

Der Einfluss von Cloud-Computing auf die Sicherheit im Straßenverkehr

DISSERTATION

zur Erlangung des akademischen Grades

**Doktoringenieur
(Dr.-Ing.)**

genehmigt

an der Fakultät für Verkehrswissenschaften „Friedrich List“

der Technischen Universität Dresden

von

Frau Dipl.-Ing. Vivian Augele

Gutachter: Prof. Dr.-Ing. Jochen Trinckauf
Prof. Dr.-Ing. Bernard Bäker

Tag der Verteidigung: 14. Juli 2023

Bibliografischer Nachweis

Name, Vorname: Augele, Vivian

Dissertation 2022

Der Einfluss von Cloud-Computing auf die Sicherheit im Straßenverkehr

Technische Universität Dresden

Fakultät Verkehrswissenschaften „Friedrich List“

Professur für Verkehrssicherungstechnik

102 Seiten, 12 Abbildungen, 10 Tabellen, 131 Quellen

Anhang: 3 Seiten, 3 Tabellen

Autorenreferat

Jährlich sterben weltweit 1,35 Millionen Menschen durch Verkehrsunfälle. Ob Cloud-Computing zu einer Reduzierung dieser Zahl beitragen wird, wird in der vorliegenden Arbeit untersucht. Zunächst werden Cloud-Anwendungen ermittelt, welche im Straßenverkehr verwendet werden und Einfluss auf die Straßenverkehrssicherheit haben. Anschließend wird deren genauer Einfluss auf die Straßenverkehrssicherheit durch die Betrachtung von Studienergebnissen, Herstellerangaben sowie eigenen Kalkulationen untersucht. Zudem werden die Gefahren von Cyberangriffen und Netzausfällen für die ermittelten Anwendungen analysiert. Es folgt eine kritische Diskussion sowie die Zusammenfassung des Erarbeiteten: Cloud-Computing ermöglicht durch den einfachen, risikoarmen Zugang zu unlimitierten Rechenressourcen die Entwicklung und den Betrieb von Anwendungen, die Einfluss auf die Verkehrssicherheit nehmen. Es ist davon auszugehen, dass die Anwendungen bei einer weiter voranschreitenden Felddurchdringungsrate positiven Einfluss auf die Straßenverkehrssicherheit in Deutschland und anderen Industriestaaten nehmen und damit aktiv zur Reduzierung der Anzahl Verkehrstoter und -verletzter beitragen werden. Cloud-Computing wird somit ein indirekt positiver Einfluss auf die Straßenverkehrssicherheit zugeschrieben.

Abstract

1.35 million people die in traffic accidents worldwide every year. Whether cloud computing contributes to a reduction of this number is examined in the present work. First, cloud computing applications are identified, which are used in road traffic and have an impact on traffic safety. The exact influence on traffic safety is then examined by considering study results, manufacturer information and through own calculations. In addition, the dangers of cyber-attacks and network failures are examined in the context of the identified applications. This is followed by a critical discussion and a summary of what has been worked out: Cloud computing enables the development and operation of applications that affect traffic safety through simple, low-risk access to unlimited computing resources. It can be assumed that the applications will have a positive influence on traffic safety in Germany and other industrialized countries and will thus actively contribute to reducing the number of deaths and injuries, given that the penetration rate is further increasing. Cloud computing is thus attributed an indirect positive influence on road safety.

Thesen zur wissenschaftlichen Arbeit

1. Cloud-Computing ermöglicht die Entwicklung und Verwendung von Anwendungen, welche Einfluss auf die Straßenverkehrssicherheit haben. Der Einfluss von Cloud-Computing auf die Straßenverkehrssicherheit ist somit von indirekter Natur.
2. Die Verwendung der Cloud-Computing Technologie wird einen positiven Einfluss auf die Straßenverkehrssicherheit haben.
3. Der Nutzen von Cloud-Computing für die Straßenverkehrssicherheit steigt mit zunehmender Felddurchdringung.
4. Die zunehmende Vernetzung von Infrastruktur und Fahrzeugen stellt eine Chance dar, die Straßenverkehrssicherheit mit Cloud-Anwendungen zu verbessern, zur selben Zeit aber auch eine Gefahr, da die Anfälligkeit des Gesamtsystems für Cyberangriffe steigt.

Danksagung

An dieser Stelle möchte ich denjenigen Personen danken, die mich während meiner Promotionszeit unterstützt und somit maßgeblich zum Entstehen dieser Arbeit beigetragen haben.

Mein besonderer Dank gilt Herrn Prof. Dr.-Ing. Jochen Trinckauf, meinem Doktorvater, für die Betreuung meiner Arbeit, für das mir entgegengebrachte Vertrauen sowie die wohlwollende und motivierende Begleitung. Die konstruktiven und pragmatischen Konsultationen haben mich sehr ermutigt und das Licht am Ende des Tunnels sehen lassen. Sein reicher Erfahrungs- und Wissensschatz hat auch über die Promotion hinaus zu meiner persönlichen Entwicklung beigetragen.

Ich danke Herrn Prof. Dr.-Ing. Bernard Bäker für die wertvollen inhaltlichen Impulse aus der Perspektive der Fahrzeugmechatronik sowie seine Hilfsbereitschaft.

Meine Eltern standen mir mit moralischer Unterstützung jederzeit zur Verfügung, und sie übernahmen das Korrekturlesen meiner Arbeit. Dafür möchte ich ihnen herzlich danken.

Mein letzter Dank geht an meinen Arbeitgeber, Siemens Mobility/Yunex Traffic, welcher diese nebenberufliche Promotion unterstützt hat, und aus dessen Beschäftigungsverhältnis sich diverse relevante Erfahrungen und Erkenntnisse für meine Dissertation ergeben haben.

Inhaltsübersicht

1	Einführung	17
1.1	Motivation und Eingrenzung des Themengebietes	17
1.2	Begriffsdefinitionen	17
1.3	Aktueller Stand der Wissenschaft	19
1.4	Forschungsfragen	20
1.5	Untersuchungsmethodik	21
2	Stand der Technik	23
2.1	Cloud-Computing	23
2.1.1	Heutiger Entwicklungsstand	23
2.1.2	Bemessung und Bewertung von Sicherheit	25
2.1.2.1	Allgemeines zur IT-Sicherheit	25
2.1.2.2	Geltende Normen und Richtlinien	26
2.1.3	Sicherheitsrisiken	27
2.2	Sicherheit im Straßenverkehr	27
2.2.1	Infrastrukturelle Verkehrssicherheit	27
2.2.2	Fahrzeugsicherheit	31
2.2.3	Straßenverkehrsunfallstatistiken	33
2.2.4	Bemessung und Bewertung von Sicherheit	37
2.2.4.1	Geltende Normen und Richtlinien	37
2.2.4.2	Maßeinheiten	38
2.2.5	Sicherheitsrisiken im heutigen Straßenverkehr	39
3	Anwendung von Cloud-Computing im Straßenverkehr	41
3.1	Übersicht	41
3.2	Straßenverkehrsmanagement	43
3.3	Kooperative intelligente Verkehrssysteme	46
3.4	Proprietäre Datenanalyse und Warnung	59
3.5	Daten- und Videoanalyse für Planungszwecke	61
3.6	Daten- und Videoanalyse für operative Zwecke	62
3.7	Community-getriebene Smartphone-Anwendungen	63
4	Positiver Einfluss auf die Straßenverkehrssicherheit	64
4.1	Straßenverkehrsmanagement	64
4.2	Kooperative intelligente Verkehrssysteme	65
4.2.1	Methodik	65
4.2.2	Einsatzfahrzeugwarnung	66
4.2.3	Knotenpunktkollisionswarnung	66

4.2.4	Falschfahrerwarnung.....	66
4.2.5	Warnung stehendes Fahrzeug.....	67
4.2.6	Verkehrssituationswarnung.....	67
4.2.7	Warnung Rotlichtverstoß.....	67
4.2.8	Baustellenwarnung.....	68
4.2.9	Dezentralisierte Floating-Car-Daten.....	68
4.2.10	Warnung ungeschützte Verkehrsteilnehmer.....	68
4.2.11	Behördliche/kontextbezogene Geschwindigkeitsbeschränkung	69
4.2.12	Kurvenwarnung	69
4.2.13	LSA-Geschwindigkeitsempfehlung	70
4.2.14	Schilder im Fahrzeug	70
4.2.15	Wetterinformationen	70
4.2.16	Bahnübergang.....	70
4.2.17	Verminderung von Stauausbreitung.....	71
4.2.18	Reduzierte Sicht	71
4.2.19	Fahrzeug-/ÖV-Priorisierung	72
4.3	Proprietäre Datenanalyse und Warnung	72
4.4	Daten- und Videoanalyse für Planungszwecke.....	72
4.5	Daten- und Videoanalyse für operative Zwecke.....	73
4.6	Community-getriebene Smartphone-Anwendungen.....	73
5	Andere Einflüsse auf die Straßenverkehrssicherheit	75
5.1	Verhaltensanpassungen.....	75
5.2	Nutzerakzeptanz	78
5.3	Cyberangriffe und Netzausfälle	78
5.4	Datenschutz.....	87
6	Ergebnisse und Diskussion	89
6.1	Positiver Sicherheitseinfluss von Cloud-Anwendungen	89
6.1.1	Übersicht.....	89
6.1.2	Kooperative intelligente Verkehrssysteme.....	91
6.1.3	Daten- und Videoanalyse für Planungszwecke	92
6.1.4	Daten- und Videoanalyse für operative Zwecke	93
6.2	Latenz in der Datenübertragung.....	94
6.3	Cloud-Computing und das automatisierte Fahren	96
6.4	Lokale Rechenzentren.....	97
6.5	Fahrerassistenzsysteme	98
6.6	Weiterer Forschungsbedarf	99
7	Zusammenfassung	101
	Literaturverzeichnis	103

Abbildungsverzeichnis

Abbildung 1: schematische Darstellung Cloud-Computing.....	24
Abbildung 2: Unfalltypenkarte [45]	34
Abbildung 3: Legende einer Unfalltypenkarte [46]	34
Abbildung 4: Entwicklung der im Straßenverkehr getöteten Personen [47]	35
Abbildung 5: Getötete Personen nach Verkehrsbeteiligungsart und Ortslage [47]	35
Abbildung 6: Fehlverhalten von Fahrern bei Unfällen mit Personenschaden [47]	36
Abbildung 7: Übersicht der identifizierten Cloud-Anwendungen im Straßenverkehr.....	42
Abbildung 8: ‚NordicWay‘-Architektur [85]	57
Abbildung 9: Architektur Unfallvorhersageplattform ‚Pioneer Corporation‘ [90].....	60
Abbildung 10: Architektur ‚cloudbasierte Falschfahrerwarnung Bosch‘ [92]	61
Abbildung 11: Übersicht Cyberangriffe 2. Halbjahr 2021 [119]	81
Abbildung 12: personenbezogene Daten im ‚DFRS-Ökosystem‘ [120].....	87

Tabellenverzeichnis

Tabelle 1: Erläuterung und Übersetzung englischer Begriffe	19
Tabelle 2: volkswirtschaftliche Unfallkosten Getötete und Verletzte 2020 [55].....	38
Tabelle 3: volkswirtschaftliche Unfallkosten Sachschäden 2020 [55].....	39
Tabelle 4: C-ITS-Anwendungsfälle ETSI (Teil 1) [79]	51
Tabelle 5: C-ITS-Anwendungsfälle ETSI (Teil 2) [79]	52
Tabelle 6: weitere C-ITS-Anwendungsfälle [77]	53
Tabelle 7: potenzielle Sicherheitsauswirkungen der C-ITS-Anwendung, ‚Warnung ungeschützter Verkehrsteilnehmer‘ nach dem Modell von Risto Kulmala [24]	77
Tabelle 8: mögliche Auswirkungen von Cyberangriffen und Netzausfällen	82
Tabelle 9: Übersicht der positiven Auswirkungen auf die Verkehrssicherheit.....	90
Tabelle 10: zurückgelegter Weg während Latenzzeit.....	94

Abkürzungsverzeichnis

ASIL	Automotive Safety Integrity Level
AWS	Amazon Web Services
BSI	Bundesamt für Sicherheit in der Informationstechnik
CODIA	Co-Operative Systems Deployment Impact Assessment
C-ITS	Cooperative – Intelligent Transportation Systems
DFRS	Data for Road Safety
DoS	Denial of Service
EN	Europäische Norm
ETSI	Europäische Institut für Telekommunikationsnormen
EU	Europäische Union
FGSV	Forschungsgesellschaft für Straßen- und Verkehrswesen
IaaS	Infrastructure as a Service
IT	Informationstechnik
LSA	Lichtsignalanlage
PaaS	Platform as a Service
SaaS	Software as a Service
SRTI	Safety Related Traffic Information
TMC	Traffic Management Centre
VDI	Verein Deutscher Ingenieure

1 Einführung

1.1 Motivation und Eingrenzung des Themengebietes

Als ich im Jahr 2020 begann, bei der Siemens Mobility GmbH im Bereich Straßenverkehrstechnik als Solution Engineer zu arbeiten, bemerkte ich, dass Cloud-Computing ein wichtiges Thema ist, und der Begriff von Kollegen und auch Wettbewerbern fast inflationär verwendet wird, es ist ein Modewort.

Die Verkehrsmanagement-Software, für die ich hauptsächlich verantwortlich war, befand sich mitten im Transformation-Prozess ‚in die Cloud‘. Zeitgleich nahm ich damals bei unseren Kunden, Städten und Kommunen, eine mehr oder weniger skeptische Zurückhaltung wahr, wenn sich Gespräche in Richtung Cloud bewegten.

Ich stellte fest, dass viele Leute gar nicht genau wissen, was Cloud-Computing bedeutet und welche Potenziale oder Gefahren diese Technologie mit sich bringt. Es gibt nur wenige wissenschaftliche Veröffentlichungen, die sich mit der Beziehung und der Wechselwirkung zwischen Straßenverkehrstechnik und Cloud-Computing beschäftigen. Daraus entstand die Idee zu dieser Dissertation.

Die Fokussierung auf die Straßenverkehrssicherheit ergab sich durch die Relevanz dieses Themas: Jährlich sterben weltweit 1,35 Millionen Menschen durch Verkehrsunfälle. [1] Eine hohe Straßenverkehrssicherheit ist somit ein außerordentlich wichtiges Ziel aller Akteure in diesem Bereich.

Die Betrachtung des Themas im Kontext des Fahrzeuges und des automatisierten Fahrens wäre ebenfalls ein interessanter Ansatz gewesen. Aufgrund meiner Beschäftigung im Bereich der Straßenverkehrstechnik und meines Verkehrsingenieursstudiums mit Fokus Verkehrstelematik liegt der Schwerpunkt der Untersuchungen in dieser Arbeit jedoch auf Cloud-Computing im Kontext der Verkehrsinfrastruktur. Schnittstellenanwendungen zwischen Infrastruktur und Fahrzeugen (kooperative intelligente Verkehrssysteme) werden untersucht und stellen die Grenze des in dieser Arbeit behandelten Untersuchungsraums dar. Abbildung 7 (Seite 42) zeigt eine Übersicht über die konkreten untersuchten Anwendungsgebiete. Des Weiteren fokussiert sich diese Arbeit auf die Auswirkungen für die Straßenverkehrssicherheit von Industriestaaten.

1.2 Begriffsdefinitionen

Die Fachbegriffe der Themengebiete Sicherheit, (Tele-)Kommunikation sowie vernetztes und kooperatives Fahren kommen im Zuge der europäischen und internationalen Bemühungen zur Standardisierung häufig aus dem Englischen. Eine Übersetzung ins Deutsche wäre zum Teil sinnentstellend und wird in dieser Arbeit, um die Namenskonvention der Standards und

Spezifikationen einheitlich zu verwenden, nicht immer vorgenommen. Deutsche Begriffe werden benutzt, sofern diese in der Fachliteratur vorhanden sind. Als Orientierung und zum besseren Verständnis dieser Arbeit sind die englischen Begriffe in Tabelle 1 aufgelistet und erläutert. Es folgen Definitionen von Begriffen, deren Bedeutung eine zentrale Rolle im weiteren Textverlauf spielen:

- **Cloud** ist ein räumlich entferntes Rechenzentrum. Die Kommunikation mit der Cloud erfolgt über das Internet.
- **Cloud-Computing** ist eine Technologie, welche Speicherplatz, Rechenleistung sowie Entwicklungsumgebung in einem zentralisierten Rechenzentrum (der Cloud) zur Verfügung stellt und dort die Implementierung von Anwendungen erlaubt. Die Kommunikation zwischen Datenquellen, den Anwendungen in der Cloud sowie Informationsempfängern erfolgt über das Internet.
- **Cloud-Anwendung** ist eine Computersoftware, welche in einer Cloudumgebung implementiert ist. Beispiele hierfür sind ‚Microsoft Office 365‘, ‚Zoom‘, ‚Amazon Web Services‘ und ‚Google Docs‘.
- **Intelligente Verkehrssysteme** (im englischen Intelligent Traffic Systems) werden vom Europäischen Parlament und Rat folgendermaßen definiert: [2]

„Intelligente Verkehrssysteme (IVS) sind hochentwickelte Anwendungen, die - ohne Intelligenz an sich zu beinhalten - darauf abzielen, innovative Dienste im Bereich verschiedener Verkehrsträger und des Verkehrsmanagements anzubieten, und die verschiedenen Nutzer mit umfassenderen Informationen zu versorgen und sie in die Lage zu versetzen, die Verkehrsnetze auf sicherere, koordinierter und ‚klügere‘ Weise zu nutzen.“

- **Safety** beschreibt die Betriebssicherheit, den Schutz der Umgebung vor einem System oder Objekt. Beispielsweise der Anschnallgurt in Kraftfahrzeugen.
- **Security** beschreibt den Schutz eines Systems vor der Umgebung. Beispielsweise eine Firewall, die Server vor Angriffen schützen kann.

Zur besseren Lesbarkeit wird in der vorliegenden Dissertation das generische Maskulinum verwendet, wobei beide Geschlechter gleichermaßen gemeint sind.

Tabelle 1: Erläuterung und Übersetzung englischer Begriffe

Englischer Begriff	Mögliche deutsche Übersetzung
cloud service provider	Cloud-Anbieter
cloud computing	Rechnerwolke
Cooperative-Intelligent Transportation Systems	kooperative intelligente Verkehrssysteme
edge computing	dezentrale Datenverarbeitung am Rand des Netzwerkes
Denial of Service	Nichtverfügbarkeit eines Internetdienstes
Infrastructure as a Service	Infrastruktur als Dienst
IT-Security	IT-Sicherheit
on-demand self service	automatisierte Bereitstellung von Diensten
Platform as a Service	Laufzeit-/Entwicklungsumgebung als Dienst
safety related traffic information	sicherheitsrelevante Verkehrsinformation
Software as a Service	Software als Dienst
vehicular cloud computing	zur Verfügung gestellte, temporär nicht genutzte Rechenressourcen von Fahrzeugen

1.3 Aktueller Stand der Wissenschaft

Die Anfänge des Cloud-Computing gehen in das Jahr 1960 zurück. Erst seit 2008 wird dieses Thema generell in der Wissenschaft diskutiert. [3] Seither wurden verschiedene Architekturen, Anwendungsfelder, Sicherheitsmaßnahmen, Geschäftsmodelle etc. vorgestellt. Diverse Veröffentlichungen sind entstanden, die sich auf den Straßenverkehr konzentrieren.

Verschiedene Publikationen sind erschienen, welche Architekturen für die Simulation von Verkehr, Optimierung von Verkehrsfluss durch LSA-Steuerung und/oder Verkehrsmanagement in einem Cloud-Computing Umfeld vorschlagen. Beispiele hierfür sind die Veröffentlichungen von Jaworski et al., Yang et al., Yu et al., Jaworski, Jankovic et al. und Trivedi et al. [4–9] Diese Veröffentlichungen vereint, dass die Erarbeitung der Fragestellungen auf einen theoretischen Ansatz beschränkt ist und keine reale Implementierung im Feld erfolgte.

Weiterhin gibt es eine Vielzahl an Publikationen, die neuartige Technologien und Algorithmen im Cloud-Umfeld mit Bezug auf den Straßenverkehr diskutieren. Beispiele hierfür sind Veröffentlichungen von Shengdong et al. und Zhang et al. [10, 11]

Ein weiteres beachtetes Thema ist das ‚vehicular cloud computing‘, das Zurverfügungstellen von nicht verwendeten Rechenressourcen in Fahrzeugen. Ein Zusammenschluss dieser Ressourcen in einer lokalen sogenannten ‚Fahrzeug-Cloud‘ erlaubt es wiederum anderen

Fahrzeugen, die Rechenressourcen benötigen, darauf zuzugreifen. Veröffentlichungen zu diesem Thema kommen von Lee et al., Goumidi et al., Skondras et al., Sharma et al., Ahmad et al. und Tahmasebi et al. [12–17]

Die oben gelisteten Publikationen im kombinierten Feld des Cloud-Computing und des Straßenverkehrs wählten alle Cloud-Computing als Technologie. Es wurde aber nicht untersucht, welche tatsächlichen Auswirkungen die vorgestellten Erkenntnisse auf die Straßenverkehrssicherheit oder andere Größen haben. Zumeist wird angegeben, dass eine Verbesserung der Sicherheit des Verkehrsflusses und/oder eine Verringerung der Emissionen angestrebt werde oder vorstellbar sei. Quantifiziert oder genauer untersucht werden diese Aussagen allerdings nicht.

Ein zweiter Forschungsbereich, welcher relevant für das Themengebiet dieser Dissertation ist, ist die Fahrzeug- und Verkehrssicherheit. In diesem Zusammenhang werden auf Basis von Datenerhebungen, -analysen und Simulationen, Erkenntnisse über Unfälle gesammelt, welche Fahrzeugherstellern, Stadtplanern, Betreibern und weiteren am Straßenverkehr Beteiligten dazu dienen, die Sicherheit im Straßenverkehr zu verbessern. Es gibt viele Publikationen, welche sich mit den Auswirkungen von speziellen Sicherheitssystemen in Fahrzeugen beschäftigen, zumeist basierend auf Simulationen. Beispiele hierfür sind Veröffentlichungen von Louwse et al., Validi et al. und Vaa et al. [18–20] Zudem gibt es Veröffentlichungen, die sich prospektiv mit den Auswirkungen neuartiger Sicherheitssysteme in Fahrzeugen oder von intelligenten Verkehrssystemen beschäftigen, zum Beispiel durch Straßenverkehrsteilnehmer- und Fahrerhaltensmodellierungen. Beispiele hierfür sind Publikationen von Mai, Silla et al., Kulmala et al. und Michon et al. [21–24]

Die Publikationen im Bereich der Verkehrssicherheit gehen auf Auswirkungen verschiedener Sicherheitssysteme ein. Eine verknüpfte Untersuchung der Themenfelder Cloud-Computing und Straßenverkehrssicherheit ist in bisherigen Publikationen nicht erfolgt. Demnach ist das Thema dieser Dissertation - Auswirkungen von Cloud-Computing auf die Straßenverkehrssicherheit - bislang kaum erforscht.

1.4 Forschungsfragen

Es ergeben sich für die vorliegende Dissertation folgende Forschungsfragen:

1. Wo wird Cloud-Computing im Straßenverkehr aktuell angewandt?
2. Welche Cloud-Anwendungen haben Einfluss auf die Straßenverkehrssicherheit?
3. Welchen Einfluss hat Cloud-Computing auf die physische Sicherheit im Straßenverkehr?
4. Welche Gefahr stellen Cyberangriffe und Netzausfälle bei Cloud-Anwendungen für die Straßenverkehrssicherheit dar?

1.5 Untersuchungsmethodik

Die Untersuchung des gewählten Dissertationsthemas startete mit einer Literaturrecherche. Hierzu wurde primär die Suchmaschine, Google Scholar, aber auch die Forschungsdatenbanken, ‚IEEE Xplore‘ und ‚ResearchGate‘ verwendet. Die vorhandene Literatur ist überwiegend in englischer Sprache verfasst. Daher wurde die Recherche hauptsächlich in Englisch durchgeführt. Folgende Suchbegriffe wurden eingegeben:

- ADAS safety impact
- cloud computing applications traffic
- cloud computing Intelligent Transportation Systems
- Cloud-Computing intelligente Verkehrssysteme
- cloud computing road traffic
- cloud computing safety impact
- cloud computing security threats
- Cloud-Computing Straßenverkehr
- Cloud-Computing Straßenverkehrsmanagement
- Cloud-Computing Straßenverkehrssicherheit
- Cloud-Computing Sicherheit
- cloud computing traffic
- cloud computing traffic control
- cloud computing traffic flow
- cloud computing traffic management
- cloud computing traffic safety
- cloud computing traffic simulation
- Intelligent Transport Systems safety impact
- vehicular cloud computing

Als Nächstes erfolgte die Erarbeitung des in Kapitel 2 beschriebenen, aktuellen Standes der Technik. Im Vordergrund standen hierfür Veröffentlichungen von Normungsinstitutionen, dem ‚Bundesamt für Informationstechnik‘ (BSI), technische Regelwerke der ‚Forschungsgesellschaft für Straßen- und Verkehrswesen‘ (FGSV) sowie Verkehrssicherheitsstatistiken.

Auf Basis der Recherchen folgte die Ausarbeitung der in Kapitel 1.4 aufgezeigten

Forschungsfragen. Zur Beantwortung dieser wurden zunächst Cloud-Anwendungen im Straßenverkehr identifiziert und untersucht. Die Erkenntnisse wurden durch Recherchen im Internet, Gespräche mit Experten und Messebesuche („Intertraffic“ und „ITS-Weltkongress“) sowie der eigenen Berufserfahrung verifiziert und sind in Kapitel 3 dargestellt.

Der Einfluss von Cloud-Computing auf die Straßenverkehrssicherheit wurde anschließend mittels publizierter Studien zu einzelnen Anwendungen ermittelt. Im Vordergrund standen hier die Ergebnisse diverser Pilotprojekte sowie simulations- und modellbasierte Auswertungen. Sofern keine Studien vorhanden waren, wurden die Auswirkungen auf Basis von Unfallstatistiken selbst berechnet und das Verfahren erläutert. Kapitel 4 fokussiert dabei auf den positiven Einflüssen, wohingegen in Kapitel 5 weitere zum Teil konträre Effekte dargestellt werden. Im Rahmen dieser Arbeiten wurden die unterschiedlichen Studienergebnisse - wenn möglich - in einheitliche Maßeinheiten (Reduktion von Verkehrstoten, Verletzten und Unfallzahl) umgerechnet, um die Bewertung des Einflusses auf die Straßenverkehrssicherheit zu erleichtern.

Zur Beantwortung der letzten Forschungsfrage, welche Gefahr Cyberangriffe und Netzausfälle bei Cloud-Anwendungen für die Straßenverkehrssicherheit darstellen, wurden die Verwendungszwecke der verschiedenen Anwendungen im Kontext verschiedener Cyber-Extrem Szenarien untersucht. Anschließend wurden die Gefahren für die Verkehrssicherheit abgeleitet.

2 Stand der Technik

2.1 Cloud-Computing

2.1.1 Heutiger Entwicklungsstand

Cloud-Computing wird von dem Bundesamt für Sicherheit in der Informationstechnik (BSI) wie folgt definiert: [25]

„Cloud-Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannweite, der im Rahmen von Cloud-Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software.“

Technologische Basis für das Cloud-Computing ist die Virtualisierung. Mit Hilfe einer Abstraktionsschicht zwischen physikalischer Hardware und den Anwendungen, können Geräte, Betriebssysteme oder Services virtuell nachgebildet werden. Dies ermöglicht die Zusammenfassung von Rechenressourcen und dadurch eine höhere Auslastung von Hardware. [26] Die Hardware wird beim Cloud-Computing in großen Rechenzentren von sogenannten Cloud-Anbietern (im Englischen bekannt als ‚cloud service provider‘) zur Verfügung gestellt. Der Zugriff auf die IT-Ressourcen erfolgt über das Internet. Aktuell wird der Cloud-Markt von folgenden drei Anbietern dominiert: ‚Amazon Web Services‘ (AWS), ‚Google Cloud‘ und ‚Microsoft Azure‘.

