158, 159].

Für den Vorgang der Verknüpfung jedes Bits eines Klartextes mit genau einem Bit eines Schlüsselstroms wird hier der Begriff „Maskierung“ eingeführt. Der Schlüssel wird entsprechend als „Chiffriermaske“ (kurz Maske) bezeichnet. Das Alphabet besteht bei der Maskierung aus den Zeichen 1 und 0.

Asymmetrische Kryptografie Bei der asymmetrischen Kryptografie werden jeweils verschiedene Schlüssel zum Ver- und Entschlüsseln eingesetzt. Ein Schlüssel bildet den *privaten*, geheim zu haltenden Schlüssel, der andere den *öffentlichen*, weiterzugebenden Schlüssel. Bekannte Verfahren sind RSA [148] und Elgamal [59]. Die praktische Anwendung asymmetrischer Kryptografie erfordert vergleichsweise große Rechenleistungen und wird daher bevorzugt zur Verteilung symmetrischer Schlüssel eingesetzt. Ist einem Angreifer einer der beiden Schlüssel bekannt (was beim öffentlichen Schlüssel anzunehmen ist), kann er daraus den anderen Schlüssel berechnen, da der mathematische Zusammenhang bekannt ist. Die Sicherheit basiert allein darauf, dass diese Berechnung eine – aktuell – nicht praktikabel lange Zeitspanne oder Rechenleistung benötigen würde.

Auch asymmetrische Kryptografie muss immer eine vertrauenswürdige dritte Instanz beteiligen, um das *MITM*-Problem bei der Kommunikation zwischen zwei Teilnehmern zu lösen. Diese Instanz ist an unterschiedlichen Stellen im Übertragungsprotokoll involviert, um die Teilnehmer und deren Schlüssel zu authentifizieren [139, 140].

Steganografie Als Steganografie werden Verfahren bezeichnet, die das Ziel haben, die Existenz oder Form einer Nachricht zu verdecken [4]. Als konkrete Verfahren sind der Spreu-und-Weizen-Algorithmus [147] oder die Nutzung eines verdeckten Kanals [178] verbreitet.

Im Fall der Kompromittierung eines steganografischen Verfahrens kann das Ziel, also die Verdeckung der Existenz oder der Form einer Nachricht, für den kompromittierten Kanal nicht mehr erreicht werden. Die Verwendung rein steganografischer Maßnahmen zum Schutz von Informationen ist daher nicht ausreichend, weil prinzipbedingt das kerckhoffssche Prinzip verletzt wird. Zudem ist in IoT-Anwendungen durch die große Anzahl vernetzter Teilnehmer, denen zur Kommunikation das steganografische Geheimnis bekannt sein muss, keine gezielte Verschlüsselung möglich. Mischformen wie *Key Whitening* [172] oder Verschleierung [82], die ein auszutauschendes Geheimnis beinhalten, können die Sicherheit kryptografischer Maßnahmen jedoch deutlich verstärken.

Kryptografische Sicherheit Ein wesentliches Sicherheitsmerkmal aller Verfahren ist der eingesetzte Schlüssel, dessen Mindestanforderungen in Unterabschnitt 2.6.3 vorgestellt wurden. Darüber hinaus kann die Sicherheit eines bestimmten kryptografischen Verfahrens aus unterschiedlichen Blickwinkeln bewertet werden, die teilweise in einem Zielkonflikt zueinander stehen:

1. Die rein informationstheoretische Betrachtung eines kryptografischen Verfahrens zielt auf geringe Wahrscheinlichkeiten, aus einem abgefangenen Schlüsseltext beliebiger Länge Rückschlüsse auf den Klartext zu gewinnen [163].

2. Die Komplexität eines Verfahrens soll so gering wie möglich gehalten werden [163]. Die Komplexität von Verfahren zur Ver- und Entschlüsselung kann weiter unterschieden werden:
   a) Die softwaretechnische Betrachtung eines Verfahrens zielt auf die Freiheit von Implementierungsfehlern und „Hintertüren“ [151] ab.
   b) Die hardwaretechnische Betrachtung eines Verfahrens zielt auf die Vermeidung von Angriffspunkten für Seitenkanalangriffe [151] ab.
   c) Die nutzerzentrierte (oder „pragmatische“) Betrachtung eines Verfahrens zielt auf die Vermeidung von Anwenderfehlern [141] ab.

3. Fortpflanzung von Chiffrierfehlern, durch die ein Verschlüsselungsfehler bei einem einzelnen Zeichen zu einem Entschlüsselungsfehler mit erheblichem Informationsverlust führt, sollte vermieden oder minimiert werden [163].

4. Ausdehnung des Schlüsseltextes gegenüber dem Klartext kann je nach Zielsetzung ein unerwünschter Effekt sein [163] oder die Sicherheit eines Verfahrens durch Verschleierung erhöhen [82, 158].

Die Vor- und Nachteile der kryptografischen Paradigmen bei Anwendung in Fahrzeugleitsystemen sind hinsichtlich der vorgestellten Schutzziele in Tabelle 3.2 zusammengefasst.

Tabelle 3.2: Bewertung kryptografischer Paradigmen für Fahrzeugleitsysteme

	Asymmetrisch		Symmetrisch	
Vertraulichkeit	−	keine perfekte Sicherheit	+	perfekte Sicherheit
Verfügbarkeit	+	gut skalierbar	*o*	Schlüsselverteilung
Integrität	−	Anfällig für MITM	+	perfekte Sicherheit
Rechenaufwand	−	Primzahlberechnung	+	*XOR*-Verknüpfung

Nur symmetrische Verschlüsselungsverfahren ermöglichen perfekte Sicherheit der Vertraulichkeit einer Nachricht durch Maskierung des Inhalts. Asymmetrische Verfahren weisen prinzipbedingt Schwächen auf, da sich der private Schlüssel aus dem öffentlichen Schlüssel berechnen lässt.

Auch das Signieren und damit die Gewährleistung der Integrität einer Nachricht sind nur mit symmetrischen Verfahren perfekt sicher möglich. Asymmetrische Verfahren sind anfällig für *Man in the Middle*-Angriffe, was auch durch den Betrieb einer Public Key

Infrastructure (PKI) nur teilweise kompensiert werden kann. Diese erleichtert lediglich die Schlüsselverteilung, beseitigt jedoch nicht die Schwächen der Verfahren an sich.

Der zusätzliche Bedarf an Übertragungsbandbreite für Zertifikatsperrlisten oder den Overhead von (D)TLS-Handshakes kann bei knapp dimensionierten Bandbreiten im IoT zusätzlich ins Gewicht fallen. Ferner ist zur Gültigkeitsprüfung der digitalen Zertifikate eine Zeitsynchronisierung notwendig. Die hierzu übliche Nutzung des GPS-Signals ist aufgrund dessen geringer Signalstärke anfällig für Angriffe mit Störsendern („Jammern“), die IoT-Geräten ein falsches Zeitsignal übermitteln können. Dadurch können bereits abgelaufene Zertifikate wieder als gültig akzeptiert werden. Gleichzeitig stellen ablaufende Root-Zertifikate ein Problem für Geräte mit langen autarken Betriebszeiten dar, da diese Geräte die mit abgelaufenen Root-Zertifikaten signierten Nachrichten als ungültig verwerfen.

Schließlich ist bei asymmetrischen Verfahren der Rechenaufwand wegen der aufwändigen Primzahlberechnungen vergleichsweise hoch, während bei symmetrischen Verfahren nur einfache Bitoperationen erforderlich sind. Dieser Aspekt spielt zwar bei der Anwendung in Kraftfahrzeugen eine untergeordnete Rolle, erschwert jedoch den Einsatz auf leistungsschwachen IoT-Geräten. In jedem Fall kann symmetrische Verschlüsselung schneller und in vorhersehbaren Zeitintervallen ausgeführt werden.

Einzig bei der Verfügbarkeit weist die asymmetrische Verschlüsselung leichte Vorteile auf, wenn eine Nachricht für mehrere Empfänger verschlüsselt werden muss: Beim Wechsel des Schlüssels kann die Nachricht bei symmetrischer Kryptografie erst dann wieder entschlüsselt werden, wenn alle Empfänger über den neuen Schlüssel verfügen. Bei asymmetrischer Kryptografie hingegen genügt ein neuer öffentlicher Schlüssel des Senders. Dieser vermeintliche Nachteil der symmetrischen Verschlüsselung kann jedoch durch Wahl einer geeigneten Architektur organisatorisch behoben werden.

Zur formalen Prüfung von Verschlüsselungsprotokollen hinsichtlich korrekter Implementierung sind Werkzeuge wie *Scyther* [25] oder die *Testing and Test Control Notation (TTCN)* [63] verfügbar. Auf derartige Werkzeuge wird insbesondere dann zurückgegriffen, wenn die entwickelten Verschlüsselungsprotokolle große Komplexität erreichen. Der Einsatz ist jedoch problematisch, da diese Werkzeuge häufig selbst komplex und nicht formal verifiziert sind. So wird bei *Scyther* generell die *unbreakable encryption assumption* zugrunde gelegt [184], die jedoch nur im speziellen Fall der perfekt sicheren Verschlüsselung gilt.

3.4.2 Authentifizierung und Autorisierung

Alle Teilnehmer eines Netzes werden durch einen ID eindeutig gekennzeichnet. Durch erfolgreiche Authentifizierung eines Teilnehmers gegenüber dem Netz kann er zur Nutzung von Netzressourcen autorisiert werden. Der ID kann gleichzeitig als Adresse für Nachrichten dienen. Die Herausforderung besteht darin, die missbräuchliche Behauptung einer Identität kryptografisch zu verhindern. Es werden hierzu im Wesentlichen drei Klassen von Authentifizierungsverfahren unterschieden [82]:

- Authentifizierung auf Basis spezifischen Wissens (zum Beispiel Passwort)
- Authentifizierung auf Basis individuellen Besitzes (zum Beispiel Chipkarte)
- Authentifizierung auf Basis biometrischer Merkmale (zum Beispiel Stimme)

Passwörter können bei asymmetrischen Kryptosystemen durch eine *PKI* [85] oder bei symmetrischen durch ein *Key Distribution Center (KDC)* [27] verteilt werden. Als PKI für Fahrzeugleitsysteme, die nach dem C-V2X-Prinzip kommunizieren, wurden für die Europäische Union (EU) das *Cooperative ITS Point of Contact (CPOC)*-Protokoll [68] und für die USA das *Security Credential Management System (SCMS)* [179] entwickelt.

Individueller Besitz kann durch besonders gesicherte Hardware (Secure Element [SE]) wie etwa einem Trusted Platform Module (TPM) oder einem Hardware-Sicherheitsmodul (HSM) [76] nachgewiesen werden. Eine Vereinheitlichung derartiger Module und deren Schnittstellen zu Geräten des IoT soll die Smart Secure Platform (SSP) des ETSI schaffen [67]. Biometrische Merkmale sind bei rein maschinellen Teilnehmern nicht verwendbar, jedoch ist eine attributbasierte Authentifizierung denkbar, beispielsweise anhand der Position im Netz [29]. Zur Verwendung humaner biometrischer Merkmale in Fahrzeugleitsystemen ist zwischen Fahrer- und Fahrzeugauthentifizierung zu differenzieren [105].

Mit Lightweight Authentication for Secure Automotive Networks (LASAN) [136] wird ein Protokoll speziell zur sicheren Authentifizierung und Autorisierung in Fahrzeugnetzen vorgestellt, das die spezifischen Anforderungen in jeder Phase des Produktlebenszyklus berücksichtigt. Konzeptionell kann LASAN damit einen vielversprechenden Bestandteil von Fahrzeugleitsystemen bilden, der auch in der vorliegenden Arbeit aufgegriffen wird. Zentrale Prozesse wie der Schlüsselaustausch werden in LASAN jedoch mit asymmetrischer Kryptografie gesichert, die, wie bereits ausgeführt wurde, mit ausreichend Rechenleistung gebrochen werden kann. Vor einem Einsatz in Fahrzeugnetzen müssen daher alle Prozesse mit nachweislich sicheren Verfahren versehen werden, um den Anforderungen an die kryptografische Sicherheit gerecht zu werden.

3.4.3 Bedrohungen für die IKT-Sicherheit und deren Abwehr

Die Sicherheit von IoT-Anwendungen ist ein weites Forschungsfeld und reicht von Penetrationstests mit frei verfügbaren Suchmaschinen [164] bis hin zu großangelegten *Denial of Service (DoS)*-Angriffen auf vernetzte Verkehrssysteme [171]. Von den zahlreichen Angriffsszenarien, die für Verkehrssysteme eine Rolle spielen [121], soll hier die Problematik der langfristigen Verwendung herkömmlicher Verschlüsselungsverfahren dargestellt werden.

Data Encryption Standard (DES) galt trotz der auf 56 bit limitierten Schlüssellänge geraume Zeit lang als Stand der Technik in der symmetrischen Kryptografie. Schon wenige Jahre nach Einführung galt er aber als gebrochen und wird seitdem vor allem aufgrund der kurzen Schlüssellänge als unsicher erachtet [58]. Anstatt DES durch ein nachweislich sichereres Verfahren zu ersetzen, wurde der Algorithmus behelfsmäßig nachgebessert (*Triple DES*) und wird in dieser Form weiterhin für sicherheitskritische Anwendungen verwendet [113].

Wireless Local Area Network (WLAN) zeigt, dass sich die im ursprünglichen Standard implementierten Maßnahmen zur Übertragungssicherheit im Laufe der Zeit als unsicher herausgestellt haben und nachgebessert werden mussten. So kann der gemäß IEEE 802.11-Standard im ursprünglichen WEP-Verschlüsselungsprotokoll verwendete RC4-Algorithmus zur Erzeugung von Pseudozufallszahlen mittlerweile in kurzer Zeit gebrochen werden [71]. Die Erweiterung IEEE 802.11i ermöglicht zwar die Kommunikation mit einer aktuell als sicher eingestuften AES-Verschlüsselung, kann aber auch nur als übergangsweise Nachbesserung dienen.

Überlastungsangriffe stellen eine besondere Gefahr für Ad-hoc-Netze dar. Diese sind aufgrund der fehlenden Kontrollinstanz anfällig für solche Angriffe und können nur durch aufwändige und komplexe Verfahren ausreichend gegen dadurch ausgelösten DoS gesichert werden [185].

AES kann nach heutigen Maßstäben als sicher angesehen werden. Dennoch ist der Schluss naheliegend, dass durch die Limitierung der Schlüssellänge bei AES auf 256 bit die für DES dokumentierten Probleme nicht konzeptuell beseitigt, sondern nur in die Zukunft verschoben wurden.

Nicht zuletzt spielen auch Bedienungsfehler bei der Anwendung von Verschlüsselungsverfahren eine Rolle, die wie folgt unterschieden werden [4]:

- Eine Klartext-Klartext-Kompromittierung (engl. *depth*) liegt vor, wenn zwei verschiedene Klartexte mit demselben Schlüssel verschlüsselt und übertragen werden.
- Eine Klartext-Geheimtext-Kompromittierung (engl. *crib*) liegt vor, wenn die verschlüsselte Nachricht (oder Teile davon) nochmal in unverschlüsselter Form übertragen wird.
- Eine Geheimtext-Geheimtext-Kompromittierung (engl. *kiss*) liegt vor, wenn der gleiche Klartext mit verschiedenen Schlüsseln verschlüsselt und übertragen wird.

Die in Fahrzeugleitsystemen versandten Nachrichten sind durch bekannten Aufbau und hohe Wiederholungsfrequenz bei oft nahezu identischem Inhalt gekennzeichnet. Symmetrische Verschlüsselungen sind daher prinzipbedingt auch bei korrekter Anwendung diesen Kompromittierungsansätzen ausgesetzt.

In Anwendungen des IoT wie Fahrzeugleitsystemen, deren Komponenten auf lange Wartungsintervalle und Lebensdauern von teilweise mehreren Jahrzehnten hin ausgelegt sind, dürfen nur langfristig perfekt sichere kryptografische Verfahren [158] zum Einsatz kommen. Ein solches Verfahren erfüllt inhärent alle gängigen Vorgaben an die IKT-Sicherheit im IoT [66] und genügt bei korrekter Implementierung auch den einschlägigen, gültigen Standards [45, 54]. Zudem ist die Fähigkeit zur Skalierung langfristig gegeben, wenn eine zentrale Instanz zur Schlüsselerzeugung und -verteilung beteiligt ist.

Kryptografie und Datenschutz Kryptografische Maßnahmen dienen stets auch dem Schutz personenbezogener oder -beziehbarer Daten. Da Nachrichten dennoch eindeutig zugestellt werden müssen, ist lediglich eine Pseudonymisierung denkbar [114]. Die Schwierigkeit besteht darin, wahre Identitäten nur bei konkretem Bedarf wie beim Vorgang der Authentifizierung aufzudecken [162] und gleichzeitig die Erreichbarkeit der Teilnehmer sicherzustellen.

3.5 Zwischenfazit

In diesem Kapitel wurde der Stand der Technik in Bezug auf die an Fahrzeugleitsysteme gestellten Anforderungen erörtert. Damit können in einem Zwischenfazit die Forschungslücke und das weitere Entwicklungsziel spezifiziert werden.

3.5.1 Forschungslücke

Die Literaturrecherche ergibt, dass Erforschung und Entwicklung von Fahrzeugleitsystemen ein etabliertes Forschungsfeld ist. Jedoch zeigt sich, dass bisherige Ansätze für die Vernetzung nahezu ausnahmslos dezentrale Konzepte favorisieren und die IKT-Sicherheit auf asymmetrischer Kryptografie basiert. Das Sicherheitsniveau der Verschlüsselung wird dann an der Länge der Schlüssel festgemacht. Mit zunehmender Mächtigkeit von Angreifern wird die Schlüssellänge lediglich *reaktiv* erhöht, anstatt *proaktiv* angemessene kryptografische Verfahren einzusetzen. Hinsichtlich des Zeitverhaltens besteht in dezentral verwalteten Netzen das Problem der Unvorhersehbarkeit der Übertragungsdauern, was echtzeitfähige Nachrichtenübertragungen unmöglich macht.

Bei oberflächlicher Betrachtung gibt es zwar Gründe, die für eine solche Kombination von Techniken sprechen. Ein konsequenter Vergleich mit den in Kapitel 2 erarbeiteten Anforderungen an Fahrzeugleitsysteme zeigt jedoch, dass essentielle Anforderungen mit bestehenden Techniken nicht oder nur unzureichend erfüllt sind. Dies führt zur Notwendigkeit, ein auf perfekt sicherer Verschlüsselung und echtzeitfähiger Mobilfunkkommunikation basierendes Fahrzeugleitsystem zu entwickeln, da ein solches Fahrzeugleitsystem bislang nicht existiert.

3.5.2 Entwicklungsziel

Der Stand der Technik offenbart zahlreiche Mängel hinsichtlich sicherer und echtzeitfähiger Datenübertragung zwischen Fahrzeugen. Die Ziele der weiteren Entwicklung eines Fahrzeugleitsystems leiten sich aus folgenden Feststellungen ab:

- Asymmetrische Kryptosysteme sind konzeptuell unsicher und anfällig für verbreitete Angriffe.
- Aktuell als sicher geltende, symmetrische Kryptosysteme können die hohen IKT-Sicherheitsanforderungen in Fahrzeugleitsystemen nicht dauerhaft erfüllen.
- Die Nachrüstung von Sicherheitsmerkmalen steigert die Komplexität und macht existierende Systeme schwer bedien- und wartbar.
- Fahrzeugnetze nach dem Ad-hoc-Prinzip sind trotz vereinzelter Lösungsansätze komplex und nicht echtzeitfähig.
- Eine Dezentrale Nutzerverwaltung ist komplex und erschwert die Skalierung.

Das übergeordnete Entwicklungsziel ist folglich eine einheitliche Kommunikationsarchitektur, die perfekte Sicherheit bei allen zum Nachrichtenaustausch notwendigen Vorgängen bietet. Die kryptografischen Verfahren müssen robust gegen bekannte und zukünftige Angriffe sein, um eine dauerhafte Unabhängigkeit von Nachbesserungen der Verschlüsselungsverfahren zu gewährleisten. Gleichzeitig muss die Kommunikationsarchitektur auf beliebige Flottengrößen skalierbar sein, ohne dabei Kompromisse hinsichtlich Echtzeitfähigkeit, Sicherheit und Verfügbarkeit einzugehen.

Es ist bemerkenswert, dass eine solche Architektur noch nicht existiert, da Abwehrmaßnahmen gegen alle bekannten Angriffsvektoren auf die IKT-Sicherheit grundsätzlich bekannt sind [82] und es somit nicht an der Verfügbarkeit sicherer Methoden mangelt. Verwundbarkeiten ergeben sich auch häufig aus nachlässiger Implementierung, die wiederum

eine Folge steigender Komplexität durch improvisiert nachgerüstete Sicherheitsmerkmale ist. Die weitere Entwicklung einer Kommunikationsarchitektur muss sich folglich auf die korrekte, sichere und dennoch handhabbare Zusammenführung bewährter Methoden fokussieren, um so den Anforderungen an Fahrzeugleitsysteme gerecht zu werden.

4 Die Sichere Kommunikationsarchitektur für Fahrzeugleitsysteme SIKAF

In diesem Kapitel wird die Sichere Kommunikationsarchitektur für Fahrzeugleitsysteme (SIKAF) vorgestellt, welche die in Kapitel 2 definierten Anforderungen an ein Fahrzeugleitsystem erfüllt und die in Kapitel 3 identifizierte Forschungslücke schließt.

Die wesentlichen Bestandteile von SIKAF sind eine hoheitliche Behörde zur Verwaltung und Verteilung aller kryptologischen Ressourcen, ein dediziertes Kommunikationsnetz zur echtzeitfähigen Datenvermittlung sowie Fahrzeuge, deren Fahrverhalten durch SIKAF geregelt und optimiert wird. Eine Übersicht dieser Akteure und deren Zusammenwirken ist in Abbildung 4.1 dargestellt. Man beachte die nur teilweise Integration der Fahrzeuge, da SIKAF die zur Kommunikation notwendigen Aufgaben abdeckt. Fahrzeuge werden hierzu zwar mit benötigten Komponenten wie einer Datenbank und einem Kommunikationsmodul ausgerüstet. Bordeigene Sensoren und Aktoren werden jedoch weiterhin von Fahrzeugherstellern bereitgestellt und können über eine Schnittstelle von SIKAF ausgelesen und angesteuert werden. Der Netzabschluss von SIKAF befindet sich an Bord der Fahrzeuge. Die Übertragung über das dedizierte Kommunikationsnetz findet mittels eines Relais statt, das die Vermittlungsstelle zwischen Sender und Empfänger einer Nachricht bildet. Damit ist SIKAF modular aufgebaut und lässt sich bei Bedarf weiter in unterschiedliche Fachschalen unterteilen.

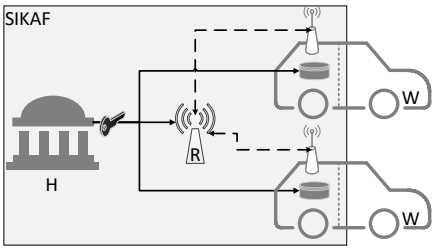


Abbildung 4.1: Interaktion der beteiligten Akteure in SIKAF: Masken verteilende Behörde (H), Relais (R) und Fahrzeuge (W)

4.1 Organisatorische Struktur

Die einzelnen Bestandteile von SIKAF werden organisatorisch jeweils einer Ebene zugeordnet, um sie damit in bestehende Strukturen einzugliedern. Abbildung 4.2 zeigt die

Einordnung von SIKAF in die Automatisierungspyramide sowie in das Referenzarchitekturmodell Industrie 4.0 (RAMI 4.0). Dadurch wird ein Bruch mit bewährten Strukturen vermieden und SIKAF leistet für den Verkehrsbereich die Übertragung der traditionellen Automatisierungspyramide auf das Internet der Dinge.

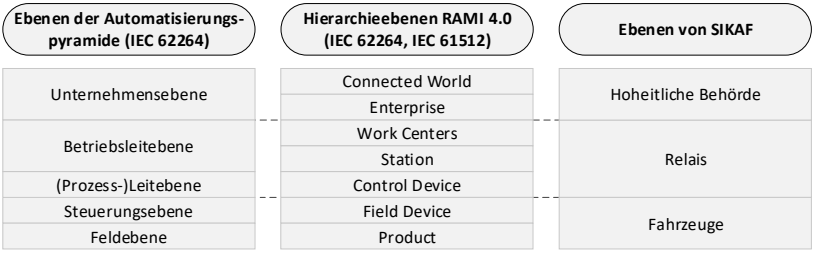


Abbildung 4.2: Organisatorische Unterteilung von SIKAF

Der Ebene der hoheitlichen Behörde werden alle Aufgaben zugeordnet, für die eine zentrale Verwaltung notwendig ist. Hierzu zählen kryptografische Funktionen sowie Zuteilung von Identifikatoren zu Fahrzeugen und Haltern. Eine solche Behörde kann hoheitliche Aufgaben wie Registrierung von Fahrzeugen und Verknüpfung mit Haltern bereits durchführen. Der Ebene des Relais werden in SIKAF alle Aufgaben der Nachrichtenvermittlung zugeordnet. Die Kommunikationen zwischen Fahrzeugen werden in SIKAF über ein dediziertes Netz abgewickelt, das aus zwei drahtlosen und einer kabelgebundenen Strecke besteht. Der Ebene der Fahrzeuge werden in SIKAF die in der physischen Welt interagierenden Fahrzeuge zugeordnet. Fahrzeuge und alle Fahrzeugtechnik, einschließlich bordeigener Sensoren und Aktoren, entsprechen der Feldebene und werden weiterhin von Automobilherstellern geliefert. SIKAF stellt jedoch einheitliche Schnittstellen bereit, um Daten von Sensoren übernehmen und Aktoren ansteuern zu können.

4.1.1 Hoheitliche Behörde

Die durch SIKAF vernetzten Fahrzeuge besitzen beim ersten Kontakt im Allgemeinen keinerlei Informationen über einen Kommunikationspartner. Identifikatoren sowie Masken zur symmetrischen Kryptografie müssen daher von einer dritten Partei verwaltet und bereitgestellt werden. Diese Institution muss

- vertrauenswürdig sein, da sie die Masken kennt,
- leistungsfähig sein, da Masken in großer Anzahl und in kurzen Zeiträumen erzeugt werden müssen, und
- einen sicheren Kanal zu allen Teilnehmern aufbauen können, um Masken und Identifikatoren zu verteilen.

Beim Einsatz von SIKAF wird diese Institution bei einer hoheitlichen Behörde angegliedert, die bereits Fahrzeuge in der physischen Welt identifiziert und verwaltet. Diese bestehenden

Funktionen werden um die Verwaltung digitaler Identitäten und das Ausstellen kryptografischer Masken erweitert. Die hoheitliche Behörde verfügt über nachgeordnete Stellen, welche regelmäßig von Fahrzeugen kontaktiert werden müssen (beispielsweise zur technischen Inspektion). Über diese nachgeordneten Stellen kann ein sicherer Kanal zu den Fahrzeugen für die Maskenverteilung und den Maskennachschub hergestellt werden. Als hoheitlicher Aufgabenträger ist die hoheitliche Behörde zudem autorisiert, die Rechte der Fahrzeuge im physischen Verkehrssystem zugunsten einer globalen Optimierung zu erweitern oder zu limitieren. Die Vertrauenswürdigkeit ist durch eine demokratische Legitimation gegeben.

4.1.2 Betreiber von Mobilfunkkommunikation

Die Datenübertragung wird in SIKAF über ein dediziertes Mobilfunknetz abgewickelt. Die Gesamtheit der zur Nachrichtenvermittlung benötigten Kommunikationsinfrastruktur wird als *Relais* bezeichnet. Das Relais besteht aus

- Funkmasten als Zugangspunkte für die Kommunikationsteilnehmer,
- Verbindungen zwischen den Funkmasten, welche die Nachrichten zuverlässig und rechtzeitig weiterleiten, und
- dem Zentralrechner für Maskierungs- und Vermittlungsaufgaben.

Das Relais ist mit einem dedizierten, abhör- und manipulationssicheren Kommunikationsnetz ausgestattet, sodass die Nachrichtenübertragung in diesem Netz echtzeitfähig abgewickelt werden kann. Es besteht zudem permanent ein sicherer Kanal zur hoheitlichen Behörde, über welchen alle benötigten kryptografischen Informationen ausgetauscht und von der Behörde nachgefordert werden können. Das Relais ist zur Maskenverwaltung mit manipulationssicheren Komponenten ausgestattet.

4.1.3 Fahrzeuge

Fahrzeuge bilden die Quellen und Senken aller Kommunikationen in SIKAF. Als Aktoren des Verkehrssystems mit zahlreichen mechanischen Komponenten sind sie dauerndem Verschleiß ausgesetzt. Deshalb ist die Durchführung regelmäßiger Inspektionen notwendig und vorgeschrieben, für die die Fahrzeuge in physischen Kontakt mit der hoheitlichen Behörde oder einer ihrer nachgeordneten Stellen treten müssen. Diese Inspektionen werden neben der Überprüfung der Hardware der Fahrzeuge genutzt, um Software und Daten wie die kryptografischen Masken zu aktualisieren.

4.2 Technischer Aufbau

Die drei vorgestellten Einheiten werden unter Beachtung der organisatorischen Unterteilung kommunikationstechnisch miteinander verbunden. Abbildung 4.3 zeigt schematisch die Struktur von SIKAF für die Nachrichtenübertragung zwischen zwei Fahrzeugen w_1 und w_2 über das Relais R. Eine hoheitliche Behörde veranlasst Maskenerzeugung und -verteilung an die Fahrzeuge und das Relais. Die Fahrzeuge kommunizieren nicht direkt miteinander, sondern stets über das Relais als Zwischenstation. Eine zu übertragende Nachricht wird vom sendenden Fahrzeug maskiert und zum Relais übertragen. Dort wird die

Nachricht demaskiert, für die Übertragung zum empfangenden Fahrzeug erneut maskiert und zu dem Funkmast vermittelt, der dem Empfänger am nächsten ist. Von dort wird die Nachricht zum Empfängerfahrzeug übertragen. Die Nachrichtenübertragung zwischen Fahrzeugen wird somit stets über insgesamt zwei Funkstrecken und eine kabelgebundene Übertragungsstrecke abgewickelt.

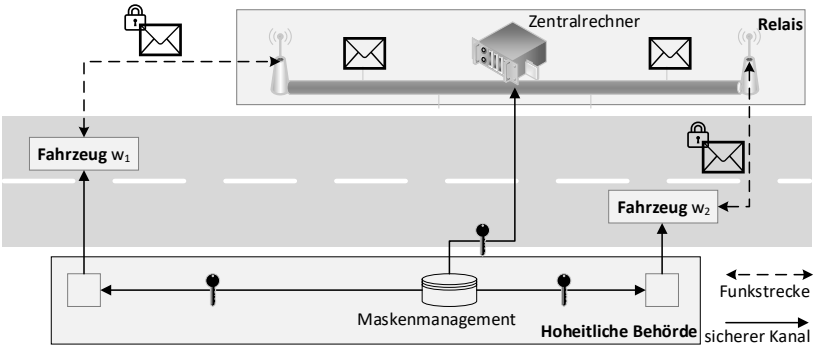


Abbildung 4.3: Schematische Struktur von SIKAF

4.2.1 Zentral ausgerichtete Architektur

SIKAF ist eine zentral ausgerichtete Architektur, um die Anforderungen an ein Fahrzeugleitsystem erfüllen zu können. Zum einen ist damit die Echtzeitfähigkeit der Nachrichtenübertragung gewährleistet: Die Übertragungsdauern sind vorhersehbar, da aus den Positionen der Fahrzeuge und den Positionen der Funkmasten die Längen der beiden Funkstrecken bestimmt werden können. Die relaisinternen Vermittlungs- und Verarbeitungsdauern können als bekannt angenommen werden, da es sich beim Relais um ein geschlossenes System mit bekannten Kabellängen und deterministischem Zeitverhalten der Digitalrechner handelt.

Zum anderen wird das Fahrzeugleitsystem damit zu einer globalen Optimierung des Verkehrssystems befähigt: Es kennt die Positionen und Ziele der beteiligten Fahrzeuge und kann sie optimal durch das Verkehrssystem leiten. Es agiert somit als Regler, der aus Regelgröße (aktueller Zustand des Verkehrssystems) und Führungsgröße (optimaler Zustand des Verkehrssystems) die notwendige Stellgröße (Fahrzeugtrajektorien) bestimmt und an die Fahrzeuge übermittelt.

4.2.2 Identifizierung und Authentifizierung der Teilnehmer

Die hoheitliche Behörde weist allen Teilnehmern eine eindeutige dID zu. Die dID kann auf bestehenden Identifikationsmerkmalen wie dem zugeteilten Kfz-Kennzeichen basieren und wird über einen sicheren Kanal einmalig zu jedem Fahrzeug übertragen. Der sichere Kanal besteht hier entweder zum Zeitpunkt der Montage im Werk oder bei einer der vorgeschriebenen Wartungen. Bei der Zuweisung der dID wird über denselben Kanal zugleich

ein initialer Satz an kryptografischen Masken zum Fahrzeug übertragen. Eine unzulässige Aneignung fremder Identitäten ist nicht möglich, da die Masken individuell für jedes Fahrzeug erstellt sind. Bei der Kommunikation authentisiert sich jedes Fahrzeug durch Vorweisen einer individuell erstellten Maske.

