

Reihe 10

Informatik/  
Kommunikation

Nr. 872

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

## Auf sichere Mobilfunkkommunikation gestütztes Fahrzeugleitsystem



**FernUniversität in Hagen**  
**Schriften zur Informations-  
und Kommunikationstechnik**

<https://doi.org/10.51202/vdi3186872104-1>

Generiert durch IP '3.133.155.100' am 21.05.2024, 23:31:32

Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.



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. Kyandoghene 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](http://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](http://www.dnb.de).

#### Schriften zur Informations- und Kommunikationstechnik

Herausgeber:

Wolfgang A. Halang, Lehrstuhl für Informationstechnik

Herwig Unger, Lehrstuhl für Kommunikationstechnik

FernUniversität in Hagen

© VDI Verlag GmbH · Düsseldorf 2021

Alle Rechte, auch das des auszugsweisen Nachdruckes, der auszugsweisen oder vollständigen Wiedergabe (Fotokopie, Mikrokopie), der Speicherung in Datenverarbeitungsanlagen, im Internet und das der Übersetzung, vorbehalten.

Als Manuskript gedruckt. Printed in Germany.

ISSN 0178-9627

ISBN 978-3-18-387210-7

<https://doi.org/10.51202/9783186872104-1>

Generiert durch IP '3.133.155.100', am 21.05.2024, 23:31:32.

Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

# 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. Kyandoghene 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	VIII
Nomenklatur	X
Zusammenfassung	XII
<b>1 Sicherheit im Internet der Dinge</b>	<b>1</b>
1.1 Kommunikation in der Automatisierungstechnik	1
1.2 Drahtlose Kommunikation beweglicher Objekte	2
1.3 Angreifbarkeit der Funkschnittstelle	2
1.4 Einsatz perfekt sicherer Verschlüsselung	3
1.5 Anwendungsgebiet Fahrzeugleitsystem	3
1.6 Beitrag der Arbeit und weitere Anwendungsgebiete	4
<b>2 Anforderungen an Fahrzeugleitsysteme</b>	<b>6</b>
2.1 Geometrische Vorbetrachtung	7
2.2 Allgemeine Anforderungen	8
2.3 Beteiligte Akteure	9
2.3.1 Fahrer und Passagiere	9
2.3.2 Fahrzeuge	10
2.3.3 Vermittlungstechnik	11
2.3.4 Administration	13
2.4 Anforderungen an die Netztechnik	13
2.4.1 Funktechnik	14
2.4.2 Topologie und Routing	14
2.4.3 Identifikatoren und Adressen	15
2.5 Anforderungen an die funktionale Sicherheit	15
2.5.1 Funktionsanalyse	16
2.5.2 Gefahren- und Risikoanalyse	19
2.5.3 Sicherheitsziele und Automotive Safety Integrity Levels	20
2.5.4 Funktionales Sicherheitskonzept	22
2.5.5 Technisches Sicherheitskonzept	22
2.6 Anforderungen an die Informations- und Kommunikationssicherheit	22
2.6.1 Allgemeine Schutzziele	24
2.6.2 Weitere Schutzziele	25
2.6.3 Schlüsselerzeugung und -verteilung	25
2.6.4 Authentisierung und Authentifizierung	27
2.6.5 Autorisierung	28
2.6.6 Ver- und Entschlüsselung	28
2.6.7 Nachrichtenübertragung	28

2.7	Anforderungen an die Informationsverarbeitung . . . . .	29
2.7.1	Datenspeicher . . . . .	30
2.7.2	Datenverarbeitungsgeräte . . . . .	31
2.7.3	Skalierung . . . . .	31
2.8	Zusammenfassung der Anforderungen . . . . .	31
2.8.1	Infrastrukturmodus anstatt Ad-hoc-Netz . . . . .	32
2.8.2	Symmetrische anstatt asymmetrischer Verschlüsselung . . . . .	34
2.8.3	Formale Sprache anstatt Freitext . . . . .	34
<b>3</b>	<b>Stand der Technik in Wissenschaft und Praxis</b>	<b>36</b>
3.1	Sicherheit mechatronischer Systeme . . . . .	36
3.1.1	Informations- und kommunikationstechnische Sicherheit . . . . .	36
3.1.2	Funktionale Sicherheit . . . . .	37
3.1.3	Echtzeit in der Automatisierungstechnik . . . . .	38
3.1.4	Systemintegration von Fahrzeugsystemen . . . . .	38
3.2	Struktur informationsverarbeitender Systeme . . . . .	39
3.2.1	Automatisierungspyramide . . . . .	39
3.2.2	Referenzarchitekturmodell Industrie 4.0 . . . . .	39
3.2.3	Open Systems Interconnection-Modell . . . . .	41
3.2.4	Internetprotokollfamilie und TCP/IP-Referenzmodell . . . . .	41
3.3	Informationsübertragung durch drahtlose Kommunikationsnetze . . . . .	42
3.3.1	Physikalische Möglichkeiten und Grenzen . . . . .	42
3.3.2	Topologie . . . . .	43
3.3.3	Identifizierung und Routing . . . . .	46
3.3.4	Synchronisierung und Konsens . . . . .	46
3.3.5	Nachrichtenübertragung in Verkehrssystemen . . . . .	47
3.4	Informationssicherheit durch angewandte Kryptologie . . . . .	48
3.4.1	Paradigmen und kryptografische Sicherheit . . . . .	49
3.4.2	Authentifizierung und Autorisierung . . . . .	52
3.4.3	Bedrohungen für die IKT-Sicherheit und deren Abwehr . . . . .	53
3.5	Zwischenfazit . . . . .	54
3.5.1	Forschungslücke . . . . .	55
3.5.2	Entwicklungsziel . . . . .	55
<b>4</b>	<b>Die Sichere Kommunikationsarchitektur für Fahrzeugsysteme SIKAF</b>	<b>57</b>
4.1	Organisatorische Struktur . . . . .	57
4.1.1	Hoheitliche Behörde . . . . .	58
4.1.2	Betreiber von Mobilfunkkommunikation . . . . .	59
4.1.3	Fahrzeuge . . . . .	59
4.2	Technischer Aufbau . . . . .	59
4.2.1	Zentral ausgerichtete Architektur . . . . .	60
4.2.2	Identifizierung und Authentifizierung der Teilnehmer . . . . .	60
4.2.3	Anbindung des Relais . . . . .	61
4.2.4	Informationsverwaltung in den Fahrzeugen . . . . .	61
4.3	Übertragungsprotokolle . . . . .	62
4.3.1	SIKAF-P (OSI-Schichten 5 bis 7) . . . . .	63
4.3.2	Vermittlung und Transport (OSI-Schichten 3 und 4) . . . . .	63