Das US-amerikanische Standardisierungsgremium ‚National Institute of Standards and Technology‘ definiert einen Cloudservice über folgende Eigenschaften: [27]

1. on-demand self service: Die Bereitstellung der Dienste läuft automatisch - ohne menschliche Interaktion - mit dem Dienstleister ab.
2. breiter Netzwerkzugriff: Die Dienstleistungen können im Netz über Standard-Mechanismen von beliebigen Endgeräten abgerufen werden.
3. Ressourcen-Pool: Der Anbieter bündelt seine Rechenressourcen, um mehrere Verbraucher zu bedienen (Mandantenfähigkeit). Die Anwender wissen nicht genau, wo sich die physischen Ressourcen befinden, können aber meist vertraglich einen bestimmten Speicherort, z.B. Land oder Region, festlegen.
4. schnelle Anpassbarkeit: Die Dienstleistungen werden schnell und flexibel zur Verfügung gestellt. Das bedeutet, dass die Anwender je nach Bedarf auf zusätzliche Ressourcen zugreifen oder nicht benötigte abgeben können. Die IT-Ressourcen erscheinen aus Anwendersicht unendlich.

5. messbare Dienste: Zur Transparenz für Anbieter und Anwender kann die Ressourcenverwendung überwacht, kontrolliert und ausgewertet werden. Eine Bezahlung erfolgt nur für die in Anspruch genommenen Ressourcen.

Cloud-Computing steht für Verbraucher in drei verschiedenen Modellen zur Verfügung:

1. Infrastructure as a Service (IaaS): Der Dienstleister stellt IT-Ressourcen - wie beispielsweise Speicherplatz, Netze oder Rechenleistung - zur Verfügung, auf denen von Anwendern eigene Dienste für den internen oder externen Gebrauch aufgebaut werden können. [27] Beispiele hierfür sind ‚Amazon Web Services‘ und ‚IBM Cloud‘.
2. Platform as a Service (PaaS): Der Dienstleister stellt nicht nur die Infrastruktur zur Verfügung, sondern auch weitere Dienste, Bibliotheken, Werkzeuge und Programmiersprachen, mit denen die Verbraucher ihre Anwendungen implementieren können. Die Plattform kann somit zum Beispiel Skalierbarkeit, Nutzerberechtigungen, Mandantenfähigkeit etc. zur Verfügung stellen. [27] Beispiele hierfür sind ‚AWS Lambda‘ und ‚SAP Cloud‘.
3. Software as a Service (SaaS): Der Anwender erhält Zugriff auf und Nutzungsrechte für Anwendungen, die in einer Cloudinfrastruktur implementiert sind. Diese können webbasiert mit beliebigen internetfähigen Endgeräten aufgerufen werden. [27] Beispiele hierfür sind ‚Dropbox‘ und ‚Microsoft 365‘.

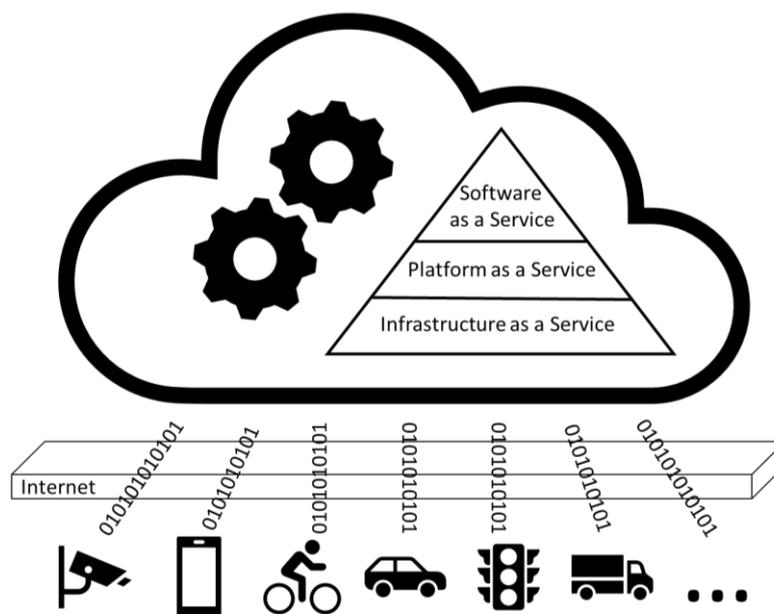


Abbildung 1: schematische Darstellung Cloud-Computing

Cloud-Computing bietet vielfältigen Nutzen für die Anwender. Ein wichtiger Vorteil ist, dass keine eigene IT-Infrastruktur aufgebaut, betrieben und gewartet werden muss. Der Cloud-Anbieter ist für die gesamte Infrastruktur verantwortlich und garantiert meist vertraglich festgehaltene Mindestverfügbarkeiten sowie die Einhaltung von Sicherheitsstandards. Außerdem

stehen IT-Ressourcen flexibel zur Verfügung und werden automatisch, verbrauchsabhängig abgerechnet. So können temporäre Leistungsspitzen leicht abgefangen werden, ohne unnötige Hardware im eigenen Rechenzentrum vorzuhalten. Da Daten in zentralisierten Rechenzentren (der Cloud) abgespeichert werden, wird der Zugriff hierauf von unterschiedlichen Standorten aus der ganzen Welt vereinfacht.

Neben den Vorteilen gibt es auch Nachteile. Aufgrund der Auslagerung der Infrastruktur besteht eine Abhängigkeit von der Internetverbindung sowie von den Cloud-Anbietern. Ersteres führt zu Zugriffsproblemen bei schlechter oder nicht vorhandener Verbindung. Letzteres führt zu einer Abhängigkeit in Bezug auf die Verfügbarkeit der Daten und Dienste, da diese nicht mehr in der eigenen Verantwortung liegt. Außerdem kann es zu Problemen mit dem Datenschutz kommen. Insbesondere personenbezogene Daten unterliegen gesetzlich einem besonderen Schutz, der nicht an den Cloud-Anbieter delegiert werden kann. [28]

2.1.2 Bemessung und Bewertung von Sicherheit

2.1.2.1 Allgemeines zur IT-Sicherheit

Cloud-Computing ist ein Teil der Informationstechnik (IT), deren Schutz allgemein als IT-Sicherheit (eng. IT-Security) bezeichnet wird. Diese wird durch folgende drei IT-Schutzziele definiert: [29]

1. Vertraulichkeit: Informationstechnik muss vertrauliche Daten und Informationen so schützen, dass nur Befugte in der vorgesehenen Art und Weise Zugriff darauf haben.
2. Integrität: Informationstechnik muss sicherstellen, dass alle Informationen korrekt, das heißt vollständig und unverändert, verarbeitet und wiedergegeben werden.
3. Verfügbarkeit: Informationstechnik muss Anwendern stets wie vorgesehen zur Verwendung zur Verfügung stehen.

Die Einhaltung der IT-Schutzziele wird meist durch ein Sicherheitskonzept, das verschiedene technische und organisatorische Maßnahmen enthält, gewährleistet. Diese können zum Beispiel folgende sein: Verschlüsselung, Zugriffskontrollen, redundanter Systemaufbau, räumlich getrennte Sicherung von Daten etc.

Des Weiteren ist im Kontext der Sicherheit der Aspekt der Funktionssicherheit zu erwähnen. Im Englischen wird dies mit ‚Safety‘ bezeichnet. Hierunter wird verstanden, dass das IT-System ordnungsgemäß funktioniert und keine ungewollten Schäden verursacht. Die beiden Begrifflichkeiten ‚Security‘ und ‚Safety‘ werden häufig verwechselt, auch weil sie im Deutschen nicht durch zwei verschiedene Worte ausgedrückt werden. Eine bekannte englische Redewendung lautet: ‚There is no safety without security‘. Im Kontext von IT-Systemen wird hierdurch der Stellenwert von IT-Security klar. ‚Safety‘ bezeichnet die Unfallvermeidung, ‚Security‘ steht für Kriminalprävention.

2.1.2.2 Geltende Normen und Richtlinien

Um die Sicherheit von Cloud-Computing zu gewährleisten, gibt es diverse Normen und Richtlinien. Anbieter von Cloud-Computing-Diensten können sich entsprechend zertifizieren lassen. Nicht alle Normen und Richtlinien sind in die deutsche Sprache übersetzt, weshalb teilweise der englische Originaltitel in der folgenden Auflistung genannt ist.

- ISO 27001 Informationstechnik - Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Anforderungen

Die ISO 27001 ist die international führende Norm für Informationssicherheits-Managementsysteme. Sie enthält Leitlinien für die Planung, Umsetzung, Überwachung und Verbesserung der Informationssicherheit in Organisationen. [30] Die Norm fokussiert nicht speziell auf Cloud-Computing, sondern Informationssicherheit im Allgemeinen.

- ISO 27002 Informationstechnik - Sicherheitsverfahren - Leitfaden für Informationssicherheitsmaßnahmen

Die ISO 27002 ist eine internationale Norm, die auf der ISO 27001 aufbaut. Sie greift die Maßnahmen der Norm ISO 27001 auf und konkretisiert sie in Bezug auf Ihre Umsetzung in der Praxis. [31]

- ISO 27017 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

Die ISO 27017 ist eine internationale Norm, welche die Normen ISO 27001 und 27002 für die Anwendungen im Bereich Cloud-Computing konkretisiert. [32]

- ISO 27018 Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

Die ISO 27018 ist eine internationale Norm für den Schutz von personenbezogenen Daten in Cloudumgebungen. Sie enthält Richtlinien und Anforderungen für Maßnahmen im Umgang mit personenbezogenen Daten in der Cloud sowie eine Methodik zur Bewertung des Schutzes von personenbezogenen Daten in der Cloud. [33]

- Kriterienkatalog Cloud-Computing C5

Der Kriterienkatalog C5 („Cloud-Computing Compliance Criteria Catalogue“) ist ein deutsches Regelwerk, das vom BSI veröffentlicht wurde und Mindestanforderungen an ein sicheres Cloud-Computing enthält. Er unterstützt Cloud-Anwender bei der Selektion eines geeigneten Cloud-Anbieters und dem Risikomanagement. [34]

2.1.3 Sicherheitsrisiken

Wie die meisten Technologien ist auch die Verwendung von Cloud-Computing mit Sicherheitsrisiken verbunden. Im Folgenden sind Relevante dargestellt: [35, 36]

1. Denial-of-Service (DoS)-Angriff: DoS-Angriffe kennzeichnen sich durch gezielte Serverüberlastungen durch ‚Bombardierung‘ mit unzähligen Anfragen und in der Folge Serverausfällen. Anwendungen auf dem attackierten Server sind dadurch nicht erreichbar.
2. unautorisierter Zugriff und Identitätsdiebstahl: Wenn es einem Hacker gelingt, das Konto eines Nutzers zu übernehmen, können Systemaktionen durchgeführt werden, die zu Schäden führen. Beispielsweise können Aktionen überwacht, Daten abgezogen, das System manipuliert oder Handlungen im Namen des Nutzers durchgeführt werden. In Public-Cloudumgebungen können zudem Fehler in der Cloud-Administration dazu führen, dass Fremde (andere Kunden des Cloud-Anbieters) unbeabsichtigt Zugriff zu Anwendungen erhalten.
3. Datenverlust: Daten sind in der Cloud sowie auf dem Weg dorthin und zurück einem erhöhten Verlustrisiko ausgesetzt. Dies kann unbeabsichtigt beispielsweise durch falsche Konfigurationen oder durch gezielte Angriffe geschehen.
4. Ausfall der Internet- oder Netzanbindung: Fällt die Anbindung an die Cloud aus, ist ein Zugriff auf die Anwendungen nicht mehr möglich.

Die in Kapitel 2.1.2.2 dargestellten Normen und Richtlinien zielen in erster Linie auf eine sichere Verwendung von Cloud-Computing ab. Zahlreiche Maßnahmen können und sollten angewandt werden, um die Bedrohungen in der Cloud auf einem geringen Maß zu halten. Des Weiteren sind die hier gelisteten Risiken nicht ausschließlich für Cloud-Computing zutreffend, sondern stellen generelle Bedrohungen für informationstechnische Systeme dar. Je komplexer die Systemarchitektur desto größer ist die Wahrscheinlichkeit, dass durch interne Nutzer, beispielsweise durch falsche Konfiguration oder Eingabe-Fehler, Schaden am System entsteht. Die Anbindung an das Internet erleichtert externen Angreifern den Zutritt ins System. Auf das Cloud-Computing treffen beide Punkte zu.

Aufgrund der zunehmenden Anzahl von Cloud-Nutzern zeichnet sich ab, dass auch die Angriffe auf Cloud-Anwendungen und Cloudinfrastruktur weiter zunehmen werden. [36] An der IT-Sicherheit von Anwendungen muss deshalb kontinuierlich gearbeitet werden.

2.2 Sicherheit im Straßenverkehr

2.2.1 Infrastrukturelle Verkehrssicherheit

Die Sicherheit im Straßenverkehr wird durch die Straßenverkehrsinfrastruktur mitbeeinflusst. Hierzu gehören Straßen, Brücken, Tunnel, Knotenpunkte und Technik, beispielweise Signalgeber, Detektoren und Steuergeräte. Außerdem dienen die in der Straßenverkehrs-

infrastruktur geltenden Regeln, unter anderem Geschwindigkeitsbeschränkungen, Vorfahrtsregelungen oder Parkverbote, der Sicherheit. Die Verkehrsinfrastruktur muss so gestaltet sein, dass sie regelkonformes Verhalten voraussetzt und fördert. [37]

Die ‚Richtlinie 2008/96/EG des Europäischen Parlaments und des Rates vom 19. November 2008 über ein Sicherheitsmanagement für die Straßenverkehrsinfrastruktur‘ gibt folgende zu beachtende Kriterien für Straßenverkehrssicherheitsüberprüfungen an, aus denen allgemeine Einflussfaktoren auf die Sicherheit abgeleitet werden können. [38]

1. Straßentrassierung und Querschnitt:

- Sichtbarkeit und Sichtweiten
- Geschwindigkeitsbeschränkung und Geschwindigkeitszonen
- selbsterklärende Trassierung (d. h. Erkennbarkeit der Trassierung durch die Verkehrsteilnehmer)
- Zugang zu angrenzenden Grundstücken und Erschließungen
- Zugang für Einsatz- und Dienstfahrzeuge
- Sicherheitsvorkehrungen an Brücken und Durchlässen
- Gestaltung des Straßenrandes (Randstreifen, unbefestigter Fahrbahnrand, Abtrage- und Aufschüttungsböschungen)

2. Knotenpunkte und Anschlussstellen:

- Angemessenheit der Art des Knotenpunktes/Anschlussstelle
- Geometrie der Gestaltung des Knotenpunktes/Anschlussstelle
- Sichtbarkeit und Erkennbarkeit (Wahrnehmung) von Knotenpunkten
- Sichtbarkeit an Knotenpunkten
- Gestaltung zusätzlicher Fahrspuren an Knotenpunkten
- Verkehrsregelung an Knotenpunkten (z. B. Halt-Zeichen, Lichtsignalanlagen (LSA))
- Vorhandensein von Fußgänger- und Radfahrerüberwegen

3. Vorkehrungen für ungeschützte Verkehrsteilnehmer:

- Vorkehrungen für Fußgänger, Radfahrer und zweirädrige Kraftfahrzeuge
- öffentliche Verkehrsmittel und Infrastrukturen
- höhengleiche Bahnübergänge (insbesondere unter Hinweis auf die Art des Übergangs und darauf, ob es sich um bemannte, unbemannte, manuell oder automatisiert betriebene Anlagen handelt)

4. Beleuchtung, Beschilderung und Markierungen:
 - kohärente Verkehrszeichen, keine Sichtbehinderung
 - Erkennbarkeit von Straßenverkehrszeichen (Anordnung, Größe, Farbe)
 - Wegweiser
 - kohärente Fahrbahnmarkierungen und Leitelemente
 - Erkennbarkeit der Fahrbahnmarkierungen (Anordnung, Abmessungen und Retroreflexion unter trockenen und feuchten Bedingungen)
 - geeigneter Kontrast von Fahrbahnmarkierungen
 - Beleuchtung von Straßen und Knotenpunkten
 - geeignete straßenseitige Ausrüstung
5. Lichtsignalanlagen:
 - Betrieb
 - Sichtbarkeit
6. Objekte, freizuhaltende Flächen und Fahrzeugrückhaltesysteme:
 - Straßenseitenraum einschließlich Vegetation
 - Gefahren am Straßenrand und Abstand vom Fahrbahn- oder Radwegrand
 - benutzerfreundliche Anpassung von Fahrzeugrückhaltesystemen (Mittelstreifen und Schutzeinrichtungen zur Vermeidung einer Gefährdung ungeschützter Verkehrsteilnehmer)
 - Endkonstruktion von Schutzeinrichtungen
 - geeignete Fahrzeugrückhaltesysteme an Brücken und Durchlässen
 - Zäune (in Straßen mit beschränktem Zugang)
 - Straßenbelag:
 - Schäden am Straßenbelag
 - Griffigkeit
 - loses Material/Kies/Steine
 - Pfützenbildung, Wasserableitung

7. Brücken und Tunnel:

- Vorhandensein und Anzahl von Brücken und Tunneln
- visuelle Elemente, die Gefahren für die Sicherheit der Infrastruktur abbilden

8. Sonstige Aspekte:

- Bereitstellung sicherer Parkplätze und Rastanlagen
- Vorkehrungen für schwere Nutzfahrzeuge
- Blendung durch Scheinwerfer
- Straßenbauarbeiten
- unsichere Tätigkeiten am Straßenrand
- geeignete Informationen in den telematischen Anlagen
- Wild- und andere Tiere
- Hinweise auf Schulen (falls zutreffend)

Lichtsignalanlagen haben als verkehrsregulierendes Medium an Knotenpunkten eine sehr wichtige Aufgabe bei der Vermeidung von Unfällen. Die Parametrierung obliegt dabei dem Zielkonflikt Effizienz, das heißt Maximierung des Fahrzeugdurchflusses durch Knotenpunkte, versus Sicherheit. Ein wichtiger Parameter für die Sicherheit bei Lichtsignalanlagen sind die Zwischenzeiten. Diese werden in Abhängigkeit der Knotenpunktgeometrie für feindliche Signalgruppen anhand vorgegebener Formeln kalkuliert, so dass alle Verkehrsteilnehmer den Knotenpunkt sicher verlassen können, bevor ein feindlicher Verkehrsstrom einfahren und Kollisionen eintreten könnten. Bei der Erstellung von LSA-Steuerungslogiken kann die Sicherheit durch eine getrennte Signalisierung von Links- und Rechtsabbiegern verbessert werden. Linksabbieger geraten an signalisierten Knotenpunkten häufig in Konflikt mit entgegenkommenden Geradeausfahrenden, Rechtsabbieger gefährden Fußgänger und Radfahrer, welche die Straße überqueren. Eine getrennte Signalisierung ist aus Perspektive der Sicherheit meistens zu bevorzugen, häufig allerdings aufgrund der Knotenpunktgeometrie nicht umzusetzen. Manchmal liegt der Fokus auch auf einer Maximierung der Leistungsfähigkeit eines Knotenpunktes, weshalb eine wünschenswerte, getrennte Signalisierung nicht umgesetzt wird.

Während des LSA-Betriebes, hat das Steuergerät die wichtige Aufgabe der Signalsicherung. Diese ist beispielsweise dafür verantwortlich sicherzustellen, dass Zwischenzeiten eingehalten werden und kein feindliches Grün angezeigt wird. Im Detail bedeutet dies für das Steuergerät folgendes: [39]

- Abschaltung der LSA bei gefährdenden Signalisierungszuständen, z. B. Ausfall von Sperrsignalen (Rotlampe), Mindestfreigabe- oder Zwischenzeitverletzung, Auftreten nicht zulässiger Signalbilder (gleichzeitiges Grün feindlicher Verkehrsströme)

- Meldung von zulässigen, aber widersprüchlichen Signalbildern, wie z. B. Grün und Rot gleichzeitig an einem Signalgeber
- Meldung von defekten Lampen, deren Ausfall noch nicht gefährdend ist (z. B. Gelb- bzw. Grünlampe)
- Überwachung von Blinksignalen
- Überwachung der internen Spannungsversorgung
- Überwachung der internen Taktgebung

Die Signalsicherung ist in jedem Steuergerät fehlersicher und unabhängig von einer Kommunikation mit übergeordneten Systemen oder anderen Steuergeräten zu implementieren, um die sichere Knotenpunktsignalisierung zu gewährleisten. Wird eine LSA abgeschaltet, regeln meistens Vorfahrtsschilder den Verkehrsablauf auf dem Knotenpunkt. Dies geht auf Kosten der Sicherheit und der Effizienz, weshalb zuverlässig funktionierende und gut versorgte LSA anzustreben sind.

Um die Sicherheit der Straßenverkehrsinfrastruktur kontinuierlich zu optimieren, werden Unfälle in Deutschland von Unfallkommissionen analysiert. Ergeben sich Unfallschwerpunkte, sind sie verpflichtet zu untersuchen, ob sich diese auf Gefahrenstellen in der Infrastruktur zurückführen lassen. Falls dies der Fall ist, müssen Maßnahmen benannt werden, um sie zu beseitigen. Beispielsweise müssen in Berlin gemäß § 21 des Mobilitätsgesetzes (MobG BE) Unfallkommissionen bei allen Unfällen mit Todesfolgen über eventuell zu ergreifende, bauliche Maßnahmen berichten. Gleiches gilt bei Unfällen mit Schwerverletzten an Unfallschwerpunkten. [37]

Im Straßenraum aufgestellte Regeln sollten regelmäßig auf ihre Sinnhaftigkeit und Einhaltung überprüft werden. Verstöße müssen geahndet werden, um die Sicherheit für alle Verkehrsteilnehmer im öffentlichen Raum zu gewährleisten. Beispiele hierfür sind Messsysteme für die Geschwindigkeitsüberwachung und Rotlichtverstöße, aber auch Polizei- und Ordnungsdienstpräsenz, welche unter anderem auf die Einhaltung von Parkverboten, ordnungsgemäße Benutzung von Fahrradwegen und Bürgersteigen und Rotlichtverletzungen von Fußgängern oder Radfahrern achten. Die Berliner Senatsverwaltung setzt für die Verkehrsüberwachung beispielsweise vermehrt ihre Fahrradstaffel ein. [37]

2.2.2 Fahrzeugsicherheit

Die Sicherheit der Fahrzeuge, welche am Straßenverkehr teilnehmen, hat einen Einfluss auf die Straßenverkehrssicherheit. Bei der Fahrzeugsicherheit wird zwischen aktiven, passiven und integralen Sicherheitssystemen unterschieden. Aktive Sicherheitssysteme fokussieren auf der Vermeidung von Unfällen. Beispiele hierfür sind im Folgenden gegeben: [40, 41]

- Antiblockiersystem (ABS)
- Elektronisches Stabilitätsprogramm (ESP)
- intelligente Geschwindigkeitsassistenten
- Müdigkeitswarnsystem
- Notbremslicht
- Spurhaltesystem
- Rückfahrassistent
- Abbiegeassistenzsystem
- Reifendrucküberwachungssystem

Passive Sicherheitssysteme zielen darauf ab, die Unfallfolgen zu verringern. Nachfolgend sind Beispiele aufgelistet: [41]

- Anschnallgurt
- Gurtstraffer
- Knautschzone
- Airbag
- Kopfstützen

Integrale Sicherheitssysteme verknüpfen passive mit aktiven Sicherheitssystemen. Ziel ist es, durch eine gesamtheitliche Betrachtung - von der Unfallentstehung über die Kollision bis hin zur Rettung - Kollisionen bzw. Unfallfolgen zu vermeiden. Beispiele hierfür sind: [42]

- Automatisches Notrufsystem
- Insassenschutzsystem
- Pre-Crash-Positionierung
- Fußgängerschutzsystem
- automatische Notbremsung zum Schutz von ungeschützten Verkehrsteilnehmern

Die Wichtigkeit von Fahrzeugsicherheitssystemen unterstreicht die am 5. Januar 2020 in Kraft getretene und ab dem 6. Juli 2022 in allen EU-Mitgliedsstaaten verpflichtend anzuwendende ‚EU-Verordnung Nr. 2019/2144 über die Typgenehmigung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge im Hinblick auf ihre allgemeine Sicherheit und den Schutz der Fahrzeuginsassen und von ungeschützten Verkehrsteilnehmern‘. Sie schreibt die Ausstattung von

Fahrzeugen mit diversen neuen Technologien und Sicherheitsmaßnahmen verpflichtend vor. Ziel ist es, die Anzahl der Getöteten und Verletzten im Straßenverkehr zu verringern. Die technischen Details wurden zum Zeitpunkt der Erstellung dieser Arbeit von einer Expertengruppe erarbeitet. [40]

2.2.3 Straßenverkehrsunfallstatistiken

In Deutschland muss gemäß dem Gesetz über ‚die Statistik der Straßenverkehrsunfälle und der Verordnung zur näheren Bestimmung des schwerwiegenden Unfalls mit Sachschaden‘ vom 21. Dezember 1994 eine Bundesstatistik über Unfälle geführt werden, bei denen infolge des Fahrverkehrs auf öffentlichen Wegen oder Plätzen Personen getötet, verletzt oder Sachschäden verursacht worden sind. [43] Straßenverkehrsunfälle werden von der Polizei aufgenommen, analysiert und anhand nachfolgender standardisierter Kriterien beschrieben: [43]

- Schwere der Unfallfolgen (Unfallkategorie)
- Beteiligte
- Unfallursachen
- Unfalltyp
- Unfallart
- Arten der Verkehrsbeteiligung
- Unfallort
- Unfallzeit (Datum und Uhrzeit)

Die Erhebung der Unfälle ist für rechtliche Fragestellungen sowie die Verbesserung der Fahrzeugsicherheit und Straßenverkehrsinfrastruktur relevant. In Deutschland sammelt das Statistische Bundesamt alle Daten, veröffentlicht diese und erstellt zudem regelmäßig Pressemitteilungen, die die Auswertung der Daten beinhalten.

Um eine bessere grafische Übersicht über die Orte mit Unfallschwerpunkten zu erlangen, werden Unfälle grafisch auf Karten visualisiert. Hierbei hilft die Unfalltypenkarte, welche in Abbildung 2 beispielhaft dargestellt ist. Früher wurden unterschiedlich farbige (Unfalltyp) Nadeln mit verschiedenen Durchmesser (Unfallkategorie) und unterschiedlichen Fähnchen (Unfallumstände) an der jeweiligen Unfallstelle in eine Kartenpinnwand geheftet. Heutzutage erfolgt dies automatisiert auf einer digitalen Karte. [44]

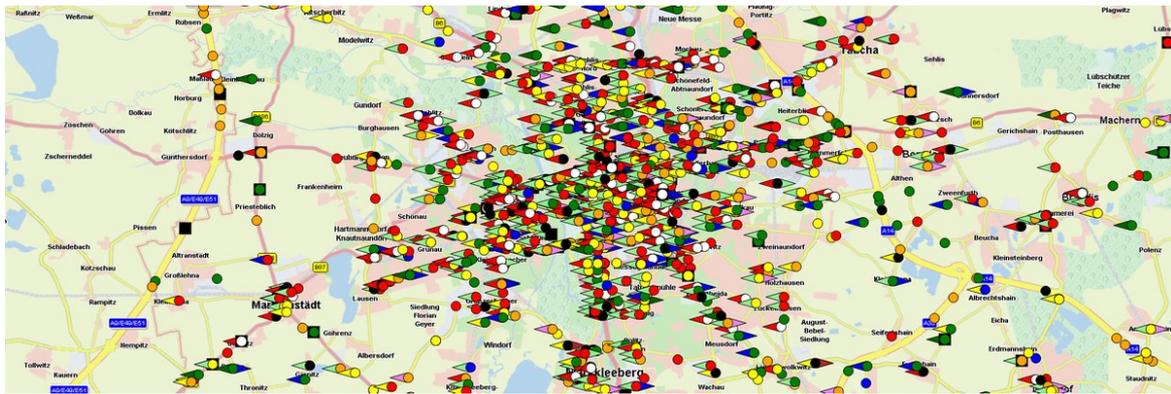


Abbildung 2: Unfalltypenkarte [45]

Unfalltypenkarte (Legende)



Abbildung 3: Legende einer Unfalltypenkarte [46]

Insgesamt ist die Zahl der im Verkehr getöteten Personen in Deutschland seit den 70er-Jahren - dank diverser gesetzlicher Anordnungen und der sicherheitstechnischen Optimierung von Fahrzeugen sowie der Verkehrsinfrastruktur - stark rückläufig. [47] Die Entwicklung der Anzahl im Straßenverkehr getöteter Personen in Deutschland wird in Abbildung 4 über den Zeitverlauf dargestellt.