4.2.3 Anbindung des Relais

Das Relais R bildet die Vermittlungsstelle zwischen zwei Fahrzeugen w_i und w_{i+1}. Jede Nachrichtenübertragung zwischen zwei Fahrzeugen wird über das Relais gemäß $w_i \rightarrow R \rightarrow w_{i+1}$ abgewickelt. Funkmasten, die entlang der Verkehrsinfrastruktur errichtet sind, bilden die Zugangspunkte zum Relais. Die Funkmasten sind über ein dediziertes Netz, das echtzeitfähige Nachrichtenübertragung ermöglicht, untereinander und mit einem Zentralrechner verbunden. Das relaisinterne Netz verfügt gleichzeitig über einen sicheren Kanal zur hoheitlichen Behörde, um Maskenverteilung und Maskennachschub für das Relais sicherzustellen.

4.2.4 Informationsverwaltung in den Fahrzeugen

Jedes Fahrzeug ist mit einem Festwertspeicher versehen, der zur Aufnahme aller übermittelten Daten ausgelegt ist. In SIKAF sind alle Speicherbereiche grundsätzlich in solche für Daten und solche für Befehle getrennt. Eine Aktualisierung des Festwertspeichers kann nur durch autorisierte Stellen unter Beachtung eines festgelegten Rechte- und Rollenmodells durchgeführt werden. Autorisierten Stellen wird dann temporär eine entsprechende Berechtigung zum Passieren des Manipulationsschutzes gewährt.

Identifikator Die dID wird manipulationssicher im Festwertspeicher hinterlegt. Manipulationen an diesem Eintrag werden erkannt und schließen das Fahrzeug von der Kommunikationsarchitektur aus. Technisch wird hierzu eine Meldung an das Relais übertragen, die die Sperrung aller Masken des betroffenen Fahrzeugs bewirkt.

Adressen Die dID wird verwendet, um das Fahrzeug in SIKAF mit einer eindeutigen Adresse zu versehen und auf dieser Grundlage Daten an avisierte Empfänger zu übertragen. Im Festwertspeicher der Fahrzeuge werden die Adressen möglicher Empfänger hinterlegt. Die Aktualisierung dieser Liste kann mit demselben Prozess wie die Aktualisierung der kryptografischen Masken durchgeführt werden.

Die dID und die Adresse können auch identisch sein.

Positionen Im Fahrzeug sind die Positionen der Funkmasten hinterlegt, damit aus deren Position und der Position des Fahrzeugs die Übertragungsstrecke bestimmt werden kann. Zusammen mit weiteren Parametern kann damit die Dauer zur Nachrichtenübertragung berechnet werden. Die Dauer ist folglich vorhersehbar und der Sender kann entscheiden, ob diese Dauer für den jeweiligen Anwendungsfall ausreichend ist. Diese Vorhersehbarkeit macht den Übertragungsprozess echtzeitfähig.

Informationsfusion Die permanente Positionserfassung ermöglicht die Verortung statischer und dynamischer Objekte, die ein Hindernis für andere Fahrzeuge darstellen könnten. Es wird eine komplementäre Fusion eingesetzt, da eine Fehldetektion nicht vernetzter Objekte als Sicherheitsziel mit dem höchsten ASIL identifiziert wurde. Bei der Informationsfusion werden Sensoren aller an SIKAF beteiligten Fahrzeuge und im Verkehrsraum montierte Sensoren berücksichtigt.

4.3 Übertragungsprotokolle

Auf der Anwendungsschicht wird in SIKAF ein optimiertes Übertragungsprotokoll eingesetzt, SIKAF-P genannt. Abbildung 4.4 zeigt den mit SIKAF-P entstehenden Protokollstapel im Vergleich zum OSI-Modell. Durch dieses Konzept kann auf den unteren Schichten des Protokollstapels auf erprobte Übertragungsprotokolle wie IEEE 802.11, 4G und 5G oder eine mögliche künftige Entwicklung zurückgegriffen werden. Bei der Verwendung von SIKAF-P gilt die Direktive, dass jedes Datagramm (auch Paket genannt) eine vollständige Information in Form einer Nachricht transportiert. Die Aufteilung einer Nachricht in mehrere Datagramme, deren Übertragung und anschließende Rekonstruktion am Zielort vermeidet SIKAF-P. Ein solches Vorgehen würde aufwändige Mechanismen zur korrekten Übertragungs- und Sequenzkontrolle notwendig machen. Overhead, Übertragungszeit und Fehlerquellen können dadurch minimiert werden.

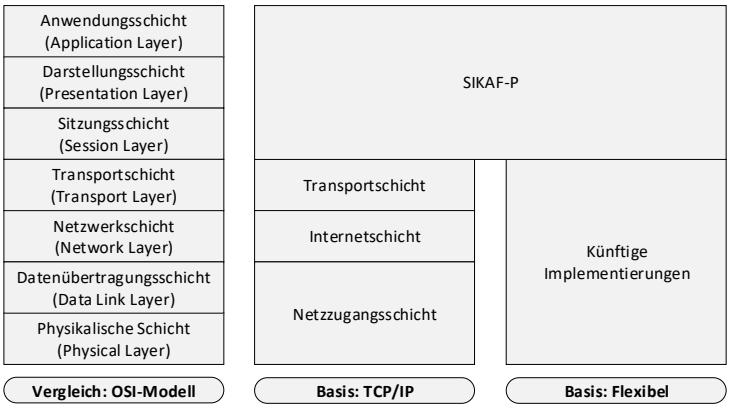


Abbildung 4.4: Protokollstapel von SIKAF

Ein wichtiges Entwurfsmerkmal zur Implementierung der Maskierung ist die Reservierung eines Bereichs im Header des Datagramms für den Maskenanzeiger. Damit wird dem Empfänger einer Nachricht mitgeteilt, welche Maske verwendet wurde, damit zur Demaskierung die passende Maske angewendet werden kann. Die Maskierung dient gleichzeitig der Authentifizierung des Senders gegenüber dem Relais, da nur bei berechtigtem Sender Maske und Maskenanzeiger so zusammenpassen, dass die Nachricht vom Relais sinnhaft demaskiert werden kann. Empfängt das Relais hingegen eine Nachricht, die sich mit der

angezeigten Maske nicht sinnhaft demaskieren lässt, so kann auf einen Übertragungsfehler oder eine beabsichtigte Störung geschlossen werden. Das Relais kann die Nachricht entsprechend als kompromittiert klassifizieren und kennzeichnen oder umgehend verwerfen.

4.3.1 SIKAF-P (OSI-Schichten 5 bis 7)

Die Funktionen Authentifizierung und Autorisierung werden ab der Sitzungsschicht des OSI-Modells durchgeführt, weshalb SIKAF-P als Protokoll für die Kommunikationen ab OSI-Schicht 5 benötigt wird. SIKAF-P ist durch folgende Eigenschaften bestimmt:

- Ein Datenpaket umfasst die zu übertragende Nachricht vollständig, sodass keine Sequenzkontrolle notwendig ist.
- Jedes Datenpaket enthält Felder für den Maskenanzeiger.
- Jedes Datenpaket enthält die Adresse des Senders, ein spezifischer Empfänger wird nur bei Bedarf angegeben.
- Jedes Datenpaket umfasst eine feste Datenmenge.
- SIKAF-P kann im Einzel- oder im Intervallmodus betrieben werden:
  - Im Einzelmodus wird eine Nachricht erneut gesendet, wenn nach einer festgelegten Zeitspanne keine Empfangsbestätigung vorliegt. Diese Zeitspanne ist frei wählbar und wird von SIKAF situationsbezogen festgelegt.
  - Im Intervallmodus werden Datenpakete mit einer einstellbaren Frequenz gesendet.
- Das Relais hält eine statische Routingtabelle für alle möglichen Relationen zwischen den beteiligten Sendern und Empfängern vor.
- Es müssen keine Maßnahmen zur Transportkontrolle implementiert werden, mit Ausnahme einer optionalen Empfangsbestätigung durch das empfangende Fahrzeug.

Senke der übertragenen Nachrichten ist die Bordelektronik des empfangenden Fahrzeugs. Von dort werden die in den Nachrichten enthaltenen Steuermeldungen über Schnittstellen zu den Fahrzeugaktoren weitergeleitet. Die zur unmittelbaren Steuerung der Fahrzeuge notwendigen Komponenten wie beispielsweise die Controller für Beschleunigungs-, Lenk- und Bremsvorgänge sind damit nicht Bestandteil von SIKAF, sondern werden vom jeweiligen Fahrzeughersteller integriert. Die fahrzeugseitige Anpassung notwendiger Schnittstellen an SIKAF sowie die Gewährleistung der funktionalen Sicherheit aller Aktoren liegt somit in dessen Verantwortung.

4.3.2 Vermittlung und Transport (OSI-Schichten 3 und 4)

Für Vermittlung und Transport der Datenpakete können in SIKAF zwei Möglichkeiten verwendet werden. Wird SIKAF als Overlay-Netz realisiert, beispielsweise auf einem TCP/IP-Protokollstapel, so kann zur Nachrichtenweiterleitung auch die Adresse des darunterliegenden Netzes („Basisnetz“) verwendet werden. In diesem Fall wird beim Relais eine Verknüpfung zwischen der SIKAF-P-Adresse und der Adresse des Basisnetzes hergestellt und in

Form von Umsetzungstabellen verwaltet. Dadurch ist es möglich, Datenpakete auf den unteren Schichten des Protokollstapels unter Verwendung der Identifizierung des Basisnetzes zu routen. Auf den höheren Schichten werden die Nachrichten durch Verwendung der SIKAF-P-Adresse weitergeleitet.

Wird für SIKAF ein speziell entwickelter Protokollstapel für die OSI-Schichten 1 bis 4 verwendet, so können SIKAF-spezifische Adressen verwendet werden. Je nach konkreter Ausgestaltung der darunterliegenden Schichten muss die SIKAF-P-Adresse noch in die jeweilige Hardwareadresse des genutzten Protokollstapels umgesetzt werden, um korrekt zu vermitteln.

4.3.3 Netzzugang (OSI-Schichten 1 und 2)

Wird auf dem TCP/IP-Modell aufgesetzt, so kann SIKAF ein autonomes System im Sinne des Request for Comments (RFC) 4271 bilden. Wie in Kapitel 3 gezeigt wurde, ist Kommunikation gemäß TCP/IP zwar grundsätzlich nicht echtzeitfähig. Durch geeignete Anpassungen kann dies durch SIKAF-P auf der Anwendungsschicht jedoch kompensiert werden, beispielsweise durch Protokollerweiterungen mit entsprechender Transportkontrolle oder Nutzung reservierter Bereiche in 5G.

Problematische Paketverluste können in SIKAF an zwei Stellen auftreten: Auf der Luftschnittstelle durch natürliche oder mutwillige Störung im genutzten Frequenzband und am Funkmast durch Auftreten der Hidden-Terminal-Problematik. Störungen auf der Luftschnittstelle wird mit permanentem Kanalmonitoring durch SIKAF begegnet. Die Hidden-Terminal-Problematik kann einerseits durch ausreichend Kapazität und Verarbeitungsgeschwindigkeit auf Seiten der Funkmasten verhindert oder durch Einsatz von Datenflusssteuerung (*Ready For Receiving [RFR]*/*Clear To Send [CTS]*) koordiniert und dadurch zumindest deterministisch gestaltet werden. Hierzu deaktiviert das Relais die RFR-Leitung und signalisiert damit den Fahrzeugen, dass derzeit keine Daten entgegengenommen werden können. Sind wieder Kapazitäten vorhanden, so wird dies durch Aktivierung der CTS-Leitung signalisiert. Auf Seiten der Fahrzeuge wird ebenso verfahren. Die Hidden-Terminal-Problematik besteht in diesem Fall nicht, da Fahrzeuge ohnehin nur von einer Gegenstelle Signale erwarten, nämlich dem nächstgelegenen Funkmast.

Werden Verfahren verfügbar, welche die Anforderungen an die Datenübertragung besser als IEEE 802.11 oder 5G erfüllen, so sind die Übertragungsmethoden auf den OSI-Schichten 1 bis 4 in SIKAF-P austauschbar. Die weiteren Konzepte, darunter die kryptografischen Maßnahmen, werden stets nach dem vorgesehenen Verfahren umgesetzt.

4.4 Nachrichten

Als Nachrichten werden die Dateneinheiten bezeichnet, mit denen Informationen zwischen Fahrzeugen oder zwischen Fahrzeugen und der Infrastruktur ausgetauscht werden. Die ausgetauschten Nachrichten enthalten Informationen, die zur Steuerung und Regelung der Fahrzeuge benötigt werden. Mit den Nachrichten werden die Stellgrößen vom Fahrzeugleitsystem an die Fahrzeuge übermittelt.

Durch lokale Regelungen werden die Wechselwirkungen von Fahrzeugen kontrolliert, die aktuell in der physischen Welt interagieren. In diesem Fall ist vorzugsweise nur ein Funkmast einschließlich Relais beteiligt. Durch eine globale Regelung wird eine Optimierung des

Verkehrssystems erreicht, indem die zur Optimierung vorgesehenen Fahrzeugtrajektorien von SIKAF berechnet und übertragen werden.

4.4.1 Nachrichtenstruktur

Jedes SIKAF-P-Paket umfasst 1460 Byte (B), da diese Datenmenge dem Nutzdatenteil eines TCP/IP-Pakets entspricht[1] und damit die Kompatibilität zu TCP/IP gegeben ist. Jeder von SIKAF verwendete Nachrichtentyp benötigt nur ein einziges Paket. SIKAF kann mit spezifischen Netzzugangsprotokollen oder als Overlay-Netz genutzt werden. Die verwendete Nachrichtenstruktur ist in Abbildung 4.5 dargestellt.

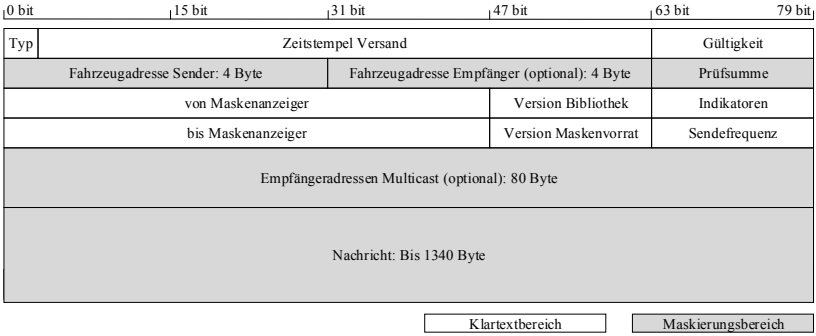


Abbildung 4.5: Nachrichtenstruktur von SIKAF

Adressen Eine SIKAF-Adresse zur eindeutigen Kennzeichnung eines Fahrzeugs besteht aus 4 B (32 bit). Damit stehen $2^{32} = 4\,294\,967\,296$ verschiedene Adressen für Fahrzeuge zur Verfügung. Sowohl die Sender- als auch die Empfängeradresse können maskiert werden.

Für einen Broadcast können in einer Nachricht bis zu 21 Empfänger (80 B „Empfängeradressen Multicast“ plus 4 B „Fahrzeugadresse Empfänger“) angegeben werden.

Maskenanzeiger Der Empfänger muss die vom Sender verwendete Maske kennen, um eine empfangene Nachricht zu demaskieren. Masken werden grundsätzlich nicht über denselben Kanal wie Nachrichten übertragen, da dieser unsicher ist. Über den unsicheren Nachrichtenkanal wird vielmehr lediglich der Maskenanzeiger übertragen, damit der Empfänger die korrekte Maske aus seinem Vorrat auswählen kann.

Indikatoren In SIKAF werden vor jeden Nachrichteninhalt ein Meldungs- und ein Maskierungsindikator in Form einer booleschen Variable gesetzt. Der Meldungsindikator gibt an, ob der folgende Nachrichteninhalt mit Daten befüllt ist. Der Maskierungsindikator gibt an, ob der folgende Nachrichteninhalt maskiert ist oder ob die Daten im Klartext vorliegen.

[1] 1500 B Ethernet-Nutzdaten − 20 B TCP-Header − 20 B IP-Header

Zeitstempel Die Einhaltung von Zeitbedingungen zu garantieren, ist eine wichtige Anforderung an SIKAF. In einer Nachricht sind daher 60 bit zur Darstellung von Zeitstempeln vorgesehen. Weitere 2 B sind für die Anzeige der Gültigkeit und damit der spätestmöglichen Zustellung reserviert. Damit kann bei jedem Empfang entschieden werden, ob die Nachricht rechtzeitig vorliegt.

Versionierung Die verwendeten Masken und die verwendete Sprachdefinition (Bibliothek) werden bei Bedarf aktualisiert. In jeweils 2 B des Nachrichtenheaders wird die aktuell verwendete Version übertragen, um Missverständnisse zwischen Fahrzeug und Relais zu vermeiden.

Sendefrequenz Die Sendefrequenz gibt an, mit welcher Rate Nachrichten erzeugt und versandt werden. Sie stellt eine wesentliche Einflussgröße auf die benötigte Maskengröße dar. Die Sendefrequenz ist nicht mit der Trägerfrequenz zu verwechseln.

Nutzdaten Die verbleibenden 1340 B jedes SIKAF-Pakets werden für die Nutzdaten des Fahrzeugleitsystems verwendet. Dieser Nachrichtenteil wird in einer speziell entworfenen Sprache abgefasst. Über die gesamte Nachricht wird eine auf 2 B limitierte Prüfsumme gebildet.

Die vorgestellte Nachrichtenstruktur ist als Maximalfall zu betrachten. Durch Spezifizierungen für den konkreten Anwendungsfall kann die Datengröße der einzelnen Inhalte weiter reduziert werden.

4.4.2 Klassifizierung der Nachrichten

Zur effizienten Übertragung werden die Nachrichten nach verschiedenen Aspekten klassifiziert. Auf dieser Grundlage können einerseits die zu übertragende Datenmenge und andererseits die Verarbeitungsdauer reduziert werden. Dies geht mit einer Reduzierung der benötigten Maskengröße einher.

Schutzklasse der Information Die ausgetauschten Nachrichteninhalte werden unterteilt in solche, die schützenswerte Informationen, und solche, die für die Allgemeinheit bestimmte Informationen enthalten. Nachrichten sind immer dann geheim zu halten, wenn der Zugriff auf die enthaltenen Informationen durch unbefugte Dritte zu unerwünschtem Systemverhalten führen kann. Deshalb müssen Nachrichten, die nur allgemein zugängliche Informationen enthalten, nicht geheim gehalten werden. Es ist jedoch stets eine Authentifizierung des Senders notwendig.

Diskretisierbarkeit der Information Bei Informationen, die sich in diskrete Werte unterteilen lassen, kann durch Verwendung vordefinierter und vorverteilter Codes die Anzahl der zu übertragenden Zeichen reduziert werden. Im Installationsmodus werden hierzu die ausführlichen Nachrichteninhalte über eine Kommunikationsschnittstelle mit hohem Datendurchsatz auf einen Festwertspeicher im Fahrzeug übertragen und mit Codes versehen. Über die Funkverbindung muss dann lediglich ein Code übertragen werden, um im Fahrzeug die Verarbeitung des zugeordneten Inhalts anzustoßen. Die damit verbundene Reduzierung der Nachrichtenlänge führt zu einem geringeren Bedarf an Übertragungsbandbreite

und zur Verringerung der benötigten Maskengröße. In SIKAF werden Nachrichten daher unterteilt in solche, die sich vorcodieren lassen, und solche, bei denen dies nicht möglich ist.

4.4.3 Formale Sprachdefinition

Die mit SIKAF ausgetauschten Nachrichten müssen von allen Teilnehmern gleichartig und widerspruchsfrei verstanden werden. Mit dem eingesetzten Protokoll SIKAF-P wird eine formale und auf den Anwendungsfall Fahrzeugleitsystem zugeschnittene Sprache verwendet. Diese Sprache wird von allen Teilnehmern zur Darstellung der Nachrichteninhalte genutzt.

Wörter Allgemein ist diese Sprache in der Lage, den aktuellen Zustand (Regelgröße) sowie den gewünschten Zustand (Führungsgröße) eines Verkehrssystems eindeutig darzustellen und im Fahrzeugleitsystem zu kommunizieren. Darauf aufbauend werden die zur Korrektur notwendigen Maßnahmen (Stellgrößen) errechnet und von SIKAF an die einzelnen Fahrzeuge übermittelt. Wörter der formalen Sprache werden verwendet, um diese Systemzustände eindeutig zu bezeichnen. Es liegt ein dediziertes Wort für jeden definierten Systemzustand vor. Jedes als diskretisierbar klassifizierte Wort kann mit einem Code verknüpft werden, um die zu übertragende Datenmenge weiter zu reduzieren.

Nachrichtenbibliothek Eine Bibliothek verknüpft die Codes mit den zuvor festgelegten Informationen. Sie liefert somit zu jedem Code eine ausführliche Beschreibung des konkreten Ablaufs eines definierten Vorgangs. Die Bibliothek wird bei allen Fahrzeugen einheitlich hinterlegt, kann aktualisiert werden und ist stets abwärtskompatibel. Sie ermöglicht die Reduzierung der zu übertragenden Daten, da es genügt, einzelne Codes zu senden und zu empfangen. Deren Bedeutung wird vom Empfänger in der Bibliothek nachgeschlagen und löst jeweils die Ausführung eines komplexeren Algorithmus aus. Die Verwendung einer Bibliothek ermöglicht darüber hinaus die Erstellung eines Index der Codes, was schnelleren Zugriff auf die Codes erlaubt und somit die Datenverarbeitung beschleunigt.

Lexikon Digitale Lexika sind die einzelnen Einheiten der Bibliothek. Sie stellen die konkrete Verknüpfung von Codes mit Nachrichteninhalten dar. Sie enthalten die zulässigen Zeichen und Wörter zusammen mit einer Grammatik, die Wörter zu sinnvollen Nachrichten zusammenfügt. Die Lexika werden durch eine zentrale Verwaltung stets aktuell gehalten. Dies ermöglicht eine einfache Aktualisierung der Bibliothek, indem bei Änderungen lediglich einzelne Lexika versioniert und aktualisiert werden müssen. Ferner ist so die Abwärtskompatibilität der gesamten Bibliothek gewährleistet, da alle Fahrzeuge durch einheitlich versionierte Lexika über einen gemeinsamen, konsistenten Stand verfügen.

4.5 Kryptografische Absicherung

SIKAF setzt perfekt sichere Verschlüsselung ein, um die informations- und kommunikationstechnische Sicherheit hinreichend zu gewährleisten. Die praktische Umsetzung der Informationssicherheit wird in diesem Abschnitt vorgestellt, Abbildung 4.6 zeigt den Ablauf der Maskenerzeugung und -verteilung.

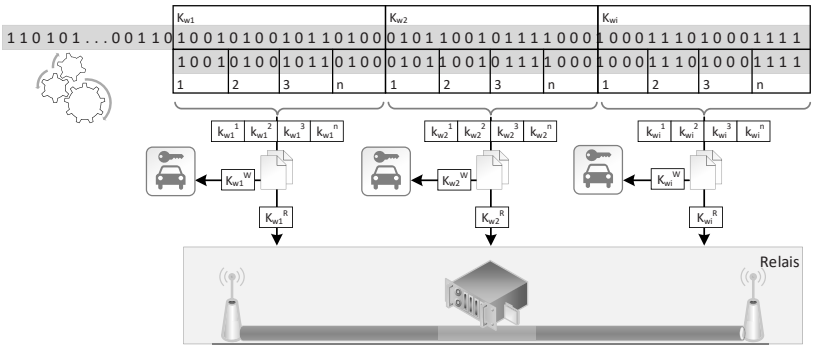


Abbildung 4.6: Maskenerzeugung und -verteilung in SIKAF

4.5.1 Maskenerzeugung und Maskenverteilung

Bei der Erzeugung von Masken muss auf den Einsatz echter Zufallsprozesse geachtet werden. Die Masken werden an zentraler Stelle erzeugt, da hierzu permanent ausreichende Ressourcen notwendig sind. Beim Einsatz von SIKAF führt die hoheitliche Behörde die Maskenerzeugung durch. Technisch kommen für die Erzeugung echter Zufallszahlen folgende Prozesse in Betracht:

Maskenerzeugung mittels physikalischem Prozess Echte Zufallsbits werden durch eine Kombination aus abgetastetem Prozessorrauschen und dem Farbwert von zufällig aufgenommenen Bildern erzeugt. Die jeweils entstehenden Bitströme werden mit dem *XOR*-Operator zu Masken verknüpft.

Maskenerzeugung mittels Chaosprozess Eine weitere Möglichkeit zur Erzeugung von Zufallszahlen ist die Verwendung von Rekurrenz in einem Chaosprozess, in dem nur der Initialisierungsvektor x_0 als Saatwert bereitgestellt werden muss. Weitere Zahlen können dann nach

$$x_{n+1} = rx_n(1 - x_n) \tag{4.1}$$

erzeugt werden, wobei $r = const$. Der Unterschied zum physikalischen Prozess ist, dass lediglich der Saatwert das auszutauschende Geheimnis darstellt und daraus die eigentliche Maske bei allen Teilnehmern erzeugt werden kann.

Die Zufallsbits werden in beiden Fällen einem Bitstrom entnommen. Sie werden zunächst in Blöcke K unterteilt, denen die jeweilige digitale Identifikation (dID) eines Teilnehmers zugeordnet wird. Die Blöcke werden anschließend in einzelne Masken k aufgeteilt und jede Maske wird mit einem Maskenanzeiger n versehen. Die so unterteilten Blöcke bilden dann den jeweiligen Maskenvorrat. Alle K_{dID} werden zu K^R_{dID} und K^W_{dID} dupliziert, da ein jeweils identischer Maskenvorrat beim Fahrzeug $w_{dID} \in W$ und beim Relais R vorhanden sein muss. Dabei gilt:

$$K^R_{dID} = K^W_{dID} \quad \forall dID \tag{4.2}$$

Der Maskenvorrat K^W_{dID} wird zur Verteilung an die Fahrzeuge, der Maskenvorrat K^R_{dID} zur Verwendung durch das Relais vorbereitet[2].

Maskenverteilung Jeder Sender muss in der Lage sein, eine beliebige Nachricht für jeden Empfänger zu maskieren. Bei i Fahrzeugen kann jedoch nicht jedes Fahrzeug die Masken aller $i-1$ anderen Fahrzeuge erhalten. Die resultierende Komplexitätsklasse $\mathcal{O}(i^2)$ würde in diesem Fall die Skalierbarkeit, also die Möglichkeit zum flexiblen Hinzufügen weiterer Fahrzeuge zur Kommunikationsarchitektur, unverhältnismäßig erschweren. Es ist ausreichend, wenn jedes Fahrzeug einen individuellen Maskenvorrat $K^W_{dID_i}$ erhält, da das Relais als Zwischenstation der Kommunikationen dient und die Nachrichten nur auf der Funkstrecke zwischen dem Fahrzeug und dem Relais maskiert werden. Das Relais verfügt dann über das entsprechende Gegenstück $K^R_{dID_i}$ und ist damit zur Demaskierung der Nachrichten aller Fahrzeuge in der Lage.

Es müssen $K^R_{dID_i}$ an das Relais und $K^W_{dID_i}$ an die Fahrzeuge verteilt werden. Von der hoheitlichen Behörde zum Relais R besteht ein konstanter, sicherer Kanal, beispielsweise über einen dedizierten Lichtwellenleiter. Über diesen können Maskenverteilung und Maskennachschub von der hoheitlichen Behörde zu R abgewickelt werden. Zu den Fahrzeugen werden die Masken während eines physischen Kontakts mit einer nachgeordneten Stelle der hoheitlichen Behörde verteilt. Hierzu kommen in Frage:

Übertragung während der Fertigung im Werk Während der Fahrzeugproduktion wird ein initialer Maskenvorrat auf den Festwertspeicher im Fahrzeug übertragen. Von der hoheitlichen Behörde zum Fahrzeugwerk ist ein ausreichender Schlüsselnachschub gegeben.

Wartung oder Kraftstoffaufnahme Kraftfahrzeuge müssen in regelmäßigen Abständen Inspektionen und Wartungen unterzogen werden, um ihre Betriebs- und Verkehrssicherheit sicherzustellen. Bestandteil einer Inspektion ist das Auslesen aufgezeichneter Sensorwerte über standardisierte Diagnoseprotokolle (*On-Board-Diagnose [OBD]*), wozu eine kabelgebundene Verbindung zur Fahrzeugelektronik hergestellt wird. Auch bei der Kraftstoffaufnahme werden physische Verbindungen zu Fahrzeugen hergestellt. Bei Elektrofahrzeugen ist aufgrund der Laderegelung der Einsatz von Digitalrechnern ohnehin notwendig. Die in beiden Fällen benötigte Versorgungsinfrastruktur kann mit einem sicheren Kanal zur Masken erzeugenden Stelle ausgestattet werden. Beide Verbindungen können dann benutzt werden, um die zur Anwendung von SIKAF benötigten Daten auf die Festwertspeicher in den Fahrzeugen zu übertragen.

Kennzeichen Es ist in vielen Staaten üblich, dass Kfz-Kennzeichen von hoheitlichen Behörden ausgegeben und erneuert werden. Die physischen Kennzeichen werden dabei entweder ganz oder teilweise ersetzt, um die Gültigkeit zu verlängern. Bei diesem Vorgang steht ein unidirektionaler sicherer Kanal von Masken erzeugender Stelle zu Fahrzeugen zur Verfügung, der zur Übertragung neuer Masken auf die Festwertspeicher genutzt werden kann.

Carsharing oder Mietwagen Wird ein Fahrzeug von mehreren Personen genutzt, so muss die Weitergabe des Fahrzeugschlüssels verwaltet werden. Bei Verwaltung an zentra-

[2]Eine weitere Unterteilung wird in Eingangs- und Ausgangsmasken vorgenommen [146], die aus Gründen der Übersichtlichkeit nicht dargestellt ist.

ler Stelle kann von dieser Stelle aus auch ein sicherer Kanal zur Masken erzeugenden Behörde hergestellt werden. Der Fahrzeugschlüssel (oder ein anderer physischer Zugangstoken) kann als Datenträger genutzt werden, um die zur Anwendung von SIKAF benötigten Daten auf die Festwertspeicher im Fahrzeug zu übertragen. Dadurch ist zudem eine Zuordnung zum tatsächlichen Fahrer möglich.

Die entsprechenden Versorgungseinrichtungen sind über einen sicheren Kanal mit der hoheitlichen Behörde verbunden, beispielsweise durch einen dedizierten Lichtwellenleiter. Auch die Verteilung durch Kuriere ist möglich. Vor Ort kann per Kabel oder durch Nutzung physischer Datenträger ein sicherer Übertragungskanal zum Fahrzeug hergestellt werden, wie es bereits mit Diagnosegeräten gehandhabt wird. Somit wird insbesondere kein drahtloser, abhörbarer Übertragungskanal benötigt. Notwendige Aktualisierungen der Bibliotheken oder anderer Softwarebestandteile werden durch den gleichen Prozess durchgeführt. Die aktuell zu beobachtenden Trends zugunsten der Elektromobilität und der gemeinschaftlichen Nutzung von Fahrzeugen begünstigen die dargestellten Möglichkeiten zur Gewährleistung des Maskennachschubs.

Durch diese Art der Maskenübergabe lässt sich perfekt sichere Verschlüsselung robust implementieren. Weitere sicherheitsbezogene Maßnahmen müssen lediglich auf die Minimierung des Risikos von Seitenkanalangriffen abzielen. Der Empfang aller Masken wird in SIKAF quittiert, um Abstreitbarkeit zu unterbinden. So kann das Gesamtverfahren gerichtsfest implementiert werden.

4.5.2 Maskensperrung

Kommunikationsteilnehmern, welche gegen die Vorgaben der Kommunikationsarchitektur verstoßen oder eine Gefahr für das Gesamtsystem darstellen, entzieht SIKAF die zugeteilten Rechte ganz oder teilweise. Dadurch werden die betroffenen Kommunikationsteilnehmer an der weiteren Verbreitung schädlicher Nachrichten gehindert. Notwendige Maßnahmen zur Sperrung einzelner Knoten können in SIKAF allein auf Seiten des Relais ergriffen werden. Werden einem Fahrzeug $w_i \in W$ die Rechte entzogen, so werden beim Relais die Masken $k_n \in K^R_{w_i}\ \forall n$ als gesperrt gekennzeichnet. Das Fahrzeug w_i kann damit den Maskenvorrat $K^W_{w_i}$ nicht mehr zur maskierten Datenübertragung oder zur Authentifizierung einsetzen, weil die Verwendung gesperrter Masken durch das Relais erkannt wird. Das Relais ersetzt dann Nachrichten des Fahrzeugs durch eine entsprechende Sperrmeldung, um den Nachrichtenempfänger über die Sperrung des Senders zu informieren. Durch dieses Verfahren ist keine Meldung der Sperrung an die weiteren Fahrzeuge erforderlich. Zudem entfällt ein aufwändiger Rückruf von Masken oder Zertifikaten. Bei der Versorgung der Fahrzeuge mit neuen Versionen der Masken wird dennoch zugleich eine Liste mit gesperrten Teilnehmern verteilt, sodass bei allen Fahrzeugen eine aktuelle Version diese Sperrliste hinterlegt ist.