4.3.3	Netzzugang (OSI-Schichten 1 und 2)	64
4.4	Nachrichten	64
4.4.1	Nachrichtenstruktur	65
4.4.2	Klassifizierung der Nachrichten	66
4.4.3	Formale Sprachdefinition	67
4.5	Kryptografische Absicherung	67
4.5.1	Maskenerzeugung und Maskenverteilung	68
4.5.2	Maskensperrung	70
4.5.3	Maskierung	71
4.5.4	Demaskierung	71
4.6	Datenübertragung	72
4.6.1	Betrachtung der Teilstrecken	72
4.6.2	Multicast und Broadcast	72
4.6.3	Filterung	73
4.7	Zusammenfassung der Eigenschaften von SIKAF	74
<b>5</b>	<b>Implementierung und Evaluierung</b>	<b>75</b>
5.1	Entwurf angepasster Testverfahren	75
5.1.1	Testverfahren zur Evaluierung der Maskierung und Demaskierung	76
5.1.2	Testverfahren zur Evaluierung der Datenübertragung	78
5.1.3	Testverfahren zur Evaluierung der Datenverarbeitung	80
5.2	Prototypische Implementierung	81
5.2.1	Eingesetzte Hardware	82
5.2.2	Betriebssystem	84
5.2.3	Formale Sprache für Nachrichten	85
5.2.4	Exemplarische Nachrichten	85
5.2.5	Klassifizierung von Nachrichteninhalten	96
5.2.6	Benötigte Maskengröße	99
5.2.7	Softwarearchitektur	104
5.3	Funktionale Sicherheit von Fahrzeugleitsystemen	106
5.3.1	Status und Abgrenzung	107
5.3.2	Vermeidung systematischer Fehler	107
5.3.3	Beherrschung zufälliger Fehler	108
5.3.4	Induktive und deduktive Fehleranalyse	109
5.4	Anwendungen und Geschäftsmodelle	110
5.4.1	Ausstattung der Fahrzeugflotte	110
5.4.2	Basis- und Komfortfunktionen	111
5.5	Zusammenfassung von Evaluierung und Implementierung	112
<b>6</b>	<b>Gesamtzusammenfassung und Ausblick</b>	<b>114</b>
6.1	Einordnung der Architektur	114
6.2	Möglichkeiten und Grenzen der Architektur	115
6.3	Technische Erweiterungen	116
6.4	Neue Konzepte für dezentrale autonome Systeme	116
6.5	Schlussbetrachtung	117

---

# Abkürzungsverzeichnis

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

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

---

# Nomenklatur

<b>Alphabet</b>	Ein Alphabet ist eine Menge von Zeichen, aus denen durch Verkettung Klartext, Schlüssel, Maske und Schlüsseltext zusammengesetzt werden.
<b>Chiffriermaske</b>	Eine Chiffriermaske (kurz Maske) ist ein Parameter des eingesetzten kryptografischen Verfahrens. Durch <i>XOR</i> -Verknüpfung von Klartext und Maske entsteht der Schlüsseltext. Durch <i>XOR</i> -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.
<b>Codebuch</b>	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.
<b>Maske</b>	Kurzform von Chiffriermaske
<b>Maskengröße</b>	siehe Schlüsselgröße
<b>Maskenlänge</b>	siehe Schlüssellänge
<b>Maskenvorrat</b>	siehe Schlüsselvorrat
<b>Maskierung</b>	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. <i>One Time Pad</i> ).
<b>Nachricht</b>	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.
<b>Nachrichtenlänge</b>	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.
<b>Prüfsumme</b>	Eine Prüfsumme ist eine Zeichenkette fester Länge, die durch einen Algorithmus aus einer Nachricht beliebiger Länge erzeugt wird. Eine

---

	<p>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.</p>
<b>Relais</b>	<p>Ein Relais ist eine Vermittlungsstelle zwischen zwei Kommunikationsteilnehmern. Alle Nachrichten werden vom Sender zum Relais geschickt und von dort zum Empfänger weitergeleitet.</p>
<b>Schlüssel</b>	<p>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.</p>
<b>Schlüsselgröße</b>	<p>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.</p>
<b>Schlüssellänge</b>	<p>Die Schlüssellänge ist die Anzahl der Zeichen eines einzelnen Schlüssels.</p>
<b>Schlüsseltext</b>	<p>Ein Schlüsseltext ist die durch Verschlüsselung oder Maskierung eines Klartextes entstandene Zeichenkette. Weitere Bezeichnungen sind Geheimtext, Kryptogramm oder Chiffre.</p>
<b>Schlüsselvorrat</b>	<p>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.</p>
<b>Verschlüsselung</b>	<p>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.</p>

---

# 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 perfekte 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 Fahrzeugsystem, 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.