Entwicklung der Zahl der im Straßenverkehr Getöteten
in Tausend

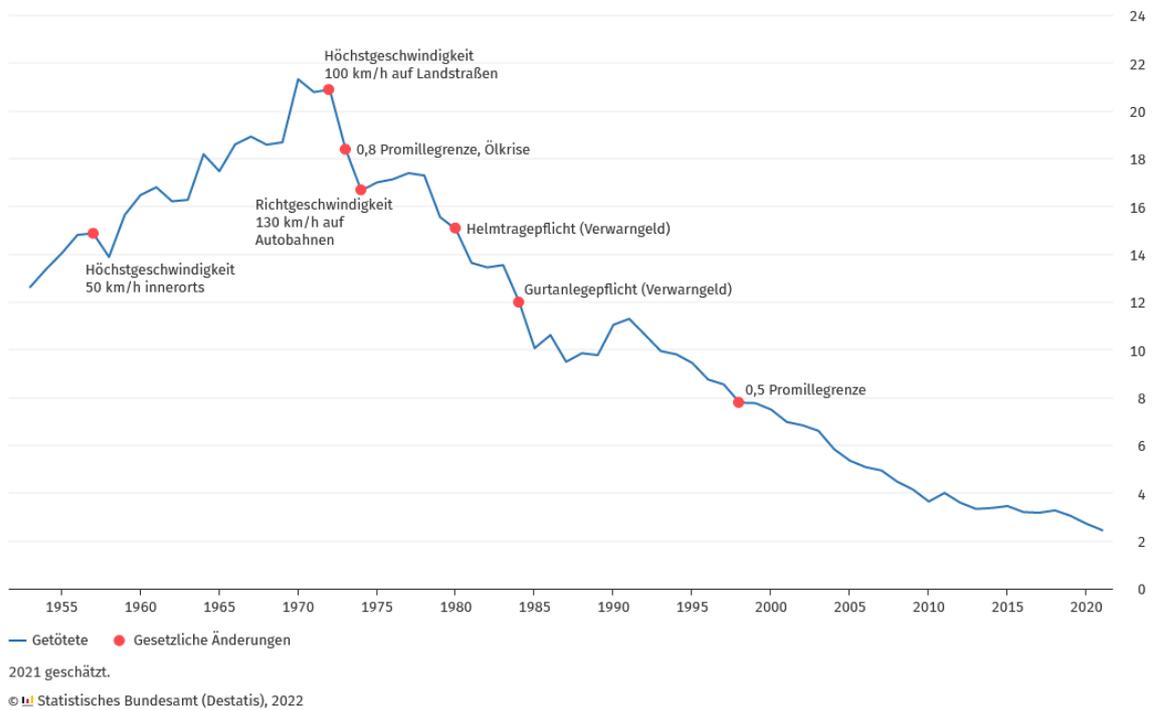
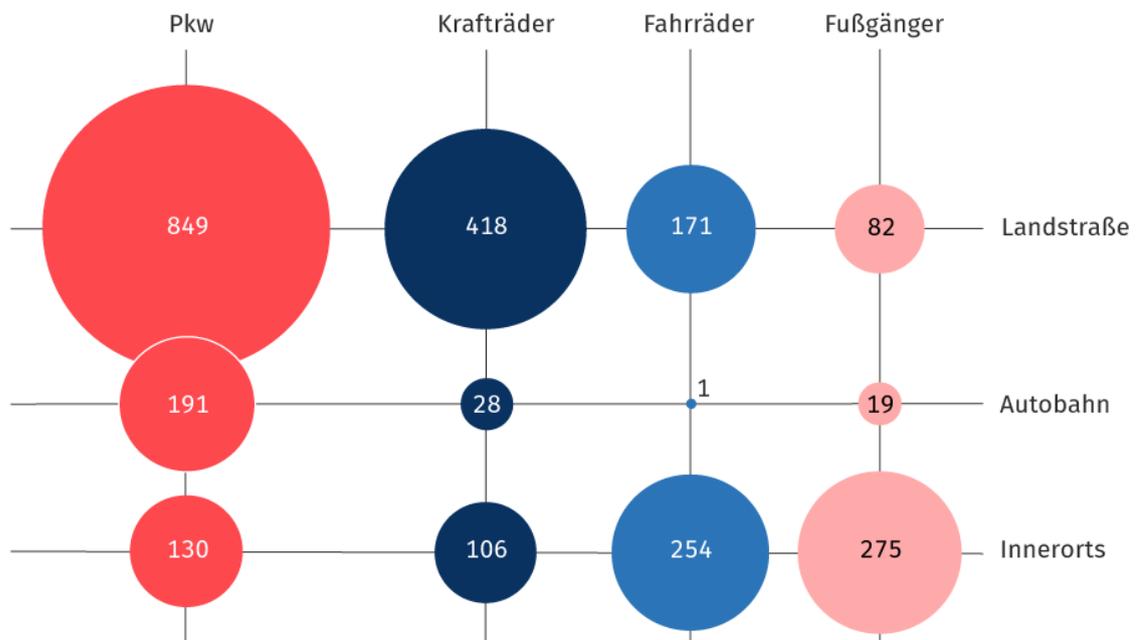


Abbildung 4: Entwicklung der im Straßenverkehr getöteten Personen [47]

Getötete im Straßenverkehr 2020

nach ausgewählter Verkehrsbeteiligungsart und Ortstagen



© Statistisches Bundesamt (Destatis), 2021

Abbildung 5: Getötete Personen nach Verkehrsbeteiligungsart und Ortstagen [47]

Interessant ist zudem die Auswertung der in Verkehrsbeteiligungsart und Ortslage aufgeteilten getöteten Personen des Jahres 2020, welche in Abbildung 5 dargestellt ist. Erkennbar ist hier, dass die absolute Zahl der Getöteten auf Landstraßen am höchsten ist. Zudem zeigt die Grafik, dass Radfahrer und Fußgänger innerorts am meisten gefährdet sind und einen Großteil der Verkehrstoten ausmachen. [47]

Abbildung 6 zeigt das Fehlverhalten von Fahrern bei Unfällen mit Personenschäden. Die meisten Unfällen beruhen auf Fehlern beim Abbiegen, Wenden, Rückwärtsfahren, Ein- oder Ausfahren. Des Weiteren sind die Missachtung von Vorfahrt, korrektem Abstand, Geschwindigkeitsbeschränkungen sowie die falsche Straßenbenutzung, Hauptgründe für Unfälle mit Personenschaden. [47]

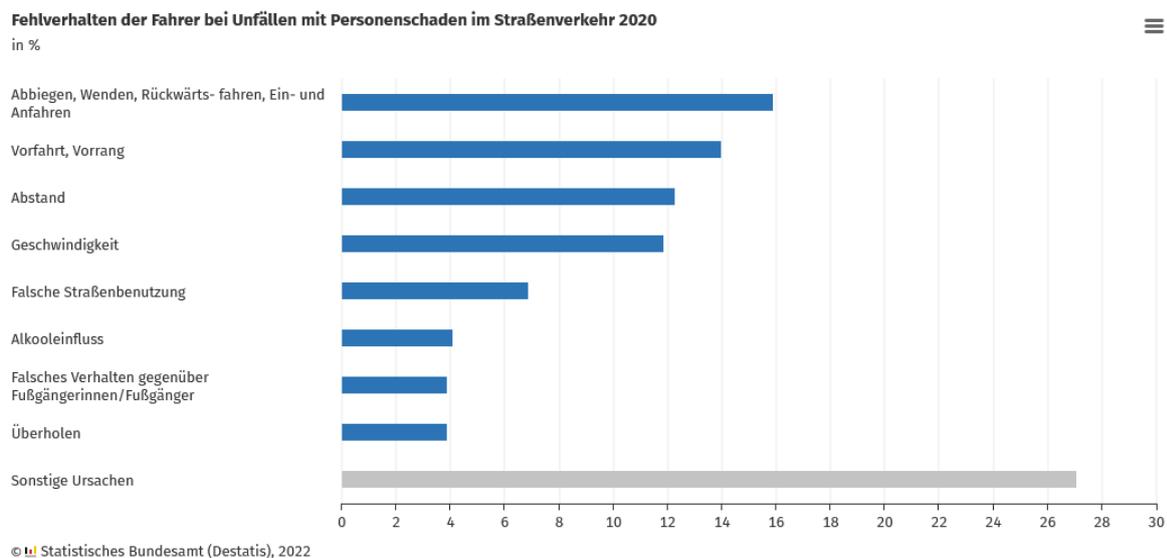


Abbildung 6: Fehlverhalten von Fahrern bei Unfällen mit Personenschaden [47]

Das Jahr 2021 war in Deutschland durch weniger Todesopfer und Verletzte als die Vorjahre gekennzeichnet. Die Zahl der Verkehrstoten sank mit 2569 Todesopfern auf den niedrigsten Stand seit 60 Jahren. Grund hierfür könnte die Corona-Pandemie sein, welche unter anderem mit Lockdowns, Homeoffice und Homeschooling große Auswirkungen auf das Verkehrsgeschehen hatte. Erfreulich ist, dass die Anzahl der Getöteten bei den Radfahrern und Fußgängern prozentual am meisten zurückging. Es ist davon auszugehen, dass die Unfallzahlen im Jahr 2022 ansteigen werden, wenn die pandemiebedingten Mobilitätsbeschränkungen wegfallen. [48]

Die Teilnahme am Straßenverkehr mit zweirädrigen (Kraft-)Rädern ist gemäß den statistischen Auswertungen die gefährlichste. Nicht nur das Verletzungsrisiko ist höher, es sind auch die Unfallfolgen im Vergleich zu Pkw-Insassen schwerwiegender. Im Jahr 2020 war das Risiko, auf einem zugelassenen Kraftrad im Straßenverkehr getötet zu werden, viermal größer als im Auto. Der Grund hierfür ist naheliegend: (Kraft-)Radfahrer sind fast ungeschützt im Straßenverkehr unterwegs. [43]

In der Europäischen Union außerhalb von Deutschland erfolgt die Unfallaufnahme

und -auswertung ähnlich wie in Deutschland. Die Europäische Kommission sammelt und veröffentlicht Unfalldaten sowie Presseberichte. Innerhalb der EU war Schweden im Jahr 2020 das Land mit den sichersten Straßen (18 Verkehrstote pro 1 Million Einwohner). Rumänien bildete im Jahr 2020 das europäische Schlusslicht (85 Verkehrstote pro 1 Million Einwohner). Deutschland lag 2020 mit 33 Verkehrstoten pro 1 Million Einwohner auf den siebten Platz. Die Teilnahme am Verkehr in der EU ist mit einem Durchschnitt von 42 Verkehrstoten pro 1 Million Einwohner im Jahr 2020, verglichen mit dem weltweiten Durchschnitt von mehr als 180 Verkehrstoten pro 1 Millionen Einwohner, vergleichsweise sicher. [49, 50]

2.2.4 Bemessung und Bewertung von Sicherheit

2.2.4.1 Geltende Normen und Richtlinien

Für die Gewährleistung von Sicherheit im Straßenverkehr gibt es verschiedene Normen. Im Folgenden sind die wichtigsten aufgelistet:

- ISO 26262: Road vehicles– Functional safety

Diese Norm stellt die Anpassung der EN 61508 Norm für Automobile dar. Sie definiert Maßnahmen zur Gewährleistung der Sicherheit sowie Verfahren zur Beurteilung von Gefährdungen von elektrischen und elektronischen Komponenten. In ihr werden die ‚Automotive Safety Integrity Level‘ (ASIL) definiert. [51]

- ISO/SAE DIS 21434: Road vehicles - Cybersecurity engineering

Diese zurzeit in Entwicklung befindliche Norm fokussiert auf Maßnahmen, welche die Konnektivitäts- und Informationsaustauschfunktionalitäten in modernen Straßenfahrzeugen in Hinblick auf die Cybersicherheit verbessern sollen. Durch die stetig steigende Anzahl solcher Funktionen steigt die Vulnerabilität von Fahrzeugen in Bezug auf Hackerangriffe und damit die Notwendigkeit einer cybersicheren Konzeption. Ein Entwurf der Norm wurde 2018 veröffentlicht. Die Veröffentlichung einer finalen Version der Norm steht aus. [52]

- UN-Regelung Nr. 155: Einheitliche Bedingungen für die Genehmigung von Fahrzeugen hinsichtlich der Cybersicherheit und des Cybersicherheitsmanagementsystems (2021/387)

Diese Regelung der ‚Wirtschaftskommission für Europa‘ (UNECE) stellt Anforderungen an die Sicherheit von Kraftfahrzeugen gegen Cyber-Angriffe, welche bei einer Genehmigung fahrzeugspezifisch einzuhalten sind. [53]

- VDE 0832-700: Branchenspezifischer Sicherheitsstandard (B3S) für Verkehrssteuerungs- und Leitsysteme im kommunalen Straßenverkehr

Diese Norm des Verbandes der Elektrotechnik, Elektronik und Informationstechnik fokussiert auf die sichere Gestaltung des gesamten Lebenszyklus der digitalen

Infrastruktur der Straßenverkehrstechnik, das heißt Lichtsignalanlagen, Verkehrsbeeinflussungsanlagen und Zentralensteuerung. Sie stellt den branchenspezifischen Sicherheitsstandard (B3S) für Verkehrssteuerungs- und Leitsysteme im kommunalen Straßenverkehr dar. [54]

2.2.4.2 Maßeinheiten

Um die Sicherheit auf Straßen zu bewerten, werden zumeist die beiden Größen ‚Anzahl Verletzter‘ sowie ‚Anzahl getöteter Personen‘ verwendet. Diese werden wie folgt definiert: [43]

- Getötete: Personen, welche innerhalb von 30 Tagen an den Unfallfolgen starben
- Verletzte:
 - Schwerverletzte: Personen, welche unmittelbar zur stationären Behandlung (mindestens 24 Stunden Aufenthalt) ins Krankenhaus gebracht wurden
 - Leichtverletzte: alle anderen Verletzten

Des Weiteren wird häufig die Anzahl der Unfälle als Maßeinheit verwendet. Hierbei spielt die Anzahl der involvierten bzw. zu Schaden gekommenen Personen keine Rolle und Unfälle mit reinem Sachschaden werden mitberücksichtigt. Da nicht alle Unfälle, insbesondere solche mit reinen Sachschäden, an die Polizei gemeldet werden, ist die Zahl der Unfälle nicht so aussagekräftig wie die der getöteten und verletzten Personen.

Eine weitere Möglichkeit der Betrachtung von Sicherheit auf Straßen ist die Umrechnung in volkswirtschaftliche Unfallkosten. Diese beziffern die Reproduktions- und Ressourcenaufwandskosten, die durch Personen- und Sachschäden bei Unfällen entstehen. Tabelle 2 zeigt die volkswirtschaftlichen Unfallkosten für getötete und verletzte Personen in Deutschland.

Ebenso wie bei der Unfallzahl ist bei der Betrachtung der volkswirtschaftlichen Unfallkosten zu berücksichtigen, dass nicht alle Unfälle von der Polizei erfasst werden und somit eine nicht bekannte Anzahl der Unfälle in den Statistiken fehlt. Dennoch ermöglicht dieser Ansatz, die Unfälle in Relation zu anderen Kosten, beispielsweise der Entwicklung und Einführung neuer Technologien, zu setzen.

Tabelle 3 zeigt die volkswirtschaftlichen Unfallkosten für Sachschäden in Deutschland in Abhängigkeit der Unfallkategorie.

Die Kosten werden von der Bundesanstalt für Straßenwesen ermittelt und in regelmäßigen Abständen beispielsweise an die Preis- und Kaufkraftindizes, die Fahrleistungsanteile und die Lebensarbeitszeit angepasst. [55]

Tabelle 2: volkswirtschaftliche Unfallkosten Getötete und Verletzte 2020 [55]

Kategorie	Kostensätze pro Person
Getötete	1.219.396 €
Schwerverletzte	119.788 €
Leichtverletzte	5.391 €

Ebenso wie bei der Unfallzahl ist bei der Betrachtung der volkswirtschaftlichen Unfallkosten zu berücksichtigen, dass nicht alle Unfälle von der Polizei erfasst werden und somit eine nicht bekannte Anzahl der Unfälle in den Statistiken fehlt. Dennoch ermöglicht dieser Ansatz, die Unfälle in Relation zu anderen Kosten, beispielsweise der Entwicklung und Einführung neuer Technologien, zu setzen.

Tabelle 3: volkswirtschaftliche Unfallkosten Sachschäden 2020 [55]

	Kostensätze pro Unfall
Unfall mit Personenschaden	15.705 €
Unfall mit Getöteten	44.504 €
Unfall mit Schwerverletzten	21.642 €
Unfall mit Leichtverletzten	13.908 €
schwerwiegender Unfall nur mit Sachschaden	22.422 €
sonstiger Sachschadensunfall	7.344 €

2.2.5 Sicherheitsrisiken im heutigen Straßenverkehr

Das größte Sicherheitsrisiko im Straßenverkehr ist der Mensch selbst. Regelmissachtung, Fehlverhalten und Unaufmerksamkeit führen zu kritischen Situationen, aus denen häufig Unfälle entstehen. Folgende Verhaltensweisen sind besonders riskant:

- Vorfahrtsmissachtung

Im Jahr 2020 wurde eine Vorfahrtsmissachtung in Deutschland bei 43.378 Unfällen als Ursache angegeben. [56]

- unangemessene Abstände

Im Jahr 2020 wurden in Deutschland bei 38.377 Unfällen unangemessene Abstände als Ursache angegeben. [56]

- unangemessene Geschwindigkeitwahl

Im Jahr 2020 wurde in Deutschland bei 37.105 Unfällen eine nicht angepasste Geschwindigkeit als Ursache angegeben. [56]

- Fahren unter Alkohol oder Einfluss anderer berauschender Mittel

Bei 1,6 %, das entspricht 35 623 Unfälle aller im Jahr 2020 in Deutschland polizeilich registrierten Unfälle, stand mindestens ein Beteiligter unter dem Einfluss berauschender Mittel. Unfälle unter Einfluss von Rauschmitteln oder Alkohol haben eine überdurchschnittlich hohe Schwere: Alkoholeinfluss war bei 4,9 % aller Unfälle mit Personenschaden eine Unfallursache. 5,7 % aller tödlich Verunglückten starben in Folge eines solchen Unfalles. [57]

- Überholvorgänge

Im Jahr 2020 wurden 12.177 Unfälle in Deutschland registriert, bei denen Überholvorgänge eine Unfallursache war. [56]

- Übermüdung

Im Jahr 2020 wurden 1507 Unfälle mit Personenschäden und 1132 Unfälle mit Sachschaden registriert, bei denen Übermüdung eine Unfallursache darstellte. [56]

- Ablenkung

Ablenkung im Straßenverkehr ist allgegenwärtig und kann verschiedene Ursachen haben. Beispielsweise können Tagträume, das Smartphone, Situationen und Personen außerhalb des Fahrzeuges, Mitreisende, das Bedienen des Navigationsgerätes, Radios oder der Klimaanlage sowie das Verzehren von Getränken und Speisen zu Ablenkung und darauffolgenden Unfällen führen. Es gibt keine verlässlichen Zahlen, die auf die Anzahl der hierdurch entstandenen Unfälle rückschließen lassen. Experten sind sich allerdings einig, dass die Ablenkung ein erhebliches Risiko im Straßenverkehr darstellt. [58]

Bei den in der Aufzählung angegebenen Zahlen ist zu beachten, dass einem Unfall mehrere Ursachen zugeteilt werden können. Oft kommen mehrere Ursachen zusammen, die in ihrer Summe zu einem Unfall führen. Beispielsweise ist davon auszugehen, dass Unfälle durch Überholen häufig im Zusammenhang mit überhöhter Geschwindigkeit stehen.

Technische Mängel oder Defekte, beispielweise an der Bremsanlage oder den Reifen, sind in Deutschland eine weniger häufige Unfallursache. 2020 wurden 3.350 Unfälle mit Personenschäden registriert, welche auf technische Mängel zurückzuführen waren. [56] Die kontinuierliche Inspektion von Fahrzeugen (TÜV) und Wartung trägt dazu bei, dass Unfälle durch technische Mängel in Deutschland vergleichsweise selten vorkommen. In anderen Ländern mit älteren und schlechter gewarteten Fahrzeugen ist davon auszugehen, dass die Unfallzahlen aufgrund dieser Ursache deutlich höher sind.

Die Mehrzahl aller Unfälle im Straßenverkehr ist auf menschliches Versagen zurückzuführen. Die menschliche Fehlerhäufigkeit wird allgemein mit $10^{-3}/h$ angenommen. [59] Die empfohlenen Ausfallsicherheiten für technische Systeme von Fahrzeugen, definiert in den ASIL-Kategorien, betragen $10^{-6}/h$ bis $10^{-8}/h$ je nach Risikobewertung der Funktionalität. [51] Die Richtlinie VDI 4006 („Menschliche Zuverlässigkeit“) des Vereins Deutscher Ingenieure (VDI) beschäftigt sich mit der menschlichen Zuverlässigkeit insbesondere im Kontext eines Mensch-Maschine-Systems, welches im Straßenverkehr durch die Kombination von Fahrzeug und Fahrer gegeben ist. In ihr sind Maßnahmen - in erster Linie in Bezug auf die ergonomische Gestaltung – enthalten, die Möglichkeiten zur Erhöhung der Sicherheit bieten. [59]

3 Anwendung von Cloud-Computing im Straßenverkehr

3.1 Übersicht

Wie in Kapitel 1.5 beschrieben, wurden Cloud-Anwendungen im Straßenverkehr - aufbauend auf der eigenen Berufserfahrung - durch Recherchen, Gespräche mit Experten sowie Messebesuche (‘Intertraffic’ und ‘ITS-Weltkongress’) identifiziert. Die ermittelten Anwendungen wurden in unterschiedliche Kategorien gruppiert und sind in Abbildung 7 dargestellt. Die Anwendungen der nachfolgenden, in Abbildung 7 blau eingefärbten Kategorien, werden in den folgenden Kapiteln näher erläutert. Die Analysen in Kapitel 4 und 5 bauen ebenfalls auf diesen Kategorien auf.

1. Straßenverkehrsmanagement
2. kooperative intelligente Verkehrssysteme
3. proprietäre Datenanalyse und Warnung
4. Daten- und Videoanalyse für Planungszwecke
5. Daten- und Videoanalyse für operative Zwecke
6. community-getriebene Smartphone-Anwendungen

Die grau eingefärbten Kategorien werden in dieser Arbeit aus den in Kapitel 1.1 genannten Gründen nicht weiter analysiert. Sie sind der Vollständigkeit halber dennoch dargestellt, um einen Gesamtüberblick über Cloud-Anwendungen im Straßenverkehr zu gewährleisten.