Um ein Fahrzeug zu sperren, müssen Verstöße oder Gefahren durch den betroffenen Teilnehmer klar nachgewiesen werden. Die Möglichkeit zur Sperrung einzelner Teilnehmer darf nicht zu willkürlicher Zensur führen. Die Sperrung eines Teilnehmers w_i kann durch SIKAF wieder aufgehoben werden, indem der Maskenvorrat $K^R_{w_i}$ wieder als gültig gekennzeichnet wird. Alle hierzu notwendigen Vorgänge können ebenfalls allein auf Seiten des Relais durchgeführt werden.

4.5.3 Maskierung

Nachrichten werden in SIKAF paketweise maskiert, es liegt also eine Blockverschlüsselung vor. Die zur Maskierung einer Nachricht verwendete Maskierungsfunktion e nutzt die *XOR*-Verknüpfung der Nachricht im Klartext (p) mit der Maske (k) zur Erzeugung des Schlüsseltextes (c) gemäß

$$c = e_k(p) = p \oplus k \tag{4.3}$$

Dabei gilt:

$$|k| \geq |p| \tag{4.4}$$

Das sendende Fahrzeug $w_i \in W$ kann zur Maskierung jede Maske $k_n \in K_{w_i}^W$ wählen, die noch nicht als verwendet gekennzeichnet ist. Die verwendete Maske k_n wird anschließend zunächst vom Fahrzeug w_i als verwendet gekennzeichnet und nach dem Kommunikationsvorgang vernichtet.

4.5.4 Demaskierung

Die Demaskierungsfunktion $d = e^{-1}$ stellt aus dem Schlüsseltext (c) mit Hilfe der passenden Maske (k) und wiederum durch *XOR*-Verknüpfung den ursprünglichen Klartext (p) gemäß

$$p = d_k(c) = d_k(e_k(p)) = k \oplus c \tag{4.5}$$

wieder her.

Durch den Einsatz der symmetrischen Verschlüsselung mittels einfacher *XOR*-Verknüpfung ist die Dauer t zur Maskierung und Demaskierung direkt proportional zur Nachrichtenlänge $|p|$, da alle Bits einer Nachricht einmal durchlaufen werden müssen:

$$t = \mathcal{O}(|p|) \tag{4.6}$$

Die zur Maskierung und Demaskierung benötigte Zeitspanne ist somit für den Sender vorhersehbar und er kann entscheiden, ob die gesamte für die Nachrichtenübertragung benötigte Zeitspanne für den Anwendungsfall ausreichend ist.

Mit der Maskierung wird zunächst die Vertraulichkeit des Nachrichteninhalts erreicht. Darüber hinaus wird die Maskierung auch zur Überprüfung von Authentizität und Integrität einer Nachricht eingesetzt, auch wenn der Nachrichteninhalt selbst nicht vertraulich ist. Hierzu wird aus der Nachricht eine kryptografische Prüfsumme berechnet, beispielsweise mit einer zyklischen Redundanzprüfung. Die Prüfsumme wird maskiert und zusammen mit der Nachricht übertragen. Der Empfänger bildet zunächst aus der Nachricht und mit der gleichen zyklischen Redundanzprüfung die Prüfsumme und demaskiert anschließend die erhaltene Prüfsumme. Stimmen die aus der Nachricht selbst gebildete Prüfsumme und die empfangene, demaskierte Prüfsumme überein, kann der Empfänger von der Authentizität und Integrität der Nachricht ausgehen. Wird die Prüfsumme nicht maskiert, kann sie lediglich als technische Prüfsumme zur Verifizierung der korrekten Übertragung verwendet werden. Ein Schutz gegen mutwillige Veränderungen der Nachricht ist in diesem Fall nicht gegeben.

4.6 Datenübertragung

In SIKAF werden alle Teilstrecken der Datenübertragung $\vec{z_i}$ auf echtzeitfähige Datenübertragung ($t(\vec{z_i}) \leq t_{krit}$) hin ausgelegt, sodass auch für die gesamte Nachrichtenübertragung gilt:

$$\sum_i t(\vec{z_i}) \leq t_{krit} \tag{4.7}$$

Dabei stellt t_{krit} jeweils ein festzulegendes, oberes Zeitintervall für den jeweiligen Übertragungsvorgang dar.

4.6.1 Betrachtung der Teilstrecken

Die Nachrichtenübertragung findet in SIKAF immer indirekt über das Relais R statt, da die Entfernung zwischen zwei Fahrzeugen w_i und w_{i+1} für eine direkte Funkübertragung im Allgemeinen zu groß ist. Nach der Übertragung von w_i zu R findet die Weiterleitung von R zu w_{i+1} statt.

Teilstrecke zwischen Fahrzeug und Relais Die Positionen $\vec{r_m}$ aller Funkmasten $r \in R$ des Relais sind SIKAF bekannt. Die Positionen $\vec{w_i}$ der Fahrzeuge $w \in W$ werden von diesen laufend ermittelt und über SIKAF an den Zentralrechner übertragen. Aus diesen Informationen können die Differenzvektoren $\vec{z_i} = \vec{w_i} - \vec{r_m}$ sowie deren Längen $|\vec{z_i}|$ für alle i und für alle m bestimmt werden. Aus Entfernung, Ausbreitungsgeschwindigkeit elektromagnetischer Wellen und protokollspezifischer Verarbeitungsdauer ergibt sich die Laufzeit eines Nachrichtenpakets auf den Funkstrecken. Dies gilt sowohl für die Übertragung vom Fahrzeug zum Relais als auch für die Übertragung vom Relais zum Fahrzeug.

Verarbeitungsdauer Fahrzeug Die in SIKAF vorgesehenen Baseband-Prozessoren der Fahrzeuge sind in der Lage, die Nachrichten dem Trägersignal echtzeitfähig aufzumodulieren. Die eingesetzten Digitalrechner werden mit einem Echtzeitbetriebssystem ausgestattet. Die Gesamtdauer der Nachrichtenverarbeitung an Bord der Fahrzeuge ist folglich stets vorhersehbar.

Verarbeitungsdauer Relais Die Funkmasten sind untereinander und mit dem Zentralrechner über eine dedizierte Leitung verbunden, welche alle relaisseitigen Kommunikationen in Echtzeit und ohne Bandbreitenbeschränkung durchführen kann. Die Gesamtdauer der relaisinternen Übertragungen ist folglich stets vorhersehbar.

Aus der Teilstreckenbetrachtung ergibt sich, dass die Dauer der Datenübertragung in SIKAF stets vorhersehbar ist und SIKAF somit für die Echtzeitkommunikation eingesetzt werden kann.

4.6.2 Multicast und Broadcast

SIKAF kann Nachrichten als Uni-, Multi- oder Broadcast übertragen. Während der Unicast bereits ausführlich beschrieben wurde und Broadcast durch unverschlüsselte Übertragung die triviale Lösung darstellt[3], wird für einen Multicast durch das sendende Fahrzeug ein

[3]Der Sender wird jedoch durch Verwendung einer Maske durch das Relais authentifiziert.

spezielles, in Abbildung 4.7 schematisch dargestelltes Paket verschickt. Für die notwendigen Angaben ist ein Bereich im Nachrichtenheader reserviert (vgl. Abbildung 4.5). Dieses Paket enthält für das Relais im Klartext den Index der verwendeten Maske und (optional maskiert) im dafür reservierten Bereich des Pakets die Nachricht selbst zusammen mit dem avisierten Empfängerkreis. Der Sender schickt die Nachricht wie einen Unicast an das Relais. Den Multicast übernimmt im Anschluss das Relais, indem es die Nachricht einzeln für alle avisierten Empfänger maskiert und an diese adressiert. Der Sender sendet die Nachricht auf diese Weise nur einmal, während das Relais, welches über eine größere Rechenkapazität und Sendeleistung verfügt, die individuelle Maskierung und Zustellung der Nachricht durchführt. Der Vorgang ist zusammenfassend in Abbildung 4.8 anhand eines

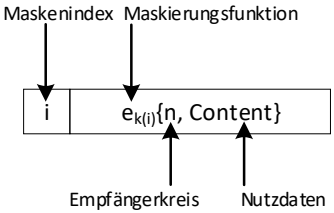


Abbildung 4.7: Nachrichtenformat für einen Multicast in SIKAF

Beispiels dargestellt. Fahrzeug 8 überträgt darin eine Nachricht per Multicast an die Fahrzeuge 3, 5 und 7. Prinzipiell können alle Fahrzeuge, darunter im Beispiel das Fahrzeug 6, die Nachricht empfangen, da sie Zugriff auf die Luftschnittstelle haben. Durch die Maskierung mit den individuellen Masken der berechtigten Empfänger sind jedoch nur diese zur sinnhaften Demaskierung der Nachricht in der Lage. Ist der Empfängerkreis größer als der im Adressblock reservierte Bereich (vgl. Abbildung 4.5), so muss der Sender den Prozess iterieren, indem er mehrere gleichartige Pakete mit verändertem Empfängerkreis an das Relais schickt, welches seinerseits den Multicast iterativ ausführt. Wird kein Multicast ausgeführt, wird der in der Nachricht für die Multicast-Adressen reservierte Bereich mit Nullen befüllt oder ist für zusätzliche Nachrichteninhalte verfügbar.

4.6.3 Filterung

Eine weitere Funktion des Relais ist die Filterung unerwünschter Nachrichten. Das Relais wird als Moderator für alle Kommunikationen zwischen Fahrzeugen eingesetzt und stuft in dieser Funktion Nachrichten im Bedarfsfall als unerwünscht (*Spam*) ein. Dies ist möglich, da alle Nachrichten beim Relais im Klartext vorliegen. Unerwünschte Nachrichten werden dann entweder verworfen, nicht weitergeleitet oder dienen als Begründung zur Sperrung des verursachenden Teilnehmers. SIKAF entscheidet über die Einstufung einer Nachricht als Spam durch

- Whitelisting durch Abgleich mit der Bibliothek oder
- Blacklisting durch Prüfung auf unzulässige Inhalte.

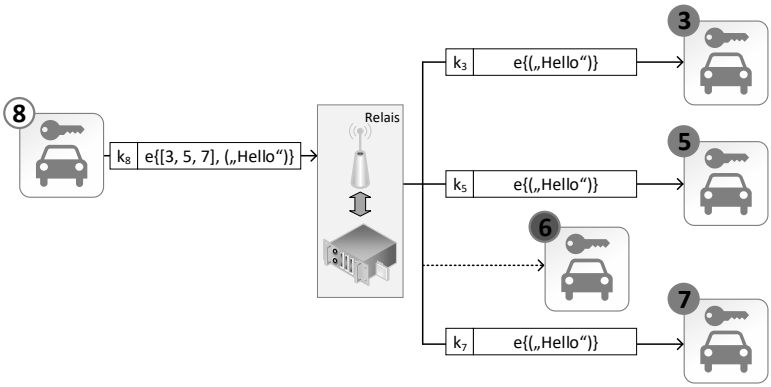


Abbildung 4.8: Ablauf eines Multicasts in SIKAF

Auch lang andauerndes oder hochfrequentes Senden von Nachrichten kann als Hinweis auf Spam dienen und Grund für eine weitergehende Prüfung sein. Nachrichten mit sicherheitsrelevanten Inhalten werden nie gefiltert, da sie bei korrekter Codierung aufgrund des Whitelistings den Filter passieren. Durch die Filterung wird verhindert, dass die im Allgemeinen limitierten Übertragungskapazitäten auf der Luftschnittstelle überlastet werden. Die Ressourcen bleiben somit den notwendigen Übertragungen vorbehalten.

Willkürliches Filtern (Zensur) wird in SIKAF verhindert, indem die benötigten Black- und Whitelists von der hoheitlichen Behörde generiert werden. Auf diese Weise findet eine gegenseitige Kontrolle zwischen bewertender Behörde und ausführendem Relais statt.

4.7 Zusammenfassung der Eigenschaften von SIKAF

Übergeordnetes Ziel eines Fahrzeugleitsystems ist Optimierung des Verkehrs, wozu es regelnd in das Fahrverhalten der beteiligten Kraftfahrzeuge eingreift. In diesem Kapitel wurde die Sichere Kommunikationsarchitektur für Fahrzeugleitsysteme (SIKAF) zur Übertragung notwendiger Steuermeldungen zu Kraftfahrzeugen vorgestellt. SIKAF ist in der Lage, Steuermeldungen rechtzeitig, perfekt sicher verschlüsselt und auch bei limitierter Bandbreite zuverlässig zu übertragen. Ein besonderes Merkmal von SIKAF ist die zentral ausgerichtete Topologie, die Vorcodieren und Verteilen von Nachrichteninhalten sowie laufenden Maskennachschub ermöglicht.

5 Implementierung und Evaluierung

Vor einem Einsatz ist zu überprüfen, ob SIKAF mit den vorgegebenen Eigenschaften umsetzbar ist und die Anforderungen an eine sichere Kommunikationsarchitektur in einem Fahrzeugleitsystem erfüllen kann. Für die erforderlichen Nachweise werden in diesem Kapitel zunächst Testszenarien entworfen, denen sich die Kommunikationsarchitektur unterziehen muss. Anhand einer prototypischen Implementierung wird gezeigt, dass SIKAF die Testszenarien erfolgreich durchlaufen kann und damit realisierbar ist. Abschließend werden Anwendungen von SIKAF als Grundlage möglicher Geschäftsmodelle vorgestellt.

5.1 Entwurf angepasster Testverfahren

Verifikation und Validierung sind zum Nachweis sowohl informations- und kommunikationstechnischer [84] als auch funktionaler [149] Sicherheit durchzuführen. „Verifikation ist ein Überprüfungsvorgang in jeder Phase des Software-Lebenszyklus' zur Entscheidung, ob alle Anforderungen einer Phase korrekt in der nächsten umgesetzt sind" [84]. Bei der Validierung wird geprüft, „ob die Software in einer vollständigen Systemumgebung richtig funktioniert" [84]. Tests allein ermöglichen allerdings nur das Auffinden von Fehlern, mit ihnen kann kein Korrektheitsnachweis im mathematischen Sinne geführt werden. Dennoch haben sich Verfahren zum Test technischer Systeme nach standardisierten und wiederholbaren Verfahren allgemein etabliert. Bei Fahrzeugleitsystemen werden Tests zumeist in Simulationen durchgeführt (vgl. Kapitel 3).

Im Folgenden werden einige bekannte Methoden an Testverfahren für die Kommunikationsarchitektur eines Fahrzeugleitsystems angepasst. Die Testverfahren orientieren sich an den Stufen von Softwaretests nach dem V-Modell [92], also Komponenten-, Integrations-, System- und Abnahmetest, da sich SIKAF auf die softwaretechnische Umsetzung eines Fahrzeugleitsystems fokussiert.

Die drei zentralen und damit zu testenden Komponenten von SIKAF sind

1. Maskierung und Demaskierung,
2. Datenübertragung sowie
3. Datenverarbeitung.

Für diese Bestandteile muss mit Testverfahren die Erfüllung der zentralen Anforderungen *Zuverlässigkeit und Sicherheit* sowie *Zeitanforderungen und Skalierbarkeit* empirisch überprüft werden. Auf den Einsatz von Werkzeugen wie *Scyther* kann hier verzichtet werden, da sich diese auf den isolierten Test des Verschlüsselungsprotokolls beschränken (vgl. Abschnitt 3.4.1). Die Sicherheit von SIKAF basiert jedoch auf dem organisatorischen und technischen Zusammenwirken der zuvor genannten Komponenten, die einzelnen Vorgänge des Maskenaustauschs und der Maskierung sind dagegen trivial.

5.1.1 Testverfahren zur Evaluierung der Maskierung und Demaskierung

Die Anforderungsanalyse hat gezeigt, dass nur solche Methoden in einem Fahrzeugleitsystem eingesetzt werden sollten, die kryptografisch perfekte Sicherheit ermöglichen. Es werden daher geeignete Testverfahren benötigt, um deren korrekte Implementierung und zuverlässige Arbeitsweise zu überprüfen.

Zuverlässigkeit und Sicherheit

In einem Fahrzeugleitsystem steht neben der Unbrechbarkeit des eingesetzten kryptografischen Verfahrens die Verhinderung von Seitenkanalangriffen im Vordergrund. Es sind daher die softwaretechnische und die nutzerzentrierte Sicherheit zu evaluieren. Testverfahren sind:

Test perfekt sicherer Verschlüsselung Es muss nachgewiesen werden, dass das zur Maskierung und Demaskierung eingesetzte Verfahren kryptografisch perfekte Sicherheit ermöglicht. Ausgetauschter Schlüsseltext darf keinerlei Rückschluss auf den korrespondierenden Klartext zulassen. Ein Test ist erfolgreich, wenn

- die eingesetzte Methode perfekt sichere Verschlüsselung ermöglicht,
- die Masken in ausreichender Anzahl, rechtzeitig und mit korrekten Verfahren erzeugt werden sowie
- alle Masken über einen sicheren Kanal ausgetauscht werden.

Zur Maskierung der Nachrichten wird in SIKAF das One Time Pad (OTP) eingesetzt. Dabei handelt es sich um ein perfekt sicheres Einmalverschlüsselungsverfahren, dessen Unbrechbarkeit bei korrekter Implementierung mathematisch bewiesen wurde [163]. Die Masken werden mit einem echten Zufallsprozess erzeugt und gemäß Spezifikation über einen sicheren Kanal verteilt. Systeme mit asymmetrischen Verschlüsselungsverfahren können diesen Test prinzipbedingt nicht bestehen.

Test von Authentisierung, Authentifizierung sowie Autorisierung In SIKAF werden Authentisierung, Authentifizierung sowie Autorisierung durch perfekt sichere Verschlüsselung mit symmetrischen Masken des Teilnehmers erreicht. Ein Test des Verfahrens an sich ist daher nicht notwendig, jedoch sind mögliche Ansatzpunkte für Seitenkanalangriffe zu identifizieren und abzusichern. Durch korrekte Implementierung wird verhindert, dass nicht autorisierte Stellen Zugriff auf die Masken erhalten. Die Integrität des Relais und seiner Verbindungen mit der hoheitlichen Behörde muss durch geeignete Qualitätssicherungsmaßnahmen gewährleistet sein. Hier gilt entsprechend, dass asymmetrische Verschlüsselungsverfahren einsetzende Systeme diesen Test prinzipbedingt nicht bestehen können. Zum Test wird die Authentisierung mit einer Maske versucht, die nicht von der hoheitlichen Behörde erstellt und verteilt wurde. Der Test ist erfolgreich, wenn SIKAF das Fahrzeug mit dieser falschen Maske nicht authentifiziert.

Zeitanforderungen und Skalierbarkeit

Zum Test der Echtzeitfähigkeit ist zu überprüfen, ob alle Prozesse in vorhersehbaren Zeitintervallen ablaufen. Testverfahren sind:

Test des Skalierungsverhaltens der Maskierung Alle zur Maskierung und Demaskierung benötigten Zeiten t_i dürfen maximal linear mit der Anzahl beteiligter Fahrzeuge $|W|$ steigen. Dies wird überprüft, indem Nachrichten variabler Länge und in variabler Anzahl mit dem eingesetzten Verfahren maskiert werden. Der Test ist bestanden, wenn stets gilt:

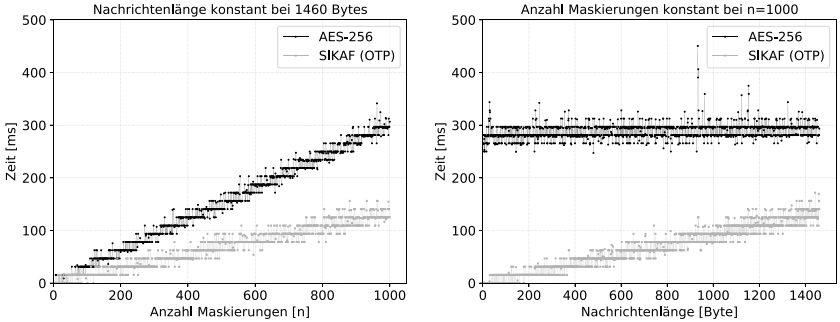
$$t_i \leq \mathcal{O}(|W|) \quad \forall i \tag{5.1}$$

Das in SIKAF eingesetzte Verschlüsselungsverfahren besteht aus einer einmaligen bitweisen *XOR*-Verknüpfung von Nachrichtentext und Maske. Daher kann die zur Maskierung benötigte Zeit t durch eine lineare Funktion τ ermittelt werden, die von den beiden Variablen Nachrichtenlänge $|p|$ und Anzahl maskierter Nachrichten $|P|$ abhängt:

$$t = \tau(|p|, |P|) = \sigma|p| + \epsilon|P| \tag{5.2}$$

In SIKAF ist die Nachrichtenlänge konstant ($|p| = const.$) und die Anzahl maskierter Nachrichten ist proportional zur Anzahl vernetzter Fahrzeuge ($|P| \propto |W|$), sodass Gleichung 5.1 erfüllt ist.

Die Maskierung wird in einer Testumgebung umgesetzt und hinsichtlich des Zeitverhaltens ausgewertet, um Erfüllung der Zeitanforderungen und Skalierbarkeit empirisch zu validieren. Hierzu werden Nachrichten unterschiedlicher Länge mehrere Male hintereinander maskiert. Die zur Maskierung benötigten Zeiten werden mit den zur Verschlüsselung benötigten Zeiten bei einer Verwendung des alternativ einzusetzenden Advanced Encryption Standards bei 32 B Schlüssellänge (AES-256) verglichen. Es wird jeweils eine Zeichenfolge mit vorgegebener Länge maskiert oder verschlüsselt, die wie die Maske oder der Schlüssel selbst mit einem Pseudozufallszahlengenerator erzeugt wird. Ausgewählte Resultate sind in Abbildung 5.1 dargestellt.



(a) Nachrichtenlänge konstant **(b)** Anzahl Maskierungen konstant

Abbildung 5.1: Zeitvergleich von Maskierung (SIKAF) und Verschlüsselung (AES)

Das wichtigste Ergebnis ist die empirische Bestätigung einer linearen Abhängigkeit zwischen der zur Maskierung benötigten Zeit, der Nachrichtenlänge und der Zahl der Maskierungen in SIKAF. Bei konstanter Nachrichtenlänge von 1460 B steigt sowohl

die in SIKAF zur Maskierung als auch die beim Einsatz von AES zur Verschlüsselung benötigte Zeit linear mit der Anzahl durchgeführter Vorgänge (Abbildung 5.1a) an. SIKAF weist mit dem OTP hier einen Geschwindigkeitsvorteil gegenüber der Verschlüsselung mit AES auf.

Die zur AES-Verschlüsselung benötigte Zeit steigt grundsätzlich mit der Nachrichtenlänge und der Anzahl der Verschlüsselungen [60]. Im vorliegenden Aufbau wird mit dem eingesetzten Rechner[1], der verwendeten Programmiersprache[2], den importierten Bibliotheken[3] und insbesondere dem gewählten Parametersatz ein nahezu konstantes Zeitverhalten der AES-Verschlüsselung beobachtet (Abbildung 5.1b). Bereits bei einer Nachrichtenlänge von 1 B werden zur 1000-maligen Verschlüsselung rund 300 ms benötigt. Die zur Verschlüsselung mit dem AES benötigte Zeit ist somit zunächst von den Dauern der Verfahrensschritte bestimmt, die unabhängig sind von der Nachrichtenlänge wie Schlüsselexpansion und Blockeinteilung[4].

Die in SIKAF zur Maskierung benötigte Zeit steigt bei konstanter Anzahl der Maskierungen linear mit der Nachrichtenlänge. Sie beginnt jedoch auf niedrigerem Niveau als bei der AES-Verschlüsselung, da im Gegensatz zu dieser keine vorbereitenden Verfahrensschritte notwendig sind. Die Maskierung in SIKAF weist damit zunächst einen Zeitvorteil auf. Bei konstanter Anzahl durchgeführter Maskierungen scheint sich bei längeren Nachrichten dieser Zeitvorteil allerdings zugunsten der Verschlüsselung mit dem AES-256 zu verschieben. Datagramme größer als 1460 B sind in SIKAF jedoch nicht vorgesehen. Mit 1000 Maskierungen wurde im Test zudem eine Größenordnung gewählt, die bei der Nachrichtenübertragung in SIKAF nicht zu erwarten ist. Im relevanten Bereich bis 1460 B ist die Geschwindigkeit der Maskierung (SIKAF) höher als die der Verschlüsselung (AES). Insgesamt werden bei der Maskierung in SIKAF keine zeitlichen Skalierungsprobleme beobachtet.

Test der sicheren Maskenverteilung Für neu hinzugefügte Fahrzeuge wird getestet, ob das Fahrzeugleitsystem Maskenverteilung und Maskennachschub konzeptuell über einen sicheren Kanal ermöglicht. Dies muss sowohl für die initiale Maskenverteilung als auch den Maskennachschub gegeben sein. Der Test ist erfolgreich, wenn ein Nachweis erbracht werden kann, dass dieser Kanal mindestens den gleichen Sicherheitsanforderungen genügt wie die Nachrichtenübertragung zwischen Teilnehmern selbst. In SIKAF steht ein dedizierter, abhörsicherer Kanal für die Maskenverteilung zur Verfügung. Dieser wird für Maskenverteilung und -nachschub zu jedem neu hinzugefügten Relais und zu jedem neu hinzugefügten Fahrzeug genutzt. In SIKAF können daher Maskenverteilung und -nachschub über einen sicheren Kanal gewährleistet werden.

5.1.2 Testverfahren zur Evaluierung der Datenübertragung

Aus den Anforderungen an ein Fahrzeugleitsystem wurde abgeleitet, dass das zugrunde liegende Übertragungsnetz für SIKAF nur im Infrastrukturmodus betrieben werden sollte.

[1] Intel(R) Core(TM) i7-4510U CPU @ 2.00GHz, 8 GB RAM, 64-bit-Betriebssystem
[2] Python 3.8.3
[3] pycryptodome 3.9.7, pandas 1.0.3
[4] Bei der Wahl einer größeren Nachrichtenlänge (bis 500 000 B) konnte mit dem gleichen Aufbau die erwartete Zunahme der Verschlüsselungsdauer mit der Nachrichtenlänge beobachtet werden.

Mit Tests muss nachgewiesen werden, dass diese Topologie implementiert wurde und alle Kommunikationen gemäß den Spezifikationen abwickeln kann.

Zuverlässigkeit und Sicherheit

Es ist zu überprüfen, ob für jedes Fahrzeug stets ein Funkmast mit freien Kapazitäten zum Senden und Empfangen von Nachrichten zur Verfügung steht. Der Funkmast muss sich zudem innerhalb einer Entfernung befinden, die eine für den Vorgang ausreichende Übertragungsdauer ermöglicht. Natürliche oder künstliche Störungen dürfen die echtzeitfähige Datenübertragung nicht beeinträchtigen oder zu sonstigen gefährlichen Situationen führen. Hierzu muss SIKAF auch im autarken Betrieb in einem sicheren Zustand verbleiben oder in einen solchen überführt werden können. Testverfahren sind:

Test der Abdeckung des Projektgebiets Alle Strecken, auf denen SIKAF zum Einsatz kommen soll, müssen mit Messfahrzeugen befahren werden. Es muss stets eine ausreichende Verbindung zu einem Funkmast gegeben sein. Eine rein rechnerische Bestimmung der Sende- und Empfangsreichweite ist im Allgemeinen nicht ausreichend, da dabei Einflüsse wie Orographie oder atmosphärische Störungen nur vereinfacht oder gar nicht berücksichtigt werden können. Zudem bleiben mutwillige Störungen des Funkkanals unberücksichtigt. Der Test ist erfolgreich, wenn auf der gesamten Strecke ein ausreichender Signalpegel für den Nachrichtenempfang gemessen werden kann.

Test mit Störsender Der Funkkanal von SIKAF wird durch eine technische Einrichtung zu zufällig ausgewählten Zeitpunkten gezielt gestört. Hierzu wird die gesamte Bandbreite mit einem Signal hoher Leistung blockiert, sodass in SIKAF keine Kommunikationen mehr stattfinden können. Zeitpunkte und Dauern der Störungen werden zufällig über einen Testzeitraum verteilt und protokolliert. Die Systemreaktion wird unter kontrollierten Bedingungen beobachtet. Der Test ist erfolgreich, wenn das Fahrzeugleitsystem eine Störung des Funkkanals erkennt und in einem sicheren und kontrollierten Zustand verbleibt oder in einen solchen überführt wird.

Zeitanforderungen und Skalierbarkeit

Der Test der Zuverlässigkeit muss um einen Test der Rechtzeitigkeit erweitert werden. Es muss überprüft werden, ob SIKAF ausreichende Übertragungskapazität auch bei steigender Teilnehmerzahl gewährleisten kann. Testverfahren sind:

Test variabler Übertragungsstrecken Das Systemverhalten muss bei dynamisch veränderlichen Funkübertragungsstrecken getestet werden, da Fahrzeugleitsysteme durch bewegliche Objekte geprägt sind. Nachrichten müssen zuverlässig, sicher und rechtzeitig zugestellt werden, auch wenn sich Sender und Empfänger bewegen. Hierzu zählt auch das Wechseln von einer Funkzelle in eine andere (*Handover* oder *Roaming*). Für den Test bewegen sich Sender und Empfänger voneinander weg. Mindestens einer der Beteiligten wechselt dabei in eine andere Funkzelle, während eine Datenübertragung stattfindet. Der Test ist erfolgreich, wenn die Nachrichten unter diesen Voraussetzungen zuverlässig, sicher und rechtzeitig zugestellt werden oder das System in einen sicheren autarken Betriebsmodus wechselt.

Test zur Bestimmung der Latenzzeiten Dazu werden Nachrichten jeweils beim Senden und beim Empfangen mit Zeitstempeln versehen. Die Latenzzeiten werden dann aus der Differenz der beiden Zeitstempel errechnet. Die maximal zulässigen Werte ergeben sich aus den Zeitanforderungen, die im aktuellen Anwendungsfall zur echtzeitfähigen Übertragung notwendig sind. Der Test ist erfolgreich, wenn die gemessenen Latenzzeiten mit den rechnerisch ermittelten Werten einschließlich Toleranzbereichen übereinstimmen.

Test hoher Teilnehmerdichte Singuläre Ansammlungen zahlreicher vernetzter Fahrzeuge um einzelne Funkmasten herum werden betrachtet, die beispielsweise im Fall von Staus auftreten. Es ist insbesondere nicht ausreichend, die Kapazität von SIKAF nur bei gleichförmiger Verteilung der Teilnehmer über das von allen Funkmasten abgedeckte Gebiet sicherzustellen. Stattdessen muss rechnerisch ermittelt werden, wie viele Fahrzeuge sich maximal im Einzugsbereich eines einzelnen Funkmastes befinden können. Aufgrund bekannter Abmessungen der Fahrzeuge und Kenntnis der geometrischen Gegebenheiten (vgl. Abschnitt 2.1) kann diese Fahrzeuganzahl ermittelt werden. Der Test ist erfolgreich, wenn die Funktionsfähigkeit von SIKAF mit der so ermittelten maximalen Teilnehmerdichte um einen Funkmast herum gegeben ist.

5.1.3 Testverfahren zur Evaluierung der Datenverarbeitung

Testverfahren müssen überprüfen, ob Informationen zur Übertragung mit SIKAF korrekt aufbereitet werden. Empfangene Nachrichten müssen in den Fahrzeugen korrekt weiterverarbeitet und die Inhalte an die Fahrzeugelektronik übergeben werden.

Zuverlässigkeit und Sicherheit

Ein Fahrzeugleitsystem muss robust gegenüber fehlerhaften oder falschen Nachrichten sein. Auch wenn es Angreifern gelingt, unautorisiert Meldungen zu verbreiten, darf dies nicht zu gefährlichen Systemzuständen führen. Testverfahren sind:

Test zur Behandlung falscher Nachrichten Unter kontrollierten Bedingungen werden Nachrichten in SIKAF eingeschleust, die zu unerwünschtem Systemverhalten führen oder bei ungeprüfter Verarbeitung gefährliche Systemzustände herbeiführen würden. Dadurch wird die Robustheit von SIKAF gegen mutwillig oder durch Fehlfunktion verfälschte Nachrichten getestet. Der Test besteht darin, eine falsche Information zu einem Fahrzeug zu übertragen und das Systemverhalten zu beobachten. Der Test ist erfolgreich, wenn SIKAF diese gefälschten Nachrichten erkennt und verwirft sowie optional eine Warnmeldung generiert.

Test des Malwareschutzes Auf den Digitalrechnern von hoheitlicher Behörde, Relais und Fahrzeug darf die versuchte Ausführung von Schadprogrammen (engl. *malware*) nicht zu unerwünschtem Systemverhalten führen. Es muss nachgewiesen werden, dass prinzipbedingt nur solche Programme zur Ausführung kommen, welche nach einem zuvor definierten Sollverhalten ablaufen. Als Test wird unter kontrollierten Bedingungen versucht, Schadprogramme auszuführen, und das Systemverhalten beobachtet. Die Abwehr von Malware darf dabei nicht lediglich auf der Kenntnis von Signaturen

bekannter Schadprogramme beruhen. Dies kann beispielsweise getestet werden, indem ein bereits bekanntes Schadprogramm so abgeändert wird, dass sich die Signatur ändert, oder die Signatur eines Schadprogramms wird gezielt aus den Abwehrprogrammen entfernt. Der Test ist erfolgreich, wenn die Ausführung von Schadsoftware nicht zugelassen und optional eine Warnmeldung generiert wird.

In SIKAF können keine unautorisierten Programme zur Ausführung kommen, da die Speicherbereiche für Programme und Daten getrennt sind und jede Programmfunktion durch eine Offenbarungsdatei spezifiziert und freigegeben werden muss.