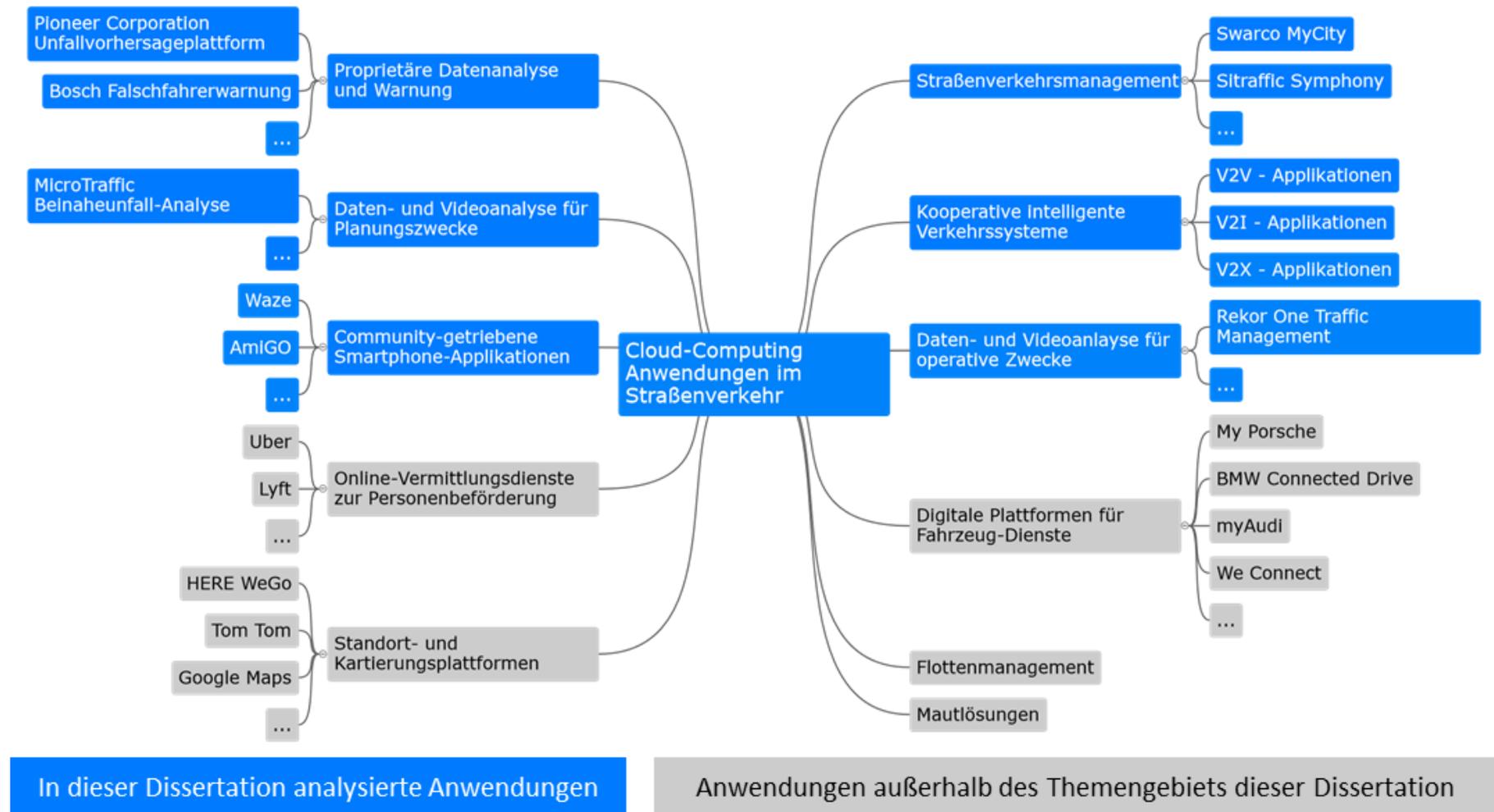


Abbildung 7: Übersicht der identifizierten Cloud-Anwendungen im Straßenverkehr

3.2 Straßenverkehrsmanagement

Im Bereich der Straßenverkehrstechnik gibt es heute bereits einige Anbieter, die Straßenverkehrsmanagement und LSA-Steuerung aus der Cloud ermöglichen. Die Software des Verkehrsrechners bzw. der Verkehrsmanagementzentrale ist dabei in einer Cloud gehostet und befindet sich nicht vor Ort in einem Rechenzentrum der Stadt. Die Kommunikation zwischen den Feldgeräten, Bedienendgeräten und der zentralen Software erfolgt über das Internet. Beispiele für solche Lösungen sind:

- Firma Swarco:
 - ‚Swarco MyCity‘: Software für urbanes Verkehrsmanagement, welches in der Cloud oder vor Ort in städtischen Rechenzentren gehostet werden kann. Die Plattform basiert gemäß Herstellerangaben auf einer Microservice-Architektur und ist damit für die Cloud gut geeignet. [60]
 - ‚Swarco OMNIA‘: Software für Verkehrsmanagement, welche vom Hersteller als Smart Mobility Management Suite bezeichnet wird. Die Software kann sowohl in der Cloud als auch vor Ort in städtischen Rechenzentren gehostet werden. Über die Architektur des Systems sind keine Informationen verfügbar. [61]
- Firma Yunex Traffic:
 - ‚Sittraffic Symphony‘: Modulare Plattform für intelligentes Verkehrsmanagement, welche sowohl in der Cloud als auch vor Ort einsetzbar ist. [62]
- Firma Parsons:
 - ‚iNET‘: Die intelligente Smart Mobility Plattform Intelligent NETworks (iNET) ist laut Hersteller ein cloudbasiertes System, welches in einer virtualisierten Server-Umgebung installiert werden kann. [63]
- Firma Econolite:
 - ‚Centracs Mobility‘: Mobilitätsplattform, welche laut Hersteller über eine flexible Architektur verfügt und sowohl in der Cloud als auch vor Ort in Städten installiert werden kann. [64]

- Firma Q-Free:
 - ‚Open TMS‘: Verkehrsmanagementsystem, welches vom Hersteller als cloudfähig beschrieben wird. Es ist daher davon auszugehen, dass die Architektur nicht für die Nutzung der Vorteile der Cloud, insbesondere die dynamischen Skalierungsmöglichkeiten, ausgelegt ist. Dennoch ist ein Hosting in der Cloud wie auch vor Ort möglich. [65]
 - ‚Kinetic Mobility‘: Laut Hersteller eine cloudbasierte Plattform, welche verschiedene ältere Experten-Produkte von Q-Free vereinen soll. Die Plattform befindet sich noch in der Entwicklung und verfügt aktuell über zwei Anwendungen für LSA-Steuerung und Datenaggregation für vernetzte Fahrzeuge. Weitere Anwendungen sollen folgen, um die Plattform zu einer umfassenden Verkehrsmanagementplattform zu verwandeln. [66]
- Firma Cubic:
 - ‚Transport Management Platform‘: Laut Hersteller eine cloudbasierte intelligente Verkehrssystem-Datenintegrationsmanagement-Plattform, welche verschiedene Verkehrs- und Transportmanagementsysteme vereinen soll. [67]
- Firma Notraffic:
 - ‚Autonomous Traffic Management Platform‘: Laut Hersteller eine KI-gestützte LSA-Plattform. Städte definieren Verkehrsrichtlinien, die über die Plattform sowohl auf lokaler Knotenpunkt- als auch auf Netzebene umgesetzt werden. Wichtige Daten aller Verkehrsteilnehmer werden zur weiteren Verarbeitung in Echtzeit in die Cloud gestreamt. Die Plattform arbeitet dann automatisiert, um die Wartezeiten zu reduzieren, indem sie die LSA-Steuerung auf Stadtnetzebene optimiert. [68]

Trotz zahlreicher Anbieter, die Verkehrsrechner und -managementlösungen in der Cloud anbieten, gibt es bislang nur wenige Städte weltweit, die ein solches System tatsächlich betreiben. ‚Iowa Department of Transportation‘ (Vereinigte Staaten von Amerika) war im Jahr 2019 unter den ersten, die ein Cloud-System ausgeschrieben und vergeben haben, und nun für den Betrieb verwenden. [69] Seither zeigt sich in den USA ein Trend hin zu Cloud-Systemen. Diese werden zunehmend häufiger ausgeschrieben. Beispiele hierfür sind im Folgenden aufgelistet.

- ‚Artificial Intelligence-Based Decision Support System (AI-DSS) for Enhancing Transportation Incident Management‘, ausgeschrieben als cloudbasiert am 02.02.2022 [70]
- ‚Chattanooga Advanced Transportation Management System‘, ausgeschrieben als cloudbasiert im Dezember 2020 [71]
- ‚Advanced Traffic Management System for Scott County‘, ausgeschrieben als ‚cloud based server solution‘ am 13.04.2021 [72]

In Deutschland gibt es aktuell auch einige Städte, welche cloudbasierte Verkehrsmanagementlösungen ausschreiben. Allerdings scheint dieser Trend weniger ausgeprägt zu sein als in den USA. Beispiele hierfür finden sich im Folgenden:

- ‚DAnalytics Umweltsensitives Verkehrsmanagement‘ - Komponente Ampelphasenassistent, ausgeschreiben als cloudbasierte Lösung am 24.11.2021 [73]
- ‚Digitale Verkehrsflussoptimierung Landeshauptstadt Stuttgart‘, ausgeschreiben als Cloud-Service am 14.05.2020 [74]

Es fällt auf, dass die Systeme, welche in der Cloud ausgeschrieben sind, zumeist nicht direkt mit den Feldgeräten verbunden sind und somit über sie nicht steuernd eingegriffen werden kann. Dies könnte auf vier verschiedene Ursachen zurückzuführen sein:

1. Städte haben aktuell keinen Bedarf, ihre steuernden Bestandssysteme zu erneuern.
2. Städte bevorzugen die Implementierung von operativen, steuernd eingreifenden Verkehrsmanagementlösungen auf eigener IT-Infrastruktur.
3. Aktuell zur Verfügung stehende Fördergelder fördern in erster Linie innovative neuartige Systeme, welche zusätzlich zu bestehenden Systemen (meist die steuernden) angeschafft werden.
4. Städte kennen sich mit den Möglichkeiten und dem Angebot von Verkehrsmanagement-Applikationen in der Cloud nicht aus und veröffentlichen aus diesem Grund keine solchen Ausschreibungen.

Das von ‚Virginia Department of Transportation‘ ausgeschriebene ‚Artificial Intelligence-Based Decision Support System‘ soll Daten verschiedener Quellen sammeln, diese analysieren, zukünftige Probleme im Verkehrsnetz vorhersagen und Behörden Maßnahmen empfehlen, mit denen die aktuelle Situation verbessert oder Probleme der Zukunft verhindert werden können. Für die Umsetzung dieser Maßnahmen sind die jeweiligen Behörden verantwortlich, die jeweils über eigene operative Systeme verfügen. [70]

Das in Chattanooga ausgeschriebene System umfasst die Sammlung und Aggregation verschiedenartiger (Verkehrs-)Daten, welche anschließend auf einer Karte und zur Erstellung von Berichten dem operativen Personal der Stadt und Externen, beispielsweise Bürgern, über eine Webseite zur Verfügung gestellt werden. Zudem ist eine Schnittstelle zum steuernden LSA-System vorgesehen, um den Status der Anlagen zu überwachen. [71]

Das System für die US-Grafschaft ‚Scott County‘ soll an die LSA angeschlossen werden und diese steuern. Damit kann es aktiv in den Verkehr eingreifen und unterscheidet sich von den anderen aufgelisteten Systemen. [72]

Der Ampelphasenassistent des ‚DAnalytics‘-Projektes hat die Aufgabe, die LSA-Schaltungen zu prognostizieren und greift hierfür auf aktuelle und historische LSA-Daten zurück. Die ermittelten Werte werden an Verkehrsteilnehmer gesendet und können zur Optimierung der Annäherung an die LSA verwendet werden. Ein steuernder Eingriff des Systems ist nicht

vorgesehen. [73]

Das Stuttgarter digitale Verkehrsflussoptimierungssystem sammelt ebenfalls Daten verschiedener Quellen und soll dazu verwendet werden, mittels Simulation iterativ neue Verkehrsstrategien für das operative Verkehrsmanagement zu entwickeln. Sobald die Strategien finalisiert sind, werden sie in das operative System überführt und können dort aktiviert werden. Damit ist auch bei diesem System kein direkter Eingriff in den Verkehr möglich. [74]

Diese oben beschriebenen und für die Ausschreibungen entworfenen Systeme sind demnach der Kategorie ‚Daten- und Videoanalyse für operative Zwecke‘ zuzuordnen. Weitere Informationen hierzu sind Kapitel 3.6 zu entnehmen.

3.3 Kooperative intelligente Verkehrssysteme

Ein Bereich innerhalb der intelligenten Verkehrssysteme, indem Cloud-Computing schon heute verwendet wird, ist C-ITS. C-ITS ist die Abkürzung für ‚Cooperative-Intelligent Traffic Systems‘, auf Deutsch kooperative intelligente Verkehrssysteme, und beschreibt die Vernetzung der Verkehrsteilnehmer untereinander sowie mit der Verkehrsinfrastruktur über digitale Technologien. [75]

Das ‚Europäische Institut für Telekommunikationsnormen‘ (ETSI) ist die in Europa zuständige Institution für die Standardisierung von C-ITS-Technologien. Hierunter fallen vor allem die Kommunikationsstandards, welche von Fahrzeugen und der Infrastruktur in Europa verwendet werden. In anderen Teilen der Welt gibt es ebenfalls Standardisierungsbestreben im Bereich C-ITS. In den USA ist hierfür beispielsweise die ‚Society of Automotive Engineers‘ (SAE) verantwortlich. Des Weiteren bringt sich die ‚5G Automotive Association‘, ein globaler Zusammenschluss aus Automobil- und Kommunikationsindustrie ein. Die Standardisierungsgremien wie auch Pilotprojekte definieren zumeist Anwendungsfälle von C-ITS, die sich inhaltlich ähneln, wenngleich sie nicht identisch sind. Tabelle 4 und Tabelle 5 stellen eine Übersicht über die von ETSI definierten Anwendungsfälle inklusive ihrer Gruppierung in Klassen dar. Tabelle 6 enthält weitere Anwendungsfälle, die von ETSI nicht definiert sind, allerdings in Forschungsprojekten erprobt werden.

Im Nachfolgenden werden die verschiedenen C-ITS-Anwendungen erläutert, die eine Verbesserung der Verkehrssicherheit versprechen. Die Warnungen sollen die Aufmerksamkeit des Fahrers auf die Gefahrensituation lenken und das Unfallrisiko dadurch reduzieren. Die Nachrichten werden heutzutage nur als Informationen versendet, der Fahrer muss darauf reagieren. In Zukunft ist eine automatisierte Verarbeitung in den Fahrzeugen angedacht. Die Originalnamen der Anwendungsfälle sind zusätzlich in englischer Sprache angegeben, um die Identifizierbarkeit in der Literatur zur gewährleisten.

1. Einsatzfahrzeugwarnung (emergency vehicle warning): Diese beinhaltet eine Positionsinformation/Warnung anderer Fahrzeuge durch ein Einsatzfahrzeug. Zum einen soll die Rettungszeit hierdurch verringert werden, da die Straßen frühzeitig für das Einsatzfahrzeug freigemacht werden können. Zum anderen reduziert sich das Risiko eines Zusammenstoßes mit dem Einsatzfahrzeug. [76]
2. Warnung langsames Fahrzeug (slow vehicle indication): Dies beinhaltet eine Warnung anderer Fahrzeuge durch ein Fahrzeug, welches langsam fährt, beispielweise ein Traktor. Durch die Warnung kann schärferes Abbremsen vermieden und das Risiko eines Auffahrunfalles verringert werden. [76] Die Warnung wird von dem langsamen Fahrzeug ausgestrahlt (Vehicle-to-Vehicle-Kommunikation).
3. Kollisionswarnung bei fahrbahnquerendem Abbiegeverkehr (across traffic turn collision risk warning): Dies beinhaltet eine Warnung herankommender Fahrzeuge durch ein Fahrzeug, das Abbiegen möchte und dabei die Fahrbahn des anderen Fahrzeuges überquert. [76] Die Warnung wird von dem abbiegenden Fahrzeug ausgestrahlt (Vehicle-to-Vehicle-Kommunikation).
4. Kollisionswarnung bei einfädelndem Abbiegeverkehr (merging traffic turn collision risk warning): Dies beinhaltet eine Warnung herankommender Fahrzeuge durch ein Fahrzeug, das Abbiegen möchte und sich in den Verkehr einfädeln muss. Das Risiko eines Auffahrunfalles beim Abbiegevorgang wird reduziert. [76] Die Warnung wird von dem abbiegenden Fahrzeug ausgestrahlt (Vehicle-to-Vehicle-Kommunikation).
5. Kooperative Einfädelassistentz (co-operative merging assistance): Diese beinhaltet die Kommunikation zwischen Fahrzeugen, welche an einem Einfädelvorgang beteiligt sind, zum Beispiel bei Autobahnauffahrten. Durch die Kommunikation wird der Einfädelvorgang erleichtert und das Risiko eines Unfalles reduziert. [76] Die Kommunikation findet zwischen den Fahrzeugen statt (Vehicle-to-Vehicle-Kommunikation).
6. Kollisionswarnung Knotenpunkt (intersection collision warning): Diese beinhaltet die Kommunikation zwischen Fahrzeugen an signalisierten und nicht-signalisierten Knotenpunkten zur Vermeidung von Zusammenstößen. [76]
7. Kooperative Auffahrunfallwarnung (co-operative forward collision warning): Diese beinhaltet die Kommunikation zwischen hintereinanderfahrenden Fahrzeugen zur Vermeidung von Auffahrunfällen, beispielsweise bei Bremsvorgängen. [76] Die Kommunikation findet zwischen den Fahrzeugen statt (Vehicle-to-Vehicle-Kommunikation).
8. Spurwechsel-Manöver (lane change manoeuvre): Dieses beinhaltet den Austausch von Fahrzeuginformationen (z. B. Standort und Geschwindigkeit) um einen sicheren Spurwechsel beispielsweise auf Autobahnen zu unterstützen. [76] Die Kommunikation findet zwischen den Fahrzeugen statt (Vehicle-to-Vehicle-Kommunikation).

9. Elektronisches Gefahrenbremslicht (emergency electronic brake lights): Dieses beinhaltet die Warnung nachfolgender Fahrzeuge durch ein voranfahrendes Fahrzeug, welches stark abbremst und dabei das elektronische Gefahrenbremslicht aktiviert. [76] Die Kommunikation findet zwischen den Fahrzeugen statt (Vehicle-to-Vehicle-Kommunikation).
10. Falschfahrerwarnung (wrong way driving warning): Diese beinhaltet die Warnung vor einem Falschfahrer, der eine Straße entgegen der vorgeschriebenen Richtung befährt. Diese Meldung kann entweder automatisiert vom falschfahrenden Fahrzeug versendet oder durch die Infrastruktur an betroffene Fahrzeuge versendet werden. [76]
11. Warnung stehendes Fahrzeug (stationary vehicle warning): Ein aus verschiedenen Gründen, z. B. als Folge eines Unfalls, Panne, etc., an gefährlicher Stelle lieengebliebenes Fahrzeug sendet Warnungen an sich annähernde Fahrzeuge. [76] Diese Information könnte auch zentral erfasst und an Fahrzeuge versendet werden, um den Verkehr umzuleiten.
12. Verkehrssituationswarnung (traffic condition warning): Diese beinhaltet Informationen von Fahrzeugen oder der Infrastruktur zur aktuellen Verkehrslage. [76]
13. Warnung Rotlichtverstoß (signal violation warning): Diese beinhaltet eine Warnung anderer Verkehrsteilnehmer, dass ein Rotlichtverstoß begangen wurde. [76] Zudem können Fahrer vor dem Begehen von Rotlichtverstößen gewarnt werden, indem bei zu weiter Entfernung von der Haltelinie und/oder zu kurzer verbleibender Grün-/ Gelbphase eine entsprechende Warnung für den Fahrer generiert wird.
14. Baustellenwarnung (road work warning): Die Infrastruktur versendet Informationen über Baustellen an Fahrzeuge [76]
15. dezentralisierte Floating-Car-Daten (decentralized floating car data): Fahrzeuge detektieren lokale Gefahrenherde z.B. Wind, Sichtverhältnisse, Straßenzustand, Niederschlag etc. und geben diese Informationen an andere Fahrzeuge in ihrem näheren Umfeld weiter. [76] Zudem können die Daten zentral gesammelt und auf ihre Güte überprüft werden.
16. Warnung ungeschützte Verkehrsteilnehmer (vulnerable road user warning): Befinden sich ungeschützte Verkehrsteilnehmer, beispielsweise Fußgänger oder Radfahrer in der Nähe von bzw. auf Straßen, werden Warnungen an Fahrzeuge in diesem Umfeld gesendet. Die ungeschützten Verkehrsteilnehmer können entweder durch die Fahrzeuge selbst oder die Infrastruktur detektiert werden. [76]
17. Pre-Zusammenstoß-Warnung (pre-crash sensing warning): Wird ein unvermeidlicher Zusammenstoß zwischen zwei Fahrzeugen erkannt, werden Fahrzeugattribute ausgetauscht, um die Schwere des Unfalls zu reduzieren. [76] Die Kommunikation findet zwischen den Fahrzeugen statt (Vehicle-to-Vehicle-Kommunikation).

18. Kooperative Blendungsvermeidung (co-operative glare reduction): Wird ein entgegenkommendes Fahrzeug detektiert, kann das Fernlicht automatisch ausgeschaltet werden, um den entgegenkommenden Fahrer nicht zu blenden. [76] Die Kommunikation findet zwischen den Fahrzeugen statt (Vehicle-to-Vehicle-Kommunikation).
19. Behördliche/kontextbezogene Geschwindigkeitsbeschränkungen (regulatory/contextual speed limits): Die Infrastruktur (Road Side Units) versendet lokale Geschwindigkeitsbegrenzungen an Fahrzeuge. Diese können sowohl permanente als auch temporäre Geschwindigkeitsbeschränkungen, beispielsweise aufgrund von Wetterereignissen sein. [76]
20. Kurvenwarnung (curve warning): Die Infrastruktur versendet Warnungen, um Fahrer auf Kurven im Straßenverlauf aufmerksam zu machen. Kombiniert werden können diese mit Hinweisen zur Geschwindigkeitwahl, Straßenoberflächenbeschaffenheiten, schlechter Einsehbarkeit etc.
21. LSA-Geschwindigkeitsempfehlung (green light optimal speed advisory): Die Infrastruktur (LSA) sendet Informationen über den Ampelphasenplan aus. Dadurch können Fahrzeuge die optimale Annäherungsgeschwindigkeit berechnen. Abrupte Abbremsungen vor LSA und etwaige Auffahrunfälle als Folge können hierdurch vermieden werden. [77]
22. Schilder im Fahrzeug (in-vehicle signage): Die Infrastruktur versendet Informationen zu relevanten Verkehrszeichen. Fahrer können so über potenziell gefährliche Straßenbedingungen und Geschwindigkeitsbegrenzungen informiert werden. [77]
23. Wetterwarnungen (weather warning): Die Infrastruktur versendet Informationen zu relevanten Wetterereignissen, beispielsweise starkem Wind, Schneefall, niedrigen Temperaturen etc.
24. Bahnübergang (railway crossing): Kommunikation von Fahrzeugen mit der Infrastruktur, um eine Kollision von Straßenfahrzeugen und Zügen zu vermeiden. Zum einen können Fahrzeuge vor einem herannahenden Zug gewarnt zum anderen können Warnungen von potenziell auf dem Bahnübergang liegenden gebliebenen Fahrzeugen an die Eisenbahnsicherungstechnik versendet werden. [78]
25. Verminderung von Stauausbreitung auf Autobahnen (shockwave damping): Echtzeit-Verkehrsdaten werden verwendet, um Fahrgeschwindigkeiten auf Autobahnen zu empfehlen, welche Geschwindigkeitsschwankungen verhindern. Der Verkehr wird dadurch geglättet und Stauwellen vermieden. [77]
26. reduzierte Sicht (reduced visibility): Die Infrastruktur sendet Informationen an Fahrzeuge im Fall von örtlich schlechten Sichtbedingungen. Die Daten können durch lokale Sensorik oder Sensorik von Fahrzeugen erhoben werden.

27. Fahrzeug-/ÖV-Priorisierung (vehicle/public transport prioritisation): Priorisierung von Fahrzeugen, beispielsweise Einsatzfahrzeugen oder ÖV-Fahrzeugen an Lichtsignalanlagen. Die Anforderungen der Fahrzeuge kann zentral oder lokal (Road Side Unit und Steuergerät) verarbeitet werden.

Im Rahmen dieser Arbeit wurde ermittelt, wie relevant Cloud-Computing im Kontext der verschiedenen Anwendungen ist. Die Ergebnisse sind in der Spalte ‚Cloud-Computing Relevanz‘ der nachfolgenden Tabellen (Tabelle 4 - Tabelle 6) festgehalten. Primär wurde untersucht, ob die Anwendungsfälle eine zentrale Instanz zur Datenauswertung und Informationsverteilung benötigen oder ob die Anwendung primär zwischen Fahrzeugen abläuft. In Fällen, in denen beide Möglichkeiten denkbar sind, wird Cloud-Computing eine Relevanz zugeordnet. Ein Beispiel hierfür ist die Knotenpunktkollisionswarnung. Je nach Architektur könnte entweder eine zentrale Instanz (Cloud-Computing) die Verkehrsteilnehmer inklusive ihrer Trajektorien erfassen, mögliche Konflikte kalkulieren und Warnungen aussenden. Oder die Fahrzeuge übernehmen diese Aufgabe selbst. Im letzteren Fall hat das Fahrzeug die Aufgabe, sich zu orten und mittels Positionsinformationen anderer Verkehrsteilnehmer zu kalkulieren, ob ein Zusammenstoß wahrscheinlich ist.

Zudem wurde im Rahmen dieser Arbeit eingeschätzt, welche Anwendungen Einfluss auf die Straßenverkehrssicherheit nehmen können. Dies wurde in den Tabellen in der Spalte ‚Relevanz Verkehrssicherheit‘ festgehalten. Im weiteren Verlauf werden nur solche Anwendungsfälle betrachtet, die sowohl für die Verkehrssicherheit relevant sind als auch mittels Cloud-Computing funktionieren.

Tabelle 4: C-ITS-Anwendungsfälle ETSI (Teil 1) [79]

Klasse	Gruppe	Anwendung	Cloud-Computing Relevanz	Relevanz Verkehrssicherheit
aktive Straßenverkehrssicherheit	Fahrerassistenz – kooperative Wahrnehmung	Einsatzfahrzeugwarnung	ja	ja
		Warnung langsames Fahrzeug	nein	ja
		Kollisionswarnung bei fahrbahnquerendem Abbiegeverkehr	nein	ja
		Kollisionswarnung bei einfädelndem Abbiegeverkehr	nein	ja
		kooperative Einfädelassistentz	nein	ja
		Knotenpunktkollisionswarnung	ja	ja
		kooperative Auffahrunfallwarnung	nein	ja
		Spurwechsel-Manöver	nein	ja
	Straßenhindernis Warnung	elektronisches Gefahrenbremslicht	nein	ja
		Falschfahrerwarnung	ja	ja
		Warnung stehendes Fahrzeug	ja	ja
		Verkehrssituationswarnung	ja	ja
		Warnung Rotlichtverstoß	ja	ja
		Baustellenwarnung	ja	ja
		dezentralisierte Floating-Car-Daten	ja	ja
		Warnung ungeschützte Verkehrsteilnehmer	ja	ja
		Prä-Zusammenstoß-Warnung	nein	ja
		kooperative Blendungsvermeidung	nein	ja

Tabelle 5: C-ITS-Anwendungsfälle ETSI (Teil 2) [79]

Klasse	Gruppe	Anwendung	Cloud-Computing Relevanz	Relevanz Verkehrssicherheit
kooperative Verkehrseffizienz	kooperatives Geschwindigkeitsmanagement	behördliche/kontextbezogene Geschwindigkeitsbeschränkungen	ja	ja
		Kurvenwarnung	ja	ja
		LSA-Geschwindigkeitsempfehlung	ja	ja
	kooperative Navigation	Verkehrsinformationen und Routenempfehlung	ja	nein
ÖV-Informationen		ja	nein	
Schilder im Fahrzeug		ja	ja	
kooperative lokale Dienste	standortbezogene Dienste	Point-of-Interest Informationen	ja	nein
		automatische Zugangskontrolle und Parkmanagement	ja	nein
		lokaler elektronischer Handel	ja	nein
		Medien-Download	ja	nein
globale Internet Dienste	Community Dienste	Versicherungs- und Finanzdienste	ja	nein
		Flottenmanagement	ja	nein
		Ladezonen Management	ja	nein
		Diebstahl-Dienste	ja	nein
	ITS Station Lebenszyklusmanagement	Fahrzeug-Software/Datenbereitstellung und Update	ja	nein
		Fahrzeug- und RSU-Datenkalibrierung	ja	nein
verkehrsbezogene elektronische Finanztransaktionen		ja	nein	

Tabelle 6: weitere C-ITS-Anwendungsfälle [77]

Anwendung	Cloud-Computing Relevanz	Relevanz Verkehrssicherheit
Schilder im Fahrzeug	ja	ja
Wetterinformationen	ja	ja
Bahnübergang	ja	ja
Verminderung von Stauausbreitung (Autobahnen)	ja	ja
reduzierte Sicht	ja	ja
Fahrzeug-/ÖV-Priorisierung an LSA	ja	ja
dynamische Umweltzone	ja	nein

Um Erkenntnisse über die Durchführbarkeit von C-ITS zu gewinnen und die Technologie zu erproben, wurden die Anwendungsfälle in verschiedenen Pilotprojekten erprobt. Die Pilotprojekte waren nicht Bestandteil dieser Arbeit, allerdings sind deren Ergebnisse wichtig für die Erarbeitung des Themas dieser Dissertation. Die nachfolgende Auflistung enthält einige Pilotprojekte im C-ITS-Umfeld:

1. C-Roads

In Europa arbeiten seit 2016 18 Staaten, im EU-geförderten Projekt, ‚C-Roads‘, daran, C-ITS-Dienste europaweit zu harmonisieren. Die Europäische Union und die Beteiligten erhoffen sich durch die Verwendung solcher Dienste unter anderem eine Erhöhung der Verkehrssicherheit. Das ‚C-Roads‘-Projekt umfasst insgesamt 18 Pilotprojekte, in welchen kooperative Dienste auf nationaler Ebene im realen Verkehrsumfeld implementiert und Erfahrungen in der übergeordneten ‚C-Roads-Plattform‘ eingebracht werden. [80] Im Fokus des ‚C-Roads‘-Pilotprojektes stehen folgende sicherheitsrelevante ‚C-ITS-Dienste‘: [77]

- Falschfahrerwarnung (wrong-way driving warning)
- Gefahrenbremslicht (emergency brake light)
- Schilder im Fahrzeug (in-vehicle signage)
- Bahnübergang (railway crossing)
- Stauvermeidung (Autobahn) (shockwave damping)
- temporär glatte Straße (temporarily slippery road)
- Stau Warnung (traffic jam ahead warning)
- Wetter (weather conditions)
- Einsatzfahrzeugwarnung (emergency vehicle approaching)
- Geschwindigkeitsbegrenzungen (in-vehicle speed limits)
- Fahrzeugdaten (probe vehicle data)
- reduzierte Sicht (reduced visibility)
- Rotlichtverstoß/Knotenpunktsicherheit (signal violation/intersection safety)
- Hindernis auf Straße (obstacle on the road)
- Baustellenwarnung (road works warning)
- andere Warnung (other hazardous notifications)
- langsames oder stehendes Fahrzeug (slow or stationary vehicle)

- ungeschützte Unfallstelle (unprotected accident area)
- LSA-Geschwindigkeitsempfehlung (green light optimal speed advisory)
- LSA-Priorisierung (traffic signal priority request by designated vehicle)
- ÖV-Priorisierung (public transport priority)

Zusätzlich werden auch folgende Dienste erprobt, die keine bzw. nur indirekte Auswirkungen auf die Sicherheit im Straßenverkehr haben: [77]

- dynamische Zugangskontrolle ausgewiesener Infrastruktur (dynamic access control of designated infrastructure)
- Wartezeit bis zur Grünphase (time to green)
- dynamische Umweltzone (dynamic environmental zone)
- Verkehrsinformationen und intelligentes Routing (traffic info and smart routing)

2. Talking Traffic

„Talking Traffic“ ist eine Zusammenarbeit zwischen dem niederländischen Ministerium für Infrastruktur und Wasserwirtschaft, 60 regionalen und lokalen Behörden sowie nationalen und internationalen Privatunternehmen. [81]

Gemeinschaftliches Ziel ist die Verfügbarkeit intelligenter Daten für eine breite Gruppe von Verkehrsteilnehmern (PKW, LKW, öffentliche Verkehrsmittel, Rettungsdienste, Radfahrer) zu verbessern. Auf diese Weise sollen die Sicherheit und Nachhaltigkeit von Verkehr und Transport verbessert werden, was zu einer Verkürzung der Reisezeiten und zu geringeren öffentlichen Ausgaben führt. Im Rahmen von dem Projekt wird folgendes entwickelt: [81]

- Cluster 1: Bereitstellung von LSA-Daten
- Cluster 2: Verarbeitung, Anreicherung und Verteilung einer Vielzahl von Daten und Echtzeit-Umwandlung in aussagekräftige Informationen
- Cluster 3: Bereitstellung dieser Informationen für eine Vielzahl von Verkehrsteilnehmern über Smartphones und In-Car-Systeme

Die Daten werden im „Talking Traffic“-Projekt in der Cloud erhoben, gespeichert, verarbeitet und von dort mittels verschiedener Kommunikationskanäle an die Verkehrsteilnehmer verteilt. Seit Beginn des Projektes, Anfang 2018, werden kontinuierlich neue Dienste bereitgestellt. Nachfolgende konkrete Daten bzw. Dienste sollen Straßenverkehrsteilnehmern unter anderem zur Verfügung gestellt werden: [82]

- Schilder im Fahrzeug (in-vehicle signage)
- Geschwindigkeitsbegrenzungen (in-vehicle speed limits)
- Baustellenwarnung (road works warning)
- individuelle Daten zu potenziell gefährlichen Situationen (individual real-time data on potentially dangerous situations)
- LSA-Priorisierung (traffic light prioritisation)
- Parkdaten (in-car parking data)
- LSA-Daten (real-time traffic light data)

3. Mobilidata

Mit dem Ziel frei fließende, sichere Fortbewegungsmittel zur Verfügung zu stellen, hat die flämische Regierung (Belgien) das Programm ‚Mobilidata‘ ins Leben gerufen. Im Fokus des Programms stehen: [83]

- Gewährleistung von Erreichbarkeit und Mobilität
- Verbesserung der Lebensqualität in Flandern
- Erhöhung der Verkehrssicherheit und Reduzierung von Umwelt- und Naturschäden

Um diese Ziele zu erreichen, baut ‚Mobilidata‘ in der Cloud ein Netzwerk intelligenter, nachhaltiger und zuverlässiger Datenquellen auf, an welches sich Verkehrsteilnehmer mit ihren Endgeräten anschließen können. Beispielsweise können dadurch Mobilitätsbedürfnisse von LSA besser berücksichtigt werden. Langfristig wird eine intelligente Dateninfrastruktur aufgebaut, welche den Betrieb von fahrerlosen Fahrzeugen in Flandern ermöglichen soll. [83] Das Mobilidata-Programm läuft über einen Zeitraum von fünf Jahren, von Anfang 2019 bis Ende 2023. [83]

4. NordicWay

Hinter ‚NordicWay‘ verbergen sich drei C-ITS-Pilotprojekte, die auf einer Zusammenarbeit zwischen öffentlichen und privaten Partnern in Finnland, Norwegen, Schweden und Dänemark beruhen.

Das erste Pilotprojekt ‚NordicWay 1‘ erfolgte im Zeitraum 2015 – 2017. Projektziel war die Erprobung und Förderung spezifischer C-ITS-Funktionalitäten durch eine gemeinsame Architektur. Die Ergebnisse des Projekts haben den Grundstein für eine automatisierte Cloud-Kommunikation über Mobilfunknetze mit Daten gelegt, die von fahrzeugeigenen Sensoren und der umgebenden Infrastruktur generiert werden. Es wurde eine Kommunikation zwischen Fahrzeugen, intelligenten Feldgeräten, Diensteanbietern,

Straßenverwaltungen sowie anderen öffentlichen Verwaltungen hergestellt. [84] Abbildung 8 illustriert die Architektur des Pilotprojektes. Die Abkürzung TMC steht für Traffic Management Center (deutsch: Verkehrsmanagementzentrale).

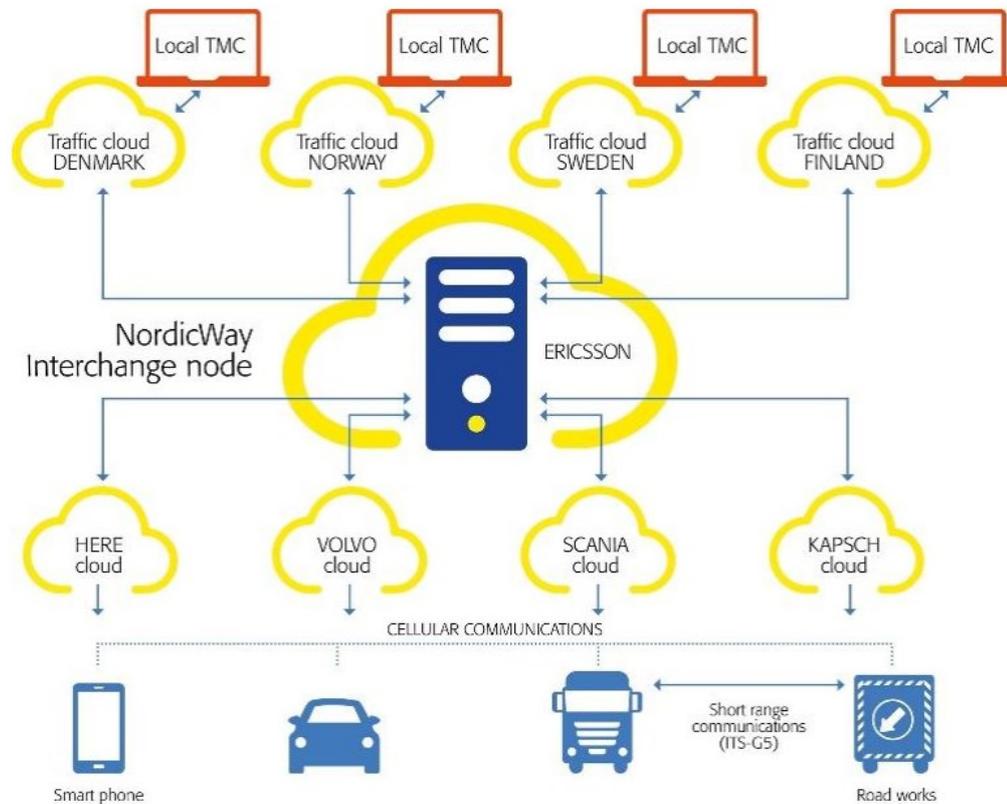


Abbildung 8: ‚NordicWay‘-Architektur [85]

‚NordicWay 2 und 3‘ bauen auf den Errungenschaften des ‚NordicWay 1‘-Projekts auf. Sie ermöglichen Fahrzeugen, Infrastruktur- und Netzbetreibern den Austausch von Daten zu Sicherheitsrisiken und andere Informationen auf Straßen in den nordischen Ländern. An ‚NordicWay 3 – Urban Connection‘ sind mehr Städte beteiligt als an ‚NordicWay 2‘. Die folgenden ITS-Dienste sind Bestandteil der Pilotprojekte: [86] [87]

- Schilder im Fahrzeug/Geschwindigkeitsbegrenzungen (in-vehicle signage/in-vehicle speed limits)
- dynamisch kontrollierte Zonen (dynamically controlled zones)
- Rotlichtverstoß (signal violation)
- Wartezeit bis zur Grün- /Rotphase (time-to-green/time-to-red)
- LSA-Geschwindigkeitsempfehlung (green light optimal speed advisory)
- LSA-Priorisierung (traffic signal priority request)

- Fahrzeugdaten (probe vehicle data)
- Baustellenwarnung (road works warning)
- Unfallwarnung (accident zone description)
- Wetter und Straßenbeschaffenheit (weather and road conditions)
- langsame und stehende Fahrzeuge (slow and stationary vehicles)
- Stauwarnung (traffic ahead warning)
- Gefahrenbremslicht (emergency brake lights)
- Einsatzfahrzeugwarnung (emergency vehicle approaching)
- Tiere oder Menschen auf der Straße (animal or person on the road)
- Hindernis auf der Straße (obstacle on the road)
- kooperative Kollisionswarnung (cooperative collision warning)

5. Data for Road Safety (DFRS)

‚Data for Road Safety‘ ist ein europäisches Konsortium verschiedener Fahrzeughersteller, Ministerien, Straßenverkehrsbetreiber und Datenlieferanten. Ziel des Konsortiums ist es, die Straßenverkehrssicherheit durch das kostenlose Teilen von sicherheitsrelevanten Verkehrsinformationen (auf englisch ‚Safety Related Traffic Information‘ (SRTI)) zu verbessern. [88]

In einem ersten Feldversuch, der von Juni 2019 bis Oktober 2020 stattfand, wurden nachfolgende Informationen von den verschiedenen Mitgliedern gesammelt, verarbeitet und wiederum allen Konsortialmitgliedern zur Verfügung gestellt: [89]

- ungesicherte Unfallstelle (unprotected accident area)
- Hindernisse auf der Fahrbahn (obstacles on the road)
- temporär rutschige Straße (temporary slippery road)
- reduzierte Sicht (reduced visibility)
- außergewöhnliche Wetterereignisse (exceptional weather conditions)
- Kurzzeitbaustellen (short-term road works)
- Falschfahrer (wrong-way driving)
- Straßensperrung (unmanaged blockage of a road)

3.4 Proprietäre Datenanalyse und Warnung

Die Anwendungen der Kategorie ‚proprietäre Datenanalyse und Warnung‘ ähneln denen der Kategorie ‚kooperative intelligente Verkehrssysteme‘ in Kapitel 3.3. Der Unterschied besteht darin, dass sie nicht den definierten C-ITS-Standards und C-ITS-Technologien entsprechen, sondern herstellerspezifische, proprietäre Lösungen sind. Nachfolgend werden Beispiele verschiedener Hersteller aufgezeigt:

1. Die japanische Firma ‚Pioneer Corporation‘ bietet folgenden Service an: Fahrzeuge werden mit einem speziellen Gerät ausgestattet, welches Daten sammelt und mit der Plattform des Herstellers in der Cloud kommuniziert. Die Daten werden in der Cloud mit anderen Daten wie beispielsweise Wetter, Topologiedaten etc. fusioniert. Extrahiert werden anschließend Gefahreninformationen, die an die Fahrzeuge zurückgesendet werden. [90]

‚Pioneer Corporation‘ hat eine Plattform aufgebaut, die die Vorhersage von Unfällen und Gefahren durch die Analyse von folgenden Informationen ermöglicht: [90]

- Zeit
- Wetter
- Katastropheninformationen
- Fahrzeuggeschwindigkeit
- LSA-Daten
- Straßentopologie (Kurven)
- Unfallschwerpunktdaten
- aggregierte Fahrzeugdaten
- crowdsource-Daten, beispielsweise Orte, an denen Fahrer dazu neigen, plötzlich langsamer zu werden und dadurch Beinahe-Unfälle auslösen

Die ermittelten Informationen werden den Fahrern, basierend auf der individuellen Fahrzeugposition, als Warnungen übermittelt. [90] Abbildung 9 zeigt die Architektur des Systems.

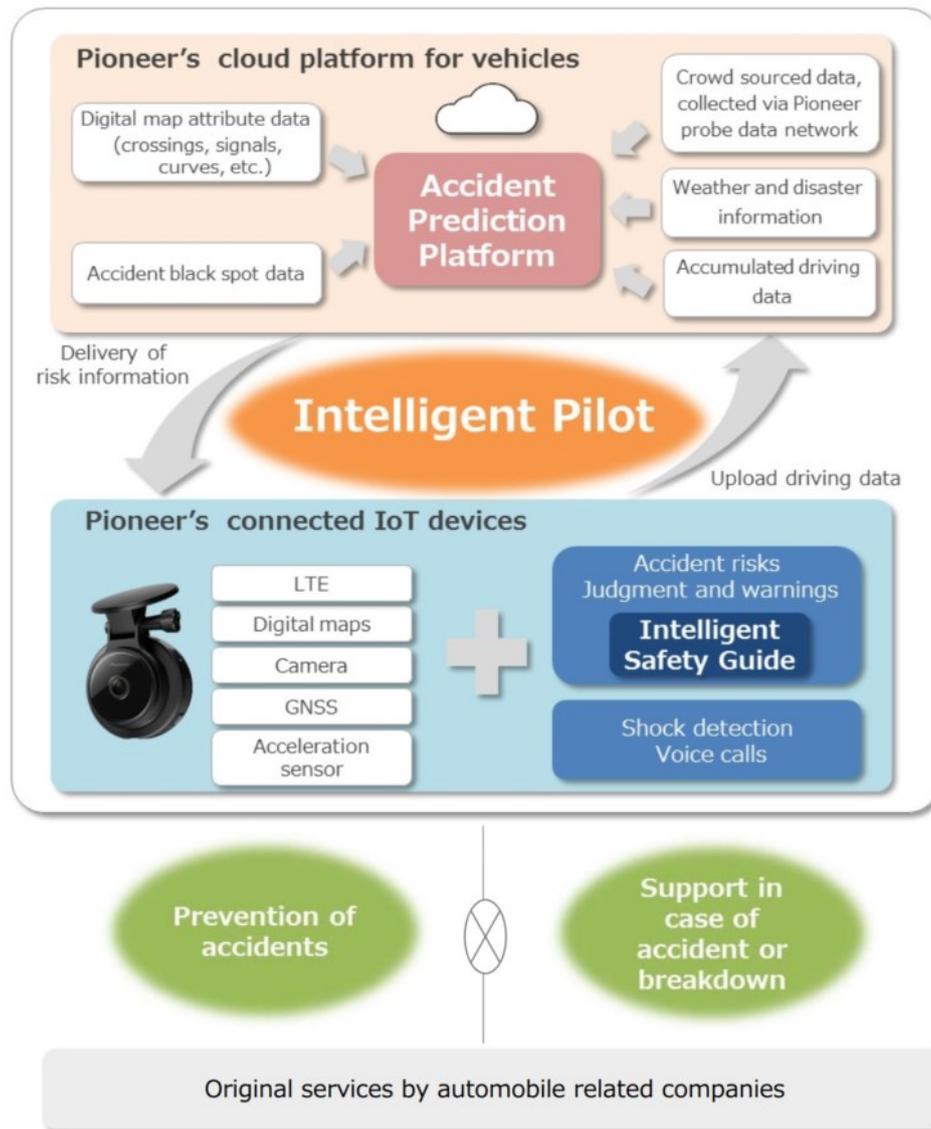


Abbildung 9: Architektur Unfallvorhersageplattform ‚Pioneer Corporation‘ [90]

2. Die Firma ‚NoTraffic‘ fusioniert in der Cloud Fahrzeugdaten mit Daten, die durch Sensorik im Feld erhoben wurden. Als Ergebnis werden Warnungen für Fahrzeuge erzeugt, im Falle, dass sich beispielsweise gefährdete Verkehrsteilnehmer, Tiere oder Hindernisse in für den Fahrer nicht einsehbaren Bereichen aufhalten und eine Kollision wahrscheinlich ist. Außerdem können mithilfe der Algorithmik Rotlichtverstöße prognostiziert werden und an Fahrzeuge in der Umgebung versendet werden. [91]
3. Die Firma ‚Bosch‘ bietet einen cloudbasierten Falschfahrerwarnungsdienst an. Die ‚Bosch‘-Software wird dabei in das On-Board-System eines Fahrzeugs integriert. Dieses sendet anonymisierte Bewegungsdaten an eine Cloud, sobald sich das Fahrzeug in der Nähe von Autobahnab- oder -auffahrten befindet. In der Cloud findet ein Abgleich mit erlaubten Bewegungsprofilen statt. Ergibt sich eine Diskrepanz, wird der Fahrer des Fahrzeugs auf sein Falschfahren aufmerksam gemacht. Außerdem werden alle mit

entsprechender On-Board-Software ausgestatteten Fahrzeuge in der Gefahrenzone vor dem Falschfahrer gewarnt. [92]

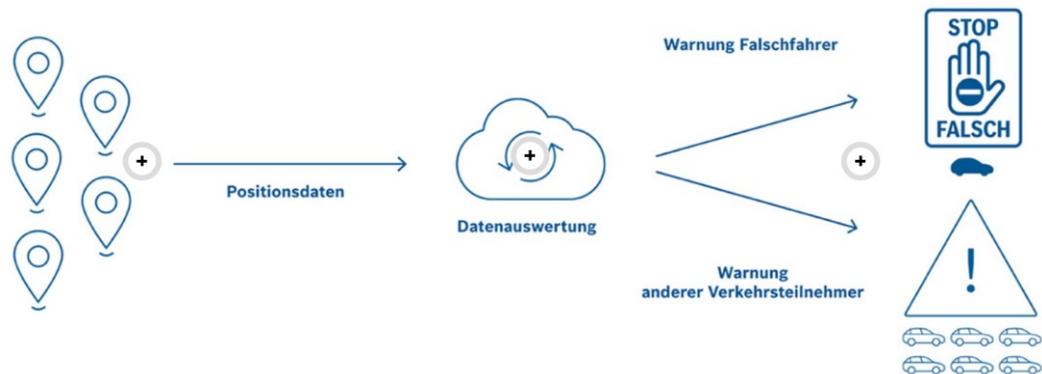


Abbildung 10: Architektur ‚cloudbasierte Falschfahrerwarnung Bosch‘ [92]

3.5 Daten- und Videoanalyse für Planungszwecke

Historische Unfalldaten sind in ihrer Anzahl und Aussagekraft limitiert. Sie stellen den einfachsten Sicherheitsindikator dar, allerdings fehlen den meisten Unfalldaten Informationen über Begleitumstände. Dies gilt insbesondere für selten gemeldete Unfallarten und Orte mit wenigen oder unvollständigen Daten. [93] Cloud-Computing ermöglicht eine unkomplizierte und kostengünstige Möglichkeit, große Datenmengen zu untersuchen und Erkenntnisse zu extrahieren.

Hersteller geben an, dass Videomaterial und Fahrzeugdaten ausgewertet werden können, um beispielsweise Beinahe-Unfälle, Beinahe-Zusammenstöße, Beinahe-Kollisionsereignisse, Konfliktereignisse, Umfeldbedingungen und das Verhalten der Verkehrsteilnehmer zu analysieren. Im Straßenverkehr ergibt sich dadurch die Möglichkeit, nicht nur historische Unfalldaten näher zu analysieren, sondern datenbasiert Erkenntnisse über Beinahe-Unfälle zu gewinnen. [93] Nachfolgend werden Anwendungen verschiedener Hersteller vorgestellt:

1. Die US-amerikanische Stadt ‚Bellevue‘ hat eine solche Technologie erprobt und resümiert, dass Knotenpunktkonfliktaten ein genauer Indikator für Unfälle sind. Die folgenden vier Anwendungsfälle für die Datenanalyse von Verkehrskonflikten wurden demonstriert, welche indirekt Auswirkungen auf die Verkehrssicherheit haben: [94]
 - Gestaltung von Projekten für die Priorisierung und Planung von ‚Vision Zero‘ (Vermeidung von Unfällen und Verletzungen)
 - Bereitstellung einer detaillierten und aktuellen Datensammlung zur Gestaltung von Sicherheitsverbesserungen
 - schnelle Vor- und Nachbewertung von Maßnahmen
 - Budgetsicherung, um Sicherheitsverbesserungen voranzutreiben

2. ‚MicroTraffic‘ ist eine weitere Firma, welche sich mit der Analyse von Beinahe-Unfällen beschäftigt. Aufnahmen von Videokameras werden von der Firma unter Verwendung der Technologien ‚Computer Vision‘, ‚Videoanalyse‘, ‚maschinelles Lernen‘ und ‚prädiktive Modellierung‘ analysiert. Die Ergebnisse dienen Ingenieuren, Verkehrsplanern und Verkehrssicherheitsexperten bei der proaktiven (Um-)Gestaltung von Straßeninfrastruktur, die Unfälle vermeidet, bevor Schaden entsteht. [95]
3. Neben der Verwendung von Videodaten kommen auch Fahrzeugdaten in Betracht, um Beinahe-Unfälle zu identifizieren. Beispielsweise weisen scharfe Bremsungen oder abrupte Lenkbewegungen auf ein Ausweichen vor möglichen Gefahrenzonen hin. ‚Michelin‘ verarbeitet solche Daten in dem ‚Data Driving to Intelligence‘-Produkt. Daten vernetzter Fahrzeuge oder externer Geräte, welche in Fahrzeugen Daten zum Fahrerverhalten und der Fahrzeugbewegung sammeln, werden von ‚Michelin‘ aggregiert, verarbeitet und visualisiert. Behörden können mit diesen Erkenntnissen Gefahrenstellen erkennen und proaktiv Beseitigungsmaßnahmen einleiten. Nach Implementierung derartiger Maßnahmen können Vorher-Nachher-Vergleiche durchgeführt und damit die Effektivität der Maßnahmen beurteilt werden. [93]

3.6 Daten- und Videoanalyse für operative Zwecke

Anwendungen der Kategorie ‚Daten- und Videoanalyse für operative Zwecke‘ ähneln jenen der Kategorie ‚Straßenverkehrsmanagement‘. Erstere haben allerdings den Charakter, Zusatzanwendungen zu eigentlichen steuernden Verkehrsmanagementanwendungen zu sein. Sie sind zudem auch für andere Nutzer relevant, dessen Aufgabe nicht das Straßenverkehrsmanagement ist, wie beispielsweise den Rettungsdienst.

Die Firma ‚Rekor‘ bietet mit ihrem ‚Rekor One™ Traffic Management‘ eine cloudbasierte Plattform, welche verschiedene Module enthält. Dies kann als Erweiterung für herkömmliche Verkehrsrechner/Verkehrsmanagementsystemen betrachtet werden, die an die tatsächliche Straßenverkehrsinfrastruktur, d. h. an die Lichtsignalanlagen, Detektoren, Wechselverkehrszeichen etc. angeschlossen sind. ‚Rekor‘ verwendet maschinelles Lernen und prädiktive Analysen, um Störungen im Verkehrsnetz automatisch zu identifizieren und gefährdete Straßenabschnitte hervorzuheben. Durch die rasche datenbasierte Erkennung von Unfällen und Echtzeit-Koordinierung von Unfallräumung durch Informationsverteilung an beteiligte Behörden leistet das Produkt einen Beitrag zur Sicherheit. Zum einen wird durch die schnellere Räumung die Wahrscheinlichkeit von Folgeunfällen reduziert, zum anderen kann die Unfallschwere durch die schnelle Bergung von Unfallopfern reduziert werden. Zudem können mit den Daten proaktive Maßnahmen zur Unfallreduzierung ermittelt werden. [96]

Die in Kapitel 3.2 aufgelisteten und beschriebenen Ausschreibungen verschiedener amerikanischer und deutscher Städte sind der Kategorie ‚Daten- und Videoanalyse für operative Zwecke‘ zuzuordnen, da der Großteil von ihnen keinen steuernden Einfluss in das Verkehrsgeschehen nehmen kann.

3.7 Community-getriebene Smartphone-Anwendungen

Anwendungen der Kategorie ‚community-getriebene Smartphone-Anwendungen‘ zeichnen sich dadurch aus, dass relevante Verkehrsinformationen durch die Nutzer einer Smartphone-Anwendung erhoben werden. Durch Standortverfolgung der Anwender kann die Verkehrslage ermittelt werden. Außerdem haben Nutzer die Möglichkeit, Straßenverkehrsinformationen in der Anwendung zu melden und dadurch anderen Nutzern zur Verfügung zu stellen. Nachfolgend werden zwei solcher Applikationen vorgestellt:

1. Die inzwischen im Hause ‚Google‘ beheimatete Smartphone-Anwendung, ‚Waze‘, bietet Nutzern Routenanweisungen auf Basis von Echtzeitverkehrsdaten. Letztere werden von den Verwendern der App selbst generiert und an einen zentralen, in der Cloud gehosteten, Server übertragen. Es werden nicht nur die Fahrten der Anwender ausgewertet, um die Verkehrslage zu bestimmen, sondern es gibt auch die Möglichkeit, verschiedene Ereignisse zu melden und andere Nutzer der App darauf aufmerksam zu machen. Beispielsweise können Unfälle, Blitzer, Polizeikontrollen, Straßensperrungen, Schlaglöcher, Überflutungen etc. gemeldet werden. ‚Waze‘ bittet andere Anwender, welche an diesen gemeldeten Problemstellen vorbeifahren, im Anschluss um Feedback und überprüft so die Korrektheit und Aktualität der Meldung.

Eine weitere Anwendung von ‚Waze‘ kann durch Behörden erfolgen, die für die Straßeninstandhaltung und das Verkehrsmanagement verantwortlich sind. Sie können die Daten nutzen, um Probleme im Netzwerk schneller zu identifizieren und zu beheben. Gefahrenstellen können so schneller eliminiert werden. [97, 98] Historische ‚Waze‘-Daten können für langfristige (operative oder planerische) Maßnahmen verwendet werden. ‚Google‘ bietet hierfür einen entsprechenden Cloud-Dienst an. [99]

Eine weitere Anwendung, welche mit ‚Waze‘ verbunden werden kann, ist ‚HAAS Alert’s Safety Cloud‘. Mittels dieser Anwendung können ‚Waze‘-Anwender über ihr Smartphone vor herannahenden Einsatzfahrzeugen gewarnt werden. Voraussetzung ist, dass eine direkte Einbindung der Applikation ins Rettungsfahrzeug erfolgt, über die die Warnungen aktiviert werden, sobald eine Rettungskraft die Warnleuchte oder Sirene einschaltet. [100, 101]

2. Die Firma ‚TomTom‘ hat mit ‚AmiGO‘ eine ähnliche Anwendung auf den Markt gebracht. Die kostenlose Smartphone App informiert über Radarkamerastandorte, Verkehrsinformationen und Gefahren sowie Straßensperrungen. Analog zu ‚Waze‘ entstammen die Informationen der Nutzer-Community, werden allerdings vor der Weitergabe an andere Nutzer von ‚TomTom‘ überprüft. [102]

4 Positiver Einfluss auf die Straßenverkehrssicherheit

4.1 Straßenverkehrsmanagement

Die klassischen Verkehrsrechner- und Verkehrsmanagementanwendungen, die in Kapitel 3.2 aufgezeigt sind, werden durch die Transition in die Cloud bei gleichbleibenden Funktionalitäten nur einen marginalen Einfluss auf die Verkehrssicherheit haben.