Zeitanforderungen und Skalierbarkeit

Die Datenverarbeitungsgeräte von Relais und Fahrzeugen müssen auch hohe Nachrichtenaufkommen in vorhersehbaren Zeitintervallen bewältigen können. Die hoheitliche Behörde muss große Mengen von Masken erzeugen und zur Verteilung bereitstellen können, um ein Fahrzeugleitsystem zu skalieren. Testverfahren sind:

Test der Unterbrechungsbehandlung Es muss permanent mit Nachrichten gerechnet werden, die von der Netzschnittstelle empfangen und zur Bearbeitung an die jeweilige Recheneinheit weitergeleitet werden. Die Datenverarbeitungssysteme aller Komponenten müssen daher zur Durchführung von Unterbrechungsroutinen in der Lage sein. Gleichzeitig müssen die Komponenten falsche oder fehlerhafte Nachrichten erkennen und adäquat behandeln. Zum Test werden jeder Komponente von SIKAF Unterbrechungen auslösende Nachrichten zugestellt, zusätzlich aufgeteilt in korrekte, fehlerhafte und falsche. Das Systemverhalten wird beobachtet. Der Test ist erfolgreich, wenn der jeweils laufende Prozess von korrekten und priorisierten Nachrichten unterbrochen, die durch die Unterbrechung ausgelöste Aktion abgearbeitet und der ursprüngliche Prozess anschließend fortgesetzt wird. Fehlerhafte oder falsche Nachrichten dürfen nicht zu unerwünschtem Systemverhalten führen.

Test des Multitaskings Die Datenverarbeitung muss auch hohe Nachrichtenaufkommen, beispielsweise bei steigender Verkehrsdichte, zuverlässig abarbeiten können. Als Test wird hierzu ein einzelnes Fahrzeug mit einem stark erhöhten Nachrichtenaufkommen konfrontiert. Das maximal mögliche Nachrichtenaufkommen kann aus der geometrisch möglichen Anzahl vernetzter Fahrzeuge auf einem definierten Streckenabschnitt ermittelt werden. Der Test ist erfolgreich, wenn auch in diesem Szenario alle eintreffenden Nachrichten in vorgegebenen Zeiten abgearbeitet werden und es zu keinem Speicherüberlauf kommt. Werden die Datenverarbeitungssysteme überlastet, kann das Fahrzeug alternativ in einen sicheren Zustand überführt werden.

5.2 Prototypische Implementierung

Durch prototypische Implementierung wird nachgewiesen, dass SIKAF unter Beachtung der gestellten Anforderungen praktisch umsetzbar ist. In diesem Stadium einer Machbarkeitsstudie können die Hard- und Softwarekomponenten frei gewählt werden, weshalb einfach und kostengünstig verfügbare Module eingesetzt werden. Bei möglicher Serienfertigung kann SIKAF auch an bestehende Fahrzeugsysteme angepasst oder in diese integriert werden.

5.2.1 Eingesetzte Hardware

Für jede Hierarchieebene von SIKAF werden eigene Prototypen angefertigt, um dem modularen Aufbau von SIKAF gerecht zu werden. Für alle Prototypen wird als Grundlage ein vorkonfektioniertes Entwicklungssystem in Form eines Einplatinenrechners verwendet. Darauf sind auch die benötigten Peripheriekomponenten bereits teilweise integriert, was die Entwicklung erheblich erleichtert. Das hier verwendete Entwicklungssystem stellt hinsichtlich Rechenleistung und Schnittstellen deutlich mehr Ressourcen bereit, als für die Prototypen benötigt würden. In der Folge sind auch Preis und Leistungsaufnahme höher als für eine optimal integrierte Lösung. Bei allen Prototypen wird ein Mikroprozessor aus der *ARM Cortex-A*-Familie eingesetzt. Zur Realisierung der drahtlosen Kommunikation werden bestehende Funkschnittstellen nach dem Bluetooth- und WLAN-Standard genutzt. Für Bluetooth wird ein Chipsatz aus der *BCM*-Familie (Hersteller „Broadcom“), für das WLAN-Modul ein Chipsatz der *RTL*-Familie (Hersteller „Realtek“) verwendet. Als Massenspeicher kommt stets ein Flash-Speicher in Form einer SD-Karte zum Einsatz. Die Verwendung der Einplatinenrechner ermöglicht vergleichsweise einfaches Implementieren und Testen verschiedener Funktionen, ohne dass für jede Funktion eine neue Komponente entwickelt werden muss. Nach erfolgreichem Test kann die fertige Implementierung für die Zielplattform im Kraftfahrzeug skaliert und dorthin portiert werden. Dabei muss es sich nicht zwingend um eine dedizierte Hardwareplattform handeln, wenn die benötigten Funktionen in bereits bestehende Systeme, beispielsweise On Board Units (OBUs) von Fahrzeugen, integriert werden können.

Die Prototypen sind in folgenden Zeichnungen teilweise vereinfacht dargestellt; beispielsweise wurde auf die Darstellung von Spannungsquellen, Kurzschlussbrücken und Vorwiderständen verzichtet, da diese Komponenten keine Bedeutung für die kommunikationstechnischen Verbindungen haben.

Prototyp der Komponenten der hoheitlichen Behörde Zur Erprobung einer Komponente für Maskenerzeugung und -verteilung wird ein Prototyp zur Erzeugung echter Zufallszahlen, deren Zwischenspeicherung und anschließende Bereitstellung erstellt. Abbildung 5.2 zeigt schematisch die eingesetzte Hardware dieser Komponente.

Zentraler Bestandteil des rechts dargestellten Einplatinenrechners ist ein integrierter Schaltkreis des Herstellers „Broadcom“, der neben dem ARM-Mikrocontroller über einige Peripheriekomponenten und Schnittstellen verfügt [11]. Hierzu zählen insbesondere ein physikalischer Zufallszahlengenerator und eine UART-Schnittstelle, über die eine Kamera angeschlossen wird. Die Schnittstelle für das (Komposit-)Videosignal (hier: CVBS) und der zugehörige Masseanschluss (GND) werden nicht benötigt, da lediglich Fotoaufnahmen und keine Videos verarbeitet werden. Der Zufallszahlengenerator kann über `rng-tools` angesteuert werden. Durch eine Kombination des CCD-Sensorrauschens mit der Ausgabe des physikalischen Zufallszahlengenerators werden echte Zufallszahlen erzeugt. Einzelne Masken gemäß dem Konzept von SIKAF werden anschließend durch die Software ausgeliefert. Die generierten Masken werden auf einem (nicht dargestellten) Massenspeicher zwischengespeichert und können über eine entsprechende Schnittstelle zur weiteren Verteilung bereitgestellt werden.

Prototyp der Komponenten des Relais Der Prototyp des Relais ermöglicht frei parametrierbare Nachrichtenverarbeitung und -übertragung. Zudem werden eine Schnittstelle

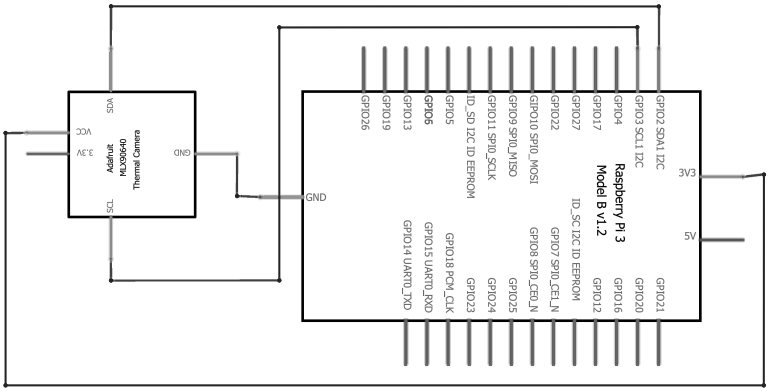


Abbildung 5.2: Prototyp: Komponente für die hoheitliche Behörde [72]

zur Übernahme der Masken sowie ein Massenspeicher für deren Verwaltung integriert. Abbildung 5.3 zeigt die eingesetzte Hardware für diesen Prototyp.

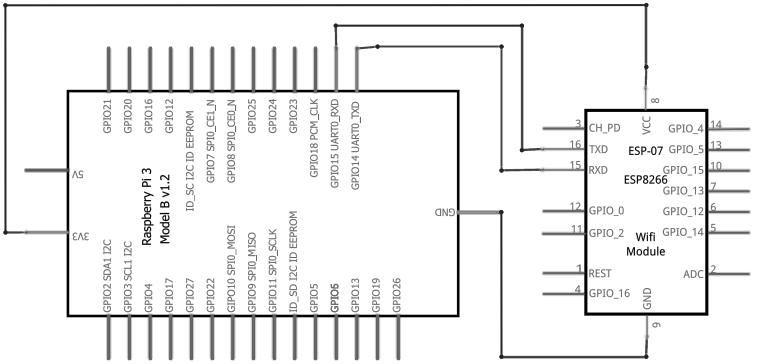


Abbildung 5.3: Prototyp: Komponente für das Relais [72]

Der im Bild links dargestellte Einplatinenrechner beinhaltet zwar bereits Schnittstellen für WLAN und Bluetooth, zur Nutzung mehrerer Kanäle und damit Flexibilisierung wurde jedoch ein zusätzlicher Mikrocontroller mit WLAN-Schnittstelle verwendet (rechts dargestellt). Mit entsprechenden Einstellungen kann das Relais somit im Vollduplexmodus betrieben werden. Durch Anbindung weiterer Mikrocontroller mit WLAN-Schnittstelle, die untereinander über ein breitbandiges Netz verbunden sind, lässt sich auf diese Weise der Betrieb mehrerer Funkmasten erproben. Der Einplatinenrechner führt Maskierung und Demaskierung der durch das Relais geleiteten Nachrichten sowie das Routing zwischen den Funkmasten durch.

Prototyp der Komponenten eines Fahrzeugs Die Komponenten an Bord der Fahrzeuge bilden den Netzabschluss von SIKAF. Der Prototyp verfügt über beispielhafte Sensoren zur Umgebungserfassung sowie Module zur Datenaufbereitung und -übertragung. Abbildung 5.4 zeigt die entwickelte Hardware der Komponente auf der Fahrzeugebene.

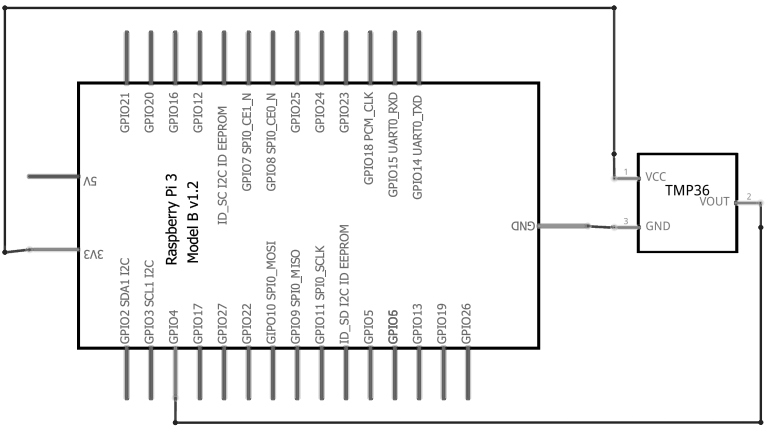


Abbildung 5.4: Prototyp: Komponente für ein Fahrzeug [72]

Zur Simulation der Datenerzeugung durch Fahrzeugsensoren wird hier exemplarisch ein Temperatursensor eingesetzt. Bei Seriensystemen kann es sich um beliebige Sensoren wie beispielsweise Radargeräte zur Abstandsmessung oder Kameras zur Videodetektion handeln. Bezüglich der Datenübertragung verfügt der Einplatinenrechner bereits über WLAN- und Bluetooth-Schnittstellen, sodass keine zusätzlichen Komponenten zur Datenübertragung verbaut werden brauchen. Der Sensor stellt Messwerte über einen 1-Wire-Bus bereit, sodass sie durch den Einplatinenrechner ausgelesen und für die Übertragung aufbereitet und maskiert werden können.

5.2.2 Betriebssystem

Die eingesetzte Entwicklungsplattformen ist ein vollwertiger Rechner, weshalb für Verwaltung der Hardware und Zuteilung der verfügbaren Ressourcen an die Anwendungsprogramme ein Betriebssystem benötigt wird. Bei den entwickelten Prototypen wird eine auf *Debian* basierende Linux-Distribution eingesetzt. Grundsätzlich wäre zwar ein Echtzeitbetriebssystem wie *RTOS-UH* oder *FreeRTOS* zu bevorzugen. Im Rahmen dieser Machbarkeitsuntersuchung werden die Funktionen eines Echtzeitbetriebssystems manuell evaluiert, indem Prozesse isoliert zur Ausführung kommen. Dadurch werden diese dem Prozessor exklusiv zugeteilt und können manuell unterbrochen werden, was die Analyse des Echtzeitverhaltens von SIKAF ermöglicht.

5.2.3 Formale Sprache für Nachrichten

Die mit SIKAF ausgetauschten Nachrichten werden in einer formalen Sprache L_{sikaf} verfasst. Das benötigte Alphabet Σ^{sikaf} setzt sich aus drei Teilen zusammen:

- Aus dem Alphabet der Nachrichteninhalte $\Sigma^{sikaf'}$ zur Beschreibung von Ereignissen und deren Quantifizierung,
- dem Alphabet zur Erzeugung von Zeitstempeln mit einer Genauigkeit von Millisekunden $\Sigma^{timestamp_{ms}}$ sowie
- dem Alphabet zur Nutzung eines standardisierten Datenformats Σ^{json}. In SIKAF wird hierzu die JavaScript Object Notation (JSON) eingesetzt, da diese Notation die Anforderungen an Rechnerverarbeitbarkeit und Menschenlesbarkeit erfüllt.

Die Nachrichten können somit aus dem Alphabet

$$\Sigma^{sikaf} = \Sigma^{sikaf'} \cup \Sigma^{timestamp_{ms}} \cup \Sigma^{json} \tag{5.3}$$

gebildet werden. Jedes Alphabet Σ und damit auch Σ^{sikaf} ist eine Menge von Zeichen. Zu beachten ist, dass es sich bei diesen Zeichen nicht um Buchstaben im Sinne einer natürlichen Sprache handelt, sondern um Schlüsselwörter zur Beschreibung der Nachrichteninhalte sowie definierte Zeichen zur Bildung des Datenformats. Ein Wort im Sinne dieser formalen Sprache ist dann eine mit SIKAF ausgetauschte Nachricht.

5.2.4 Exemplarische Nachrichten

Mit SIKAF ausgetauschte Informationen können sich entweder auf Fahrzeuge oder auf Strecken beziehen. Fahrzeugbezogene Nachrichten enthalten Informationen über den aktuellen und den prognostizierten Zustand eines Fahrzeugs, insbesondere zur Fahrzeugtrajektorie. Streckenbezogene Nachrichten enthalten Informationen über den aktuellen Zustand einzelner Streckenabschnitte. Letztere Informationen werden entweder von Fahrzeugen gemeldet, die diesen Streckenabschnitt befahren, oder von Funkbaken, die sich temporär oder dauerhaft an einem Streckenabschnitt befinden.

Im Folgenden werden beispielhafte Nachrichten in der eingeführten formalen Sprache dargestellt. Zu jedem Nachrichteninhalt wird die zur Codierung der jeweiligen Information benötigte Datenmenge angegeben. Die Reihenfolge der übertragenen Inhalte kann durch das Protokoll (SIKAF-P) vorgegeben werden, die JSON-Auszeichnungen (engl. *tags*) dienen dann lediglich zur Strukturierung der Daten und deren Darstellung in einer menschenlesbaren Form. Die Auszeichnungen bleiben bei der Bestimmung der Datenmenge unberücksichtigt, da sie zur Datenverarbeitung in den Steuergeräten nicht benötigt werden. Das genaue Nachrichtenformat kann zudem in einem *JSON-Schema* fixiert werden. Durch geeignetes Parsen lassen sich alle Nachrichteninhalte in das durch SIKAF-P festgelegte Datagrammformat bringen. Jede Nachricht wird mit einem *end of frame (EOF)* abgeschlossen, sodass nur die für die jeweilige Anforderung notwendige Datenmenge übertragen wird.

Eine Maskierung muss explizit angezeigt werden, da sowohl Bitfolgen im Klartext als auch maskierte Texte zulässige Nachrichteninhalte repräsentieren können. Ein Bit zu Beginn des jeweiligen Inhalts dient daher als Maskierungsindikator und gibt an, ob der folgende Inhalt maskiert ist. Manche Nachrichteninhalte werden optional übertragen. Mit einem

Bit als Meldungsindikator zu Beginn des jeweiligen Inhalts wird angegeben, ob dieser Inhalt der Nachricht mit Daten befüllt oder leer ist.

Streckenbezogene Nachrichten Streckenbezogene Nachrichten haben drei Hauptbestandteile: Angaben zum sendenden Fahrzeug, um den Ursprung jeder Nachricht zurückverfolgen zu können, georeferenzierte Informationen zum Zustand der Strecke, um diese Informationen weiteren Fahrzeugen zur Verfügung zu stellen, und schließlich die kryptografische Absicherung der Nachricht, um die IKT-Schutzziele zu erreichen. Durch die im Folgenden vorgestellte Tabellierung können ausführliche Inhalte durch Verknüpfung mit einer lokalen Datenbank abgeleitet werden. Beispielsweise kann das Relais weitere Attribute zum sendenden Fahrzeug, die mit der dID verknüpft sind, aus einer lokalen Datenbank nachladen.

Tabelle 5.1 stellt die Angaben über das sendende Fahrzeug und alle Informationen zusammen, die zur sinnhaften Weiterverarbeitung einer übertragenen Nachricht benötigt werden. Der Sender kann seine dID maskieren, wenn der Ursprung einer Nachricht verborgen werden soll.

Tabelle 5.1: Nachrichteninhalt: Spezifikationen (119 bit)

Code	Wert	Größe
0 … 1023	Versionsnummer SIKAF	10 bit
{0, 1}	{strecken, fahrzeug}bezogen	1 bit
{0x000…00, …, 0xfff…ff}	IRIG Zeitstempel	60 bit
{0, 1}	Sender maskiert {nein, ja}	1 bit
{0x00000000, …, 0xffffffff}	dID Sender	32 bit
0	Gültig bis auf Weiteres	11 bit
1 … 2047	Gültigkeit in Sekunden (s)	
0 … 15	Meldungen pro Sekunde (s^{-1})	4 bit

Die Informationen zum Streckenzustand beginnen mit der räumlichen Verortung der Nachricht. In Tabelle 5.2 sind die hierzu notwendigen Informationen zusammengestellt. Die Genauigkeit von 32 bit ermöglicht die Verortung auf der Erdoberfläche in einem Bereich bis 1 cm und damit die exakte Spurführung von Fahrzeugen. Die Höhe ist zur Berücksichtigung von Brücken oder Tunneln sowie weitere Anwendungen von SIKAF wie in der Luftfahrt von Bedeutung. Die Richtungsangabe bezieht sich auf die Stationierung oder Kilometrierung einer Straße. Mit 32 bit ließen sich insgesamt mehr Werte als der zur Codierung von Koordinaten benötigte Bereich von 360° darstellen. Der ungenutzte Bereich kann hier und in anderen Fällen wie bei Prozentangaben zur Befüllung mit künftigen Informationen genutzt werden. Hinsichtlich der benötigten Maskengröße ist der ungenutzte Bereich unkritisch, da die Koordinaten zur Übertragung nicht maskiert werden. Die Angaben zu Fahrbahnoberfläche, Sichtweite, Geschwindigkeitsbegrenzung und Hindernissen sollen stets allgemein für alle Fahrzeuge zugänglich sein und sind daher nie maskiert. Die übertragenen Inhalte und deren Codierungen sind in den Tabellen 5.3 bis 5.6 zusammengestellt.

Mögliche Alternativstrecken (Tabelle 5.7) sind als Splines codiert und in einer Datenbank hinterlegt. Sie können dort ausgelesen und zur automatischen Fahrzeuglenkung eingesetzt werden. Ist keine Alternativstrecke codiert, muss das Fahrzeug in manuelle Regelung

Tabelle 5.2: Nachrichteninhalt: Verortung (172 bit)

Code	Wert	Größe
$0 \dots 3\,599\,999\,999$	Länge (°)*	32 bit
$0 \dots 3\,599\,999\,999$	Breite (°)*	32 bit
$0 \dots 65\,535$	Höhe (m)	16 bit
{0x00000000, . . . , 0xffffffff}	{„A1“, „A99“, . . . , „Zusestrasse“}	32 bit
$0 \dots 1023$	Abschnitt	10 bit
$0 \dots 1023$	Station	10 bit
$0 \dots 100$	Position in Prozent (%)*	7 bit
$1 \dots 16$	Fahrspur	4 bit
0	Punktuelles Ereignis	16 bit
$1 \dots 65\,535$	Länge in Meter (m)	
$\{0, 1\}$	Richtung {in, gegen}	1 bit
$0 \dots 4094$	Zeitverlust in Sekunden (s)	12 bit
4095	Vollsperrung	

*Codes nicht ausgeschöpft

Tabelle 5.3: Nachrichteninhalt: Fahrbahnoberfläche (5 bit)

Code	Wert	Größe
$\{0, 1\}$	gemeldet {nein, ja}	1 bit
$\{0, \dots, 15\}$	{„trocken“, . . . , „vereist“}	4 bit

Tabelle 5.4: Nachrichteninhalt: Sichtweite (9 bit)

Code	Wert	Größe
$\{0, 1\}$	gemeldet {nein, ja}	1 bit
0	Sichtweite maximal	8 bit
$1 \dots 255$	Sichtweite ($\times 10$ m)	

Tabelle 5.5: Nachrichteninhalt: Geschwindigkeitsbegrenzung (11 bit)

Code	Wert	Größe
$\{0, 1\}$	gemeldet {nein, ja}	1 bit
$0 \dots 255$	Zulässige Geschwindigkeit ($\frac{\text{km}}{\text{h}}$)	8 bit
$\{0, 1\}$	Leitsystem aktiv {nein, ja}	1 bit
$\{0, 1\}$	Kontrolle {nein, ja}	1 bit

Tabelle 5.6: Nachrichteninhalt: Hindernis (6 bit)

Code	Wert	Größe
$\{0, 1\}$	gemeldet {nein, ja}	1 bit
$\{0, \ldots, 15\}$	{„Baustelle“, …, „Unfall“}	4 bit
$\{0, 1\}$	Alternativstrecke {nein, ja}	1 bit

überführt werden, was durch den Code 0 signalisiert wird. Eine Maskierung kann zur optimierten Steuerung durch das Fahrzeugleitsystem notwendig sein: Im Sinne globaler Optimierung werden auch für den einzelnen Verkehrsteilnehmer nachteilige Alternativstrecken übertragen. Durch die Maskierung wird verhindert, dass ein Fahrzeug aus allen übertragenen Alternativstrecken entgegen der globalen Optimierung die individuell vorteilhafteste Alternativstrecke auswählt. Globale Optimierung ist auch die Motivation zur Maskierung der Information über verfügbare Parkplätze (Tabelle 5.8). Durch gezieltes Zuweisen vorhandener Parkplätze zu suchenden Fahrzeugen kann das Fahrzeugleitsystem Angebot und Nachfrage optimal zusammenbringen. Zur Übertragung von Freitext (Tabelle 5.9) wird mit bis zu 20 ASCII-codierten Buchstaben eine vergleichsweise große Datenmenge benötigt, Übertragung und Maskierung sind optional. Die Inhaltsverifizierung (Tabelle 5.10) gibt an, ob eine Information bereits von anderen Fahrzeugen gemeldet und ob sie bestätigt wurde. Zudem besteht für das Fahrzeugleitsystem die Möglichkeit, eine gemeldete Information aufzuheben. Die abschließenden kryptografischen Angaben (Tabelle 5.11) werden zur Gewährleistung von Vertraulichkeit und Integrität benötigt. Mit der Übertragung einer maskierten Prüfsumme kann die Authentizität jeder Nachricht überprüft werden. Durch Angabe der verwendeten Masken kann die Nachricht beim Empfänger demaskiert werden.

Tabelle 5.7: Nachrichteninhalt: Alternativstrecke (34 bit)

Code	Wert	Größe
$\{0, 1\}$	gemeldet {nein, ja}	1 bit
$\{0, 1\}$	maskiert {nein, ja}	1 bit
0	manuelle Regelung nötig	32 bit
{`0x00000001`, …, `0xffffffff`}	hinterlegter Spline	

Tabelle 5.8: Nachrichteninhalt: Parkplätze (18 bit)

Code	Wert	Größe
$\{0, 1\}$	gemeldet {nein, ja}	1 bit
$\{0, 1\}$	maskiert {nein, ja}	1 bit
255	maximale Pkw-Parkplätze	8 bit
0 … 254	verbleibende Pkw-Parkplätze	
255	maximale Lkw-Parkplätze	8 bit
0 … 254	verbleibende Lkw-Parkplätze	

Tabelle 5.9: Nachrichteninhalt: Freitext (142 bit)

Code	Wert	Größe
$\{0,1\}$	gesetzt {nein, ja}	1 bit
$\{0,1\}$	maskiert {nein, ja}	1 bit
['H', ..., 'C']	max. 20 ASCII	140 bit

Tabelle 5.10: Nachrichteninhalt: Verifizierung (10 bit)

Code	Wert	Größe
$\{0,1\}$	bereits gemeldet {nein, ja}	1 bit
$0 \dots 255$	Anzahl Validierungen	8 bit
$\{0,1\}$	aufgehoben {nein, ja}	1 bit

Tabelle 5.11: Nachrichteninhalt: Kryptografische Angaben (100 bit)

Code	Wert	Größe
$0 \dots 1\,048\,575$	Prüfsumme	20 bit
0x000000000, ..., 0xfffffffff	Maskenanzeiger von	40 bit
0x000000000, ..., 0xfffffffff	Maskenanzeiger bis	40 bit

Listing 5.1 veranschaulicht so entstehende streckenbezogene Nachrichten.

Listing 5.1: Streckenbezogene Nachricht als JSON

```
{
  "Nachrichtenspezifikationen": {
    "Version-SIKAF": 1.0,                          // 10 bit
    "Nachrichtentyp": "streckenbezogen",           // 1 bit
    "Zeitstempel": "2020-06-14 14:26:31.3",        // 60 bit
    "Sender maskiert": false,                      // 1 bit
    "dID Sender": 0xf329123e,                      // 32 bit
    "Gueltigkeit_s": 1200,                         // 11 bit
    "Meldungsfrequenz_Hz": 5                       // 4 bit
  },
  "Senderspezifikationen": {                       // 0, da aus dID ableitbar
    "Integrationsdatum": "2013-07-12",
    "Rolle": ["Sender", "Bestaetiger"],
    "Gesperrt": false
  },
  "Nachricht": {
    "Position": {
      "geographisch": {
        "Laenge_deg": 20.389,                      // 32 bit
        "Breite_deg": 49.234,                      // 32 bit
        "Hoehe_m": 500.0                           // 16 bit
      },
      "linear": {
        "Strasse": "B 54",                         // 32 bit
```

```
        "Abschnitt": 820,                          // 10 bit
        "Station": 30,                             // 10 bit
        "Position_perc": 0.75,                     // 7 bit
        "Fahrspur": 2                              // 4 bit
      },
      "Ausdehnung": {
        "Laenge_m": 1321,                          // 16 bit
        "Richtung": 1                              // 1 bit
      }
    },
    "Zeitverlust_s": 1700,                         // 12 bit
    "Ereignisse": {
      "Fahrbahnoberflaeche": {
        "gemeldet": true,                          // 1 bit
        "Art": "nass"                              // 4 bit
      },
      "Sichtweite": {
        "gemeldet": true,                          // 1 bit
        "Sichtweite_m": 2170                       // 8 bit
      },
      "Geschwindigkeitsbegrenzung_kmh": {
        "gemeldet": true,                          // 1 bit
        "Wert": 80,                                // 8 bit
        "Leitsystem aktiv": true,                  // 1 bit
        "Kontrolle": true                          // 1 bit
      },
      "Hindernis": {
        "gemeldet": false,                         // 1 bit
        "Art": "Baustelle",                        // 4 bit
        "Alternativstrecke": false                 // 1 bit
      },
      "Alternativstrecke": {
        "gemeldet": true,                          // 1 bit
        "maskiert": false,                         // 1 bit
        "Spline": 0xdd45ae12                       // 32 bit
      },
      "Parkplaetze": {
        "gemeldet": true,                          // 1 bit
        "maskiert": true,                          // 1 bit
        "verfuegbarPKW": 255,                      // 8 bit
        "verfuegbarLKW": 37                        // 8 bit
      },
      "Freitext": {
        "gesetzt": false,                          // 1 bit
        "maskiert": false,                         // 1 bit
        "Text": ""                                 // 20 ASCII à 7 bit
      },
    },
    "Meldungsverifizierung": {
      "bereits gemeldet": true,                    // 1 bit
      "Validierungen": 13,                         // 8 bit
      "aufgehoben": false                          // 1 bit
    }
  },
  "Kryptografie": {
    "Pruefsumme": "642531",                        // 20 bit
```

```
81     "Maskenanzeiger": {
82       "Maske_von": 0x0000000000,                    // 40 bit
83       "Maske_bis": 0x0000000001                     // 40 bit
84     }
85   }
86 }
```

Eine streckenbezogene Nachricht beginnt mit allgemeinen Angaben im Teil *Nachrichtenspezifikationen*. Es gibt lediglich zwei Nachrichtentypen, die daher mit einer booleschen Variable angegeben werden können. Der IRIG-Timecode ermöglicht eine Darstellung des Zeitstempels mit 60 bit und stellt die direkte Kompatibilität zum Zeitsignal aus dem Global Positioning System (GPS) sicher. Mit der Gültigkeit wird angegeben, bis wann die Nachricht übertragen sein muss. Die Meldungsfrequenz hat neben der zu verschlüsselnden Nachrichtenlänge erheblichen Einfluss auf die zu maskierende Datenmenge und damit die benötigte Maskengröße, weshalb sie in den Spezifikationen angegeben ist. Ein Empfänger muss nicht angegeben werden, da der Empfänger streckenbezogener Nachrichten stets das Relais ist. In den *Senderspezifikationen* sind die dID des Fahrzeugs und dessen zugeteilte Rechte hinterlegt. Außerdem ist angegeben, ob das Fahrzeug bereits in SIKAF gesperrt wurde. Zur vollständigen Darstellung der Fahrzeugspezifikationen ist es ausreichend, die dID in die Nachricht aufzunehmen. Alle weiteren Informationen zum Fahrzeug können dann mit Hilfe der dID aus einer Datenbank entnommen werden. Durch Verwendung von 32 bit, hier im Hexadezimalsystem dargestellt, können die Spezifikationen von genau $2^{32} = 4\,294\,967\,296$ Fahrzeugen erfasst werden, was den aktuellen und zukünftig zu erwartenden Fahrzeugbestand deutlich übersteigt.

Eine streckenbezogene Nachricht wird durch sowohl geografische als auch kartenbezogene Koordinaten verortet. Der Wertevorrat von 32 bit ermöglicht die Codierung von insgesamt 2^{32} Straßen. An die Angabe zu erwartenden Zeitverlusts schließt sich ein modular aufgebauter *Ereignis*container an. Darin wird übertragen, ob ein Ereignis auf der Strecke vorliegt, mit welchem Wert das Ereignis quantifiziert ist und ob die Information maskiert werden muss. Ist der zu quantifizierende Wert eine diskrete Größe, wird er tabelliert und mit einem Code versehen. Die Stützpunkte und Streckenelemente von Alternativstrecken lassen sich auch in Listen schachteln, sodass theoretisch beliebige Streckenangaben übertragen werden können. In jedem Fall muss nicht der Volltext übertragen werden, sondern es genügt die Übertragung der mit den Stützpunkten verknüpften Codes. Im Bereich *Freitext* kann eine beliebige Information übertragen werden, die Verwendung von Codes ist zumindest initial nicht möglich. Ein längerer als der vorgesehene Freitext kann durch das Senden mehrerer Nachrichten hintereinander übertragen werden.

Der letzte Teil einer streckenbezogenen Nachricht ist für die *kryptografischen Angaben* vorgesehen. Mittels bekannter zyklischer Redundanzprüfung wird eine Prüfsumme der Nachricht erzeugt, mit der ihre Authentizität und Integrität überprüft werden können. Hierzu wird die Prüfsumme vom Sender erzeugt, maskiert und zusammen mit der Angabe von Block und Index der verwendeten Masken (nicht den Masken selbst) übertragen. Der Empfänger demaskiert die Prüfsumme und vergleicht sie mit dem Ergebnis der bekannten zyklischen Redundanzprüfung, mit der er aus der empfangenen Nachricht die Prüfsumme reproduziert hat. Sind die Werte der Prüfsummen identisch, kann der Empfänger von Authentizität und Integrität der Nachricht ausgehen. Bei der Länge der Prüfsumme besteht ein Zielkonflikt zwischen kryptografischer Sicherheit und Datensparsamkeit. In Anlehnung an das angeführte Beispiel der TAN bei Finanztransaktionen wird eine Länge von sechs

Stellen als hinreichend angenommen, was mit einer Ganzzahl darstellbar ist. Werden weitere Nachrichteninhalte maskiert, so werden hierzu Masken mit fortlaufendem Anzeiger verwendet. So müssen nur der erste und der letzte Maskenanzeiger mit der Nachricht übertragen werden und der Empfänger kann die Masken aus seinem Vorrat entsprechend zusammensetzen[5].