Die Überwachung und sichere Schaltung der LSA ist die Aufgabe, welche für die Sicherheit am relevantesten in diesem Kontext ist. Die Vermeidung von feindlichem Grün ist hierbei dem Steuergerät in der Feldebene zugewiesen, nicht etwa einer zentralen Instanz. Die Überprüfung der Funktionsfähigkeit von Signalgebern und Steuergerät erfolgt ebenfalls dezentral im Feld durch das Steuergerät. Sind Steuergeräte mit einer zentralen Software-Instanz verbunden, lassen sich die Überwachung und das Qualitätsmanagement besser durchführen. Allerdings sind dies Funktionalitäten, die auch in lokalen Rechenzentren verfügbar sind. Die Verwendung der Cloud-Computing-Technologie bietet hier keinen Vorteil. Kapitel 6.4 diskutiert die Verwendung von lokalen Rechenzentren im Gegensatz zum Cloud-Computing grundlegend im Kontext aller Anwendungen.

Des Weiteren sind die Aktivierung von Lenkungs- und Steuersystemen sowie die Koordination mit anderen Verkehrsträgern Aufgaben, welche Einfluss auf die Sicherheit im Straßenverkehr haben. Hierunter fallen beispielsweise das Anzeigen von Informationen auf Wechselverkehrszeichen (Warnungen, Umleitungen, etc.) oder die Regulierung von Geschwindigkeiten auf Autobahnen. Dies sind ebenfalls Funktionalitäten, welche auch in lokalen Rechenzentren verfügbar sind. Die Verwendung der Cloud-Computing Technologie bietet hier keinen Vorteil.

Ein positiver Effekt auf die Straßenverkehrssicherheit lässt sich ableiten, wenn klassische Verkehrsmanagementsysteme durch neue Anwendungen erweitert werden, wie beispielsweise C-ITS-Anwendungen (siehe Kapitel 4.2) oder datenverarbeitende Anwendungen (siehe Kapitel 4.3, 4.5, 4.6).

Ein kleiner positiver, indirekter Einfluss auf die Verkehrssicherheit ist denkbar, wenn die Verkehrsmanagement-Systeme in der Cloud eine höhere Verfügbarkeit aufweisen als artverwandte Anwendungen, die in einem lokalen Rechenzentrum implementiert sind. Grundsätzlich zeichnet sich Cloud-Computing durch eine hohe Verfügbarkeit aus. Verschiedene Anbieter von Verkehrsmanagementlösungen geben an, dass sie in der Cloud eine Verfügbarkeit von bis zu 99,9 % gewährleisten. [103] Die Systeme sind damit im Jahresverlauf maximal 46 Minuten nicht verfügbar. Vorausgesetzt, dass eine ausfallsichere und latenzarme Internetverbindung gegeben ist, kann davon ausgegangen werden, dass Systeme ihren Aufgaben in Bezug auf Verkehrssicherheit zuverlässig und kontinuierlich nachkommen. Je nach Server-Infrastruktur der Behörden sinkt die Verfügbarkeit von Systemen, die auf lokalen Rechnern installiert sind, auf ca. 97 %. Dies entspricht einer Nicht-Verfügbarkeit von 10 Tagen, 22 Stunden und 58 Minuten.

4.2 Kooperative intelligente Verkehrssysteme

4.2.1 Methodik

Wie in Kapitel 3.3 dargestellt, gibt es bereits einige Forschungsprojekte, die C-ITS-Technologie erproben. Um den Einfluss der verschiedenen C-ITS-Anwendungen auf die Straßenverkehrssicherheit zu ermitteln, wurden Ergebnisse diverser Pilotprojekte und Studien ausgewertet und im Folgenden anwendungsspezifisch dargestellt.

Eine Herausforderung stellten hierbei die verwendeten Maßeinheiten dar, die in den Forschungsprojekten unterschiedlich ausgewählt wurden. Um eine Vergleichbarkeit im Rahmen von dieser Arbeit zu ermöglichen, erfolgte eine Umrechnung in folgende Einheiten:

1. Auswirkung auf Anzahl getöteter Personen in Prozent [%]
2. Auswirkung auf Anzahl verletzter Personen in Prozent [%]
3. Anzahl Unfälle, die vermieden werden können, in Prozent [%]

Die Verwendung der Einheiten getötete und verletzte Personen oder Unfallanzahl wäre für die Auswertung wünschenswert gewesen. Allerdings ist eine Umrechnung der aufgelisteten Einheiten in die jeweils anderen aufgrund von fehlenden Daten nicht möglich. Bevorzugt werden, sofern entsprechende Zahlen verfügbar sind, die beiden ersten Größen ‚Auswirkung auf Anzahl getöteter Personen in Prozent‘ und ‚Auswirkung auf Anzahl verletzter Personen in Prozent‘, da Unfälle mit Getöteten oder Verletzten meldepflichtig sind und somit der Einfluss genauer abgeschätzt werden kann.

Die Ergebnisse nachfolgender Studien wurden in der dargestellten Weise zum Zweck der Vergleichbarkeit umgerechnet. Die detaillierten Kalkulationen können in Anhang A.1 und A.2 eingesehen werden.

- ‚Austroads‘-Studie: Die Studie schätzt die Unfallvermeidungswahrscheinlichkeit für verschiedene Anwendungsfälle anhand eines realen Unfalldatensatzes ab: Für jeden Anwendungsfall wurde die Anzahl der Unfälle ermittelt, auf die die zu betrachtende Technologie Auswirkungen hat. Anschließend wurde von den Forschern quantifiziert, wie viele Unfälle tatsächlich verhindert werden könnten. Das Ergebnis wird in Prozent (Anteil vermeidbarer Unfälle an den für die entsprechende Technologie relevanten Unfälle) angegeben. [104] Um eine Vergleichbarkeit mit den anderen Studien herzustellen, wird in dieser Arbeit der prozentuale Anteil an den Gesamtunfällen kalkuliert.

- ‚NordicWay‘-Evaluierung: Die Ermittlung der Auswirkung auf die Sicherheit erfolgte in der Evaluierung anhand folgender Formel: [105]

$$\begin{aligned} \text{Auswirkung auf die Anzahl der Unfälle} &= \\ &= \text{Anteil der Zielunfälle} \times \text{Warnungsabdeckung} \\ &\times \text{Wirksamkeit der Warnung} \\ &\times \text{Fahrzeug Infrastrukturausstattungsquote} \end{aligned}$$

Um eine Vergleichbarkeit mit den anderen Studienergebnissen in dieser Arbeit zu erzielen, wurden die Werte dahingehend umgerechnet, dass ein Abdeckungsgrad von 100 % sowie eine Fahrzeug-/Infrastrukturausstattungsrate von 100 % zugrunde liegt.

Die im Folgenden aufgezeigten Werte beruhen auf der Annahme, dass alle Fahrzeuge und die gesamte Infrastruktur mit entsprechender Technologie zum Versenden und Empfangen von C-ITS-Nachrichten ausgestattet sind. Dies stellt ein Idealszenario dar, welches heute noch nicht erreicht ist. Kapitel 6.1.2 diskutiert den heutigen Ausstattungsgrad und den Einfluss auf die Ergebnisse. Eine Zusammenfassung der Ergebnisse ist in Tabelle 9 im Kapitel 6.1.1 dargestellt.

4.2.2 Einsatzfahrzeugwarnung

Das europäische ‚DRIVE C2X‘-Projekt kam zu folgendem Ergebnis: Bei C-ITS-Warnungen vor Einsatzfahrzeugen, sind 0,9 % weniger Todesopfer und 0,9 % weniger Verletzte bei Straßenverkehrsunfällen zu erwarten. [106]

4.2.3 Knotenpunktkollisionswarnung

Eine durch den Dachverband der australischen Straßentransport- und Verkehrsbehörden, ‚Austroads‘, durchgeführte australische Studie kam zu folgendem Ergebnis: 6 % aller Unfälle in Australien könnten durch entsprechende Warnungen vermieden werden. Die Unfallhäufigkeit auf Knotenpunkten könnte weiter reduziert werden, wenn auf eine Warnung hin das Fahrzeug- und nicht der Mensch – automatisiert interveniert. 10 % der Unfälle könnten so vermieden werden. [104]

Die ‚CODIA‘ (‚Co-Operative Systems Deployment Impact Assessment‘)-Studie der Europäischen Kommission kam zu folgendem Ergebnis: Knotenpunkt-Kollisionswarnungen könnten zu 3,7 % weniger Todesopfern und 6,9 % weniger Verletzten führen. Die Studie untersuchte sowohl signalisierte als auch nicht-signalisierte Knotenpunkte. Die angegebenen Auswirkungen auf die Sicherheit verstehen sich als die Summe beider. [107]

4.2.4 Falschfahrerwarnung

Zu dem Sicherheitspotenzial des Anwendungsfalles Falschfahrerwarnung konnten keine Studien gefunden werden. Das Sicherheitspotenzial wurde deshalb im Rahmen dieser Arbeit wie

folgt berechnet:

2019 gab es in Deutschland knapp 1900 Falschfahrerermeldungen. Es resultierten daraus 61 Unfälle. Neun Kollisionen verliefen tödlich. Insgesamt starben elf Menschen. [108] Für die Berechnung wird angenommen, dass alle Fahrzeuge mit entsprechender Technologie zum Empfangen und Versenden von Falschfahrerwarnungen ausgestattet sind, die Falschfahrer zu 80 % erkannt und Unfälle zu knapp 50 % verhindert werden könnten. Die letztere Zahl wird durch folgende Argumentation begründet: Bei einer Warnung vor Falschfahrern erhöht sich die Aufmerksamkeit der Fahrer. Die Fahrtgeschwindigkeit wird reduziert, wodurch bei einer Begegnung mehr Zeit zur Reaktion bleibt. Durch die erhöhte Aufmerksamkeit ist davon auszugehen, dass Ausweichmanöver erfolgreich eingeleitet, und ein Teil der Unfälle vermieden werden könnten.

Es ergibt sich: 24 Unfälle könnten vermieden, die Anzahl der Getöteten pro Jahr um 4 reduziert werden. Im Gesamtkontext der deutschen Verkehrsunfälle des Jahres 2019 entsteht folgendes Potenzial: Die Anzahl Unfälle (insgesamt 2,69 Millionen) könnte um 0,0009 % und die Anzahl Getöteter (insgesamt 3064) um 0,1 % reduziert werden.

4.2.5 Warnung stehendes Fahrzeug

Das europäische ‚DRIVE C2X‘-Projekt kam zu folgendem Ergebnis: Bei C-ITS-Warnungen vor stehenden Fahrzeugen sind insgesamt (Autobahnen, inner- sowie außerhalb von Ortschaften) 1,0 % weniger Todesopfer und 0,6 % weniger Verletzte bei Straßenverkehrsunfällen zu erwarten. [106]

Die ‚CODIA‘-Studie der Europäischen Kommission kam zu dem Ergebnis, dass von in Unfällen involvierten Fahrzeugen ausgehende Warnungen zu 1,4 % weniger Todesopfern und 0,7 % weniger Verletzten führen könnten. [107]

Im Rahmen der finnischen Evaluierung des ‚NordicWay 1‘-Pilotprojektes wurde der Einfluss von Warnungen vor Unfällen mittels C-ITS anhand von Experteneinschätzungen analysiert. Die Evaluierung resultierte für das Land Finnland in einer Unfallvermeidung von 0,11 %. Die Informationen wurden zentral durch die Verkehrsmanagementzentralen zur Verfügung gestellt und nicht direkt von betroffenen Fahrzeugen ausgesendet. [105]

4.2.6 Verkehrssituationswarnung

Das europäische ‚DRIVE C2X‘-Projekt kam zu folgendem Ergebnis: Bei Stauwarnungen sind im Durchschnitt 1,5 % weniger Todesopfer und 2,1 % weniger Verletzte bei Straßenverkehrsunfällen zu erwarten. [106] Zu beachten bei dieser Auswertung ist, dass exklusiv vor Stau gewarnt wurde.

4.2.7 Warnung Rotlichtverstoß

Die ‚CODIA‘-Studie hat diesen Anwendungsfall zusammen mit dem ‚Knotenpunktkollisionswarnung‘-Anwendungsfall erprobt und die Auswirkungen auf die Sicherheit untersucht. In der

Studie wurde zwischen signalisierten und nicht-signalisierten Knotenpunkten unterschieden. Bei signalisierten Knotenpunkten, bei denen eine Warnung vor Rotlichtverstößen möglich ist, schätzt die Studie ein Reduktionspotenzial von 0,8 % (Getötete) und 1,1 % (Verletzte) ab. [107] Es ist von Folgendem auszugehen: Das Potenzial von Rotlichtverstoßwarnungen bei denen es sich ausschließlich um einen Verstoß gegen das Überfahren von Rotlicht handelt fällt etwas niedriger aus, da die Studie den gesamten Anwendungsfall ‚Knotenpunktkollisionswarnung‘ abdeckt. Beispielsweise können in diesem Gesamtkontext auch Abbiegeunfälle vermieden werden, welche bei ausschließlich Rotlichtverstoß-Warnungen nicht verhindert werden können.

4.2.8 Baustellenwarnung

Das europäische ‚DRIVE C2X‘-Projekt kam zu folgendem Ergebnis: Bei Warnungen vor Baustellen sind im Durchschnitt 2,5 % weniger Todesopfer und 2,0 % weniger Verletzte bei Straßenverkehrsunfällen zu erwarten. [106]

Im Rahmen der finnischen Evaluierung des ‚NordicWay 1‘-Pilotprojektes wurde der Einfluss von Warnungen vor Baustellen mittels C-ITS anhand von Experteneinschätzungen wie folgt analysiert: Die Evaluierung ergab für Finnland eine Unfallvermeidung von 0,67 %. [105]

4.2.9 Dezentralisierte Floating-Car-Daten

Die ‚CODIA‘-Studie der Europäischen Kommission kam zu folgendem Ergebnis: Lokale Gefahrenwarnungen, welche von Fahrzeugen auf Basis von Sensordaten ermittelt und verteilt werden, könnten zu einer Reduktion um 4,2 % bei den Todesopfer- und 3,1 % bei den Verletztenzahlen führen. [57] Folgende drei Gefahrentypen wurden bei der Untersuchung berücksichtigt:

- Hindernissen auf der Straße, z. B. Bäume, Gegenstände, langsame Fahrzeuge, Stau etc.
- Reduzierte Haftung auf der Fahrbahn durch Glätte oder Regen (Aquaplaning)
- Schlechte Sichtbedingungen durch Nebel, Regen oder Schnee

4.2.10 Warnung ungeschützte Verkehrsteilnehmer

Im Rahmen der finnischen Evaluierung des ‚NordicWay 1‘-Pilotprojektes wurde der Einfluss von Warnungen vor Menschen und Tieren auf der Fahrbahn mittels C-ITS anhand von Experteneinschätzungen analysiert. Die Evaluierung ergab für Finnland: 3,06 % weniger Unfälle. [105]

Eine europäische Studie, die explizit den Einfluss von verschiedenen Systemen auf die Sicherheit von bzw. für ungeschützte Verkehrsteilnehmer untersucht, kommt zu folgenden Ergebnissen: [23]

- Fahrrad – Kraftfahrzeug-Kommunikation: Die Anzahl der in Unfällen getöteten Personen könnte mittels einer Kommunikation zwischen Radfahrern (Smartphone App) und Fahrzeugen zum Zweck der gegenseitigen Warnung in Konfliktsituationen um 0,54 % reduziert werden, die Anzahl Verletzter um 0,86 %.
- Knotenpunktsicherheit: Die Anzahl der in Unfällen getöteten Personen könnte mittels der Detektion von Fußgängern und Radfahrern im Knotenpunktbereich zum Zweck der Warnung von und vor Fahrzeugen in Konfliktsituationen um 2,17 % reduziert werden, die Anzahl Verletzter um 3,23 %.
- Kraftrad – Kraftfahrzeug Informationssystem: Die Anzahl der in Unfällen getöteten Personen könnte mittels einer Kommunikation zwischen Moped-/Motorrädern und anderen Fahrzeugen zum Zweck der gegenseitigen Warnung in Konfliktsituationen um 1,01 % reduziert werden, die Anzahl Verletzter um 1,25 %.

4.2.11 Behördliche/kontextbezogene Geschwindigkeitsbeschränkung

Das europäische ‚DRIVE C2X‘-Projekt kam zu folgendem Ergebnis: Im Durchschnitt (Autobahnen, innerhalb sowie außerhalb von Ortschaften) sind 22,5 % weniger Todesopfer und 13,0 % weniger Verletzte bei Straßenverkehrsunfällen zu erwarten, wenn eine kontinuierliche Verteilung der Informationen über Geschwindigkeitsbegrenzungen gegeben ist. Die getestete Funktionalität beinhaltet das Anzeigen von permanenten Geschwindigkeitsbegrenzungen nach Passieren des Schildes sowie das Versenden einer akustischen und optischen Warnung bei Überschreitung der Geschwindigkeitsobergrenze. [106]

Eine durch ‚Austroads‘ durchgeführte australische Studie kam zu folgendem Ergebnis: 7 % aller Unfälle in Australien und Neuseeland könnten durch entsprechende Geschwindigkeitswarnung vermieden werden. Anders als im ‚DRIVE C2X‘-Projekt nahmen die Australier folgendes an: Die Geschwindigkeitsempfehlung wird automatisch in Abhängigkeit äußerer Einflussfaktoren, z. B. Wetter und Fahrbahnbeschaffenheit und nur in der Umgebung von Kurven generiert. Sie verwendeten für die Anwendung deshalb den Namen ‚Curve Speed Warning‘. [104]

Die ‚CODIA‘-Studie der Europäischen Kommission kam zu folgendem Ergebnis: Dynamische Geschwindigkeitsempfehlungen in Abhängigkeit von Wetter, Verkehrssituation und Fahrbahnhindernissen könnten zu 7,2 % weniger Todesopfern und 4,8 % weniger Verletzten führen. [107]

4.2.12 Kurvenwarnung

Wie in Kapitel 4.2.11 für die Anwendung ‚behördliche/kontextbezogene Geschwindigkeitsbeschränkung‘ dargestellt, ergab die von ‚Austroads‘ durchgeführte Studie folgendes: 7 % aller Unfälle in Australien und Neuseeland könnten durch entsprechende Geschwindigkeitswarnung im Kontext von Kurven vermieden werden. [104]

4.2.13 LSA-Geschwindigkeitsempfehlung

Das europäische ‚DRIVE C2X‘-Projekt kam folgendem Ergebnis: Es sind 0,1 % weniger Todesopfer und 0,2 % weniger Verletzte bei Straßenverkehrsunfällen zu erwarten. [106] Die Technologie verhindert in erster Linie das abrupte Abbremsen vor LSA und kann dadurch Auffahrunfälle insbesondere in Städten und verkehrsreichen Gebieten verhindern.

4.2.14 Schilder im Fahrzeug

Das europäische ‚DRIVE C2X‘-Projekt untersuchte den Einfluss von Schilderdarstellung im Fahrzeug auf die Sicherheit. Folgende Schildtypen wurden bei der Studie berücksichtigt:

- Achtung Kinder
- Einengungstafel
- Fußgängerüberweg
- Stop
- Vorfahrt gewähren

Die Studie resümierte folgendes: Insbesondere in räumlicher Nähe zu Fußgängerüberwegen und Bereichen mit Kindern auf der Straße werden Fahrgeschwindigkeiten durch die Schilddarstellung im Fahrzeug reduziert. Die Experten erwarten eine Verletzten-Reduktion um 0,4 % und eine Verkehrstoten-Reduktion um 0,9 %. [106]

4.2.15 Wetterinformationen

Das europäische ‚DRIVE C2X‘-Projekt kam zu folgendem Ergebnis: Es sind 6,2 % weniger Todesopfer und 4,7 % weniger Verletzte bei Straßenverkehrsunfällen zu erwarten, wenn Wetterinformationen mit Fahrzeugen geteilt werden. [106]

Im Rahmen der finnischen Evaluierung des ‚NordicWay 1‘-Pilotprojektes wurde der Einfluss von C-ITS-Wetterdiensten auf die Verkehrssicherheit anhand von Experteneinschätzungen analysiert. Die Evaluierung ergab für Finnland: Bei Glättewarnungen könnten 3,89 % aller Unfälle vermieden werden. Bei Warnungen vor außergewöhnlichen Wetterverhältnissen könnten 0,79 % der Unfälle vermieden werden. [105]

4.2.16 Bahnübergang

Zu dem Sicherheitspotenzial des Anwendungsfalles Bahnübergang konnten keine Studien gefunden werden. Das Sicherheitspotenzial wurde deshalb im Rahmen dieser Arbeit wie folgt berechnet:

2017 gab es in Deutschland knapp 157 Unfälle an Bahnübergängen. 42 Menschen starben hierbei, 202 Menschen wurden entweder leicht- oder schwerverletzt. [109] Es wird angenommen, dass alle Fahrzeuge mit entsprechender Technologie zum Empfangen und Versenden von

Bahnübergangswarnungen ausgestattet sind und Unfälle dadurch zu knapp 50 % verhindert werden könnten. Die letztere Zahl wird durch folgende Argumentation begründet: Bei einer Warnung vor herannahenden Zügen erhöht sich die Aufmerksamkeit der Fahrer. Die Fahrtgeschwindigkeit wird reduziert und der Bahnübergang im Zweifelsfall nicht passiert. Es kommt nicht zum Zusammenstoß zwischen Straßen- und Schienenfahrzeugen. Ebenfalls führt eine Meldung über ein liegengebliebenes Fahrzeug auf dem Bahnübergang dazu, dass der Streckenabschnitt für die Züge nicht freigegeben wird, und es damit nicht zu einem Zusammenstoß kommen kann. Es wird allerdings davon ausgegangen, dass nicht alle Fahrer auf die Warnung reagieren, bzw. die Fahrtgeschwindigkeit teilweise zu hoch ist, um das Straßenfahrzeug vor dem Bahnübergang zu stoppen. Außerdem muss davon ausgegangen werden, dass nicht alle Unfälle an Bahnübergängen zwischen Zügen und Kraftfahrzeugen stattfinden. Fußgänger und Radfahrer sind ebenso gefährdet und in Unfälle verwickelt, gehören aber nicht zur Zielgruppe dieser C-ITS-Anwendung. Die Statistik differenziert nicht zwischen Fußgängern, Radfahrern und Kraftfahrzeugen, weshalb eine präzisere Berechnung in dieser Arbeit nicht möglich ist.

Somit ergibt sich: 78 Unfälle könnten vermieden, die Anzahl der Getöteten pro Jahr um 22 und die Anzahl der Verletzten um 101 reduziert werden. Im Gesamtkontext der deutschen Verkehrsunfälle des Jahres 2017 entsteht folgendes Potenzial: Die Anzahl der Unfälle (insgesamt 2,64 Millionen) könnte um 0,003 %, die Anzahl Getöteter (insgesamt 3180) um 0,7 % und die Anzahl Verletzter (390 312) um 0,03 % reduziert werden.

4.2.17 Verminderung von Stauausbreitung

Zu dem Sicherheitspotenzial des Anwendungsfalles, ‚Verminderung von Stauausbreitung‘ insbesondere auf Autobahnen, konnten keine Studien gefunden werden. Es gibt viele Publikationen, welche sich mit den Auswirkungen auf die Effizienz des Straßenverkehrs beschäftigen. Der Einfluss auf die Sicherheit wird dabei nicht untersucht. Grundsätzlich scheint der Anwendungsfall den größten Mehrwert im Bereich Effizienz zu haben. Durch die Harmonisierung der Geschwindigkeiten auf der Autobahn könnten auch Unfälle vermieden werden, insbesondere in dem Stop-and-Go Verkehr, der im Staufall häufig entsteht. Eine Berechnung des Potenzials im Rahmen dieser Arbeit ist nicht möglich, da keine spezifischen Unfallstatistiken für Stausituationen auf Autobahnen verfügbar sind, anhand derer eine Hochrechnung erfolgen könnte.

4.2.18 Reduzierte Sicht

Im Rahmen der finnischen Evaluierung des ‚NordicWay 1‘-Pilotprojektes wurde der Einfluss von erprobten C-ITS-Wetterdiensten anhand von Experteneinschätzungen analysiert. Die Evaluierung ergab für Finnland: Warnungen vor schlechten Sichtverhältnissen könnten 0,09 % der Unfälle vermeiden. [105]

Zudem wurden schlechte Sichtverhältnisse im Rahmen der ‚CODIA‘-Studie zu ‚dezentralisierten Floating-Car-Daten‘ berücksichtigt. Weitere Informationen sind in Kapitel 4.2.9 zu finden. Bei der Studie wurden weitere Ereignisse mitberücksichtigt, sodass der Einfluss von Warnung vor reduzierter Sicht nicht exakt abgeleitet werden kann.

4.2.19 Fahrzeug-/ÖV-Priorisierung

Zu dem Sicherheitspotenzial der ‚Fahrzeug-/ÖV-Priorisierung‘, konnten keine Studien gefunden werden. Die Auswirkungen auf die Sicherheit werden von der Autorin als gering eingeschätzt. Eine Priorisierung des ÖV-Fahrzeugs an einer LSA bedeutet in den meisten Fällen eine Verlängerung der Grünphase um einige Sekunden, sodass das ÖV-Fahrzeug den Knotenpunkt ohne Halt passieren kann. In erster Linie wird damit die Reisegeschwindigkeit des ÖV-Fahrzeuges erhöht und damit die Effizienz des Öffentlichen Nahverkehrs. Durch eine Verlängerung der Grünphase sollten sich weder für feindliche Verkehrsströme noch für den Verkehrsstrom, dem das ÖV-Fahrzeug angehört, noch für Fußgänger verringerte beziehungsweise zusätzliche Sicherheitsrisiken ergeben.

Bei Einsatzfahrzeugen bewirkt eine Priorisierung, dass Knotenpunkte nicht mehr bei Rot passiert werden müssen. Dadurch wird die Sicherheit für alle Verkehrsteilnehmer erhöht. Das Risiko eines Zusammenstoßes auf dem Knotenpunkt wird reduziert. Um ein quantitatives Sicherheitspotenzial bestimmen zu können, müssten Daten zu Unfällen auf Knotenpunkten mit Einsatzfahrzeugen bei Rotlichtverstoß vorliegen. Diese Statistiken lagen zum Zeitpunkt der Erstellung dieser Arbeit jedoch nicht vor.

4.3 Proprietäre Datenanalyse und Warnung

Zu den Sicherheitspotenzialen der proprietären Lösungen, welche in Kapitel 3.4 vorgestellt wurden, gibt es herstellerseitig keine Angaben. Es ist davon auszugehen, dass eine Bewertung analog zu den verschiedenen C-ITS-Anwendungsfällen erfolgen kann. Zu beachten ist, dass aufgrund der proprietären Natur der Dienste vermutlich niemals ein Ausstattungsgrad von 100 % eintreten wird. Demnach sind die Sicherheitspotenziale deutlich geringer anzusetzen als bei den C-ITS-Anwendungsfällen, bei denen aufgrund der Standardisierung von einer flächendeckenden Ausbreitung in der Zukunft ausgegangen werden kann.

4.4 Daten- und Videoanalyse für Planungszwecke

Die Firma ‚MicroTraffic‘ gibt folgendes an: Sie kann durch die in Kapitel 3.5 beschriebene Verfahrensweise Pläne für Knotenpunkte erstellen, die zu einer Risikoreduzierung von 80 % führt. [95] Unklar bleibt hierbei, was mit Risiko konkret gemeint ist. Das Unternehmen reagierte auf eine schriftliche Nachfrage zu diesem Thema nicht. Da die Firma mit ihrer Technologie in erster Linie Beinahe-Unfälle detektiert, und basierend hierauf eine Umgestaltung der Infrastruktur vorgenommen werden kann, kann von Folgendem ausgegangen werden: Auf Basis der Beinahe-Unfalldaten können sicherheitsoptimierende Planungen erstellt werden, die zu einer 80 %-igen Reduzierung von Beinahe-Unfällen führt. Nach entsprechender Umsetzung wird sich die Zahl der tatsächlichen Unfälle vermutlich ebenfalls reduzieren.