Fahrzeugbezogene Nachrichten Fahrzeugbezogene Nachrichten beinhalten Informationen zum sendenden Fahrzeug, insbesondere zu dessen aktueller und prognostizierter Trajektorie. Das wechselseitige Verhalten von Fahrzeugen kann mit dieser Information antizipiert werden. Jede fahrzeugbezogene Nachricht beginnt mit Nachrichtenspezifikationen wie in Tabelle 5.12 dargestellt. Sowohl Sender als auch Empfänger können maskiert werden, um Ursprung und Ziel einer Nachricht zu verbergen. Im Gegensatz zu streckenbezogenen Nachrichten ist die Angabe einer Gültigkeit vorgeschrieben. Mit der dID des Senders können weitere Angaben zum Fahrzeug wie Hersteller und Modell verknüpft sein, die in einer lokalen Datenbank hinterlegt sind. Mit weiteren Attributen gemäß Tabelle 5.13 können temporäre Angaben zu Eigenschaften des Fahrzeugs übertragen und im Bedarfsfall maskiert werden. Dies kann sinnvoll sein, wenn Ladung oder Auftrag des Fahrzeugs verborgen werden sollen. Angaben zur Trajektorie (Tabelle 5.14) bilden den größten Bestandteil der Nachricht. Die Verortung des Fahrzeugs ist aus Sicherheitsgründen redundant ausgelegt. Durch Kenntnis der aktuellen und beabsichtigten Fahrzeugtrajektorie kann das Fahrzeugleitsystem das Fahrverhalten aller Fahrzeuge optimal abstimmen. Die nicht ausgeschöpften Codes bei Verortung und Richtung können bei künftigen Anwendungen belegt werden. Angaben zum Kraftstoff (Tabelle 5.15) sind zur Erkennung der verbleibenden Reichweite notwendig. Das Fahrzeugleitsystem kann ein Fahrzeug im Bedarfsfall zur Kraftstoffaufnahme leiten und diesen Vorgang auch zur Versorgung mit neuen Masken nutzen. Der Freitext (Tabelle 5.16) wird äquivalent zu streckenbezogenen Nachrichten als optionaler Inhalt übertragen. Die benötigten kryptografischen Angaben (Tabelle 5.17) für Vertraulichkeit und Integrität werden ebenso äquivalent zu streckenbezogenen Nachrichten behandelt.

Tabelle 5.12: Nachrichteninhalt: Spezifikationen (152 bit)

Code	Wert	Größe
$0 \ldots 1023$	Versionsnummer SIKAF	10 bit
$\{0, 1\}$	{strecken, fahrzeug}bezogen	1 bit
{0x000...00, ..., 0xfff...ff}	IRIG-Zeitstempel	60 bit
$\{0, 1\}$	Sender maskiert {nein, ja}	1 bit
{0x00000000, ..., 0xffffffff}	dID Sender	32 bit
$\{0, 1\}$	Empfänger maskiert {nein, ja}	1 bit
{0x00000000, ..., 0xffffffff}	dID Empfänger	32 bit
$1 \ldots 2048$	Gültigkeit in Millisekunden (ms)	11 bit
$0 \ldots 15$	Meldungen pro Sekunde (s^{-1})	4 bit

[5] Die Verwendung fortlaufender Maskenanzeiger kann eine Sicherheitsverletzung darstellen, wenn Tatsache, Umfang oder Reihenfolge von Nachrichtenübertragungen verborgen werden soll [146]. Diese Kenntnis ist im vorliegenden Anwendungsfall jedoch unkritisch.

Tabelle 5.13: Nachrichteninhalt: Attribute (7 bit)

Code	Wert	Größe
$\{0,1\}$	maskiert {nein, ja}	1 bit
$\{0,1\}$	Einsatzfahrzeug {nein, ja}	1 bit
$\{0,1\}$	Gefahrgut {nein, ja}	1 bit
$\{0,\ldots,15\}$	{„Pkw“, „Tram“, …, „Bus“}	4 bit

Tabelle 5.14: Nachrichteninhalt: Trajektorie (224 bit)

Code	Wert	Größe
$\{0,1\}$	maskiert {nein, ja}	1 bit
$0\ldots3\,599\,999\,999$	Länge (°)*	32 bit
$0\ldots3\,599\,999\,999$	Breite (°)*	32 bit
$0\ldots65\,535$	Höhe (m)	16 bit
{`0x00000000`, …, `0xffffffff`}	{„A1“, „A99“, …, „Zusestrasse“}	32 bit
$0\ldots1023$	Abschnitt	10 bit
$0\ldots1023$	Station	10 bit
$0\ldots100$	Position in Prozent (%)*	7 bit
$1\ldots16$	Fahrspur	4 bit
$0\ldots255$	Geschwindigkeit aktuell ($\frac{\text{km}}{\text{h}}$)	8 bit
$0\ldots255$	Geschwindigkeit in 0,5 s ($\frac{\text{km}}{\text{h}}$)	8 bit
$0\ldots255$	Geschwindigkeit in 1,0 s ($\frac{\text{km}}{\text{h}}$)	8 bit
$0\ldots255$	Geschwindigkeit in 1,5 s ($\frac{\text{km}}{\text{h}}$)	8 bit
$0\ldots3599$	Richtung aktuell (°)*	12 bit
$0\ldots3599$	Richtung in 0,5 s (°)*	12 bit
$0\ldots3599$	Richtung in 1,0 s (°)*	12 bit
$0\ldots3599$	Richtung in 1,5 s (°)*	12 bit

*Codes nicht ausgeschöpft

Tabelle 5.15: Nachrichteninhalt: Kraftstoff (12 bit)

Code	Wert	Größe
$\{0,1\}$	maskiert {nein, ja}	1 bit
$\{0,\ldots,15\}$	{„Benzin“, …, „Batterie“}	4 bit
$0\ldots100$	Füllstand in Prozent (%)*	7 bit

*Codes nicht ausgeschöpft

Tabelle 5.16: Nachrichteninhalt: Freitext (142 bit)

Code	Wert	Größe
$\{0,1\}$	gesetzt {nein, ja}	1 bit
$\{0,1\}$	maskiert {nein, ja}	1 bit
[`'H'`, …, `'C'`]	max. 20 ASCII	140 bit

Tabelle 5.17: Nachrichteninhalt: Kryptografische Angaben (100 bit)

Code	Wert	Größe
0 . . . 1 048 575	Prüfsumme	20 bit
0x000000000, . . . , 0xfffffffff	Maskenanzeiger von	40 bit
0x000000000, . . . , 0xfffffffff	Maskenanzeiger bis	40 bit

Listing 5.2 veranschaulicht so entstehende fahrzeugbezogene Nachrichten.

Listing 5.2: Fahrzeugbezogene Nachricht als JSON

```
{
  "Nachrichtenspezifikationen": {
    "Version-SIKAF": 1.0,                          // 10 bit
    "Nachrichtentyp": "fahrzeugbezogen",           // 1 bit
    "Zeitstempel": "2020-06-14 14:26:31.1",        // 60 bit
    "Sender maskiert": false,                      // 1 bit
    "dID Sender": 0x3ffd923a,                      // 32 bit
    "Empfaenger maskiert": false,                  // 1 bit
    "dID Empfaenger": 0x2d5b27f8,                  // 32 bit
    "Gueltigkeit_ms": 700,                         // 11 bit
    "Meldungsfrequenz_Hz": 5                       // 4 bit
  },
  "Senderspezifikationen": {                       // 0, da aus dID ableitbar
    "Integrationsdatum": "2013-07-12",
    "Rolle": ["Sender", "Bestaetiger"],
    "Gesperrt": false
  },
  "Fahrzeugspezifikationen": {                     // 0, da aus dID ableitbar
    "Kennzeichen": "M-AB-1234",
    "Laenge_m": 5,
    "Breite_m": 1.8,
    "Gewicht_kg": 1600.0,
    "Marke": "Audi",
    "Typ": "A6"
  },
  "Attribute": {
    "maskiert": false,                             // 1 bit
    "Einsatzfahrzeug": false,                      // 1 bit
    "Gefahrgut": false,                            // 1 bit
    "Verkehrsmittel": "mIV"                        // 4 bit
  },
  "Trajektorie": {
    "maskiert": false,                             // 1 bit
    "Position": {
      "geographisch": {
        "Laenge_deg": 20.389,                      // 32 bit
        "Breite_deg": 49.234,                      // 32 bit
        "Hoehe_m": 348                             // 16 bit
      },
      "linear": {
        "Strasse": "Musterstrasse",                // 32 bit
        "Abschnitt": 820,                          // 10 bit
        "Station": 30,                             // 10 bit
```

```
44        "Position_perc": 0.75,                    // 7 bit
45        "Fahrspur": 3                             // 4 bit
46      }
47    },
48    "Kinetik": {
49      "Geschwindigkeit_kmh": {
50        "aktuell": 85.0,                          // 8 bit
51        "0p5_Sek": 85.0,                          // 8 bit
52        "1p0_Sek": 84.0,                          // 8 bit
53        "1p5_Sek": 83.0                           // 8 bit
54      },
55      "Richtung_deg": {
56        "aktuell": 270.0,                         // 12 bit
57        "0p5_Sek": 271.0,                         // 12 bit
58        "1p0_Sek": 271.0,                         // 12 bit
59        "1p5_Sek": 272.0                          // 12 bit
60      }
61    }
62  },
63  "Kraftstoff": {
64    "maskiert": false,                            // 1 bit
65    "Typ": "Batterie",                            // 4 bit
66    "Fuellstatus_perc": 0.49                      // 7 bit
67  },
68  "Freitext": {
69    "gesetzt": false,                             // 1 bit
70    "maskiert": false,                            // 1 bit
71    "Text": ""                                    // 20 ASCII à 7 bit
72  },
73  "Kryptografie": {
74    "Pruefsumme": "135246",                       // 20 bit
75    "Maskenanzeiger": {
76      "Maske_von": 0x0000000004,                  // 40 bit
77      "Maske_bis": 0x0000000007                   // 40 bit
78    }
79  }
80 }
```

Zu Beginn einer fahrzeugbezogenen Nachricht stehen wiederum die *Nachrichtenspezifikationen* mit einem genauen Zeitstempel im IRIG-Timecode-Format und der Angabe der Gültigkeit in Millisekunden. Angaben zum Fahrzeug ermöglichen die Nachverfolgung jeder abgesetzten Nachricht, wobei die dID gleichzeitig als Absenderadresse dient. Weitere *Sender- und Fahrzeugspezifikationen* lassen sich auch hier durch die dID mit einer Länge von 32 bit aus einer Datenbank abrufen und müssen nicht übertragen werden. Für fahrzeugbezogene Nachrichten sind in dieser Datenbank zusätzlich die physischen Eigenschaften der Fahrzeuge hinterlegt. Im Gegensatz zu streckenbezogenen Nachrichten ist die Angabe eines Empfängers in Form der dID notwendig, um die Nachricht korrekt vermitteln zu können. Die möglichst exakte räumliche Verortung des Fahrzeugs zum Zeitpunkt der Nachrichtengenerierung wird äquivalent zur streckenbezogenen Nachricht als geografische und streckenbezogene Koordinate dargestellt. Die doppelte Verortung dient auch der Redundanz, da es sich bei der Position um ein sicherheitsrelevantes Datum handelt.

Attribute geben an, ob es sich um ein Einsatzfahrzeug mit hoheitlichen Rechten handelt, ob Gefahrgut geladen ist und welcher Verkehrsmittelkategorie das Fahrzeug zugeordnet ist.

Im vorliegenden Beispiel handelt es sich um ein Fahrzeug des motorisierten Individualverkehrs (mIV).

Der größte Nachrichteninhalt ist die *Trajektorie*, womit Informationen zum aktuellen und beabsichtigen Fahrverhalten übertragen werden. Genaue Daten zum aktuellen Geschwindigkeitsvektor, bestehend aus Betrag und Richtung, erlauben Koordination und Optimierung der Fahrzeugbewegungen. Jedes Fahrzeug sendet zudem Angaben zum beabsichtigen Fahrverhalten bis zu einem Zeithorizont von 1,5 s, um den umgebenden Fahrzeugen die Antizipation der Fahrsituation zu ermöglichen. Auf eine separate Angabe der Beschleunigung wird verzichtet, da die gefahrene Geschwindigkeit die entscheidende Führungsgröße zur Koordinierung ist und sich der Beschleunigungswert im Bedarfsfall aus der Zeitreihe der Geschwindigkeiten ableiten lässt. Auf die Übertragung redundanter Informationen kann dann zugunsten reduzierten Datenumfangs verzichtet werden. Ein längerer als der vorgesehene *Freitext* kann wie bei streckenbezogenen Nachrichten durch Senden mehrerer Nachrichten hintereinander übertragen werden. Im Bedarfsfall wird mit einer booleschen Variable angegeben, ob der jeweilige Inhalt maskiert ist.

5.2.5 Klassifizierung von Nachrichteninhalten

Nachrichteninhalte können nach zwei wesentlichen Gesichtspunkten klassifiziert werden: Zum einen besteht die bereits beschriebene Möglichkeit zur Vorcodierung von Informationen, wodurch die Übertragung von Volltexten vermieden wird. Der Volltext einer Information wird in diesem Fall tabelliert und mit Hilfe eines Codebuchs einem Code zugewiesen. Zum anderen wird nach der Vertraulichkeit des Inhalts klassifiziert, ob der Inhalt maskiert werden muss oder im Klartext übertragen werden kann.

Die Inhalte der beiden Nachrichtentypen sind gemäß dieser Klassifizierung in den folgenden Tabellen zusammengestellt. Der codierte Anteil entspricht den tabellierten Nachrichteninhalten. Jedem maskierbaren Nachrichteninhalt geht ein Maskierungsindikator voraus, der wie der Meldungsindikator mit einer booleschen Variable codiert ist. Die *Prüfsumme* muss zur Authentifizierung einer Nachricht immer maskiert werden, beim *Maskenanzeiger* ist grundsätzlich keine Codierung möglich.

Streckenbezogene Nachrichteninhalte Tabelle 5.18 stellt die streckenbezogenen Nachrichteninhalte nach dieser Klassifizierung zusammen. Zur Verwendung von Codes sind folgende Inhalte vorgesehen:

- Bei den Nachrichtenspezifikationen lassen sich der Zeitstempel nach dem IRIG-Format codieren und die dID mit einem beliebigen Datum wie dem Kfz-Kennzeichen verknüpfen.
- Zur Verortung werden alle Straßen einer digitalen Karte tabelliert, die Fahrtrichtung wird codiert.
- Mögliche Zustände von Fahrbahnoberflächen werden definiert und codiert.
- Geschwindigkeitsbegrenzungen ließen sich bei Verwendung diskreter Klassen codieren. In SIKAF ist dies ein ganzzahliger, stetiger Wert. Kontrolle und Anzeige der Geschwindigkeit durch ein Leitsystem werden mit einer booleschen Variable codiert.

Tabelle 5.18: Klassifikation der Nachrichteninhalte (streckenbezogen)

Nachrichteninhalt	Datenmenge gesamt	davon codiert	davon maskierbar
Nachrichtenspezifikationen	119 bit	94 bit	32 bit
Verortung	172 bit	33 bit	0 bit
Fahrbahnoberfläche	5 bit	5 bit	0 bit
Sichtweite	9 bit	1 bit	0 bit
Geschwindigkeitsbegrenzung	11 bit	3 bit	0 bit
Hindernis	6 bit	6 bit	0 bit
Alternativstrecke	34 bit	34 bit	32 bit
Parkplätze	18 bit	2 bit	16 bit
Freitext	142 bit	2 bit	140 bit
Inhaltsverifizierung	10 bit	2 bit	0 bit
Prüfsumme	20 bit	0 bit	20 bit
Maskenanzeiger	80 bit	0 bit	0 bit
Summe	626 bit	182 bit	240 bit

- Mögliche Hindernisse werden definiert und codiert. Das Vorliegen einer Alternativstrecke wird mit einer booleschen Variable angezeigt.

- Angezeigte Alternativstrecken werden durch Splines codiert.

Bei den weiteren Inhalten werden nur der Meldungs- und der Maskierungsindikator mit booleschen Variablen codiert.

Maskierung von Informationen über den ohnehin öffentlich einsehbaren Streckenzustand ist bis auf wenige Ausnahmen nicht notwendig:

- Bei den Fahrzeugspezifikationen wird die dID maskiert oder pseudonymisiert, wenn keine personenbeziehbaren Daten im Klartext übertragen werden sollen.

- Informationen über Parkplätze oder eine Alternativstrecke werden maskiert, wenn dies zur globalen Optimierung notwendig ist.

- Der Freitext wird abhängig vom konkreten Inhalt maskiert.

- Die Prüfsumme muss zur Gewährleistung von Authentizität und Integrität einer Nachricht maskiert werden.

Die zwingend notwendige Maskengröße ergibt sich bei den streckenbezogenen Nachrichten somit allein aus der Länge der Prüfsumme. In SIKAF werden für die Prüfsumme 20 bit vorgesehen, es sind jedoch variable Längen vorstellbar. So besteht die in Kapitel 3 angeführte TAN zur Autorisierung von Finanztransaktionen häufig ebenfalls aus sechs Dezimalziffern, folglich maximal 12 B, da $6\,\text{Integer} \cdot 2\,\frac{\text{B}}{\text{Integer}} = 12\,\text{B}$ oder (wie in SIKAF) minimal 20 bit, da $10^6{}_{(10)} = 1111\,0100\,0010\,0100\,0000_{(2)}$.

Fahrzeugbezogene Nachrichteninhalte Mit fahrzeugbezogenen Inhalten werden Informationen in zwei Richtungen übertragen: Einerseits dienen sie als Träger der Regelgröße (Istwert) von Fahrzeugen zum Fahrzeugleitsystem, um dieses mit aktuellen Informationen über die Fahrzeugtrajektorien zu versorgen. Andererseits wird mit fahrzeugbezogenen Nachrichten die Führungsgröße (Sollwert) vom Fahrzeugleitsystem zu den einzelnen Fahrzeugen übertragen, nachdem diese vom Fahrzeugleitsystem berechnet wurde. Das Datenmodell der fahrzeugbezogenen Nachrichten ist in beiden Fällen identisch. Im Gegensatz zu streckenbezogenen Nachrichten muss immer der Empfänger angegeben werden (bei der streckenbezogenen Nachricht ist der Empfänger stets das Relais, welches die weitere Nachrichtenvermittlung veranlasst). Aus diesen Annahmen ergibt sich eine gegenüber den streckenbezogenen Nachrichten leicht veränderte Übersicht, die in Tabelle 5.19 zusammengestellt ist.

Tabelle 5.19: Klassifikation der Nachrichteninhalte (fahrzeugbezogen)

Nachrichteninhalt	Datenmenge gesamt	davon codiert	davon maskierbar
Nachrichtenspezifikationen	152 bit	127 bit	64 bit
Attribute	7 bit	7 bit	6 bit
Trajektorie	224 bit	33 bit	223 bit
Kraftstoff	12 bit	5 bit	11 bit
Freitext	142 bit	2 bit	140 bit
Prüfsumme	20 bit	0 bit	20 bit
Maskenanzeiger	80 bit	0 bit	0 bit
Summe	637 bit	174 bit	464 bit

Für die Verwendung von Codes sind die folgenden Inhalte vorgesehen:

- Bei den Nachrichtenspezifikationen lassen sich der Zeitstempel nach dem IRIG-Format codieren sowie die dID des Senders und des Empfängers mit einem beliebigen Datum wie dem Kfz-Kennzeichen verknüpfen.
- Zusätzliche Fahrzeugattribute werden tabelliert und mit Codes versehen.
- Zur Verortung werden alle Straßen einer digitalen Karte tabelliert.
- Mögliche Kraftstoffe werden in einer Liste vorcodiert.

Die weiteren Inhalte sind stetige Größen, die abhängig von der geforderten Genauigkeit in voller Länge übertragen werden.

Eine Maskierung kann für folgende Inhalte angezeigt sein:

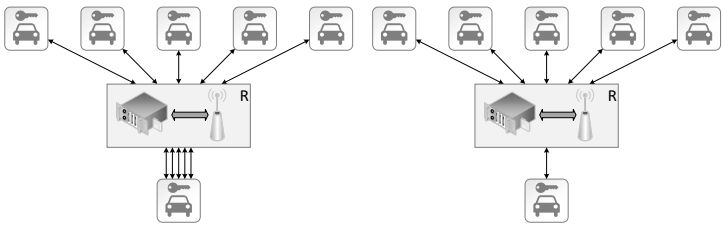
- Bei den Fahrzeugspezifikationen können die dID von Sender und Empfänger maskiert oder pseudonymisiert werden, wenn keine personenbeziehbaren Daten im Klartext übertragen werden sollen.
- In den Attributen sind Angaben über Funktion und Ladung von Fahrzeugen enthalten, die aus Gründen der Geheimhaltung maskiert werden können.

- Durch Protokollieren der Koordinaten wären systematische Auswertungen und damit die Nachverfolgung von Fahrzeugen möglich, weshalb die Trajektorien maskiert werden können.
- Der Freitext ist abhängig von den konkreten Inhalten zu maskieren.
- Wie bei den streckenbezogenen Nachrichten ist die Prüfsumme zur Gewährleistung der Nachrichtenintegrität und -authentizität immer zu maskieren.

Auch bei den fahrzeugbezogenen Nachrichten stellt folglich die Länge der Prüfsumme die mindestens zu maskierende Datenmenge dar.

5.2.6 Benötigte Maskengröße

In Kapitel 3 wurde der erhebliche Umfang der benötigten Maskengröße als ein möglicher praktischer Nachteil perfekt sicherer Verschlüsselung und damit als Hindernis beim Einsatz in einem Fahrzeugleitsystem identifiziert. Es soll daher untersucht werden, wie groß die zum Einsatz als Masken benötigte Datenmenge tatsächlich ist, um einen Maskenvorrat ausreichend dimensionieren zu können. Dabei ist zu beachten, dass Masken nicht nur zur *Ver*schlüsselung, sondern insbesondere auch zur *Ent*schlüsselung benötigt werden. Wenn ein Fahrzeug die Nachrichten aller anderen Fahrzeuge empfängt, führt dies zu einer stark erhöhten Maskengröße, da in diesem Übertragungsfall eine $n : 1$-Beziehung vorliegt (Abbildung 5.5 links). Dieses Problem tritt auch dann auf, wenn das Relais die Nachrichten aller Fahrzeuge lediglich durchleitet, wie es aktuelle Konzepte vorsehen, die den Infrastrukturmodus zugrunde legen. Der Vorteil von SIKAF liegt hingegen darin, dass das Relais die Nachrichten vorverarbeitet und nur konsolidierte Informationen an das betroffene Fahrzeug weiterleitet. Das Relais erfüllt damit die Funktion eines Verteilers (engl. *switch*). Der Maskennachschub für das Relais kann aufgrund der festen Verbindung zur hoheitlichen Behörde als unkritisch angesehen werden. Können Informationen durch das Fahrzeugleitsystem gebündelt und in kombinierten Nachrichten durch das Relais verschickt werden (Abbildung 5.5 rechts), so wird beim empfangenden Fahrzeug auch nur jeweils eine Maske benötigt. In diesem Übertragungsfall liegt eine $1 : 1$-Beziehung vor.



(a) $n : 1$-Beziehung **(b)** $1 : 1$-Beziehung

Abbildung 5.5: Kardinalität der Nachrichtenübertragung

Folgende Faktoren haben einen Einfluss auf die benötigte Maskengröße G_K in einem Fahrzeug w, in Klammern sind die jeweiligen Maßeinheiten angegeben:

- Datenmenge D des zu maskierenden Nachrichtenteils ($[D] = \text{bit}$)
- Sendefrequenz f_{send} maskierter Nachrichten ($[f_{send}] = \text{Hz}$)
- Empfangsfrequenz f_{empf} maskierter Nachrichten ($[f_{empf}] = \text{Hz}$)
- Aktivitätsdauer t_A von SIKAF ($[t_A] = \text{s}$)

Die Aktivitätsdauer t_A kann sich aus Teilaktivitätsdauern t'_A zusammensetzen, sodass sich für die gesamte Aktivitätsdauer ergibt: $t_A = \sum t'_A$. Datenmenge D, Sendefrequenz f_{send} und Empfangsfrequenz f_{empf} sind nicht konstant, sondern abhängig von der aktuellen Fahr- und Umgebungssituation, welche unterschiedliche Übertragungsintervalle notwendig machen können. Die Fahr- und Umgebungssituation ist wiederum abhängig von Ort und Zeit des betroffenen Fahrzeugs. Da der Ort als eine Funktion der Zeit angenommen werden kann, gilt ohne Beschränkung der Allgemeinheit:

- $D = D(t)$
- $f_{send} = f_{send}(t)$
- $f_{empf} = f_{empf}(t)$

Eine zusätzliche Unterscheidung bei den Parametern Datenmenge $D(t)$, Sendefrequenz $f_{send}(t)$ und Empfangsfrequenz $f_{empf}(t)$ muss in fahrzeugbezogene und streckenbezogene Nachrichten vorgenommen werden, da die Frequenzen und Datenmengen situationsabhängig variieren können. Die Unterscheidung wird mit den zusätzlichen Indizes b für streckenbezogen und w für fahrzeugbezogen kenntlich gemacht. Die benötigte Maskengröße G_K kann mit diesen Eingangsgrößen und unter Berücksichtigung von Gleichung 4.4 dann nach folgender Formel berechnet werden:

$$G_K \geq \sum_{t'_A} \int_{t'_A} \Big[\big(f_{send_b}(t) + f_{empf_b}(t) \big) \cdot D_b(t) + \big(f_{send_w}(t) + f_{empf_w}(t) \big) \cdot D_w(t) \Big] dt \quad (5.4)$$

Die (Teil-)Aktivitätsdauern müssen geeignet bestimmt werden, um die jeweils benötigte Maskengröße und damit die Kapazität der Festwertspeicher zu bestimmen. Sollte ein Festwertspeicher nicht ausreichend sein, müssen kürzere (Teil-)Aktivitätsdauern oder zusätzliche Wartungsintervalle für den Maskennachschub vorgesehen werden.

Für die genannten Parameter liegen keine Erfahrungswerte vor, da keine Referenzimplementierung des vorgestellten Fahrzeugleitsystems existiert. Im Folgenden werden daher vier Szenarien betrachtet, um die Spanne der benötigten Maskengröße abzuschätzen. Die für die einzelnen Parameter getroffenen Annahmen werden im Einzelnen erläutert.

Der Parameter, der alle Szenarien gleichermaßen betrifft, ist die Aktivitätsdauer von SIKAF t_A. Hierzu würde zunächst die Betriebsdauer eines Fahrzeugs benötigt, für die sich jedoch kaum belastbare Quellen finden lassen. Besser dokumentiert ist die Fahrleistung von Kraftfahrzeugen (Verkehr in Kilometern (VK) mit [VK] = km). Zusammen mit der durchschnittlichen Reisegeschwindigkeit v_R in den unterschiedlichen Szenarien kann die Teilaktivitätsdauer für ein Jahr t'_A nach

$$t'_A = \frac{\text{VK}}{v_R} \quad (5.5)$$

bestimmt und auf Fahrzeug (Fz) und Jahr (a) bezogen werden. Offizielle Statistiken weisen für Deutschland folgende Werte aus, die für die nachfolgenden Berechnungen benötigt werden [18]:

- Länge der öffentlichen Straßen (ohne Gemeindestraßen): 229 800 km
  - Bundesautobahnen: 13 100 km
  - Bundesstraßen: 37 900 km
  - Landesstraßen: 86 900 km
  - Kreisstraßen: 91 900 km
- Länge der Gemeindestraßen: 659 000 km
- Durchschnittliche Fahrleistung ($\frac{\mathrm{VK}}{\mathrm{a\,Fz}}$) pro Jahr: 13 700 $\frac{\mathrm{km}}{\mathrm{a\,Fz}}$

Mit der Gleichung 1 a = 8760 h und der Umrechnung 13 700 $\frac{\mathrm{km}}{\mathrm{a\,Fz}} \approx 1{,}56\ \frac{\mathrm{km}}{\mathrm{h\,Fz}}$ kann ein anderer Bezugswert gewählt werden, da sich der Verkehr in Kilometern (VK) auf ein Kalenderjahr bezieht.

Szenario 1: Mindestens benötigte Maskengröße Wird das vorgestellte Fahrzeugleitsystem zur vollautomatischen Fahrzeuglenkung eingesetzt, können für ein Fahrzeug theoretisch alle Geschwindigkeiten gewählt werden, für die die Fahrzeugmechanik ausgelegt ist. Für dieses Szenario wird eine konstante Reisegeschwindigkeit von 130 km/h gewählt, da damit weitere Randbedingungen wie Lärmschutz und Komfort der Passagiere erfüllt sind. Sie entspricht zudem der derzeitigen Geschwindigkeitsbegrenzung in vielen Staaten. Nach Gleichung 5.5 ergibt sich die Aktivitätsdauer von SIKAF bezogen auf ein Jahr zu $t'_A = \frac{13\,700\,\mathrm{km}}{130\,\mathrm{km/h}} \approx 105\,\mathrm{h}$. Bei automatischer Fahrzeuglenkung wird das Fahrzeug allein über fahrzeugbezogene Nachrichten gesteuert. Die Übertragung streckenbezogener Meldungen wäre somit grundsätzlich nicht notwendig, da alle benötigten Stellgrößen durch das Fahrzeugleitsystem ermittelt werden. Zur Gewährleistung funktionaler Sicherheit muss das Fahrzeug jedoch auch zu einem autarken Betrieb fähig sein. Aus diesem Grund müssen ständig die benötigten Informationen zum Straßenzustand vorliegen, die mit streckenbezogenen Nachrichten übertragen werden. In diesem Szenario wird ferner die kleinste vorgesehene Nachrichtenfrequenz von $f_{send_b} = f_{empf_b} = f_{send_w} = f_{empf_w} = f_{min} = 1\,\mathrm{Hz}$ und lediglich die Prüfsumme mit $D_b = D_w = D_{min} = 20\,\mathrm{bit}$ als zu maskierender Nachrichtenteil angenommen. Eine weitere Reduzierung ist nicht möglich, da ansonsten die Authentizität der Nachrichten nicht sichergestellt werden kann. Mit diesen Annahmen ergibt sich die Maskengröße gemäß Gleichung 5.4 zu

$$G_{min} \geq t'_A \cdot 4 \cdot f_{min} \cdot D_{min} = 105\,\mathrm{h} \cdot 3600\,\frac{\mathrm{s}}{\mathrm{h}} \cdot 4 \cdot 1\,\mathrm{Hz} \cdot 20\,\mathrm{bit} = 30\,240\,000\,\mathrm{bit} = 3\,780\,000\,\mathrm{B} \quad (5.6)$$

bei einer typischen Fahrleistung eines Fahrzeugs in einem Jahr. In jedem Fahrzeug wird dazu eine Maskengröße von rund 3,60 MiB benötigt[6].

[6] bei Umrechnung von 1 MiB = 1024 KiB = 1024 × 1024 B

Szenario 2: Benötigte Maskengröße bei manueller Fahrzeuglenkung Bei manueller Fahrzeuglenkung durch einen menschlichen Fahrer sind die kinetischen Parameter weiteren Einschränkungen unterworfen, insbesondere können Fahrzeugabstände und -geschwindigkeiten nur in limitierten Bereichen liegen. Im Jahre 2020 wird die Reisegeschwindigkeit im deutschsprachigen Raum für Kraftfahrzeuge über Land mit rund 60 km/h angegeben, kann innerorts jedoch unter die Geschwindigkeit von Fahrrädern (mit rund 15 km/h angegeben) sinken [166]. Daher wird in diesem Szenario von einem Durchschnittswert von 36 km/h ausgegangen, der jedoch grundsätzlich anpassbar ist. Ein Empfang fahrzeugbezogener Nachrichten mit hoher Frequenz ist nicht erforderlich, da das Fahrzeug manuell geregelt wird: $f_{send_w} = f_{empf_w} = 0$ und $D_w = 0$. Dafür müssen die Informationen über das Straßennetz durch streckenbezogene Nachrichten hochaktuell gehalten werden, damit der Fahrer seine Route optimal planen kann. Mit $f_{send_b} = f_{empf_b} = f_{man} = 5\,\text{Hz}$ wird eine hohe Frequenz zur Abschätzung einer oberen Schranke für die benötigte Maskengröße in diesem Szenario angenommen. Es werden keine Inhalte, sondern wiederum lediglich die Prüfsumme maskiert, da die streckenbezogenen Informationen ohnehin für alle Verkehrsteilnehmer zugänglich sein sollen. Die Authentizität der Nachrichten wird mit einer Datenmenge von $D_b = D_{man} = 20\,\text{bit}$ abgesichert. Nach Gleichung 5.5 ergeben sich die Aktivitätsdauer von SIKAF bei der Fahrleistung eines Jahres zu $t'_A = \frac{13\,700\,\text{km}}{36\,\text{km/h}} \approx 381\,\text{h}$ und nach Gleichung 5.4 die benötigte Maskengröße zu

$$\begin{aligned} G_{man} &\geq t'_A \cdot 2 \cdot f_{man} \cdot D_{man} = 381\,\text{h} \cdot 3600\,\frac{\text{s}}{\text{h}} \cdot 2 \cdot 5\,\text{Hz} \cdot 20\,\text{bit} \\ &= 274\,320\,000\,\text{bit} = 34\,290\,000\,\text{B} \end{aligned} \tag{5.7}$$

bei einer typischen Fahrleistung eines Fahrzeugs in einem Jahr. In jedem Fahrzeug wird dazu eine Maskengröße von rund 32,70 MiB benötigt.

Szenario 3: Benötigte Maskengröße bei automatischer Fahrzeuglenkung Zur Annäherung an eine obere Grenze der benötigten Maskengröße bei automatischer Fahrzeuglenkung werden die Parameter auf die Maximalwerte heutiger Fahrzeugnutzung gesetzt: Die fahrzeugbezogenen und streckenbezogenen Nachrichten werden mit einer Frequenz von $f_{send_b} = f_{empf_b} = f_{send_w} = f_{empf_w} = f_{auto} = 10\,\text{Hz}$ aktualisiert, was in den bestehenden Standards aktuell als eine obere Grenze angenommen wird [61, 62]. Ferner wird davon ausgegangen, dass die vollständigen Nachrichten mit einer Datenmenge von $D_b = 626\,\text{bit}$ (streckenbezogen) und $D_w = 637\,\text{bit}$ (fahrzeugbezogen) maskiert werden. Beides stellt eine obere Schranke dar, da auch die nicht zu maskierenden Inhalte wie Maskenanzeiger und Maskierungsindikator in die Berechnung mit einfließen. Es wird wiederum eine konstante Reisegeschwindigkeit von 130 km/h angenommen, da das Fahrzeug vollständig automatisch geregelt wird. Nach Gleichung 5.5 ergeben sich $t'_A = \frac{13\,700\,\text{km}}{130\,\text{km/h}} \approx 105\,\text{h}$ und nach Gleichung 5.4 die benötigte Maskengröße zu

$$\begin{aligned} G_{auto} \geq\ & t'_A \cdot (2 \cdot f_{auto} \cdot D_b + 2 \cdot f_{auto} \cdot D_w) \\ &= 105\,\text{h} \cdot 3600\,\frac{\text{s}}{\text{h}} \cdot (2 \cdot 10\,\text{Hz} \cdot 626\,\text{bit} + 2 \cdot 10\,\text{Hz} \cdot 637\,\text{bit}) \\ &= 9\,548\,280\,000\,\text{bit} = 1\,193\,535\,000\,\text{B} \end{aligned} \tag{5.8}$$

bei einer typischen Fahrleistung eines Fahrzeugs in einem Jahr. In jedem Fahrzeug wird dazu eine Maskengröße von rund 1,11 GiB benötigt[7].

[7] bei Umrechnung von $1\,\text{GiB} = 1024\,\text{MiB} = 1024 \times 1024\,\text{KiB} = 1024 \times 1024 \times 1024\,\text{B}$

Szenario 4: Maximal benötigte Maskengröße Durch autonome Fahrzeuge könnte sich die tägliche Betriebsdauer von Kraftfahrzeugen deutlich erhöhen, da diese Fahrzeuge keinen Limitationen durch Bedürfnisse menschlicher Fahrer unterworfen sind. Zur Bestimmung einer oberen Grenze der benötigten Maskengröße wird eine tägliche Betriebsdauer von 20 h angenommen, folglich 7300 h pro Jahr. Damit bestehen keine Einschränkungen hinsichtlich Lenk- und Ruhezeiten eines autonomen Fahrzeugs und es sind dennoch Standzeiten für Wartung und Kraftstoffzufuhr berücksichtigt. Auch die weiteren Parameter werden mit $f_{send_b} = f_{empf_b} = f_{send_w} = f_{empf_w} = f_{max} = 10\,\mathrm{Hz}$, $D_b = 626\,\mathrm{bit}$ (streckenbezogen) und $D_w = 637\,\mathrm{bit}$ (fahrzeugbezogen) auf die jeweils maximalen Werte gesetzt. Damit ergibt sich die benötigte Maskengröße nach Gleichung 5.4 zu

$$\begin{aligned} G_{max} &\geq t'_A \cdot (2 \cdot f_{max} \cdot D_b + 2 \cdot f_{max} \cdot D_w) \\ &= 7300\,\mathrm{h} \cdot 3600\,\frac{\mathrm{s}}{\mathrm{h}} \cdot (2 \cdot 10\,\mathrm{Hz} \cdot 626\,\mathrm{bit} + 2 \cdot 10\,\mathrm{Hz} \cdot 637\,\mathrm{bit}) \\ &= 663\,832\,800\,000\,\mathrm{bit} = 82\,979\,100\,000\,\mathrm{B} \end{aligned} \tag{5.9}$$

bei der Fahrleistung eines hypothetischen autonomen Fahrzeugs in einem Jahr. In jedem Fahrzeug wird damit eine Maskengröße von rund 77,28 GiB benötigt.

Quantelung und Indizierung der Masken Die kleinste in einem Vorgang zu maskierende Datenmenge ist die Prüfsumme mit 20 bit. Es ist daher naheliegend, die in Unterabschnitt 2.6.3 eingeführte Maskenlänge mit $|k| = 20\,\mathrm{bit}$ zu wählen, sodass jede einzeln verwendete Maske ebendiese Länge hat. Im Maximalszenario werden somit für eine Betriebsdauer von 30 Jahren[8]

$$\frac{30 \cdot G_{max}}{|k|} = \frac{30 \cdot 663\,832\,800\,000\,\mathrm{bit}}{20\,\mathrm{bit}} = 995\,749\,200\,000 \tag{5.10}$$

Masken von je 20 bit Länge benötigt. Für den Maskenanzeiger wurden 40 bit veranschlagt, sodass insgesamt $2^{40} = 1\,099\,511\,627\,776$ Masken indiziert werden können. Gemäß dem Resultat von Gleichung 5.10 ist dies zur Indizierung aller Masken ausreichend, die im Maximalszenario während der Lebensdauer eines Fahrzeugs benötigt werden. Dies gilt selbst dann, wenn die Masken einzeln anstatt durch Angabe von Anfang und Ende verkettet indiziert werden oder wenn der Maskenvorrat aus nicht absehbaren Gründen weiter vergrößert werden muss.

Im vorgestellten Datenmodell sind die Inhalte der mit SIKAF ausgetauschten Nachrichten zu einem großen Teil tabelliert, dennoch bleibt die Möglichkeit zur freiformatigen Übertragung von Inhalten im *Freitext*-Bereich erhalten. Durch das festgelegte Datenmodell wird die Prüfung von Nachrichten auf unerwünschte Inhalte erleichtert und diese können bei der Vermittlung markiert oder als Spam aussortiert werden. Mittels der eindeutigen Senderkennung kann das verursachende Fahrzeug identifiziert und bei anhaltendem Versenden von Spam in SIKAF blockiert werden.

Im Fall eines zur Neige gehenden Maskenvorrats könnte eine entsprechende Warnung versendet werden. Die mit einem Maskenvorrat mögliche Betriebsdauer übersteigt jedoch

[8] Mindestbetriebsdauer für das H-Kennzeichen nach § 23 StVZO, die bei täglichem Fahrzeugbetrieb von 20 h jedoch kaum erreichbar ist. Die Schätzung der aus dem Maximalszenario hergeleiteten Maskengröße wird daher als hinreichend hoch angenommen.

die Dauer eines typischen Wartungsintervalls. Es reicht daher aus, die verbleibenden Masken im Rahmen einer Fahrzeugwartung passiv zu überprüfen und somit auf eine aktive Warnung zu verzichten.

Die angestellten Berechnungen dienen allein einer Abschätzung der Maskengröße. Die Datagramme können Datenmengen bis zu der durch SIKAF-P vorgegebenen Obergrenze annehmen. Darüber hinausgehende Informationen müssen auf mehrere Datagramme aufgeteilt werden; ein Datagramm muss gemäß Protokoll jedoch immer eine in sich abgeschlossene Information transportieren. Die Aufteilung von Inhalten auf mehrere Datagramme in einer Form, die eine Sequenzkontrolle notwendig macht, ist nicht zulässig.

Abschließend sei betont, dass es sich hierbei um Beispielrechnungen handelt. Die Variation eines jeden Parameters kann zu teilweise erheblichen Abweichungen bei den Ergebnissen führen. Hierzu zählt nicht zuletzt die Länge der Prüfsumme, die das Sicherheitsniveau der Nachrichtenintegrität mitbestimmt. Durch Berechnungen in einem moderaten Szenario konnte insgesamt gezeigt werden, dass die Bevorratung von Masken für mehrere Jahre auf Festwertspeichern marktgängiger Kapazität möglich ist.

5.2.7 Softwarearchitektur

Zur Programmierung der Prototypen wird, soweit möglich, freie Software eingesetzt. Damit wird zum einen ihre Validierung durch einen großen Anwenderkreis (engl. *community*) und zum anderen ihre weitere Verwendung ohne aufwändige lizenzrechtliche Betrachtung ermöglicht. Alle Komponenten sind hier in der Unified Modeling Language (UML) dargestellt, was Überprüfung und Implementierung der Konzepte ermöglicht. Die Software ist in zweierlei Hinsicht modular erstellt. Zum einen werden die Funktionen der einzelnen SIKAF-Komponenten gegeneinander abgegrenzt. Zum anderen werden auf jeder Komponente die Speicher für Daten und Programme getrennt. SIKAF wird somit nicht nach der verbreiteten *Von-Neumann*-Architektur erstellt, sondern orientiert sich an der *Harvard*-Architektur.

Abbildung 5.6 zeigt das UML-Klassendiagramm für die Software auf den SIKAF-Hierarchieebenen hoheitliche Behörde, Relais und Fahrzeuge, wobei jede Ebene in einem UML-Paket abgegrenzt ist. Das Paket der hoheitlichen Behörde ist in der Mitte und nicht wie in der organisatorischen Darstellung an erster Stelle platziert, um alle Abhängigkeiten übersichtlich abbilden zu können. Die dargestellten Klassen bilden die softwaretechnischen Implementierungen der in Kapitel 4 vorgestellten Konzepte. Die Klassen sind zumeist in *Python* geschrieben. Die einzelnen Python-Programme werden durch Shell-Skripte aufgerufen, die wiederum direkt durch die Prozessverwaltung des Betriebssystems ausgeführt und (zeit)gesteuert werden.

Hoheitliche Behörde Das Paket der hoheitlichen Behörde beinhaltet als zentrales Element die abstrakte Klasse *Maske*. Diese Klasse kann nicht instanziiert werden, sondern von ihr leiten sich die konkreten Klassen *MaskeRelais* und *MaskeFahrzeug* ab. Entsprechend dem in Abschnitt 4.5 vorgestellten Verfahren werden Instanzen dieser abgeleiteten Klassen als Masken sowohl bei den vernetzten Fahrzeugen als auch beim Relais hinterlegt. Die Masken werden durch eine Instanz des *Zufallszahlengenerators* erzeugt, für den Empfängerkreis aufbereitet und mit einem Maskenanzeiger indiziert. Im UML-Paket der hoheitlichen Behörde ist zudem *RechteRollen* als Klasse zur Festlegung und Vergabe der

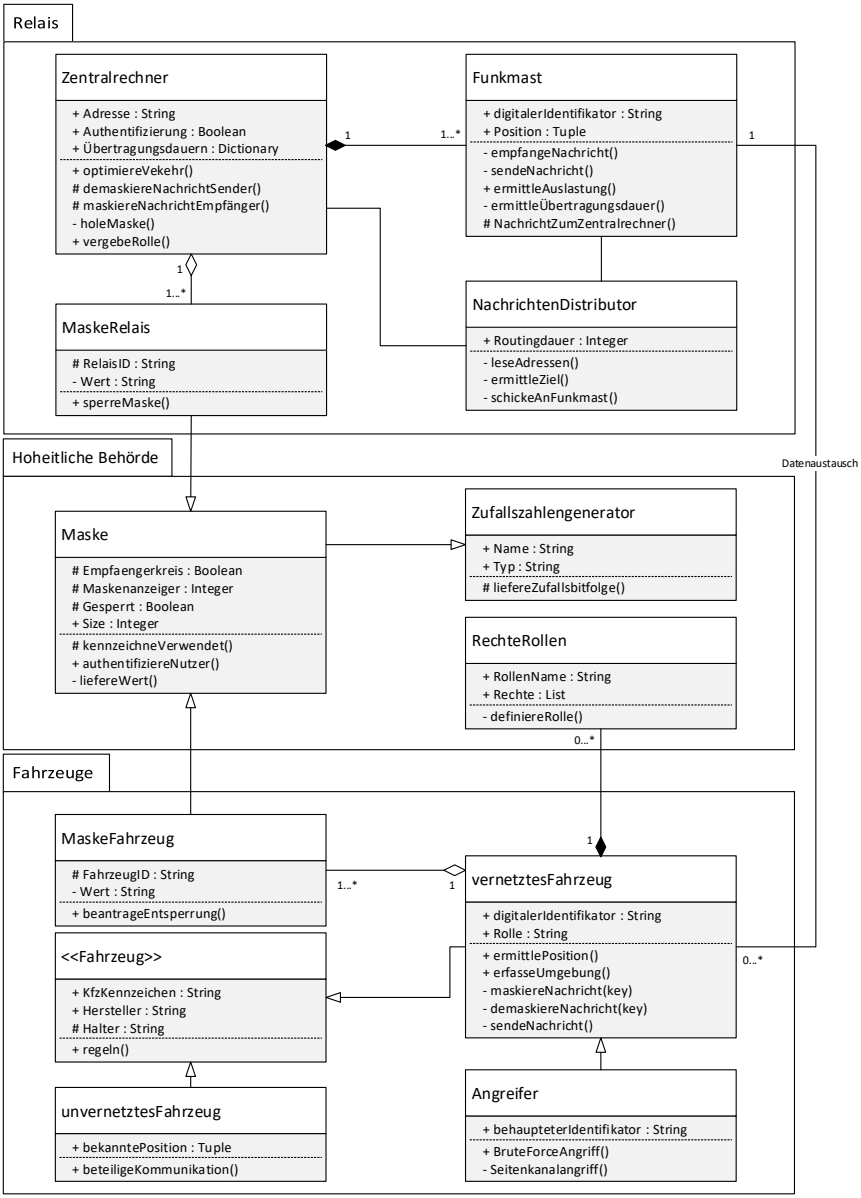


Abbildung 5.6: UML-Klassendiagramm von SIKAF

Berechtigungen an vernetzte Fahrzeuge enthalten. Jede Benutzerrolle umfasst eine Menge von Rechten, die als Liste zusammengefasst und den Fahrzeugen zugeteilt werden.

Relais Das UML-Paket des Relais beinhaltet die Klasse zur Instanziierung genau eines *Zentralrechners*, der die Methoden zur Verkehrsoptimierung und zur Nachrichtenverarbeitung implementiert. Die Datenübertragung zu den vernetzten Fahrzeugen findet über mindestens einen *Funkmast* statt, dessen Eigenschaften durch die entsprechende Klasse spezifiziert sind. Die Nachrichten werden über einen *NachrichtenDistributor* zum Empfänger vermittelt. Durch Instanzen der Klasse *MaskeRelais* verfügt das Relais über die zur Demaskierung notwendigen Masken. Bei der Instanziierung der Klasse *MaskeRelais* ist zu beachten, dass für die Attribute keine beliebigen Werte gesetzt werden können. Werte für das geerbte Attribut *Wert* sind vielmehr durch die abstrakte Klasse *Maske* so vorgegeben, dass zu jeder Instanz von *MaskeRelais* ein kryptografisches Gegenstück als Instanz von *MaskeFahrzeug* existiert.

Fahrzeuge Zentrales Element dieses UML-Pakets ist die abstrakte Klasse *Fahrzeug*, aus der sich die konkreten Klassen *vernetztesFahrzeug* und *unvernetztesFahrzeug* ableiten. Durch Vererbung entsteht zudem ein *Angreifer*, welcher alle Funktionalitäten der Klasse *vernetztesFahrzeug* nutzt und um zusätzliche Attribute und Methoden erweitert, die zur widerrechtlichen Aneignung von Rechten und Rollen dienen sollen. Instanzen der Klasse *MaskeFahrzeug* besitzen stets ein Gegenstück in Form einer Instanz der Klasse *MaskeRelais*, die beide aus der abstrakten Klasse *Maske* abgeleitet werden. Diese sich entsprechenden Instanzen bilden die Masken, mit denen eine durch das Fahrzeug maskierte und durch das Relais übertragene Nachricht demaskiert oder authentifiziert wird.

Die Implementierungen bauen auf bekannten Konzepten zur perfekt sicheren Verschlüsselung in der Automatisierungstechnik auf [158]. In SIKAF werden die Funktionen des „Leitmoduls“ von der hoheitlichen Behörde und die Funktionen des „Kryptomoduls“ von Fahrzeug und Relais implementiert. Technisch stellt diese Aufteilung auf zwei Typen von Kryptomodulen somit eine Erweiterung der bekannten Konzepte dar. Organisatorisch ist SIKAF in eine hierarchische Struktur eingebunden, was über die bekannten Konzepte hinaus eine feinere Ausdifferenzierung von Rechten und Rollen ermöglicht. Hard- und Software können prinzipiell unabhängig voneinander implementiert werden. Bestehende Verkehrssysteme können somit entweder durch entsprechende Komponenten nachgerüstet werden oder die Software wird auf bereits vorhandenen Komponenten installiert und konfiguriert. Dies setzt jedoch voraus, dass die vorhandene Hardware den vorgestellten Spezifikationen entspricht und auch entsprechend geprüft wurde.

5.3 Funktionale Sicherheit von Fahrzeugleitsystemen

In Abschnitt 2.5 wurden die Anforderungen an die funktionale Sicherheit eines Fahrzeugleitsystems dargestellt. Zur Implementierung in SIKAF ist die Norm ISO 26262 als Anpassung der Norm IEC 61508 anzuwenden, da es sich um ein System zur Steuerung von Kraftfahrzeugen handelt.

5.3.1 Status und Abgrenzung

Mit der Entwicklung eines Prototyps wurden alle Phasen des Produktlebenszyklus bis zur Inbetriebnahme umgesetzt. Die mit der Interaktion der Komponenten eintretenden Wechselwirkungen ermöglichen, die funktionale Sicherheit des Gesamtsystems zu evaluieren. Ziele der ISO 26262 sind Vermeidung systematischer Fehler und Beherrschung zufälliger Fehler. Die ISO 26262 fordert zum Nachweis

- die Inspektion des Systementwurfs,
- die Evaluierung des Prototyps oder alternativ die Simulation des Systems sowie
- die Analyse des Systementwurfs.

Die funktionale Sicherheit kann daher abschließend erst im Rahmen der Projektierung eines Produktivbetriebs analysiert werden, der auch die örtlichen Gegebenheiten und Besonderheiten des jeweiligen Verkehrssystems berücksichtigt [149]. Für den zentralen Bereich Kommunikation können hier jedoch bereits allgemeine Methoden zur Vermeidung systematischer Fehler und zur Kontrolle zufälliger Fehler vorgestellt werden.

5.3.2 Vermeidung systematischer Fehler

Der erste Schritt zur Vermeidung systematischer Fehler ist striktes Qualitätsmanagement bei der Produktion der Komponenten, die beim Produktivbetrieb zum Einsatz kommen. Systematische Fehler im Entwurf von Kommunikationsarchitekturen fallen dann auf, wenn erfolgreiche Angriffe auf diese Kommunikationsarchitekturen bekannt werden. Der wichtigste Ansatz zur Vermeidung systematischer Fehler in SIKAF ist daher die Analyse bekannter Angriffsvektoren auf Kommunikationssysteme, um SIKAF inhärent sicher zu konzipieren und stets geeignete Gegenmaßnahmen ergreifen zu können. Typische Angriffsvektoren auf Kommunikationssysteme wie SIKAF und deren Abwehr sind die Folgenden:

Unautorisiertes Auslesen von Informationen aus Massenspeichern Ist der Haupt- oder Arbeitsspeicher eines Teilnehmers unzureichend geschützt, können aus diesem sicherheitsrelevante Informationen wie Passwörter oder andere Sicherheitsparameter ausgelesen werden. Ein zentrales Angriffsziel ist dabei das Relais, da dieses die Passwörter aller Kommunikationsteilnehmer speichert.

Solches Auslesen wird in SIKAF verhindert, indem Speicher für Daten und Programme strikt getrennt sind. Programme, die auf Massen- oder Arbeitsspeicher zugreifen, können nur nach authentifizierter Offenbarung der Programmfunktionalität ausgeführt werden. Somit erhalten nur authentifizierte und autorisierte Nutzer Zugriff auf die Inhalte von Datenspeichern.

Identitätsdiebstahl und Klon-Attacken Ein Angreifer kann versuchen, sich durch Kopieren digitaler Identifikationsmerkmale als ein beliebiger Teilnehmer auszugeben und damit dessen Rechte und Rollen missbräuchlich zu verwenden. Der Angreifer kann sich dadurch als legitimer Teil des Netzes ausgeben und dieses zu seinen Zwecken beeinflussen. Ein solcher Angriff ist in Mobilfunknetzen, die nach dem GSM-Standard arbeiten, vergleichsweise einfach möglich, da sich Funkmasten nicht gegenüber dem Teilnehmer authentisieren müssen [134].

In SIKAF wird dies durch Authentifizierung bei der Maskenübergabe verhindert. Das Relais muss sich beim Empfang von Masken gegenüber der hoheitlichen Behörde authentisieren. Fahrzeuge und Relais müssen sich bei Maskenübergabe und -übernahme gegenseitig authentifizieren, wodurch lückenlose Authentifizierungsketten sichergestellt sind. So ausgetauschte Masken werden zum Maskieren oder Signieren von Nachrichten eingesetzt. Aufgrund der perfekt sicheren Verschlüsselung ist es völlig ausgeschlossen, die Maskierungen zu brechen.

Angreifer, die sich missbräuchlich als Relais ausgeben, können abgefangene Nachrichten dann ebenso wenig sinnhaft demaskieren wie Angreifer, die sich missbräuchlich als berechtigte Empfänger ausgeben. Beide Angreifer verfügen zu keinem Zeitpunkt über korrekte Masken.

Lausch- und *Man in the Middle*-Angriffe Aufgrund der drahtlosen Übertragung ist SIKAF Lausch- und *Man in the Middle (MITM)*-Angriffen ausgesetzt. Ohne Gegenmaßnahmen können Angreifer Nachrichten abfangen und verändern. Diese Integritätsverletzungen werden in SIKAF verhindert, indem perfekt sichere Einmalverschlüsselung eingesetzt wird und gleichzeitig ein Verfahren sowie ein sicherer Kanal zum Verteilen der benötigten Masken zur Verfügung stehen. Der Erstkontakt zwischen zwei Teilnehmern wird dadurch nie über einen unsicheren Kanal hergestellt, der meist das Einfallstor für MITM-Angriffe bei asymmetrischen Kryptosystemen darstellt. Damit ist der entscheidende Angriffspunkt für Lausch- und MITM-Angriffe unschädlich gemacht.

Verbreiten falscher Informationen Angreifer können versuchen, falsche Informationen durch SIKAF zu verbreiten, um missbräuchliches Systemverhalten herbeizuführen. Eine geeignete Gegenmaßnahme ist es, einzelne Informationen stets von weiteren Teilnehmern bestätigen zu lassen, bevor sie vom Fahrzeugleitsystem übernommen werden. Eine konkrete Möglichkeit ist die Mehrheitsentscheidung durch mehrere Fahrzeuge, wobei das Fahrzeugleitsystem entsprechend zu parametrieren ist, welche Teilnehmer zu einer solchen Bestätigung berechtigt sind. Alternativ kann die hoheitliche Behörde nur bestimmte Fahrzeuge mit speziellen Rechten zur Verifikation von Informationen ausstatten.

VANets sind anfällig für Sybil-Attacken, bei denen ein Angreifer Pseudonyme erstellt und mit diesen falschen Identitäten im Netz agiert [144]. Dieser Angriff ist ein großes Problem bei Mehrheitsentscheidungen oder wenn derart kompromittierte Teilnehmer ihre Rolle im Netz missbräuchlich verwenden. In SIKAF können keine beliebigen Instanzen von Kommunikationsteilnehmern erzeugt werden, da die benötigten Identifikatoren von der hoheitlichen Behörde erstellt und verteilt werden. Sybil-Attacken werden folglich inhärent unterbunden, da das Relais keine Informationen von Fahrzeugen weiterleitet, die sich nicht mit einer passenden Maske authentisieren können. Fahrzeuge, die Informationen verbreiten, welche sich als falsch herausstellen, werden bei der künftigen Bestätigung von Informationen nicht mehr berücksichtigt.

5.3.3 Beherrschung zufälliger Fehler

Eine wichtige Entwurfsentscheidung zur Vermeidung zufälliger Fehler ist die technische und organisatorische Aufteilung in die drei Ebenen Fahrzeug, Relais und hoheitliche Behörde. Zum einen bleiben zufällig auftretende Fehler damit auf die jeweilige Ebene begrenzt. Zum

anderen erlaubt dies die Durchführung von Systemtests getrennt für jede Ebene, unter kontrollierten Bedingungen und in großer Zahl. Konkrete Testverfahren wurden zu Beginn dieses Kapitels vorgestellt.

Fähigkeit zum autonomen Betrieb Dennoch auftretenden, zufälligen Fehlern wird zunächst begegnet, indem bei Ausfall oder Fehlfunktion von SIKAF jedes Fahrzeug in einen autonomen Betrieb überführt wird. Hierzu werden Fahrfunktionen den Fahrern übertragen. Im Bedarfsfall unterstützen sie Fahrerassistenzsysteme beim Überführen der Fahrzeuge in einen sicheren Zustand. Auch vollautonom gesteuerte Fahrzeuge werden so betrieben, dass stets auf einen abrupten Ausfall von SIKAF reagiert werden kann. Die bordeigenen Systeme sind dann grundsätzlich in der Lage, die Fahrzeuge in einen sicheren Zustand, beispielsweise Halten am Fahrbahnrand, zu überführen. Störquellen durch zufällig auftretende, natürliche Ereignisse werden mit den zu Beginn des Kapitels vorgestellten Tests untersucht. Liegen konkrete Informationen zu derartigen Störungen vor, kann die Wahrscheinlichkeit für daraus entstehende Fehler durch einen geeigneten Systementwurf minimiert werden. Auf dennoch eintretende Störungen wird ebenfalls mit der Überführung der Fahrzeuge in einen autonomen Betrieb oder einen sicheren Zustand reagiert.

Parallelredundante Datenverarbeitung Als weitere Maßnahme zur Vermeidung zufälliger Fehler wird auf redundante Informationserfassung und Datenverarbeitung gesetzt. Die Umsetzung folgt der aus LOGISIRE [118] bekannten Betriebsweise, wobei die zu vergleichenden Prozessdaten nicht aus demselben technischen Prozess, sondern einmal aus SIKAF und einmal von den Sensoren an Bord der Fahrzeuge stammen. Außerdem besteht der sichere Zustand nicht in Abschaltung der Spannungsversorgung, sondern erfüllt die spezifischen Anforderungen an die funktionale Sicherheit in einem Fahrzeugleitsystem.

Diese Übertragung von LOGISIRE auf SIKAF wird anhand von Abbildung 5.7 erläutert: Zwei Mikrorechner (MR_1 und MR_2) bereiten die Prozessdaten auf, die von der Funkschnittstelle über SIKAF sowie lokal von den Sensoren eines Fahrzeugs geliefert werden. Die Mikrorechner prüfen, welche der vorliegenden Informationen über das Fahrzeugumfeld und das Verkehrssystem vergleichbar sind, und übergeben diese an eine zentrale Komponente, den *Vergleicher*. Dieser stellt durch Koordination sicher, dass stets die einander entsprechenden Daten verglichen werden, und kann Abweichungen zwischen den gemessenen und den empfangenen Daten feststellen. Treten Abweichungen auf, generiert LOGISIRE eine entsprechende Meldung für das Fahrzeug. Auf deren Grundlage kann über erneute Anforderung der Information über SIKAF und die Fahrzeugsensoren oder unmittelbares Überführen des Fahrzeugs in einen sicheren Zustand entschieden werden. Das Prinzip entspricht dem eines Kalman-Filters [120] mit dem Unterschied, dass es sich bei den Vergleichswerten nicht um berechnete oder modellierte Werte handelt, sondern um empfangene und lokal gemessene Informationen.

5.3.4 Induktive und deduktive Fehleranalyse

Die vorgestellten Prüfungen erlauben sowohl induktive („Bottom-up-Methode“) als auch deduktive („Top-down-Methode“) Sicherheitsanalysen. Die ISO 26262 fordert den Einsatz beider Methoden, um Analysen der funktionalen Sicherheit mit prinzipiell unabhängigen Vorgehensweisen zu ermöglichen.

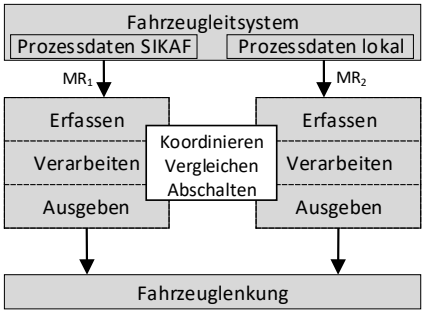


Abbildung 5.7: Parallelredundante Datenverarbeitung in SIKAF nach LOGISIRE [84]

In SIKAF wird mit der *induktiven* Methode untersucht, ob Fehlfunktionen bei einem Fahrzeug sicherheitskritische Effekte beim Relais oder bei der hoheitlichen Behörde auslösen können. Mit der *deduktiven* Methode wird untersucht, ob Fehlfunktionen bei der hoheitlichen Behörde oder beim Relais zu sicherheitskritischen Zuständen der Fahrzeuge führen können.

5.4 Anwendungen und Geschäftsmodelle

Ein Fahrzeugleitsystem soll Sicherheit, Effektivität und Effizienz sowie Komfort eines Verkehrssystems steigern. Wie bisher dargestellt, steht mit SIKAF eine Kommunikationsarchitektur zur Verfügung, die die notwendigen Kommunikationen abwickeln kann. Auf dieser Grundlage sollen abschließend konkrete Anwendungen vorgestellt werden, die sich diese Kommunikationsarchitektur zum Erreichen der vorgenannten Ziele zunutze machen. Dabei wird zwischen Sicherheitsfunktionen als SIKAF-Basisanwendungen einerseits und Komfortfunktionen als Grundlage zur Wertschöpfung andererseits unterschieden.

5.4.1 Ausstattung der Fahrzeugflotte

Die erste Herausforderung einer Einführung von SIKAF besteht in der Ausstattung der technisch sehr heterogenen Fahrzeugflotte mit der notwendigen Informations- und Kommunikationstechnik (IKT). Fahrzeuge, die über keine geeignete Hardware zur Verwendung von SIKAF verfügen, müssen entsprechend ertüchtigt werden. Zudem müssen in den Fahrzeugen Schnittstellen zu den vorhandenen Aktoren geschaffen werden, um über SIKAF direkt auf die Fahrzeugsteuerung einwirken zu können.

Komfortfunktionen stellen einen Lösungsansatz für diese Herausforderung dar. Die Verfügbarkeit von Komfortfunktionen bildet für Halter von Fahrzeugen einen Anreiz, diese mit benötigten Komponenten auszustatten, da die Halter von Vorteilen profitieren. Folglich profitiert auch die gesamte Flotte, weil die ertüchtigten Fahrzeuge dann Bestandteil von SIKAF werden. Durch die Sensorik der neu hinzukommenden Fahrzeuge steht ein umfassenderes Bild des Verkehrssystems zur Verfügung und durch entsprechende Regelung der Fahrzeuge kann das Systemoptimum weiter angenähert werden.

5.4.2 Basis- und Komfortfunktionen

Basisfunktionen des Fahrzeugleitsystems müssen allen Nutzern frei zur Verfügung gestellt werden, weil sie der Befolgung ordnungspolitischer Vorgaben und damit besonders der sicheren Verkehrsabwicklung dienen. Zudem ist eine globale Optimierung des Verkehrssystems nur möglich, wenn ein möglichst großer Anteil der Fahrzeugflotte mit SIKAF ausgestattet ist.

Basisfunktion: Regelung von Abständen und Geschwindigkeiten

Ein Fahrzeugleitsystem regelt die Abstände zwischen Fahrzeugen, damit es zu keinen Kollisionen kommt. Durch den Einsatz von Digitalrechnern können Abstände gegenüber menschlicher Regelung theoretisch zwar deutlich verringert werden. Allerdings muss stets eine vollumfängliche Information über die Positionen und Geschwindigkeiten aller Fahrzeuge vorliegen, die sich potentiell auf Kollisionskurs befinden. Die hierzu mindestens benötigte Ausstattungsrate mit SIKAF hängt von verschiedenen Faktoren ab, beispielsweise von der Qualität der bordeigenen Sensoren, die die autarke Erfassung der Verkehrssituation auch ohne Kommunikationsfunktionen ermöglichen.

Basisfunktion: Warnung vor Falschfahrern

Fahrzeuge, die die Fahrbahn in der entgegengesetzten Richtung nutzen („Geisterfahrer“), stellen eine erhebliche Gefahr für den Straßenverkehr dar. Mit SIKAF können solche Falschfahrten verhindert werden, indem das Fahrzeugleitsystem Position und Geschwindigkeitsvektor aller Fahrzeuge ständig erfasst und prüft. Bewegt sich ein Fahrzeug in die falsche Richtung, kann über SIKAF ein Haltesignal versendet werden, um das betroffene Fahrzeug in einen sicheren Zustand zu überführen. Wird das Signal willentlich ignoriert oder handelt es sich um ein nicht vernetztes Fahrzeug, so können alternativ alle weiteren Fahrzeuge im Gefahrenbereich durch SIKAF gewarnt werden und eine sichere Position einnehmen.