Offen bleibt, in welchem Maße tatsächliche Unfälle reduziert werden können. Besteht ein linearer oder anderer Zusammenhang zwischen der Anzahl reduzierter Beinahe-Unfälle und

der Anzahl tatsächlicher Unfälle? Eine Literaturrecherche zu diesem Thema erbrachte keine weiteren Erkenntnisse. Es herrscht in der Wissenschaft Einigkeit darüber, dass die Analyse von Beinahe-Unfällen für die Verbesserung der Sicherheit wichtig ist. [93, 110] Welchen quantitativen Einfluss dies auf die Unfallzahlen hat, scheint bislang unerforscht zu sein.

Die Firma ‚Michelin‘ gibt keine Kennwerte an, die die Einschätzung des Sicherheitsverbesserungspotenzials ihrer Lösung erlauben.

4.5 Daten- und Videoanalyse für operative Zwecke

Die Firma ‚Rekor‘ gibt in einer Fallstudie, die im südlichen Teil des amerikanischen Bundesstaats Nevada durchgeführt wurde, folgendes an: Durch Ihre Technologie wurden 18 % aller Unfälle vermieden und Höchstgeschwindigkeitsüberschreitung um 43 % verringert. Konkret analysierte die Software Daten verschiedener Quellen und ermittelte daraufhin Orte und Zeiten, an bzw. zu denen eine überproportional hohe Häufung von Geschwindigkeitsüberschreitungen vorkommt. Diese Erkenntnisse werden von zuständigen lokalen Behörden verwendet, um gezielte Geschwindigkeitsüberwachungen durchzuführen und Einsatzkräfte zu verteilen. [111]

4.6 Community-getriebene Smartphone-Anwendungen

Zu den Sicherheitspotenzialen der ‚community-getriebenen Smartphone-Anwendungen‘, welche in Kapitel 3.7 vorgestellt wurden, gibt es keine konkreten Angaben. Der Hauptfokus der Anwendungen liegt auf der Verbesserung der Fahrerlebnisse der individuellen Nutzer, in erster Linie einer Optimierung der Reisezeit. Denkbar sind allerdings auch Auswirkungen auf die Sicherheit. Laut Firma ‚Waze‘ erhöhen die Applikationen durch die Hinweise die Sicherheit im Straßenverkehr. [98, 101, 112] Allerdings gibt es auch Gegenstimmen, die in der Verwendung der Anwendung während der Fahrt eine Gefährdung sehen, da das Ablenkpotezial groß ist. Kritisiert wird außerdem die Unterstützung von regelwidrigem und kriminellem Verhalten durch die Publikation von Blitzern und Polizeikontrollen. [113–115]

Es ist davon auszugehen, dass das Sicherheitspotenzial der Straßenverkehrsteilnehmerwarnungen den jeweiligen C-ITS-Anwendungsfällen ähnelt, da die Verarbeitung der Warnung durch den Nutzer in beiden Fällen gleich erfolgt - unabhängig von der Entstehung oder der Übertragung der Information. Im Vergleich zu den C-ITS und zu den proprietären Datenanalyse- und Warnungsanwendungen geht die Verbreitung von ‚Waze‘ deutlich schneller voran. In naher Zukunft kann bereits eine relativ hohe Felddurchdringung erreicht werden. Dies liegt an der geringen Anfangshürde - die Anwendung ist gratis auf jedes Smartphone herunterzuladen. Der direkte Anwendernutzen ist hoch, z.B. durch die Ermittlung der optimalen Reiseroute und Verkürzung der Reisezeit. Außerdem lockt und bindet die Applikation durch ihren Gamification-Ansatz Nutzer. Es werden verschiedene Anwendungsfälle unterstützt: Verkehrsteilnehmer werden vor diversen Gefahren gewarnt.

Zudem werden die Daten für Städte bereitgestellt, um die Reaktionszeiten für Unfälle zu

reduzieren oder Straßeninfrastruktur umzuplanen. Demnach werden auch die Sicherheitspotenziale größer als für die proprietären Datenanalyse- und Warnungsanwendungen eingeschätzt.

Auch einige Städte, die Kooperationen mit ‚Waze‘ gestartet haben, sehen solch ein Sicherheitspotenzial. Über das sogenannte ‚Waze for Cities‘-Netzwerk teilt der Verkehrsbetreiber Daten zu Straßensperrungen und Verspätungen mit und erhält im Gegenzug Zugriff auf die Verkehrsdaten der App, um seine Dienste zu verbessern. Ein Beispiel ist die Stadt London. ‚Transport for London‘ ist eine Kooperation mit ‚Waze‘ eingegangen, um Sicherheitsmeldungen über ein neues Warnsystem direkt an Fahrer zu senden. [116] Das ‚Volpe Center for Transportation Research‘ nutzt im Auftrag der ‚Tennessee Highway State Patrol‘ ‚Waze‘-Daten zur besseren Vorhersage und Vermeidung von Unfällen sowie zur besseren Reaktion auf Unfälle. [112]

Das ‚Rochester Hills Fire Department‘ (Michigan, USA) verwendet ‚Waze‘ und die ‚HAASAlert Safety Cloud‘, um Straßenverkehrsteilnehmer über ein herannahendes Einsatzfahrzeug zu informieren. Verkehrsteilnehmer werden so mehr als 30 Sekunden vor dem Eintreten der Gefahrensituation gewarnt und können besser reagieren. ‚Waze‘ und die Anwender erhoffen sich dadurch eine Reduzierung der Unfälle mit Einsatzfahrzeugen sowie ein schnelleres Vorankommen der Einsatzfahrzeuge. Laut ‚Waze‘ gibt es neben dem ‚Rochester Hills Fire Department‘ über 100 weitere Kommunen und Sicherheitsabteilungen, die die Anwendung einsetzen. [101]

5 Andere Einflüsse auf die Straßenverkehrssicherheit

5.1 Verhaltensanpassungen

Im Zusammenhang mit der Einführung neuer Anwendungen, die die Sicherheit im Straßenverkehr positiv beeinflussen sollen, ist davon auszugehen, dass die Verkehrsteilnehmer ihr Verhalten anpassen. Verhaltensanpassungen können allerdings den positiven Effekten entgegenwirken.

Forscher beschäftigen sich schon seit den 60er-Jahren mit der Modellierung von Fahrerverhalten. Ein prominenter Vertreter, John Michon, stellte ein Modell auf, welches die Entscheidungsfindung von Fahrern in drei Ebenen unterteilt: strategisch (planend), taktisch (manövrierend) und operativ (kontrollierend). [22]

Die strategische Ebene definiert die allgemeine Planungsphase eines Weges einschließlich der Bestimmung von Reiseziel, Route und Verkehrsmittelwahl sowie einer Bewertung der damit verbundenen Kosten und Risiken. Die individuellen Planungen leiten sich zudem aus allgemeinen Überlegungen zu Verkehr und Mobilität ab, aber auch aus Begleitfaktoren, wie zum Beispiel Zufriedenheit und Komfort. [22]

Auf taktischer Ebene werden beispielsweise Fahrbahnen, Fahrtgeschwindigkeiten oder der Abstand zum vorausfahrenden Fahrzeug gewählt. Die operative Ebene beschreibt die Reaktion auf vorherrschende Situationen und die damit verbundene Akzeptanz von beispielsweise tatsächlichen Fahrgeschwindigkeiten, Abständen zu vorausfahrenden Fahrzeugen, Wachsamkeit etc. [24] Die Cloud-Anwendungen der Kategorien ‚kooperative intelligente Verkehrssysteme‘, ‚proprietäre Datenanalyse und Warnung‘ sowie ‚community-getriebene Smartphone-Anwendungen‘, welche im Rahmen dieser Arbeit vorgestellt wurden und an Kraftfahrzeugführer gerichtet sind, beeinflussen alle drei Ebenen.

Allerdings wirken sich diese Anwendungen nicht nur auf das Verhalten der Fahrer aus, sondern auch auf andere Verkehrsteilnehmer, wie beispielsweise Fußgänger, Radfahrer etc. Ein Ansatz, der im europäischen Raum häufig zur ganzheitlichen Abschätzung von Sicherheitsauswirkungen intelligenter Verkehrssysteme verwendet wird, wurde von Risto Kulmala erstellt. Er enthält folgende neun Untersuchungspunkte: [24]

1. direkte Veränderung der Aufgaben der Verkehrsteilnehmer
2. direkte Beeinflussung durch infrastrukturseitige Systeme
3. indirekte Veränderung des Nutzerverhaltens in vielfältiger, überwiegend unbekannter Weise
4. indirekte Veränderung des Verhaltens von Nicht-Nutzern
5. Veränderung der Interaktion zwischen Nutzern und Nicht-Nutzern
6. Veränderung der Exposition von Verkehrsteilnehmern
7. Veränderung der Verkehrsmittelwahl
8. Veränderung der Routenwahl
9. Veränderung von Unfallfolgen

Beispielhaft wird nach diesem Ansatz für die C-ITS-Anwendung ‚Warnung ungeschützter Verkehrsteilnehmer‘ in Tabelle 7 abgeleitet, welche Sicherheitsauswirkungen sich im Gesamtkontext ergeben können. Die Ergebnisse sind als mögliche Szenarien zu verstehen und somit hypothetisch. Eine Überprüfung bedarf einer entsprechenden Studie - im Idealfall durch Verwendung einer derartigen Anwendung in der Realität oder alternativ durch eine Simulation. Dies hat bis zum heutigen Zeitpunkt noch nicht stattgefunden.

Eine in einem Fahrsimulator durchgeführte Studie über Verhaltensanpassungen durch vorausschauende Warnsysteme am Beispiel von Stauendwarnungen kam zu folgenden Ergebnissen: Gehen die Autofahrer von einer Unterstützung durch Stauendwarnungen aus, erhöht sich die maximale Geschwindigkeit. Dadurch reduziert sich die Zeit bis zur Kollision. Außerdem wurde festgestellt, dass jüngere Fahrer ca. 40 % mehr Nebenaufgaben bearbeiten, also abgelenkter sind, wenn sie durch ein solches Assistenzsystem unterstützt werden. Der Abstand zu vorausfahrenden Fahrzeugen und die Bremsbereitschaft veränderten sich nicht. Die Studie schlussfolgert, dass bei der Einführung von vorausschauenden Warnsystemen mit Verhaltensanpassungen zu rechnen ist. Anpassungen und Auswirkungen in der Realität können anders ausfallen als in der simulierten Testumgebung und weisen auf den Mehrwert von Feldversuchen unter realen Bedingungen hin.[117]

Tabelle 7: potenzielle Sicherheitsauswirkungen der C-ITS-Anwendung, ‚Warnung ungeschützter Verkehrsteilnehmer‘ nach dem Modell von Risto Kulmala [24]

Untersuchungspunkt	Potenzielle Auswirkungen der C-ITS-Anwendung ,Warnung ungeschützter Verkehrsteilnehmer‘
direkte Veränderung der Aufgaben der Verkehrsteilnehmer	Verkehrsteilnehmer achten weniger auf die Umgebung, da sie sich auf die Warnung der Technik verlassen.
direkte Beeinflussung durch infrastruktureitige Systeme	keine
indirekte Veränderung des Nutzerverhaltens in vielfältiger, überwiegend unbekannter Weise	Die Reaktionszeiten von Fahrzeugführern erhöhen sich, sollten Ereignisse nicht von der Technik erkannt und entsprechend gemeldet werden. Nutzende ungeschützte Verkehrsteilnehmer nehmen mit verringerter Aufmerksamkeit am Straßenverkehr teil, da sie von einer Warnung vor Kraftfahrzeugen ausgehen.
indirekte Veränderung des Verhaltens von Nicht-Nutzern	Ungeschützte Verkehrsteilnehmer nehmen mit verringerter Aufmerksamkeit am Straßenverkehr teil, da sie sich auf die Warnsysteme der Fahrzeuge verlassen und davon ausgehen, dass Fahrer reagieren und ihnen den Vorrang lassen.
Veränderung der Interaktion zwischen Nutzern und Nicht-Nutzern	Abrupte Bremsungen durch Nutzer aufgrund von Warnungen, können für Nicht-Nutzer als unvorhergesehen wahrgenommen werden und zu Unfällen führen.
Veränderung der Exposition von Verkehrsteilnehmern	Ungeschützte Verkehrsteilnehmer wännen sich in trügerischer Sicherheit und neigen zu unachtsamen Verhalten.
Veränderung der Verkehrsmittelwahl	Durch die höhere subjektive Sicherheit werden mehr Wege mit dem Fahrrad zurückgelegt.
Veränderung der Routenwahl	Ungeschützte Verkehrsteilnehmer wählen „gefährlichere“ Routen, da ihr subjektives Sicherheitsempfinden höher ist.
Veränderung von Unfallfolgen	vermutlich keine Eventuell könnte allerdings die Unfallschwere reduziert werden unter der Annahme, dass die Anwendung einen Bremsvorgang initiiert, der anschließend zu einem weniger starken Aufprall führt.

Bei ‚community-getriebenen Smartphone-Anwendungen‘ könnte bei der Verwendung während der Fahrt die Aufmerksamkeit von der Fahrbahn abgelenkt sein. Nutzer werden während der Fahrt gebeten, Informationen zur aktuellen Verkehrslage und Ereignisse zu teilen oder neue Probleme oder Ereignisse zu melden. Aus der hierdurch entstehenden Unachtsamkeit könnten Unfälle entstehen, die den Sicherheitsbestrebungen der Anwendung entgegenwirken und eine zusätzliche Gefahr im Straßenverkehr darstellen. Ein weiterer Begleiteffekt, der durch die Verwendung solcher Applikationen entstehen kann, ist die vermehrte Nutzung von Seitenstraßen anstelle von Hauptstraßen, um die Reisezeit des Einzelnen zu verringern. Es kommt zu einer unerwünschten Verkehrsverlagerung in Wohngebiete. Das Unfallrisiko steigt, da diese Straßen nicht für den Durchgangsverkehr konzipiert wurden.

5.2 Nutzerakzeptanz

Die Akzeptanz der verschiedenen Anwendungen bei den Nutzern ist ein Aspekt, der den in Kapitel 4 aufgeführten Sicherheitspotenzialen entgegenwirken kann. Sie beeinflusst die Straßenverkehrssicherheit nicht negativ, kann aber indirekt die prognostizierten positiven Effekte reduzieren. Sehen Nutzer keinen Mehrwert für sich und/oder ist ihnen der Mehrwert für andere nicht ersichtlich, werden sie die Dienste nicht verwenden bzw. ignorieren. Zudem muss darauf geachtet werden, dass die Qualität der Ergebnisse hoch ist. Insbesondere bei den Anwendungen der Kategorien ‚kooperative intelligente Verkehrssysteme‘, ‚proprietäre Datenanalyse und Warnung‘ sowie ‚community-getriebenen Smartphone-Anwendungen‘ ist es wichtig, dass Warnungen nur angezeigt werden, wenn tatsächlich eine Gefahr vorhanden ist. Werden häufig Warnungen ohne erkennbares Unfallrisiko ausgegeben, stumpfen Anwender ab und reagieren im Ernstfall nicht mehr auf die Warnungen.

Eine Studie, die die Nutzerakzeptanz von C-ITS-Diensten untersuchte, kam zu folgendem Ergebnis: Die Dienste werden gut angenommen. 91 % der Testanwender gaben an, gewillt zu sein, entsprechende Systeme weiterhin zu nutzen. Allerdings waren nur 42 % bereit, Geld auszugeben, um ihre Fahrzeuge mit einer entsprechenden Technologie ausstatten zu lassen. [106]

5.3 Cyberangriffe und Netzausfälle

Um die Gefahr von Cyberangriffen und Netzausfällen für Cloud-Anwendungen zu bewerten, die Einfluss auf die Straßenverkehrssicherheit nehmen, werden die Verwendungszwecke der Anwendungen betrachtet und in verschiedenen Extremszenarien untersucht. Im Folgenden werden die Szenarien skizziert, welche potenziell als Folge von Cyberangriffen oder Netzausfällen eintreten könnten. Den negativen Auswirkungen der meisten Szenarien kann mit Maßnahmen entgegengewirkt werden. Diese sind allerdings meist aufwendig und/oder so teuer, dass die Anwendungen dadurch unter Umständen nicht mehr wirtschaftlich sind. Mögliche vorbeugende Maßnahmen werden der Vollständigkeit halber für die verschiedenen Szenarien nachfolgend aufgeführt:

- Verbindungsstörung

Die Internetverbindung bricht ab, der Dienst in der Cloud ist nicht mehr erreichbar.

vorbeugende Maßnahme: Für Verkehrsmanagementzentralen, die Feldgeräte steuern, kann eine dezidierte, redundante Standleitung zwischen lokalem Netzwerk und Cloud aufgebaut werden.

- Infrastruktur physikalisch gestört

Als Folge einer Umweltkatastrophe, eines Brandes, eines Einbruches etc. kann es zu einer Unverfügbarkeit der Rechenressourcen inklusive Verlust der dort gespeicherten Daten kommen.

vorbeugende Maßnahme: Notfallwiederherstellungsmechanismen, die auf Redundanzen, Ersatzhardware, Datensicherungen etc. aufgebaut sind. Professionelle Cloud-Anbieter bieten solche Dienstleistung an. Es können zusätzliche Kosten anfallen.

- Cyberangriff auf Infrastruktur

DoS-Angriffe, das Einbringen einer Schadsoftware, welche die Daten in Computern löscht, oder Ransomware-Angriffe etc., können die Rechen-Infrastruktur so schädigen, dass sie (temporär) unverfügbar ist. Daten können gestohlen werden.

vorbeugende Maßnahme: Notfallwiederherstellungsmechanismen, die auf Redundanzen, Ersatzhardware, Datensicherungen etc. aufgebaut sind. Professionelle Cloud-Anbieter bieten solche Dienstleistung an. Es können zusätzliche Kosten anfallen.

- Cyberangriff auf Anwendung

Ein Angriff auf die Anwendung, beispielsweise durch Malware oder Code-Modifizierung, kann dazu führen, dass die Anwendung nicht verfügbar ist oder in ihrer Funktionalität (Integrität) gestört wird, und dadurch potenziell (indirekter) Schaden entsteht.

vorbeugende Maßnahme: Schutz der Anwendungen, Implementierung von Anwendungsselbstschutz und Code-Härtungsmaßnahmen sowie Durchführung von Schwachstellenanalysen

Im Rahmen dieser Szenarien kann es durch Cyberangriffe und Netzausfälle auf in der Cloud gehostete Anwendungen zu diesen Folgen kommen:

1. Dienst ist nicht verfügbar
2. Integrität des Dienstes ist gestört (Übermittlung falscher Daten oder Verwendung des Dienstes als Übertragungsmedium für Schadsoftware)
3. Datenverlust

Die Gefahr des Datenverlustes im Zusammenhang mit den in dieser Arbeit herausgearbeiteten Anwendungen wird in Kapitel 5.4 untersucht. Welche Konsequenzen die ersten beiden Folgen auf die Sicherheit im Straßenverkehr haben können und welche Risiken sich hieraus ergeben, wird für die in Kapitel 3 und 4 erläuterten Anwendungskategorien in Tabelle 8 detailliert analysiert.

Zusammenfassend lässt sich festhalten: Die beiden erstgenannten Folgen haben einen zu meist indirekten, sicherheitskritischen Einfluss auf die Verkehrssicherheit. Die Auswirkungen einer Störung der Integrität eines Dienstes wird dabei als potenziell gefährlicher eingeschätzt, als wenn dieser Dienst nicht verfügbar ist. Positiv ist, dass die Straßenverkehrssicherheit in den meisten Fällen nur indirekt beeinflusst wird, da die Anwendungen auf das Teilen von Informationen beschränkt sind und nicht aktiv in das Verkehrsgeschehen eingreifen. Eine Ausnahme bilden hier Anwendungen aus dem Bereich der kooperativen intelligenten Verkehrssysteme, da diese eine direkte informationstechnische Schnittstelle zum Fahrzeug beinhalten. Es ist denkbar, dass Cyberangriffe dadurch Fahrzeuge manipulieren und damit ein großes Risiko für die Straßenverkehrssicherheit darstellen. Cyberangriffe auf Cloud-Anwendungen und Netzausfälle im Bereich der ‚kooperativen intelligenten Verkehrssysteme‘ sowie der ‚proprietäre Datenanalyse und Warnung‘ - sofern diese eine direkte Schnittstelle zum Fahrzeug aufweisen und nicht auf einem separaten Endgerät verwendet werden - werden als am kritischsten eingestuft. Cyberangriffe auf Cloud-Anwendungen und Netzausfälle im Bereich ‚Daten- und Videoanalyse für Planungszwecke‘ werden als unkritisch eingestuft. Detaillierte Erläuterungen sind in Tabelle 8 zu finden.

Die Verkehrsinfrastruktur ist für die Versorgung der Bevölkerung und die öffentliche Sicherheit relevant und gehört in Deutschland daher zu den Kritischen Infrastrukturen, die ausreichend gegen Cyberangriffe zu schützen sind. Es existieren diverse, zum Teil verpflichtende Richtlinien, siehe Aufstellung in Kapitel 2.1.2.2, um die Risiken zu minimieren.

Abbildung 11 zeigt eine unvollständige Übersicht über Cyberangriffe im Verkehr-, Transport- und Logistiksektor für das zweite Halbjahr 2021. Die Anzahl der Fälle weist auf die Wichtigkeit des Themas Cyber-Security hin, auch wenn davon auszugehen ist, dass die Verkehrssicherheit nur bei sehr wenigen der aufgelisteten Fälle gefährdet war. Bei dem Angriff auf den Autobahnbetreiber in Charleston, USA am 12.11.2021 wurde beispielsweise ein internes System angegriffen, welches für E-Mails, Telefonate und diverse andere nicht-sicherheitskritische Anwendungen verwendet wird. Der Autobahnbetrieb und damit die Verkehrssicherheit war nicht betroffen. [118]

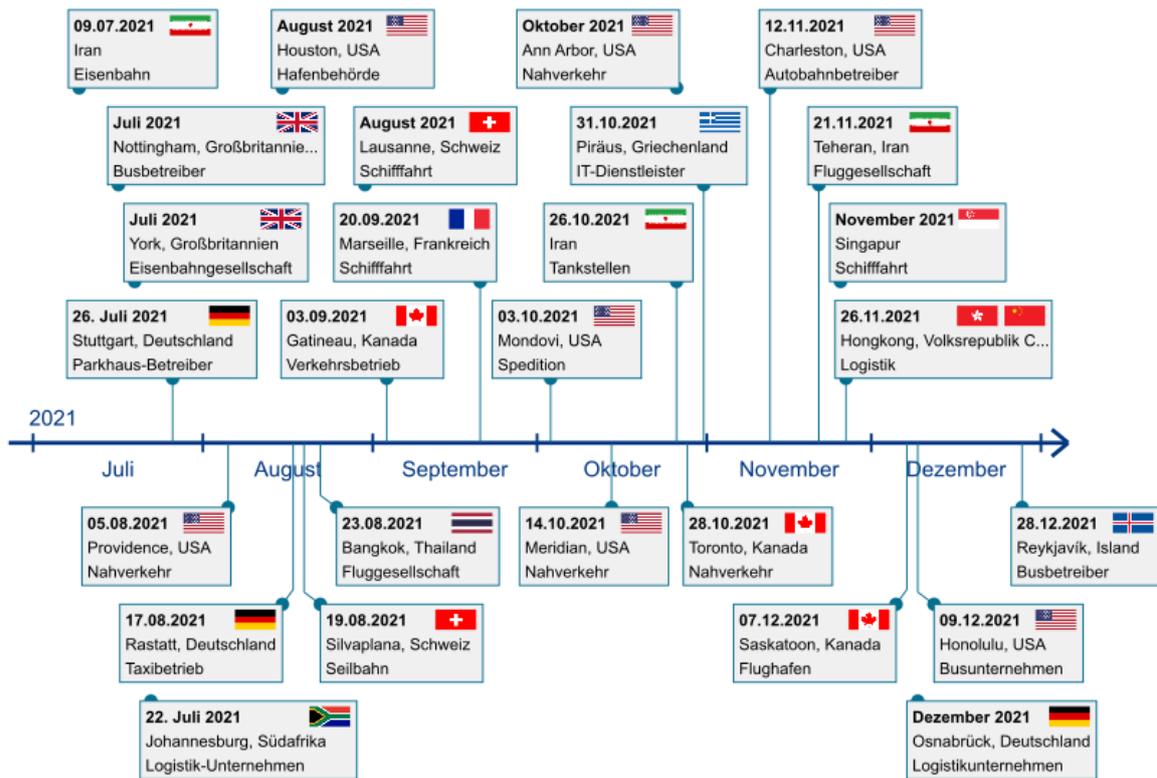


Abbildung 11: Übersicht Cyberangriffe 2. Halbjahr 2021 [119]

Tabelle 8: mögliche Auswirkungen von Cyberangriffen und Netzausfällen

Anwendung	Szenario 1: Dienst ist nicht verfügbar	Szenario 2: Integrität des Dienstes ist gestört
<p>Straßenverkehrsmanagement</p>	<p>Wenn in der Cloud bereitgestellte Straßenverkehrsmanagementsysteme, welche steuernd in den Verkehr eingreifen, nicht verfügbar wären, fielen Feldgeräte auf ihre lokale Steuerungsebene zurück. Lichtsignalsteuerungen könnten damit nicht mehr durch zentrale Algorithmen und Eingriffe optimiert werden. Ebenfalls würde die Steuerung des Verkehrs über dynamische Schilder verhindert. Es könnte insgesamt von einer Verschlechterung des Verkehrsablaufes ausgegangen werden und einem indirekten negativen Einfluss auf die Verkehrssicherheit, da das Verkehrsmanagement seiner eigentlichen Aufgabe, die Verkehrssicherheit zu verbessern, nicht nachkommen könnte.</p>	<p>Wenn die Integrität eines in der Cloud bereitgestellten Straßenverkehrsmanagementsystems gestört wäre, könnten viele Situationen eintreten, welche den Straßenverkehr primär in einen chaotischen Zustand versetzten und die Straßenverkehrssicherheit damit negativ beeinträchtigen könnten. Beispielsweise könnten alle Lichtsignalanlagen auf rot, ausgeschaltet oder auf gelb-blinkend gesetzt werden, was insbesondere in Spitzenverkehrsstunden zu erheblichen Beeinträchtigungen des Verkehrsablaufes führte. Das Schalten von feindlichem Grün ist in den Steuergeräten durch die Signalsicherung abgesichert, sodass dieser Fall nicht eintreten könnte. Ein weiteres denkbare Szenario wäre, dass dynamische Geschwindigkeitsanzeigen falsche Informationen anzeigten, die zu gefährlichen Situationen führen könnten. Auch könnten dynamische Verkehrsschilder falsche Informationen anzeigen, beispielsweise ‚Bombenalarm‘ oder ‚Achtung Atomkrieg‘, die die Verkehrsteilnehmer psychisch beeinflussen und vom Straßenverkehr ablenken. Damit würde die Sicherheit im Straßenverkehr indirekt negativ beeinflusst.</p>

Tabelle 8: mögliche Auswirkungen von Cyberangriffen und Netzausfällen

Anwendung	Szenario 1: Dienst ist nicht verfügbar	Szenario 2: Integrität des Dienstes ist gestört
<p>Kooperative intelligente Verkehrssysteme</p>	<p>Der Ausfall einer Anwendung aus dem Feld der ‚kooperativen intelligenten Verkehrssysteme‘ hätte heutzutage (menschliche Intervention) in erster Linie als Konsequenz, dass der Fahrer Informationen nicht erhielte. Dies könnte indirekt negative Auswirkungen auf die Straßenverkehrssicherheit haben, weil zum einen die eigentliche Aufgabe, die Verbesserung der Verkehrssicherheit, nicht erfüllt würde. Zum anderen könnte es aufgrund von Verhaltensanpassungen (Gewöhnung an die Dienste), beispielsweise Warnungen vor einem herannahendem Stauende (vergleiche Kapitel 5.1), zu vermehrt kritischen Situationen und somit zu einem negativen Einfluss auf die Straßenverkehrssicherheit kommen, wenn Informationen nicht wie gewohnt zur Verfügung stünden.</p> <p>Bei einer zukünftigen automatischen, fahrzeugseitigen Intervention als Folge auf eine Meldung wäre bei der Unverfügbarkeit eines Dienstes davon auszugehen, dass auf eine lokale Rückfallebene, vermutlich also auf die Sensorik des Fahrzeuges, zurückgegriffen würde. Dies könnte zum Stillstand des Fahrzeuges, einer Verschlechterung des Verkehrsflusses oder einer Verringerung der Verkehrssicherheit führen.</p>	<p>Wenn die Integrität einer Anwendung aus dem Feld der kooperativen intelligenten Verkehrssysteme gestört wäre, könnte es zu Übermittlungen von falschen Informationen kommen. Die hierauf folgenden Reaktionen (menschliche oder automatisierte fahrzeugseitige Intervention) könnten die Sicherheit gefährden. Beispielsweise könnten abrupte Bremsungen aufgrund von Falschwarnungen zu Auffahrunfällen führen.</p> <p>Denkbar wäre zudem, dass Anwendungen aus dem Feld der ‚kooperativen intelligenten Verkehrssysteme‘ durch ihre direkte Anbindung an Fahrzeuge andere (sicherheitsrelevante) elektronische Funktionen angegriffen. Beispielsweise könnte in den Brems- oder Lenkmechanismus des Fahrzeuges eingegriffen werden. Im besten Fall erkennen Fahrzeuge solche Störungen und bleiben stehen, im schlechtesten Fall käme es dadurch zu Kontrollverlust und Unfällen.</p>

Tabelle 8: mögliche Auswirkungen von Cyberangriffen und Netzausfällen

Anwendung	Szenario 1: Dienst ist nicht verfügbar	Szenario 2: Integrität des Dienstes ist gestört
Proprietäre Datenanalyse und Warnung	Die Auswirkungen eines Ausfalls einer Anwendung aus dem Feld der proprietären Datenanalyse und Warnung ist gleich zu bewerten wie der einer Anwendung aus dem Feld der kooperativen intelligenten Verkehrssysteme, da die funktions- und wirkweise der Dienste identisch sind. Genauere Informationen können daher der entsprechenden Spalte entnommen werden.	
Daten- und Videoanalyse für Planungszwecke	Die Unverfügbarkeit eines Dienstes aus dem Bereich der ‚Daten- und Videoanalyse für Planungszwecke‘ stellte kein Risiko für die Straßenverkehrssicherheit dar. Wie bereits im Namen enthalten, wird der Dienst nur für planerische Zwecke verwendet. Er greift nicht aktiv ins Verkehrsgeschehen ein und wird nicht operativ verwendet. Bei temporärer Unverfügbarkeit könnte die Analyse zu einem späteren Zeitpunkt wiederholt werden.	Wäre die Integrität eines Dienstes aus dem Bereich der ‚Daten- und Videoanalyse für Planungszwecke‘ gestört, stellte dies kein Risiko für die Straßenverkehrssicherheit dar. Wie bereits im Namen enthalten, wird der Dienst nur für planerische Zwecke verwendet. Er greift nicht aktiv ins Verkehrsgeschehen ein und wird nicht operativ verwendet. Die Ergebnisse der Analyse müssen in stadt- und verkehrsplanerischen Konzepten umgesetzt werden, bevor sie in der Realität zum Einsatz kommen. Es ist davon auszugehen, dass die Ergebnisse in diesem Vorprozess kritisch hinterfragt werden und falsche Ergebnisse aufgedeckt werden.