Basisfunktion: Verkehrsführung in Baustellenbereichen

Durch digitale Karten sind dem Fahrzeugleitsystem alle statischen Details des Verkehrssystems bekannt. Kommt es jedoch zu temporären Änderungen im Verkehrssystem, beispielsweise durch Baustellen, so müssen entsprechende Informationen den betroffenen Fahrzeugen bekannt gemacht werden. Dies gilt insbesondere für solche Fahrzeuge, deren geplante Routen über betroffene Streckenabschnitte führen.

SIKAF kann einerseits verwendet werden, um Informationen über temporäre Änderungen im Verkehrssystem zu empfangen. Fahrzeuge, welche eine Baustelle passieren, übertragen Informationen über diese Baustelle mittels SIKAF. Wird die Information von weiteren Fahrzeugen validiert, wird die geänderte Streckenführung als korrekt eingestuft und in die digitalen Karten übernommen. Diese Information muss im Anschluss zu allen betroffenen Fahrzeugen übertragen werden. Die dazu bevorzugte Option ist die Übertragung per SIKAF, sofern die Bibliothek die vorliegende Baustellensituation bereits in Form eines Splines umfasst. Eine weitere Option ist die Übertragung der Information durch lokale Sender, beispielsweise durch Funkbaken auf Baustellenfahrzeugen. Diese nutzen die regulären Übertragungsfunktionen von SIKAF zum Broadcast und zur Authentifizierung der gesendeten Nachrichten.

Komfortfunktion: Optimierung des Verkehrssystems

Die Gesamtkapazität eines Verkehrssystems ist selten ausgeschöpft. Engpässe ergeben sich, wenn die Nachfrage räumlich und zeitlich ungleich auf das Angebot verteilt ist, wie es insbesondere in Spitzenzeiten vorkommt. Wenn dem Fahrzeugleitsystem die Nachfrage bekannt ist, kann es diese durch Optimierung so auf das Angebot verteilen, dass es zu weniger oder keinen Kapazitätsengpässen kommt. Voraussetzung hierfür ist, dass Nutzer des Verkehrssystems ihre geplanten Fahrten mitteilen. Die notwendigen Informationen können durch SIKAF an den Zentralrechner übermittelt werden, der daraus die für alle Fahrzeuge optimalen Routen berechnet.

Komfortfunktion: Verknüpfung und Bevorrechtigung von Verkehrsträgern

Werden Kapazitätsgrenzen erreicht, kann das Fahrzeugleitsystem einzelne Nutzer oder Nutzergruppen bevorzugen. Nutzergruppen können beispielsweise solche Fahrzeuge sein, die den Verkehrssystemen des öffentlichen Verkehrs zugerechnet werden. Das Fahrzeugleitsystem kann Verkehrssysteme verknüpfen und Verkehrsströme von einem Verkehrssystem auf ein anderes verlagern. Konkurrieren Verkehrssysteme um begrenzte Kapazitäten, kann das Fahrzeugleitsystem mit einer entsprechenden Priorisierung reagieren, wobei stets zwischen Nutzeroptimum und Systemoptimum abgewogen werden muss. Mit SIKAF können die benötigten Nachrichten systemübergreifend ausgetauscht werden.

Komfortfunktion: Vollautomatisiertes Fahren

Vollautomatisiertes Fahren bietet Fahrern die Möglichkeit, die Zeit des Transports für andere Aktivitäten zu nutzen. Das Fahrzeugleitsystem muss über eine vollumfängliche Kenntnis der Fahrsituation aller Fahrzeuge im Verkehrsraum verfügen, um die Fahrzeuge sicher durch den Verkehrsraum bewegen zu können. Das Fahrzeugleitsystem muss über Schnittstellen Zugriff auf Steuerfunktionen der zu regelnden Fahrzeuge verfügen, um die notwendigen Längs- und Querregelungen auszuführen. Die betroffenen Fahrzeuge müssen zudem Informationen zu Position und Geschwindigkeitsvektor untereinander austauschen. SIKAF ist aufgrund der gegebenen Sicherheit bei der Datenübertragung für diesen Anwendungsfall prädestiniert.

Bei den vorgestellten Anwendungen handelt es sich um eine nicht abschließende Auswahl an Möglichkeiten, die ein Fahrzeugleitsystem auf Basis von SIKAF bieten kann. Sollen weitere Anwendungen abgedeckt werden, ist die konkrete Implementierung von SIKAF daran anzupassen. Offenheit, Skalierbarkeit und die definierten Schnittstellen von SIKAF erlauben es, die Kommunikationsarchitektur und damit das Fahrzeugleitsystem flexibel in verschiedenste Anwendungen zu integrieren und für neue Anwendungen einzusetzen.

5.5 Zusammenfassung von Evaluierung und Implementierung

In diesem Kapitel wurde gezeigt, dass ein Fahrzeugleitsystem mit den zuvor identifizierten Anforderungen umsetzbar ist und alle benötigten Funktionen implementieren kann.

Insbesondere konnte gezeigt werden, dass bei entsprechender Vorcodierung von Nachrichteninhalten die benötigte Maskengröße gering im Vergleich zur Kapazität gängiger Speichermedien ist. Damit ist es möglich, Masken für die komplette Lebensdauer eines Kraftfahrzeugs an Bord zu bevorraten. Die benötigte Maskengröße stellt somit kein praktisches Hindernis beim Einsatz perfekt sicherer Verschlüsselung in Fahrzeugleitsystemen dar. Durch eine prototypische Implementierung wurde gezeigt, dass auch das Nachrüsten existierender Fahrzeuge durch kostengünstige Komponenten möglich ist. Fahrzeughalter können über Anreize zum Einsatz von SIKAF bewegt werden.

Mit RDS-TMC sowie CAM und DENM wurden bereits Ansätze für strecken- und fahrzeugbezogene Nachrichten vorgestellt. SIKAF erweitert diese Konzepte zu einer integrierten und sicheren Lösung für ein Fahrzeugleitsystem. Entscheidend sind hierzu die folgenden Punkte:

- Vereinheitlichung der Datenmodelle beider Nachrichtentypen hinsichtlich dID und Verortung
- Gleichartige Vermittlung und Verarbeitung beider Nachrichtentypen
- Trennung von Nachrichtenverortung und -inhalt
- Vertraulichkeit und Integrität bei allen Meldungstypen
- Reduzierung der Inhalte auf die Anforderungen eines Fahrzeugleitsystems
- Vorsehen eines Rückkanals

Codierung der Inhalte und Reduzierung der benötigten Maskengröße erlauben erstmals den Einsatz perfekt sicherer Verschlüsselung in einem Fahrzeugleitsystem. Wie bereits gezeigt wurde, können existierende Ansätze wie RDS-TMC, CAM oder DENM die hohen Sicherheitsanforderungen in einem Fahrzeugleitsystem nicht erfüllen.

6 Gesamtzusammenfassung und Ausblick

Es wurde eine neuartige Architektur – SIKAF genannt – zur drahtlosen Kommunikation mobiler Teilnehmer vorgestellt, die speziell für die Anforderungen an IKT-Sicherheit und Echtzeitfähigkeit in Fahrzeugleitsystemen optimiert ist. IKT-Sicherheit wird durch perfekt sichere Verschlüsselung erreicht, die durch Maskierung von Inhalten und Prüfsummen erstmals konsequent für diesen Anwendungsfall umgesetzt wird. Echtzeitfähigkeit wird durch Ausschluss jeglicher stochastischer Prozesse erreicht, die bei herkömmlichen Architekturen meist aus der Netztopologie resultieren. Für alle zur Evaluierung verwendeten Parameter wurden konkrete Werte hergeleitet, da keine Referenzimplementierung existiert. Durch Variation dieser Parameter können weitere Szenarien evaluiert oder SIKAF für andere Anwendungsfälle optimiert werden.

Durch Systematisierung der erarbeiteten Konzepte lassen sich in diesem abschließenden Kapitel die vorgestellte Architektur in aktuelle Systemlandschaften einordnen und weitere mögliche Anwendungsfälle skizzieren.

6.1 Einordnung der Architektur

SIKAF lässt sich wie jede Kommunikationsarchitektur nach den Aspekten Topologie, Kryptologie und Administration systematisieren. Topologisch handelt es sich um ein Infrastrukturnetz mit einem zentralen Zugangspunkt, hier als Relais bezeichnet. Die kryptografische Maxime ist symmetrische Verschlüsselung, was die Implementierung perfekt sicherer Kommunikation ermöglicht. Zur notwendigen Administration wird auf eine vertrauenswürdige Stelle gesetzt, die bei einer hoheitlichen Behörde eingerichtet ist.

Die vorgestellte Architektur steht damit im Gegensatz zu Direktverbindungen nach dem Ad-hoc-Prinzip, welches in zahlreichen anderen Ansätzen zur Fahrzeugvernetzung verbreitet und bevorzugt mit asymmetrischer Kryptografie gesichert ist. Wie gezeigt wurde, erfüllt dieses Prinzip jedoch nicht die hohen Sicherheitsanforderungen in Fahrzeugleitsystemen.

Jeder der genannten Aspekte stellt für sich ein buchfüllendes Forschungsgebiet dar. Mit der vorliegenden Arbeit konnten jeweils spezifische Stärken an die Anforderungen eines Fahrzeugleitsystems angepasst und zusammengeführt werden. Mit dem Einsatz im Verkehrsbereich wurde zudem ein Anwendungsfall gewählt, der alle „Irrtümer der verteilten Datenverarbeitung“ [150] berührt. Mittels der prototypischen Umsetzung der vorgestellten Architektur konnte gezeigt werden, dass eine korrekte Implementierung in einfacher Weise möglich ist und damit diese „Irrtümer“ aufgelöst werden.

6.2 Möglichkeiten und Grenzen der Architektur

Es wurde dargestellt, dass die vorgestellte Architektur die Anforderungen an Sicherheit, Verarbeitungsdauer und Komplexität in einem Fahrzeugleitsystem erfüllen kann. Darüber hinaus stellen nahezu beliebige Skalierbarkeit, Herstellerunabhängigkeit und konsequente Ausrichtung auf das Internet der Dinge entscheidende Vorteile gegenüber bisherigen Konzepten dar. SIKAF ist daher zum direkten Einsatz in bestehenden Verkehrssystemen geeignet.

Die Kommunikation zwischen zwei Fahrzeugen kann nicht ohne dedizierte Infrastruktur stattfinden. Steht eine solche nicht zur Verfügung, ist mit dem vorgestellten Konzept keine Kommunikation von Fahrzeug zu Fahrzeug möglich. Angesichts der Bedeutung und weiter zunehmenden Verbreitung von Kommunikationstechniken ist jedoch nicht zu erwarten, dass dieser Aspekt ein entscheidendes Hindernis bei einer möglichen Einführung von SIKAF darstellt.

Verschiedene Autoren bezeichnen die Schlüsselverteilung als den schwierigsten Teil eines Verschlüsselungsverfahrens [4]. Als Lösung wurde in SIKAF die Errichtung und Nutzung einer dedizierten Infrastruktur vorgeschlagen. Anwendungen im Verkehrsbereich (European Train Control System) oder Bankensektor (SWIFTNet) zeigen, dass eine solche Infrastruktur auch parallel zu bereits etablierten Netzen wie dem Telefonnetz oder dem Internet sinnvoll und umsetzbar ist. Alternativ kommt ein Schlüsselversand durch Kuriere in Betracht, notwendige Verfahren zur Authentifizierung und Autorisierung von Transporteinheiten sind hinreichend bekannt [83]. Zur Speicherung der Masken sind bereits heute Speichermedien mit ausreichender Kapazität einfach verfügbar. Diese müssen jedoch noch mit geeigneten Schutzeinrichtungen versehen werden, um sie gegen Seitenkanalangriffe wie den Diebstahl des physischen Datenträgers abzusichern. Hierzu kommen beispielsweise Sabotageschalter in Betracht [83], deren Auslösen alle betroffenen Masken auf Seiten des Relais sperrt.

Kritiker mögen bei SIKAF das Fehlen einer echten Ende-zu-Ende-Verschlüsselung bemängeln. Wie jedoch gezeigt wurde, ist es konzeptuell nicht möglich, perfekt sichere Verschlüsselung und gleichzeitig kontinuierliche, echtzeitfähige Datenübertragung ohne eine vertrauenswürdige zentrale Instanz zu garantieren. Aufgezeigte Trends im Internet der Dinge sprechen grundsätzlich für die Entwurfsentscheidung zugunsten zentraler, hoheitlicher Instanzen zur Verwaltung sicherheitsrelevanter Parameter.

Die Prototypen wurden mit Komponenten aus dem Bereich der Konsumelektronik (engl. *consumer electronics*) entwickelt, die nicht für industriellen Einsatz zugelassen sind. Die Umsetzbarkeit der Architektur konnte daher nur in Form einer Machbarkeitsstudie nachgewiesen werden. Die Diskussion, ob die eingesetzten Plattformen gänzlich unzuverlässig hinsichtlich Verfügbarkeit und Ausfallsicherheit sind oder ob sie sich sogar im industriellen Umfeld zur Anlagensteuerung einsetzen ließen, wird kontrovers geführt. Die hier gemachte Erfahrung zeigt, dass es einen großen Anwenderkreis dieser Komponenten gibt, wodurch auf eine umfassende Dokumentation und die Erfahrungen einer großen Nutzergemeinde zurückgegriffen werden kann. Aufgrund der Verbreitung lohnt sich zudem langfristige Produktpflege für die Hersteller, insbesondere hinsichtlich Ersatzteilversorgung und Softwareaktualisierungen. Insgesamt summieren sich durch die verbreitete Nutzung zahlreiche Betriebsstunden, was das Auffinden systematischer Fehlfunktionen begünstigt. Die Verbreitung offener Hardware wird nicht zuletzt aus diesen Gründen auch durch aktuell veröffentlichte technische Regeln gefördert [55].

Zur Steigerung der Zuverlässigkeit bei der Funkübertragung ist in SIKAF die Nutzung eines dedizierten Frequenzbereichs vorgesehen, was angesichts der intensiven Nutzung des Funkspektrums nicht vorausgesetzt werden kann. Es wäre daher angebracht, die Entscheidung, das Frequenzband bei 5 GHz für unsichere Ad-hoc-Netze mit einer PKI zu reservieren [69], zu überdenken. Zielführender könnte dieses Band für nachweislich sichere Systeme wie SIKAF eingesetzt werden.

6.3 Technische Erweiterungen

Als mögliche Substitution der zusätzlich benötigten Infrastruktur könnten Hybridfahrzeuge eingesetzt werden, welche sowohl als Teilnehmer als auch als Relais fungieren. Diese würden somit anstelle der Funkmasten die Zugangspunkte zum Relais bilden und gleichzeitig die Nachrichtenverarbeitung und -weiterleitung initiieren. Derartige Konzepte werden vor allem unter dem Begriff „Georouting“ entwickelt und bilden weiterhin hierarchisch strukturierte Netze im Infrastrukturmodus. Zentrale Aspekte sind jedoch noch ungeklärt. Hierzu zählen der benötigte Anteil der Hybridfahrzeuge am Gesamtkollektiv, die notwendigen Maßnahmen zur Gewährleistung der Netzverfügbarkeit und die Kommunikationssicherheit.

Das Einsatzgebiet von Fahrzeugleitsystemen ist nicht auf die hier vorgestellten Straßenfahrzeuge beschränkt. Die Nutzung des Luftraums mit autonomen Drohnensystemen zum Passagier- und Warentransport ist ein viel diskutiertes Thema [122]. Die genaue Ausgestaltung derartiger Verkehrssysteme ist zwar noch Gegenstand der Forschung. Es besteht jedoch weitestgehend Konsens über die Notwendigkeit der automatischen Steuerung dieser Verkehrssysteme, da die Menge der Objekte nicht mehr von menschlichen Lotsen überwacht werden kann. SIKAF ist für diesen Anwendungsfall aus zwei Gründen prädestiniert: Zum einen kann SIKAF die hohen Sicherheitsanforderungen in der Luftfahrt nachweislich erfüllen, die sich durch eine zusätzliche Verschleierung [81] sogar noch steigern lassen. Zum anderen besteht bei Luftfahrzeugen ein weitaus regelmäßigerer Kontakt mit (Boden-)Infrastruktur, als es bei Kraftfahrzeugen der Fall ist. Der Maskennachschub kann durch diesen Kontakt in besonders einfacher Weise gewährleistet werden.

6.4 Neue Konzepte für dezentrale autonome Systeme

Hier wurde ein Fahrzeugleitsystem als zwar skalierbares, aber dennoch gegenüber anderen Akteuren abgeschlossenes Automatisierungssystem betrachtet. Durch die weitere Ausbreitung des industriellen Internets der Dinge ist unmittelbare Interaktion gegenseitig unbekannter, digitaler Entitäten (vergleichbar mit einem *Cyberflâneur* [24]) vorstellbar. Permanenter Zugriff auf Informationen einer zentralen oder hoheitlichen Instanz ist in diesem Fall nicht mehr gegeben. Es müssen daher Lösungen gefunden werden, um die Prozesse Authentisierung, Authentifizierung und Autorisierung auch in autarken Umgebungen zu gewährleisten. Im übertragenen Sinn muss hierzu das Prinzip *Vertrauen* auf offene cyberphysische Systeme übertragen werden.

Generieren und Verwalten von Vertrauen Die Übertragung von Informationen, besonders wenn diese sicherheitsrelevant für den Einzelnen oder ein Kollektiv sind, setzt als zentrale Eigenschaft Vertrauen in die jeweiligen Kommunikationspartner voraus. In einem

sozialen Kontext wird Vertrauen durch positive, teils subjektiv geprägte Erfahrungen mit bisherigem Verhalten erworben. Auch in einem cyberphysischen System muss ein Nachweis vorhanden sein, dass übertragene Informationen vom Empfänger nicht missbräuchlich verwendet werden. Für den technischen Einsatz muss somit der Wert *Vertrauen* durch definierbare, messbare Eingangsgrößen quantifiziert und potentiellen Kommunikationsteilnehmern verfügbar gemacht werden.

Zur Quantifizierung ist eine geeignete Kostenfunktion zu finden, die den Vertrauenswert jedes Teilnehmers definiert. Zudem wird ein dezentrales und konsistentes Datenbankmanagementsystem benötigt, welches es jedem Kommunikationsteilnehmer jederzeit ermöglicht, den Vertrauenswert des jeweiligen Kommunikationspartners ohne eine zentrale Datenbank zu ermitteln.

Blockchain Ein Datenbanksystem, welches diese speziellen Anforderungen erfüllen kann, war lange nicht verfügbar und hat sich erst in jüngerer Zeit durch das Konzept der *Blockchain* etabliert [137]. Eine Blockchain bildet eine dezentrale Datenbank mit den Eigenschaften, wie sie zur Speicherung und Bereitstellung von Vertrauenswerten in autark agierenden cyberphysischen Systemen benötigt werden. Das Konzept der Blockchain einschließlich der Anwendung „Bitcoin“ kann auf ein Fahrzeugleitsystem übertragen werden, wenn drei wesentliche Hürden überwunden werden: Erstes kann eine Blockchain in ihrer bisherigen Ausprägung keine Echtzeitbedingungen erfüllen. Die Berechnung neuer Blöcke nimmt Zeitspannen unvorhersehbarer Dauer in Anspruch, vollständige Berechnungen können daher unter vorgegebenen zeitlichen Schranken nicht garantiert werden. Zweitens kann eine Blockchain bei längerer Benutzung ein sehr großes Datenvolumen annehmen. Dieses stellt große Anforderungen an Bandbreite und Übertragungsdauern. Die notwendige redundante Speicherung bei allen Teilnehmern macht zudem große Speicherkapazitäten notwendig. Drittens kann das Problem eines Flutens des Netzes mit konkurrierenden Blöcken auftreten, insbesondere wenn die Anzahl vernetzter Fahrzeuge steigt. Die Datenbank würde sich in diesem Fall temporär in einem inkonsistenten Zustand befinden und damit die Integrität verletzen.

Mit aktuellen Implementierungen ist die Skalierung einer Blockchain folglich nur unzureichend möglich. Könnten diese Hindernisse beseitigt werden, so würde das Prinzip der Blockchain aber eine vielversprechende Möglichkeit für die dezentrale Informationsverwaltung in cyberphysischen Systemen darstellen, da ein vollständig autarker Betrieb bei gleichzeitigem Verzicht auf eine zentrale Instanz erreicht werden könnte.

6.5 Schlussbetrachtung

Wird ein technisches System wie ein Fahrzeugleitsystem durch entsprechende Programmierung zu *eigenständigem* Handeln befähigt, so sind zwangsläufig Handlungsprämissen für Situationen vorzusehen, die eine ethische Bewertung notwendig machen [94]. Diese Handlungsprämissen müssen vollumfänglich behandelt werden, bevor ein Automatisierungssystem wie SIKAF zum steuernden Eingriff in das Fahrverhalten bemannter Fahrzeuge eingesetzt wird. Einschlägige Standards, wie die hier behandelte Norm ISO 26262, sind um Vorgaben zur Konzeption, Erstellung und Evaluierung einer solchen „künstlichen Intelligenz“ zu erweitern. Erste Arbeitsgruppen der Europäischen Kommission berichten zur Klärung ethischer Fragen, die sich aus der möglichen Verbreitung vernetzter und autono-

mer Fahrzeuge ergeben können [89]. Wie in der vorliegenden Arbeit gezeigt wurde, können zentrale Anforderungen an Sicherheit, Privatsphäre, Transparenz und Verantwortlichkeit durch den Einsatz der vorgestellten Architektur bereits gelöst werden.

Literaturverzeichnis

[1] Akwir, N. ; Chedjou, J. ; Kyamakya, K.: Neural-Network-Based Calibration of Macroscopic Traffic Flow Models. In: *Recent Advances in Nonlinear Dynamics and Synchronization* (2018), S. 151–173

[2] Aslam, B.: *Networking and Security Solutions for VANET Initial Deployment Stage*, University of Central Florida, Diss., 2009

[3] Auerbach, H. ; Issing, M.: Fahrzeuggestützte Notrufsysteme (eCall) für die Verkehrssicherheit in Deutschland. In: Bundesanstalt für Strassenwesen (Hrsg.): *Berichte der Bundesanstalt für Straßenwesen* Bd. F 69. Wirtschaftsverlag NW, 2008

[4] Bauer, F.: *Entzifferte Geheimnisse: Methoden und Maximen der Kryptologie*. Berlin, Heidelberg : Springer-Verlag, 2000

[5] Bauer, W. ; Schlund, S. u. a.: Industrie 4.0 – Volkswirtschaftliches Potenzial für Deutschland / Fraunhofer IAO. 2014. – Forschungsbericht

[6] Bencsáth, B. ; Pék, G. ; Buttyán, L. ; Félegyházi, M.: Duqu: A Stuxnet-like malware found in the wild / BME – Laboratory of Cryptography and System Security (CrySyS). Version: 2011. `crysys.hu/publications/files/bencsathPBF11duqu.pdf`. 2011. – Forschungsbericht. – Zuletzt abgerufen am 25.07.2020

[7] Berger, K. ; Linz, C. ; Lipski, C. ; Stich, T. ; Magnor, M.: Echtzeiterkennung von befahrbaren Bereichen in urbanen Szenarien. In: Halang, W. (Hrsg.) ; Holleczek, P. (Hrsg.): *Echtzeit 2008 – Aktuelle Anwendungen in Technik und Wirtschaft*. Berlin, Heidelberg : Springer, 2008, S. 1–10

[8] Bittl, S.: *Efficient Secure Communication in VANETs under the Presence of new Requirements Emerging from Advanced Attacks*, Humboldt-Universität zu Berlin, Diss., 2017

[9] Brauer, H.: Das Sichere Mikrorechnersystem Logisafe. In: Baumann, R. (Hrsg.): *Fachtagung Prozeßrechner* Bd. 39. Berlin, Heidelberg : Springer, 1981 (Informatik-Fachberichte), S. 261–269

[10] Bregulla, M. ; Feucht, W. u. a.: Funklösungen in der Automation / Zentralverband Elektrotechnik- und Elektronikindustrie e. V. 2011. – Forschungsbericht

[11] Broadcom Europe Ltd.: *BCM2835 ARM Peripherals*. `datasheetspdf.com/pdf/1408704/Broadcom/BCM2835/1`. Version: 2012. – Zuletzt abgerufen am 06.08.2020

[12] Bundesamt für Sicherheit in der Informationstechnik: *Drahtlose Kommunikationssysteme und ihre Sicherheitsaspekte*. Online. www.bsi.bund.de. Version: 2009. – Zuletzt abgerufen am 11.12.2019

[13] Bundesamt für Sicherheit in der Informationstechnik: *BSI TR-03159 Mobile Identities*. Online. www.bsi.bund.de. Version: 2019. – Zuletzt abgerufen am 09.08.2020

[14] Bundesamt für Sicherheit in der Informationstechnik: *Die Lage der IT-Sicherheit in Deutschland 2019*. Online. www.bsi.bund.de. Version: 2019. – Zuletzt abgerufen am 09.08.2020

[15] Bundesamt für Sicherheit in der Informationstechnik: *BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen*. Online. www.bsi.bund.de. Version: 2020. – Zuletzt abgerufen am 09.08.2020

[16] Bundesgesetzblatt 1977 II S. 809: *Gesetz zu den Übereinkommen vom 8. November 1968 über den Straßenverkehr und über Straßenverkehrszeichen, zu den Europäischen Zusatzübereinkommen vom 1. Mai 1971 zu diesen Übereinkommen sowie zum Protokoll vom 1. März 1973 über Straßenmarkierungen*. Bundesanzeiger Verlag, 1977

[17] Bundesministerium für Verkehr und digitale Infrastruktur: *Strategie automatisiertes und vernetztes Fahren*. Online. www.bmvi.de. Version: 2015. – Zuletzt abgerufen am 03.07.2019

[18] Bundesministerium für Verkehr und digitale Infrastruktur: *Verkehr in Zahlen 2019/2020*. Online. www.bmvi.de. Version: 2019. – Zuletzt abgerufen am 03.09.2020

[19] Bundesministerium für Verkehr und digitale Infrastruktur u. a.: *IVS-Aktionsplan „Straße“*. Online. www.bmvi.de. Version: 2012. – Zuletzt abgerufen am 03.07.2019

[20] Bundesministerium für Verkehr und digitale Infrastruktur u. a.: *Innovationscharta „Digitales Testfeld Autobahn“*. Online. www.bmvi.de. Version: 2015. – Zuletzt abgerufen am 03.07.2019

[21] Bök, P. ; Noack, A. ; Müller, M. ; Behnke, D.: *Computernetze und Internet of Things*. Berlin, Heidelberg : Springer Vieweg, 2020

[22] Cacilo, A. u. a.: Hochautomatisiertes Fahren auf Autobahnen – Industriepolitische Schlussfolgerungen / Fraunhofer IAO. Version: 2015. www.bmwi.de. 2015. – Forschungsbericht. – Zuletzt abgerufen am 04.07.2020

[23] Coll, J.: *Channel Characterization and Wireless Communication Performance in Industrial Environments*, KTH Royal Institute of Technology, Diss., 2014

[24] Coltzau, H.: *Dezentrale Netzwelten als Interaktions- und Handelsplattformen*, FernUniversität in Hagen, Diss., 2012

[25] Cremers, C. ; Mauw, S.: *Operational Semantics and Verification of Security Protocols*. Berlin, Heidelberg : Springer-Verlag, 2012 (Information Security and Cryptography)

[26] Dannheim, C.: *The Vehicle as Mobile Sensor in a Collaborative Network*, FernUniversität in Hagen, Diss., 2015

[27] D'Arco, P. ; Stinson, D.: On Unconditionally Secure Robust Distributed Key Distribution Centers. In: Zheng, Y. (Hrsg.): *Advances in Cryptology – ASIACRYPT 2002*. Berlin, Heidelberg : Springer, 2002, S. 346–363

[28] de Andrade Ferreira Alves, M.: *Real-Time Communications over Hybrid Wired/Wireless PROFIBUS-Based Networks*, Universidade do Porto, Diss., 2002

[29] Defrawy, K.: *Security and Privacy in Location-Based Mobile Ad-Hoc Networks*, University of California Irvine, Diss., 2010

[30] Di Pietro, R. ; Guarino, S. ; Verde, N. ; Domingo-Ferrer, J.: Security in Wireless Ad-hoc Networks – A Survey. In: *Computer Communications* 51 (2014), S. 1–20

[31] DIN 66253:2018-03: *Informationsverarbeitung – Programmiersprache PEARL – SafePEARL*. Berlin : Beuth Verlag, 2018

[32] DIN CEN ISO/TS 21177:2020-01: *Intelligente Verkehrssysteme – Sicherheitsdienste für eine ITS-Station zum sicheren Aufbau von Sitzungen und zur Authentisierung zwischen vertrauenswürdigen Geräten (ISO/TS 21177:2019)*. Berlin : Beuth Verlag, 2020

[33] DIN CEN/TS 17182:2019-03: *Intelligente Verkehrssysteme – eSicherheit – eCall über eine ITS-Station*. Berlin : Beuth Verlag, 2019

[34] DIN CEN/TS 17380:2019-12: *Intelligente Verkehrssysteme – Urbane ITS – Steuerung in einer kontrollierten Zone unter Verwendung von C-ITS (CEN/TS 17380:2019)*. Berlin : Beuth Verlag, 2019

[35] DIN CEN/TS 17395:2020-04: *Intelligente Verkehrssysteme – eSicherheit – eCall für automatisierte und autonome Fahrzeuge*. Berlin : Beuth Verlag, 2020

[36] DIN EN 302636-1:2014-09: *Intelligente Transportsysteme (ITS) – Fahrzeugkommunikation – GeoNetworking – Teil 1: Anforderungen*. Berlin : Beuth Verlag, 2014

[37] DIN EN 303613:2020-03: *Intelligente Verkehrssysteme (IVS) – Spezifikation der LTE-V2X-Zugriffsschicht für Intelligente Verkehrssysteme zum Betrieb im 5-GHz-Frequenzband*. Berlin : Beuth Verlag, 2020

[38] DIN EN 419241-1:2018-09: *Vertrauenswürdige Systeme, die Serversignaturen unterstützen – Teil 1: Allgemeine Systemsicherheitsanforderungen*. Berlin : Beuth Verlag, 2018

[39] DIN EN 61508-1:2011-02: *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme (IEC 61508-1:2010).* Berlin : Beuth Verlag, 2011

[40] DIN EN 61907:2010-09: *Zuverlässigkeit von Kommunikationsnetzen (IEC 61907: 2009).* Berlin : Beuth Verlag, 2010

[41] DIN EN 62264-1:2014-07: *Integration von Unternehmensführungs- und Leitsystemen – Teil 1: Modelle und Terminologie (IEC 62264-1:2013).* Berlin : Beuth Verlag, 2014

[42] DIN EN 62591:2017-02: *Industrielle Kommunikationsnetze – Drahtlose Kommunikationsnetze und Kommunikationsprofile – WirelessHARTTM (IEC 62591:2016).* Berlin : Beuth Verlag, 2017

[43] DIN EN 62657-1:2018-05: *Industrielle Kommunikationsnetze – Funk-Kommunikationsnetze – Teil 1: Anforderungen und Überlegungen zur Frequenznutzung (IEC 62657-1:2017).* Berlin : Beuth Verlag, 2018

[44] DIN EN IEC 61158-1:2020-04: *Industrielle Kommunikationsnetze – Feldbusse – Teil 1: Überblick und Leitfaden zu den Normen der Reihen IEC 61158 und IEC 61784 (IEC 61158-1:2019).* Berlin : Beuth Verlag, 2020

[45] DIN EN IEC 62443-4-2:2019-12: *IT-Sicherheit für industrielle Automatisierungssysteme – Teil 4-2: Technische Sicherheitsanforderungen an Komponenten industrieller Automatisierungssysteme (IACS) (IEC 62443-4-2:2019).* Berlin : Beuth Verlag, 2019

[46] DIN EN ISO 14819-1:2014-03: *Intelligente Transportsysteme – Verkehrs- und Reiseinformationen über Verkehrsmeldungskodierung – Teil 1: Kodierungsprotokoll für den digitalen Radiokanal für Verkehrsmeldungen (RDS-TMC) unter Nutzung von ALERT-C (ISO 14819-1:2013).* Berlin : Beuth Verlag, 2014

[47] DIN EN ISO 17287:2003-10: *Straßenfahrzeuge – Ergonomische Aspekte von Fahrerinformations- und Assistenzsystemen – Verfahren zur Bewertung der Gebrauchstauglichkeit beim Führen eines Kraftfahrzeugs (ISO 17287:2003).* Berlin : Beuth Verlag, 2003

[48] DIN EN ISO 17419:2018-09: *Intelligente Verkehrssysteme – Kooperative Systeme – Global eindeutige Identifikation (ISO 17419:2018).* Berlin : Beuth Verlag, 2018

[49] DIN EN ISO 17427-1:2018-10: *Intelligente Transportsysteme – Kooperative ITS – Teil 1: Rollen und Verantwortlichkeiten im Zusammenhang mit kooperativer(n) ITS-Architektur(en) (ISO 17427-1:2018).* Berlin : Beuth Verlag, 2018

[50] DIN EN ISO 18542-1:2013-04: *Straßenfahrzeuge – Standardisierte Terminologie für Reparatur- und Wartungsinformationen (RMI) – Teil 1: Allgemeine Informationen und Beschreibung der Anwendungsfälle (ISO 18542-1:2012).* Berlin : Beuth Verlag, 2013

[51] DIN EN ISO 18750:2018-09: *Intelligente Verkehrssysteme – Kooperative ITS – Lokale dynamische Karten (ISO 18750:2018)*. Berlin : Beuth Verlag, 2018

[52] DIN EN ISO 24534-3:2016-08: *Intelligente Verkehrssysteme – Automatische Identifizierung von Fahrzeugen und Ausrüstungen – Elektronische Identifizierung für die Registrierung (ERI) von Fahrzeugen – Teil 3: Fahrzeugdaten (ISO 24534-3:2016)*. Berlin : Beuth Verlag, 2016

[53] DIN EN ISO/IEC 15408-1:2020-06: *Informationstechnik – IT-Sicherheitsverfahren – Evaluationskriterien für IT-Sicherheit – Teil 1: Einführung und allgemeines Modell (ISO/IEC 15408-1:2009)*. Berlin : Beuth Verlag, 2020

[54] DIN EN ISO/IEC 27000:2020-06: *Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Überblick und Terminologie (ISO/IEC 27000:2018)*. Berlin : Beuth Verlag, 2020

[55] DIN SPEC 3105-2:2020-07: *Open Source Hardware – Teil 2: Community-basierte Bewertung*. Berlin : Beuth Verlag, 2020

[56] DIN SPEC 91345:2016-04: *Referenzarchitekturmodell Industrie 4.0*. Berlin : Beuth Verlag, 2016

[57] Dorst, W. ; Diegner, B. u. a.: *Umsetzungsstrategie Industrie 4.0 – Ergebnisbericht*. Online. www.bitkom.org. Version: 2015. – Zuletzt abgerufen am 03.02.2020

[58] Electronic Frontier Foundation: *Cracking DES: Secrets of Encryption Research, Wiretap Politics and Chip Design*. O'Reilly, 1998

[59] Elgamal, T.: A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. In: *IEEE Transactions on Information Theory* 31 (1985), Nr. 4, S. 469–472

[60] Elminaam, D. ; Kader, H. ; Hadhoud, M.: Performance Evaluation of Symmetric Encryption Algorithms. In: *International Journal of Computer Science and Network Security* 8 (2008), Nr. 12, S. 280–286

[61] ETSI EN 302 637-2: *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service*. Online. www.etsi.org. Version: 2019. – Zuletzt abgerufen am 02.01.2020

[62] ETSI EN 302 637-3: *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service*. Online. www.etsi.org. Version: 2019. – Zuletzt abgerufen am 02.01.2020

[63] ETSI ES 201 873-1: *Methods for Testing and Specification (MTS); The Testing and Test Control Notation version 3; Part 1: TTCN-3 Core Language*. Online. www.etsi.org. Version: 2020. – Zuletzt abgerufen am 02.06.2020

[64] ETSI TR 102 638: *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions*. Online. www.etsi.org. Version: 2009. – Zuletzt abgerufen am 02.01.2020

[65] ETSI TR 102 962: *Intelligent Transport Systems (ITS); Framework for Public Mobile Networks in Cooperative ITS (C-ITS)*. Online. www.etsi.org. Version: 2012. – Zuletzt abgerufen am 02.01.2020

[66] ETSI TS 103 645: *CYBER; Cyber Security for Consumer Internet of Things*. Online. www.etsi.org. Version: 2019. – Zuletzt abgerufen am 02.01.2020

[67] ETSI TS 103 666-1: *Smart Secure Platform (SSP) Part 1: General Characteristics*. Online. www.etsi.org. Version: 2019. – Zuletzt abgerufen am 02.01.2020

[68] European Commission: C-ITS Point of Contact (CPOC) Protocol / JRC114086. 2019. – Forschungsbericht

[69] Europäische Kommission: *Eine europäische Strategie für Kooperative Intelligente Verkehrssysteme*. EUR-Lex, 2016

[70] Falliere, N. ; Murchu, L. ; Chien, E.: W32.Stuxnet Dossier / Symantec Security Response. Version: 2011. nsarchive2.gwu.edu//NSAEBB/NSAEBB424/docs/Cyber-044.pdf. 2011. – Forschungsbericht. – Zuletzt abgerufen am 25.07.2020

[71] Fluhrer, S. ; Mantin, I. ; Shamir, A.: Weaknesses in the Key Scheduling Algorithm of RC4. In: Vaudenay, S. (Hrsg.) ; Youssef, A. (Hrsg.): *Selected Areas in Cryptography* Bd. 2259. Berlin, Heidelberg : Springer, 2001 (Lecture Notes in Computer Science), S. 1–24

[72] Fritzing: *fritzing.org/*. Online, 2020. – Zuletzt abgerufen am 25.07.2020

[73] Fucik, R. (Hrsg.) ; Hartl, F. (Hrsg.) ; Schlosser, H. (Hrsg.) ; Wielke, B. (Hrsg.): *Handbuch des Verkehrsunfalls / Teil 2 – Unfallaufklärung und Fahrzeugschaden*. MANZ Verlag, 2008

[74] Gholami, S. ; Meybodi, M. ; Saghiri, A.: A Learning Automata-Based Version of SG-1 Protocol for Super-Peer Selection in Peer-to-Peer Networks. In: Boonkrong, S. (Hrsg.) ; Unger, H. (Hrsg.) ; Meesad, P. (Hrsg.): *Recent Advances in Information and Communication Technology*. Berlin, Heidelberg : Springer, 2014 (Advances in Intelligent Systems and Computing), S. 189–201

[75] Gilbert, S. ; Lynch, N.: Brewer's Conjecture and the Feasibility of Consistent, Available, Partition-Tolerant Web Services. In: *ACM SIGACT News* 33 (2002), Nr. 2, S. 51–59

[76] Glas, B.: *Trusted Computing für adaptive Automobilsteuergeräte im Umfeld der Inter-Fahrzeug-Kommunikation*, Karlsruher Institut für Technologie, Diss., 2011

[77] Glöe, G. u. a.: Werkzeugunterstützung der Prüfung sicherheitsgerichteter Software auf Normenkonformität. In: Halang, W. (Hrsg.): *Echtzeit 2013 – Funktionale Sicherheit*. Berlin, Heidelberg : Springer Vieweg, 2013, S. 7–18

[78] Gomez, C. ; Arcia-Moret, A. ; Crowcroft, J.: TCP in the Internet of Things: From Ostracism to Prominence. In: *IEEE Internet Computing* 22 (2018), Nr. 1, S. 29–41

[79] González, M.: *Heuristische Routingverfahren für unstrukturierte P2P-Netzwerke*, FernUniversität in Hagen, Diss., 2012

[80] Guvenc, I. ; Gezici, S. ; Sahinoglu, Z. ; Kozat, U.: *Reliable Communications for Short-Range Wireless Systems*. Cambridge University Press, 2011

[81] Halang, W.: *Verfahren zur Binärdatenverschlüsselung*. Schutzrecht DE 10 2005 006 713, 2005

[82] Halang, W. ; Fitz, R.: *Nicht hackbare Rechner und nicht brechbare Kryptographie*. Berlin, Heidelberg : Springer Vieweg, 2018

[83] Halang, W. ; Gumzej, R.: *Automatisierte Authentifizierung und Autorisierung von Transporteinheiten bekannter Versender*. Schutzrecht DE 10 2017 000 706 A1, 2017

[84] Halang, W. ; Konakovsky, R.: *Sicherheitsgerichtete Echtzeitsysteme*. Berlin, Heidelberg : Springer Vieweg, 2013

[85] Hartenstein, H. ; Laberteaux, K.: *VANET: Vehicular Applications and Inter-Networking Technologies*. Wiley, 2010

[86] Hildebrandt, G. u. a.: Funktechnologien für die Industrie – Bessere Lösungen mit Cognitive Radio / Fraunhofer ESK. Version: 2010. publica.fraunhofer.de/. 2010. – Forschungsbericht. – Zuletzt abgerufen am 03.03.2020

[87] Hillenbrand, M.: *Funktionale Sicherheit nach ISO 26262 in der Konzeptphase der Entwicklung von Elektrik/Elektronik Architekturen von Fahrzeugen*, Karlsruher Institut für Technologie, Diss., 2012

[88] Hoeper, K. ; Gong, G.: Pre-Authentication and Authentication Models in Ad Hoc Networks. In: Xiao, Y. (Hrsg.) ; Shen, X. (Hrsg.) ; Du, D. (Hrsg.): *Wireless Network Security*. Berlin, Heidelberg : Springer, 2002 (Signals and Communication Technology), S. 65–82

[89] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659): *Ethics of Connected and Automated Vehicles: Recommendations on road safety, privacy, fairness, explainability and responsibility*. Publications Office of the European Union, 2020

[90] Hotter, D. ; Nazareth, D.: Verwendungsfähigkeit von Android-CE-Geräten für Car2X-Anwendungen am Beispiel einer Geschwindigkeitsregelung. In: Halang, W. (Hrsg.) ; Unger, H. (Hrsg.): *Echtzeit 2014 – Industrie 4.0 und Echtzeit*. Berlin, Heidelberg : Springer Vieweg, 2014, S. 101–110

[91] Hund, J.: *Entwurf eines robusten drahtlosen Kommunikationssystems für die industrielle Automatisierung unter harten Echtzeitbedingungen auf Basis von Ultrawideband-Impulsfunk*, Brandenburgische Technische Universität Cottbus, Diss., 2012

[92] Höhn, R. ; Höppner, S.: *Das V-Modell XT*. Berlin, Heidelberg : Springer-Verlag, 2008

[93] IEEE 802.3 Working Group: IEEE Standard for Ethernet. In: *IEEE Std 802.3-2018 (Revision of IEEE Std 802.3-2015)* (2018)

[94] IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems: *Ethically Aligned Design*. Online. `standards.ieee.org`. Version: 2019. – Zuletzt abgerufen am 05.05.2020

[95] Imtiaz, J. ; Jasperneite, J.: Common Automation Protocol Architecture and Real-time Interface (CAPRI). In: Halang, W. (Hrsg.): *Echtzeit 2012 – Kommunikation unter Echtzeitbedingungen*. Berlin, Heidelberg : Springer Vieweg, 2012, S. 79–88

[96] Ioana, A. ; Korodi, A.: VSOMEIP – OPC UA Gateway Solution for the Automotive Industry. In: *IEEE International Conference on Engineering, Technology and Innovation*, IEEE, 2019, S. 1–6

[97] ISO 13849-1:2015-12: *Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze*. Berlin : Beuth Verlag, 2015

[98] ISO 14296:2016-02: *Intelligente Verkehrssysteme – Erweiterung von Karten-Datenbankspezifikationen für Anwendungen von kooperativer ITS*. Berlin : Beuth Verlag, 2016

[99] ISO 17572-1:2015-01: *Intelligente Verkehrssysteme (ITS) – Positionsreferenzierung für geografische Datenbanken – Teil 1: Allgemeine Anforderungen und konzeptuelle Modelle*. Berlin : Beuth Verlag, 2015

[100] ISO 26262-1:2018-12: *Straßenfahrzeuge – Funktionale Sicherheit – Teil 1: Vokabular*. Berlin : Beuth Verlag, 2018

[101] ISO/IEC 7498-1:1994-11: *Informationstechnik – Kommunikation Offener Systeme – Basis-Referenzmodell*. Berlin : Beuth Verlag, 1994

[102] ISO/SAE DIS 21434:2020-02 – Entwurf: *Straßenfahrzeuge – Cybersecurity engineering*. Berlin : Beuth Verlag, 2020

[103] ISO/TR 21718:2019-01: *Intelligente Verkehrssysteme – Räumliches und zeitliches Datenwörterbuch für kooperative ITS und automatisierte Fahrsysteme 2.0*. Berlin : Beuth Verlag, 2019

[104] ISO/TR 21959-1:2020-01: *Straßenfahrzeuge – Menschliche Ausführungen und Zustände im Kontext des automatisierten Fahrens – Teil 1: Gemeinsame grundlegende Konzepte*. Berlin : Beuth Verlag, 2020

[105] Jemberu, E.: *Identity Management on VANETS*, Norwegian University of Science and Technology, Diss., 2012

[106] Jiang, D. ; Delgrossi, L.: IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments. In: *IEEE Vehicular Technology Conference*, IEEE, 2008, S. 2036–2040

[107] Jung, H. ; Ahn, J. ; Park, S.: A JXTA-based System for Adaptive and Collaborative Learning. In: Eichler, G. (Hrsg.) ; Kropf, P. (Hrsg.) ; Lechner, U. (Hrsg.) ; Meesad, P. (Hrsg.) ; Unger, H. (Hrsg.): *International Conference on Innovative Internet Community Systems* Bd. P-165, GI, 2010 (LNI), S. 462–471

[108] Jungnickel, D.: *Graphen, Netzwerke und Algorithmen*. BI-Wissenschaftsverlag, 1994

[109] Kafka, P.: The Automotive Standard ISO 26262, the Innovative Driver for Enhanced Safety Assessment & Technology for Motor Cars. In: *International Symposium on Safety Science and Technology* 45 (2012), S. 2–10

[110] Kalenderi, M. ; Pnevmatikatos, D. ; Papaefstathiou, I. ; Manifavas, C.: Breaking the GSM A5/1 Cryptography Algorithm with Rainbow Tables and High-end FPGAs. In: *International Conference on Field Programmable Logic and Applications* (2012), S. 747–753

[111] Karaoglu, B.: *Efficient Use of Resources in Mobile Ad Hoc Networks*, University of Rochester, Diss., 2013

[112] Kasper, B.: *Industrie 4.0: Technologieentwicklung und sicherheitstechnische Bewertung von Anwendungsszenarien*. Dortmund : Bundesanstalt für Arbeitsschutz und Arbeitsmedizin, 2019

[113] Kasper, T. ; Kühn, A. ; Oswald, D. ; Zenger, C. ; Paar, C.: Rights Management with NFC Smartphones and Electronic ID Cards: A Proof of Concept for Modern Car Sharing. In: Hutter, M. (Hrsg.) ; Schmidt, J. (Hrsg.): *Radio Frequency Identification* Bd. 8262. Berlin, Heidelberg : Springer, 2013 (Lecture Notes in Computer Science), S. 34–53

[114] Kaufmann, S.: Implementation and Adaptation of the Pseudonymous PKI for Ubiquitous Computing for Car-2-car Communication. In: Klenk, H. (Hrsg.) ; Keller, H. (Hrsg.) ; Plödereder, E. (Hrsg.) ; Dencker, P. (Hrsg.): *Automotive – Safety & Security 2014*, Gesellschaft für Informatik e. V., 2015, S. 95–108

[115] Kerper, M.: *Ursachen- und wirkungsorientierte Analyse gesammelter Fahrprofile zur taktischen Fahrtoptimierung*, Heinrich-Heine-Universität Düsseldorf, Diss., 2013

[116] Klasen, F. ; Oestreich, V. ; Volz, M.: *Industrielle Kommunikation mit Feldbus und Ethernet*. VDE-Verlag, 2010

[117] Kleinemeier, M.: Von der Automatisierungspyramide zu Unternehmenssteuerungsnetzwerken. In: Bauernhansl, T. (Hrsg.) ; ten Hompel, M. (Hrsg.) ; Vogel-Heuser, B. (Hrsg.): *Industrie 4.0 in Produktion, Automatisierung und Logistik*. Berlin, Heidelberg : Springer Vieweg, 2014, S. 571–579

[118] Kloppenburg, T.: Logisire, A Safe Computer System for Process-automation. In: Belli, F. (Hrsg.) ; Görke, W. (Hrsg.): *Fehlertolerierende Rechensysteme* Bd. 147. Berlin, Heidelberg : Springer, 1987 (Informatik-Fachberichte), S. 378–382

[119] Kyamakya, K. ; Chedjou, J. ; al Machot, F. ; Fasih, A.: Enabling a Driver-Specific „Real-Time Road Safety“ Assessment through an „Extended Floating Car Data“ and Visualization System. In: *Studies in Computational Intelligence* 391 (2011), S. 277–292

[120] Kálmán, R.: A New Approach to Linear Filtering and Prediction Problems. In: *Transaction of the ASME, Journal of Basic Engineering* D (1960), Nr. 82, S. 35–45

[121] La, V. ; Cavalli, A.: Security Attacks and Solutions in Vehicular Ad Hoc Networks: A Survey. In: *International Journal on AdHoc Networking Systems* 4 (2014), S. 1–20

[122] Lee, P. ; Idris, H. ; Helton, D. ; Davis, T. ; Lohr, G. ; Oseguera-Lohr, R.: Integrated Trajectory-Based Operations for Traffic Flow Management in an Increasingly Diverse Future Air Traffic Operations. In: *IEEE/AIAA Digital Avionics Systems Conference* (2019), S. 1–9

[123] Lertsuwanakul, L.: *Multiple Criteria Routing Algorithms in Mesh Overlay Networks*, FernUniversität in Hagen, Diss., 2011

[124] Lindner, W. ; Meier, J.: Towards a Secure Data Stream Management System. In: Draheim, D. (Hrsg.) ; Weber, G. (Hrsg.): *Trends in Enterprise Application Architecture* Bd. 3888. Berlin, Heidelberg : Springer, 2006 (Lecture Notes in Computer Science), S. 114–128

[125] Liu, C. ; Wu, J.: Adaptive Routing in Dynamic Ad Hoc Networks. In: *IEEE Wireless Communications and Networking Conference*, IEEE, 2008, S. 2603–2608

[126] Maget, C.: Architecture for Trust-based Machine to Machine Communication. In: Kubek, M. (Hrsg.) ; Li, Z. (Hrsg.): *Autonomous Systems 2018 – Proceedings of the 11th Conference*, VDI Verlag, 2018, S. 114–126

[127] Maget, C.: Zur sicheren Vernetzung von Kraftfahrzeugen. In: Unger, H. (Hrsg.): *Echtzeit 2019*, Springer Vieweg, Wiesbaden, 2019 (Informatik aktuell), S. 89–98

[128] Maget, C.: Sichere Mobilfunkkommunikation für ein Fahrzeugleitsystem. In: Unger, H. (Hrsg.): *Echtzeit 2020*, Springer Vieweg, Wiesbaden, 2020 (Informatik aktuell)

[129] Maget, C.: Vehicle Guidance System based on Secure Mobile Communication. In: Magaia, N. (Hrsg.) ; Mastorakis, G. (Hrsg.) ; Mavromoustakis, C. (Hrsg.) ; Pallis, E. (Hrsg.) ; Markakis, E. (Hrsg.): *Intelligent Technologies for Internet of Vehicles*, 2021 (Internet of Things – Technologies, Communications and Computing)

[130] Manzei, C. (Hrsg.) ; Schleupner, L. (Hrsg.) ; Heinze, R. (Hrsg.): *Industrie 4.0 im internationalen Kontext*. VDE Verlag, 2017

[131] Maurer, M. (Hrsg.) ; Gerdes, J. (Hrsg.) ; Lenz, B. (Hrsg.) ; Winner, H. (Hrsg.): *Autonomes Fahren – Technische, rechtliche und gesellschaftliche Aspekte*. Berlin, Heidelberg : Springer Vieweg, 2015

[132] Messmer, R.: *A New Methodology in Network Reliability*, FernUniversität in Hagen, Diss., 2013

[133] Metzner, A.: *Effizienter Entwurf verteilter eingebetteter Echtzeit-Systeme*, Carl von Ossietzky Universität Oldenburg, Diss., 2006

[134] Meyer, U. ; Wetzel, S.: A Man-in-the-Middle Attack on UMTS. In: *Proceedings of the 3rd ACM Workshop on Wireless Security*, Association for Computing Machinery, 2004, S. 90–97

[135] Molina-Masegosa, R. ; Gozalvez, J.: LTE-V for Sidelink 5G V2X Vehicular Communications: A New 5G Technology for Short-Range Vehicle-to-Everything Communications. In: *IEEE Vehicular Technology Magazine* 12 (2017), Nr. 4, S. 30–39

[136] Mundhenk, P. u. a.: Security in Automotive Networks: Lightweight Authentication and Authorization. In: *ACM Transactions on Design Automation of Electronic Systems* 22 (2017), Nr. 2, S. 1–27

[137] Nakamoto, S.: *Bitcoin: A Peer-to-Peer Electronic Cash System*. Online. `bitcoin.org/bitcoin.pdf`. Version: 2008. – Zuletzt abgerufen am 14.05.2017

[138] National Institute of Standards and Technology: Framework for Improving Critical Infrastructure Cybersecurity. Version: 2018. `nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf`. 2018. – Forschungsbericht. – Zuletzt abgerufen am 15.10.2019

[139] Needham, R. ; Schroeder, M.: Using Encryption for Authentication in Large Networks of Computers. In: *Communications of the ACM* 21 (1978), Nr. 12, S. 993–999

[140] Neuman, C.: *RFC 4120 – The Kerberos Network Authentication Service*. 2005

[141] Orgill, G. ; Romney, G. ; Bailey, M. ; Orgill, P.: The Urgency for Effective User Privacy-Education to Counter Social Engineering Attacks on Secure Computer Systems. In: *Proceedings of the 5th Conference on Information Technology Education*, Association for Computing Machinery, 2004 (CITC5 '04), S. 177–181

[142] Ortgiese, M. u. a.: Hinweise zur Strukturierung einer Rahmenarchitektur für Intelligente Verkehrssysteme (IVS) in Deutschland – Notwendigkeit und Methodik. In: *FGSV Technische Regelwerke*. Forschungsgesellschaft für Straßen- und Verkehrswesen, 2012 (305)

[143] Paar, C. ; Pelzl, J.: *Understanding Cryptography*. Berlin, Heidelberg : Springer-Verlag, 2010

[144] Rabieh, K. ; Azer, M.: Combating Sybil Attacks in Vehicular Ad Hoc Networks. In: Özcan, A. (Hrsg.) ; Zizka, J. (Hrsg.) ; Nagamalai, D. (Hrsg.): *Recent Trends in Wireless and Mobile Networks (CoNeCo 2011, WiMo 2011)*. Berlin, Heidelberg : Springer, 2011, S. 65–72

[145] Rehborn, H.: *Zur Automatisierung der Verkehrsdatenanalyse*, FernUniversität in Hagen, Diss., 1995

[146] Rijmenants, D.: The Complete Guide to Secure Communications with the One Time Pad Cipher / Cipher Machines & Cryptology. Version: 2014. `amrron.com/wp-content/uploads/2015/05/one_time_pad.pdf`. 2014. – Forschungsbericht. – Zuletzt abgerufen am 07.08.2020

[147] Rivest, R.: Chaffing and Winnowing: Confidentiality without Encryption / MIT Laboratory for Computer Science. Version: 1998. `pdfs.semanticscholar.org/aaf3/7e0afa43f5b6168074dae2bc0e695a9d1d1b.pdf`. 1998. – Forschungsbericht. – Zuletzt abgerufen am 07.07.2019

[148] Rivest, R. ; Shamir, A. ; Adleman, L.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems / Massachusetts Institute of Technology. Version: 1977. `people.csail.mit.edu/rivest/Rsapaper.pdf`. 1977. – Forschungsbericht. – Zuletzt abgerufen am 07.07.2019

[149] Ross, H.: *Funktionale Sicherheit im Automobil*. Carl Hanser Verlag, 2014

[150] Rotem-Gal-Oz, A.: Fallacies of Distributed Computing Explained / Sun Microsystems. Version: 1997. `rgoarchitects.com/Files/fallacies.pdf`. 1997. – Forschungsbericht. – Zuletzt abgerufen am 25.07.2020

[151] Rüdinger, J.: *Auswirkungen von Seitenkanalangriffen auf das Design kryptographischer Algorithmen*. Jörg Vogt Verlag, 2009

[152] SAE J 3016:2018-06-15: *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*. Berlin : Beuth Verlag, 2018

[153] SAE J 3061:2016-01-14: *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems*. Berlin : Beuth Verlag, 2016

[154] Sathyan, J. u. a.: *A Comprehensive Guide to Enterprise Mobility*. CRC Press, 2013

[155] Scalas, M. ; Giacinto, G.: Automotive Cybersecurity: Foundations for Next-Generation Vehicles. In: *International Conference on new Trends in Computing Sciences*, IEEE, 2019, S. 1–6

[156] Scheuer, F.: *Schutz der Privatsphäre in Ad-hoc-Fahrzeugnetzen*, Universität Hamburg, Diss., 2013

[157] Schimschar, A.: *Modellierung des Zeit- und Fehlerverhaltens industrieller Funklösungen zur Bewertung der Koexistenz*, Otto-von-Guericke-Universität Magdeburg, Diss., 2013

[158] Schleupner, L.: *Perfekt sichere Kommunikation in der Automatisierungstechnik*, FernUniversität in Hagen, Diss., 2012

[159] Schleupner, L. ; Halang, W.: *Vorrichtung und Verfahren zur authentifizierten vertraulichen Kommunikation zwischen den Knoten von Automatisierungsnetzen*. Schutzrecht DE 10 2011 016 106 A1, 2011

[160] Schnabel, P.: *Netzwerktechnik-Fibel: Grundlagen, Übertragungstechnik und Protokolle, Anwendungen und Dienste, Sicherheit.* Books on Demand, 2004 `elektronik-kompendium.de/sites/kom/0211195.htm`. – Zuletzt abgerufen am 25.07.2020

[161] Schwantuschke, R.: Hochfrequenzhandel und Echtzeit. In: Halang, W. (Hrsg.) ; Unger, H. (Hrsg.): *Echtzeit 2017 – Logistik und Echtzeit*. Berlin, Heidelberg : Springer Vieweg, 2017, S. 99–108

[162] Serna-Olvera, J.: *A Trust-driven Privacy Architecture for Vehicular Ad-Hoc Networks*, Universitat Politecnica de Catalunya, Diss., 2012

[163] Shannon, C.: Communication Theory of Secrecy Systems. In: *Bell System Technical Journal* 28 (1949), Nr. 4, S. 656–715

[164] Simon, K.: *Erschließung, Optimierung und Bewertung von Verwundbarkeitsanalysen mittels öffentlich zugänglicher Suchmaschinen*, FernUniversität in Hagen, Diss., 2017

[165] Soyata, T.: *Enabling Real-Time Mobile Cloud Computing Through Emerging Technologies*. IGI Global, 2015

[166] Statista: *de.statista.com*. Online, 2020. – Zuletzt abgerufen am 12.09.2020

[167] Stevens, W.: *TCP/IP*. VDE Verlag, 2011

[168] Strassberger, M. ; Adler, C.: Lokale Gefahrenwarnung in Fahrzeug-Ad-Hoc-Netzen – Eine umfassende Analyse und aktuelle Lösungsansätze. In: *Tagung Aktive Sicherheit durch Fahrerassistenz*, 2006

[169] Tanenbaum, A. ; Wetherall, D.: *Computernetzwerke*. Pearson Studium, 2012

[170] Tardioli, D.: *Real-Time Communications in Wireless Ad-hoc Networks. The RT-WMP Protocol*, Universidad de Zaragoza, Diss., 2010

[171] Thilak, K. ; Amuthan, A.: DoS Attack on VANET Routing and Possible Defending Solutions – A Survey. In: *International Conference on Information Communication and Embedded Systems*, IEEE, 2016, S. 1–7

[172] Tu, C. ; Zhang, L. ; Liu, Z. ; Gao, N. ; Ma, Y.: A Practical Chosen Message Power Analysis Approach Against Ciphers with the Key Whitening Layers. In: Gollmann, D. (Hrsg.) ; Miyaji, A. (Hrsg.) ; Kikuchi, H. (Hrsg.): *Applied Cryptography and Network Security* Bd. 10355. Berlin, Heidelberg : Springer, 2017 (Lecture Notes in Computer Science), S. 415–434

[173] VDI 2710:2010-04: *Ganzheitliche Planung von Fahrerlosen Transportsystemen*. Berlin : Beuth Verlag, 2010

[174] VDI/VDE 2182 Blatt 1:2020-01: *Informationssicherheit in der industriellen Automatisierung – Allgemeines Vorgehensmodell*. Berlin : Beuth Verlag, 2020

[175] VDI/VDE 2185 Blatt 1:2020-08: *Funkgestützte Kommunikation in der Automatisierungstechnik*. Berlin : Beuth Verlag, 2020

[176] Vernam, Gilbert: *Secret Signaling System*. Schutzrecht US 1310719 A, 1919

[177] Weichert, F. ; Weiskopf, A. ; Wenzel, A.: Zeitkritische Kommunikation für drahtlose Fernwartungssysteme. In: Halang, W. (Hrsg.): *Echtzeit 2012 – Kommunikation unter Echtzeitbedingungen*. Berlin, Heidelberg : Springer Vieweg, 2012, S. 59–68

[178] Wendzel, S. ; Zander, S. ; Fechner, B. ; Herdin, C.: Pattern-Based Survey and Categorization of Network Covert Channel Techniques. In: *ACM Computing Surveys* 47 (2015), Nr. 3, S. 1–27

[179] Whyte, W. ; Weimerskirch, A. ; Kumar, V. ; Hehn, T.: A security credential management system for V2V communications. In: *IEEE Vehicular Networking Conference* (2013), S. 1–8

[180] Willig, A.: *Investigations on MAC and Link Layer for a Wireless PROFIBUS Over IEEE 802.11*, TU Berlin, Diss., 2002

[181] Wischhof, L.: *Self-Organizing Communication in Vehicular Ad Hoc Networks*, TU Hamburg-Harburg, Diss., 2007

[182] Wolinsky, D. ; St. Juste, P. ; Boykin, P. ; Figueiredo, R.: Addressing the P2P Bootstrap Problem for Small Overlay Networks. In: *IEEE International Conference on Peer-to-Peer Computing*, IEEE, 2010, S. 1–10

[183] Xu, J. ; Güting, R.: A Generic Data Model for Moving Objects. In: *Geoinformatica* 17 (2013), S. 125–127

[184] Yang, H. ; Oleshchuk, V. ; Prinz, A.: Verifying Group Authentication Protocols by Scyther. In: *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* 7 (2016), S. 3–19

[185] Yi, P. ; Dai, Z. ; Zhong, Y. ; Zhang, S.: Resisting Flooding Attacks in Ad Hoc networks. In: *International Conference on Information Technology: Coding and Computing* 2 (2005), S. 657–662

[186] Yuan, C.: Mobile Autonomous Systems: Sensing, Reasoning and Acting. In: Kubek, M. (Hrsg.) ; Li, Z. (Hrsg.): *Autonomous Systems* Bd. 862, VDI Verlag, 2018 (Fortschritt-Berichte VDI), S. 2

[187] Zhang, C.: *On Achieving Secure Message Authentication for Vehicular Communications*, University of Waterloo, Diss., 2010

[188] Zöbel, D.: *Echtzeitsysteme*. Berlin, Heidelberg : Springer Vieweg, 2020

[189] Zöbel, D. ; Polock, D. ; Wojke, P.: Steering Assistance for Backing Up Articulated Vehicles. In: *Journal of Systemics, Cybernetics and Informatics* 1 (2003), Nr. 5, S. 101–106

Teilergebnisse der vorliegenden Arbeit wurden veröffentlicht oder zur Veröffentlichung eingereicht:

Maget, C.: Vehicle Guidance System based on Secure Mobile Communication. In: Magaia, N. (Hrsg.) ; Mastorakis, G. (Hrsg.) ; Mavromoustakis, C. (Hrsg.) ; Pallis, E. (Hrsg.) ; Markakis, E. (Hrsg.): *Intelligent Technologies for Internet of Vehicles*, 2021 (Internet of Things – Technologies, Communications and Computing)

Maget, C.: Sichere Mobilfunkkommunikation für ein Fahrzeugleitsystem. In: Unger, H. (Hrsg.): *Echtzeit 2020*, Springer Vieweg, Wiesbaden, 2020 (Informatik aktuell)

Maget, C.: Zur sicheren Vernetzung von Kraftfahrzeugen. In: Unger, H. (Hrsg.): *Echtzeit 2019*, Springer Vieweg, Wiesbaden, 2019 (Informatik aktuell), S. 89–98

Maget, C.: Architecture for Trust-based Machine to Machine Communication. In: Kubek, M. (Hrsg.) ; Li, Z. (Hrsg.): *Autonomous Systems 2018 – Proceedings of the 11th Conference*, VDI Verlag, 2018, S. 114–126

Die Reihen der Fortschritt-Berichte VDI:

1 Konstruktionstechnik/Maschinenelemente
2 Fertigungstechnik
3 Verfahrenstechnik
4 Bauingenieurwesen
5 Grund- und Werkstoffe/Kunststoffe
6 Energietechnik
7 Strömungstechnik
8 Mess-, Steuerungs- und Regelungstechnik
9 Elektronik/Mikro- und Nanotechnik
10 Informatik/Kommunikation
11 Schwingungstechnik
12 Verkehrstechnik/Fahrzeugtechnik
13 Fördertechnik/Logistik
14 Landtechnik/Lebensmitteltechnik
15 Umwelttechnik
16 Technik und Wirtschaft
17 Biotechnik/Medizintechnik
18 Mechanik/Bruchmechanik
19 Wärmetechnik/Kältetechnik
20 Rechnerunterstützte Verfahren (CAD, CAM, CAE CAQ, CIM ...)
21 Elektrotechnik
22 Mensch-Maschine-Systeme
23 Technische Gebäudeausrüstung

ISBN 978-3-18-387210-7