Tabelle 8: mögliche Auswirkungen von Cyberangriffen und Netzausfällen

Anwendung	Szenario 1: Dienst ist nicht verfügbar	Szenario 2: Integrität des Dienstes ist gestört
<p>Daten- und Videoanalyse für operative Zwecke</p>	<p>Sollten Anwendungen aus dem Bereich ‚Daten- und Videoanalyse für operative Zwecke‘ nicht verfügbar sein, könnte der positive Effekt auf die Straßenverkehrssicherheit nicht ausgeschöpft werden. Abgesehen hiervon ist nicht mit Einflüssen auf die Straßenverkehrssicherheit zu rechnen, da solche Dienste im Regelfall nur als zusätzliche Informationsquellen verwendet werden.</p>	<p>Wäre die Integrität eines Dienstes aus dem Bereich der ‚Daten- und Videoanalyse für operative Zwecke‘ gestört, könnte es zu Falschmeldungen kommen. Der positive Effekt der Anwendung auf die Straßenverkehrssicherheit könnte nicht ausgeschöpft werden. Zudem könnten Handlungen eingeleitet werden, die indirekte negative Auswirkungen haben können. Beispielsweise könnte von der Anwendung fälschlicherweise ein Unfall gemeldet werden, weshalb Einsatzfahrzeuge unnötig zum vermeintlichen Unfallort geschickt würden. Auf dem Weg dorthin stellten sie aufgrund ihrer erhöhten Geschwindigkeiten sowie der Rotlichtüberquerung von Knotenpunkten ein Risiko für die Straßenverkehrssicherheit dar. Insgesamt ist davon auszugehen, dass die negativen Auswirkungen auf die Sicherheit gering wären.</p>

Tabelle 8: mögliche Auswirkungen von Cyberangriffen und Netzausfällen

Anwendung	Szenario 1: Dienst ist nicht verfügbar	Szenario 2: Integrität des Dienstes ist gestört
<p>Community-getriebene Smartphone-Anwendungen</p>	<p>Die Unverfügbarkeit einer ‚community-getriebenen Smartphone-Anwendung‘ wird als nicht kritisch für die Straßenverkehrssicherheit eingestuft, da die Dienste den Anwendern lediglich als Hilfsmittel dienen. Ähnlich wie bei den Anwendungen aus dem Feld der ‚kooperativen intelligenten Verkehrssysteme‘ könnte es aufgrund der Gewöhnung an die Dienste, beispielsweise Warnungen vor einem herannahenden Stauende (vergleiche Kapitel 5.1), zu vermehrt kritischen Situationen und somit einem negativen Einfluss auf die Straßenverkehrssicherheit kommen, wenn Informationen nicht wie gewohnt zur Verfügung ständen. Da nicht davon ausgegangen wird, dass ‚community-getriebene Smartphone-Anwendungen‘ aktiv in die Fahrzeugsteuerung eingreifen, können Risiken, die in diesem Bereich entstehen, ausgeschlossen werden.</p>	<p>Wenn die Integrität einer ‚community-getriebenen Smartphone-Anwendung‘ gestört wäre, könnte es zu Übermittlungen von falschen Informationen kommen. Die hierauf folgenden Reaktionen könnten die Sicherheit gefährden. Beispielsweise könnten abrupte Bremsungen aufgrund von Falschwarnungen zu Auffahrunfällen führen. Zudem könnten ablenkende Informationen an Anwender herangetragen werden, beispielsweise ‚Bombendrohung‘ oder ‚Achtung Atomkrieg‘, die zu Irritationen bei Fahrern führten und ein Risiko darstellten. Es kann demnach ein Risiko für die Straßenverkehrssicherheit abgeleitet werden.</p>

5.4 Datenschutz

Trotz zahlreicher Sicherheitsvorkehrungen kann es bei in der Cloud gehosteten Anwendungen zu Datenpannen kommen. Daten können aktiv durch böswillige Angriffe, aber auch durch falsche Konfigurationen ungewollt abhandenkommen. Der Schaden, der hierdurch entsteht, ist in erster Linie davon abhängig, welche Daten in den Anwendungen gespeichert sind. Personenbezogene Daten sind besonders schutzwürdig.

Die Anwendungen im Bereich ‚Straßenverkehrsmanagement‘, ‚kooperative intelligente Verkehrssysteme‘, ‚Daten- und Videoanalyse für Planungszwecke‘ sowie ‚Daten- und Videoanalyse für operative Zwecke‘ speichern nur folgende personenbezogene Daten: Zugangsdaten von Nutzern sowie die im System ausgeführten Aktionen der jeweiligen Nutzer. Beispielsweise beinhaltet die Datenschutzerklärung des ‚Data for Road Safety‘ (DFRS)-Konsortiums, dass keine personenbezogenen Daten für die Erhebung, Erstellung und den Versand von sicherheitsbezogenen Informationen verwendet werden. Die benötigten Daten werden bereits anonymisiert in das ‚DFRS-Ökosystem‘ übertragen. Damit soll ausgeschlossen werden, dass es bei einem Angriff auf zugehörige Server zu einer personenbezogenen Datenpanne kommen kann. Abbildung 12 zeigt eine schematische Übersicht über den Umgang mit personenbezogenen Daten im ‚DFRS-Ökosystem‘. [120]

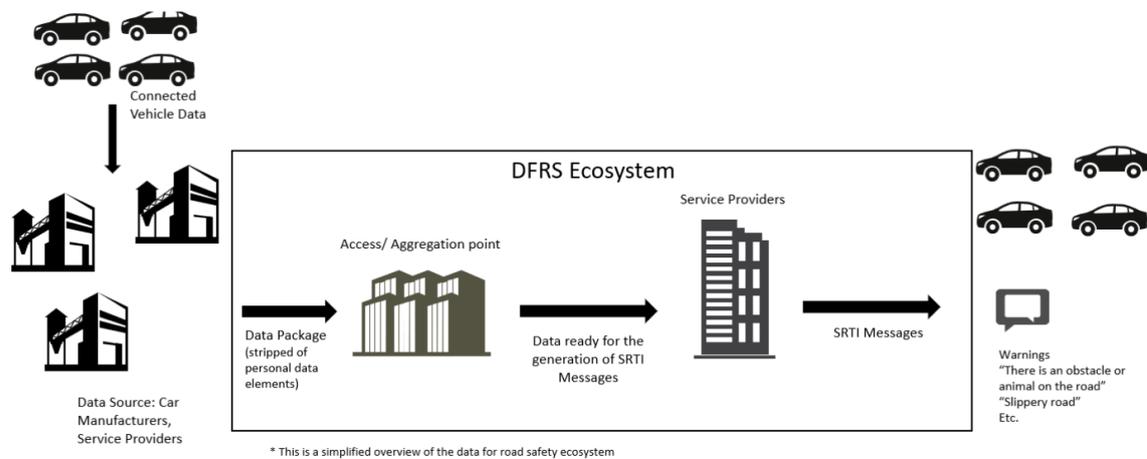


Abbildung 12: personenbezogene Daten im ‚DFRS-Ökosystem‘ [120]

Die Anwendungen im Bereich der ‚proprietären Datenanalyse und Warnung‘ sowie ‚community-getriebenen Smartphone-Anwendungen‘ bauen auf den Daten ihrer Nutzer auf. Insbesondere ist eine Positionsverfolgung der Nutzer erforderlich. Zum einen, um positionsrelevante Warnungen zu versenden und zum anderen, um Daten für die Generierung von Warnungen zu sammeln. Hier ist in der Gestaltung der Anwendung darauf zu achten, dass die Daten anonymisiert an die Anwendung übertragen und dort verarbeitet werden, um Rückschlüsse auf individuelle Personen zu verhindern. Die ‚EU-Verordnung Nr. 886/2013 zur Ergänzung der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates in Bezug auf Daten und

Verfahren für die möglichst unentgeltliche Bereitstellung eines Mindestniveaus allgemeiner für die Straßenverkehrssicherheit relevanter Verkehrsinformationen für die Nutzer‘ schreibt in Paragraf 5 folgendes vor:

„Bei der Einführung und Nutzung von IVS-Anwendungen und -Diensten werden personenbezogene Daten verarbeitet; dies sollte im Einklang mit dem Unionsrecht erfolgen, insbesondere gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (4) und der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (5). Für IVS-Anwendungen und -Dienste sollten daher die Grundsätze der Zweckbeschränkung bei der Datenerfassung und der Minimierung der Datenerhebung gelten.“ [121]

Ferner schreibt Paragraf 8 folgendes vor:

„Bei der Bereitstellung der für die Straßenverkehrssicherheit relevanten Verkehrsdaten sollten Datenschutzanforderungen eingehalten werden (z. B. Anonymisierung personenbezogener Daten). Wenn für den Informationsdienst künftig Daten wie z. B. Standortdaten, bei den Endnutzern selbst oder über Kooperationssysteme erhoben werden sollen, dann sollten die Endnutzer klar über die Erhebung dieser Daten, die Mittel der Datenerhebung und einer möglichen Nachverfolgung sowie über den Zeitraum der Datenspeicherung informiert werden. Öffentliche und/oder private Straßenbetreiber, Dienstleister und die Automobilhersteller sollten geeignete technische Maßnahmen ergreifen, um die Anonymität der von Endnutzern oder ihren Fahrzeugen übermittelten Daten zu gewährleisten.“ [121]

Systeme sollten in Bezug auf Datenschutz analog zu dem DFRS-Ökosystem, welches in Abbildung 12 dargestellt ist, aufgebaut sein. Wird dies eingehalten, können auch solche Anwendungen ohne die Speicherung oder Verwendung von kritischen personenbezogenen Daten verwendet werden. Die Umsetzung obliegt dabei den Herstellern der verschiedenen Anwendungen. ‚Bosch‘ gibt auf seiner Webseite an, dass eine Verarbeitung der Daten anonymisiert erfolgt. [92] ‚Pioneer Corporation‘ macht zu diesem Thema keine Angaben. Bei der Verwendung der ‚Waze‘ Anwendungen sollten sich Anwender bewusst sein, dass ihre Wegedaten und auch andere personenbezogene Daten wie beispielsweise Kontaktdaten aus Adressbüchern gespeichert werden und potenziell in falsche Hände gelangen können. [122]

Insgesamt lässt sich damit für die im Rahmen dieser Arbeit untersuchten Anwendungen resümieren, dass bei dem Großteil der Anwendungen nur wenige bis keine, zumeist unkritische, personenbezogene Daten gespeichert werden. Eine Ausnahme stellt ‚Waze‘ dar. Die Straßenverkehrssicherheit wird hierdurch jedoch nicht beeinflusst.

6 Ergebnisse und Diskussion

6.1 Positiver Sicherheitseinfluss von Cloud-Anwendungen

6.1.1 Übersicht

Tabelle 9 zeigt eine Übersicht über die Sicherheitspotenziale der in Kapitel 4 untersuchten Anwendungen. Die hier dargestellten und diskutierten Ergebnisse beziehen sich auf Industriestaaten mit einem ähnlichen Verkehrsablauf und ähnlichen Verkehrsstatistiken wie Deutschland. In Schwellen- und Industrieländern fallen die Potenziale unter Umständen anders aus. Zum einen sind die Straßenfahrzeuge in solchen Ländern meist in einem schlechteren Zustand, zum anderen gelten häufig andere Straßenverkehrsregeln oder diese werden nicht befolgt. Denkbar ist zum Beispiel, dass Smartphone-Anwendungen, welche auf regelwidriges Verhalten hinweisen, einen positiven Einfluss haben könnten oder, dass es Anwendungen gibt, welche mittels Videoanalyse den Zustand von Fahrzeugen analysieren können und aufzeigen, wann dringende Reparaturmaßnahmen durchzuführen sind. In diesem Kontext ergibt sich weiterer Forschungsbedarf.

Tabelle 9: Übersicht der positiven Auswirkungen auf die Verkehrssicherheit

Anwendung	Einfluss auf Unfallzahlen	Einfluss auf Verletzte	Einfluss auf Verkehrstote
Straßenverkehrsmanagement			
Cloudhosting herkömmlicher Funktionalitäten	kein Einfluss	kein Einfluss	kein Einfluss
Kooperative intelligente Verkehrssysteme			
Einsatzfahrzeugwarnung	-	- 0,9 %	- 0,9 %
Knotenpunktkollisionswarnung	- 6 %	- 6,9 %	- 3,7 %
Falschfahrerwarnung	- 0,0009 %	-	- 0,1 %
Warnung stehendes Fahrzeug	- 0,11 %	- 0,7 %	- 1,2 %
Verkehrssituationswarnung	-	- 2,1 %	- 1,5 %
Warnung Rotlichtverstoß	-	- 1,1 %	- 0,8 %
Baustellenwarnung	- 0,67 %	- 2,0 %	- 2,5 %
dezentralisierte Floating-Car-Daten	-	- 3,1 %	- 4,2 %
Warnung ungeschützte Verkehrsteilnehmer	- 3,1 %	- 4,3 %	- 3 %
behördliche/kontextbezogene Geschwindigkeitsbeschränkungen	-	- 8,9 %	- 14,9 %
Kurvenwarnung	- 7 %	-	-
LSA-Geschwindigkeitsempfehlung	-	- 0,2 %	- 0,1 %
Schilder im Fahrzeug	-	- 0,4 %	- 0,9 %
Wetterinformationen	- 4,77 %	- 4,7 %	- 6,2 %
Bahnübergang	- 0,003 %	- 0,03 %	- 0,7 %
Verminderung von Stauausbreitung	keine Daten	keine Daten	keine Daten
reduzierte Sicht	- 0,09 %	-	-
Fahrzeug-/ÖV-Priorisierung	keine Daten	keine Daten	keine Daten
Proprietäre Datenanalyse und Warnung			
siehe ‚kooperative intelligente Verkehrssysteme‘. Einfluss ist geringer, da Durchdringungsrate niemals 100 % erreichen wird aufgrund der proprietären Natur der Dienste			
Daten und Videoanalyse für Planungszwecke			
Verkehrsinfrastruktur Umgestaltung durch Beinahe-Unfalldaten	keine Daten		
Daten und Videoanalyse für operative Zwecke			
additive Verkehrsmanagementdienste für Betreiber	- 18 %	-	-
Community-getriebene Smartphone-Anwendungen			
Fahrerwarnungen	siehe ‚kooperative intelligente Verkehrssysteme‘		
additive Verkehrsmanagementdienste für Betreiber	keine Daten		

6.1.2 Kooperative intelligente Verkehrssysteme

Die Werte des prozentualen Einflusses der verschiedenen Anwendungen auf die Verkehrssicherheit in Bezug auf die Kategorie ‚kooperative intelligente Verkehrssysteme‘, werden in Kapitel 4.2 erläutert. Ebenso sind dort Verweise zur Literatur, beziehungsweise Erklärungen zur Ermittlung der Werte beschrieben. Bei zwei Anwendungsfällen aus der Kategorie ‚kooperative intelligente Verkehrssysteme‘ wurden Daten verschiedener Quellen zusammengerechnet, mit dem Ziel einen Wert zu erhalten. Im Folgenden ist die Vorgehensweise anwendungsfallsspezifisch dargestellt:

1. Warnung stehendes Fahrzeug: Das in Tabelle 9 dargestellte Gesamtergebnis für den Einfluss auf Verletzte und Verkehrstote ergibt sich aus dem Durchschnitt der im ‚DRIVE C2X‘-Projekt und der im ‚CODIA‘-Projekt ermittelten Werte.
2. Warnung ungeschützter Verkehrsteilnehmer: Das in Tabelle 9 dargestellte Gesamtergebnis für den Einfluss auf Verletzte und Verkehrstote ergibt sich aus der Addition der verschiedenen in der europäischen Studie untersuchten Anwendungen unter der Annahme, dass sich die für die Anwendungen relevanten Unfälle zu 20 % überschneiden und damit das Gesamtpotenzial nur 80 % der Summe der Einzelpotenziale entspricht.

Diese Zahlen erlauben die grundsätzliche Aussage, dass Cloud-Computing über ein positives Sicherheitspotenzial für den Straßenverkehr verfügt. Die Zahlen stammen von unterschiedlichen Quellen und sind nicht unter denselben Rahmenbedingungen erhoben worden. Ein direkter Vergleich der Zahlen, um beispielsweise die Wirksamkeit verschiedener Maßnahmen zu beurteilen, ist daher nicht möglich.

Unfälle verfügen häufig über mehrere Ursachen. Die verschiedenen Anwendungen fokussieren teilweise auf den gleichen Unfällen. Der einzelne Unfall kann aber nur einmal verhindert werden. Das Gesamtpotenzial entspricht daher nicht der Summe der Ergebnisse der verschiedenen Anwendungen. Beispielsweise könnte ein Unfall aufgrund von schlechter Sicht durch Wetterbedingungen, Schneefall, Nebel etc., durch folgende drei Anwendungen vermieden werden: ‚Wetterinformationen‘, ‚reduzierte Sicht‘ und ‚dezentralisierte Floating-Car-Daten‘. Unfälle aufgrund von überhöhten Geschwindigkeiten können mit den Anwendungen, ‚behördliche/kontextbezogene Geschwindigkeitsbeschränkungen‘, ‚Kurvenwarnung‘, ‚Verminderung von Stauausbreitung‘ verhindert werden. Zudem sind Unfälle häufig auf mehrere Unfallursachen zurückzuführen. Dies muss auch beim Interpretieren von Unfallstatistiken beachtet werden. Ein Unfall aufgrund mehrerer Ursachen ist in Realität nur ein Unfall, wird aber in der Statistik bei mehreren Ursachen aufgeführt. Beispielsweise könnte ein Überschreiten der zulässigen Höchstgeschwindigkeit in Kombination mit Eisglätte auf der Fahrbahn zu einem Unfall geführt haben. In der Realität ist dies ein Unfall, bei dem Eisglätte und Überschreiten der Höchstgeschwindigkeit als Ursachen dokumentiert wurden. Betrachtet man nur die Unfallursachen, suggeriert die Statistik, dass es zwei Unfälle gegeben habe.

Den Zahlen liegt eine menschliche Intervention im Gefahrenfall zugrunde. Menschen haben eine limitierte Informationsverarbeitungsfähigkeit. Daher wird davon ausgegangen, dass bei

einem zu hohen Informationserhalt einzelne Warnungen übersehen oder ignoriert werden. Die Wirksamkeit der Anwendungen bei gleichzeitiger Verwendung wird deshalb als geringer eingeschätzt als die einzelnen Potenziale. Die Sachlage zu diesem Punkt ändert sich, wenn die Informationen in Zukunft automatisiert von den Fahrzeugen verarbeitet werden.

Ein Aufaddieren der Einflüsse zur Bestimmung des Gesamtpotenzials wird aus den folgenden, oben erläuterten, Gründen nicht als sinnvoll erachtet:

1. Die Daten stammen aus unterschiedlichen Quellen. Die Definition der Anwendungsfälle, die Erarbeitungsmethodik sowie die zugrunde liegenden Statistiken unterscheiden sich.
2. Unfälle verfügen häufig über mehrere Ursachen.
3. Menschen können Informationen nur in einem begrenzten Umfang verarbeiten.

Den Zahlen liegt die Annahme zugrunde, dass alle Fahrzeuge und die gesamte Infrastruktur mit Technologie zum Versenden und Empfangen von C-ITS-Informationen ausgestattet sind. Dies entspricht allerdings nicht der Realität. Heutzutage ist nur ein sehr geringer Teil der Fahrzeuge und Infrastruktur mit entsprechender Technologie ausgestattet. Der positive Einfluss, insbesondere der der Anwendungen der ‚kooperativen intelligenten Verkehrssysteme‘, ist stark abhängig von dem Ausstattungsgrad. Laut ‚Car-2-Car-Communication-Konsortium‘, einem Standardisierungsgremium im Bereich vernetztes Fahren, sind erste Sicherheitseffekte bereits ab einem Ausstattungsgrad von 3 % - 5 % zu erwarten. [123] Die in Tabelle 9 dargestellten Potenziale ergeben sich dann allerdings noch nicht. Der Markt entwickelt sich bislang langsam, beispielsweise aufgrund einer mangelnden Standardisierung. Letztere ist zudem eine Gefahr für die Wirksamkeit der verschiedenen Anwendungen. Verstehen sich die Fahrzeuge untereinander bzw. die Infrastruktur aufgrund von unterschiedlichen Implementierungsverfahren oder Kommunikationstechnologien nicht, reduziert sich der Mehrwert.

Ein Beispiel hierfür ist die Verwendung eines einheitlichen Funkstandards. Aktuell gibt es den ‚IEEE 802.11p-‘ sowie den ‚LTE-V2X (PC5)-Standard‘. [123] Beide haben unterschiedliche Vor- und Nachteile. Es ist unklar, welcher Standard sich durchsetzen wird. Dies sorgt bei Automobilherstellern für Verunsicherung. Es müssen entweder beide in die Fahrzeuge implementiert werden, oder es besteht die Gefahr, den ‚falschen‘ Funkstandard ausgewählt zu haben. Dies stellt eine nicht zu unterschätzende Hürde für die Marktentwicklung dar. Solange nicht genügend Fahrzeuge und Infrastruktur ausgestattet sind, ergibt sich durch den Einbau und die Nutzung kein Mehrwert. Erfolgt die Ausstattung nicht, wird es auch nie zu der kritischen Feld-durchdringungsrate kommen.

6.1.3 Daten- und Videoanalyse für Planungszwecke

Aus den in Kapitel 4.4 aufgezeigten Anwendungen (‚Daten- und Videoanalyse für Planungszwecke‘) lässt sich ein indirekter positiver Effekt von Cloud-Computing auf die Verkehrssicherheit ableiten. Die tatsächlichen Auswirkungen sind allerdings stark abhängig von folgenden

Aspekten:

1. Verwendung der gewonnenen Erkenntnisse für die Verbesserung der Infrastruktur

Werden die Erkenntnisse nicht tatsächlich für Umplanungen verwendet und anschließend realisiert, wird sich keine Sicherheitsverbesserung zeigen.

2. zur Verfügung stehendes Budget für Infrastrukturprojekte

Stehen keine Gelder für Infrastrukturmaßnahmen zur Verfügung, kann nichts umgesetzt werden. Eine Sicherheitsverbesserung bleibt aus.

3. politische Agenda der Städte/Kommunen

Neben der Sicherheit werden politisch auch die Effizienz des Verkehrs, die Umweltbelastung, finanzielle Mittel sowie weitere Aspekte berücksichtigt. Eine sicherheitstechnisch optimale Lösung ist unter Umständen aus dem Blickwinkel von Städten und Kommunen im Gesamtkontext suboptimal. Daraus folgend könnten Lösungen umgesetzt werden, die sicherheitstechnisch nicht das volle Potenzial ausschöpfen. Beispielsweise wären eigene, von den Kraftfahrzeug-Strömen getrennte Grünphasen für Radfahrer und Fußgänger an signalisierten Knotenpunkten für deren Sicherheit erstrebenswert. Diese zusätzlichen Grünzeiten müssten bei gleichbleibender Umlaufzeit entweder den Kraftfahrzeugen weggenommen werden, oder die Umlaufzeit müsste verlängert werden. In beiden Fällen sänke die Leistungsfähigkeit des Knotenpunktes, da den Kraftfahrzeugen weniger Grünzeit zur Verfügung stände. Auch entstünden durch die längeren Wartezeiten der Fahrzeuge an den LSA zusätzliche Emissionen im Stadtgebiet.

In manchen Städten hat ein politisches Umdenken angefangen. Sie verändern ihre LSA-Steuerung zum Vorteil für Fußgänger. London beispielsweise startete einen neunmonatigen Versuch, bei dem 18 signalisierte Knotenpunkte standardmäßig Grün für Fußgänger anzeigen. Erst bei einem herannahenden Fahrzeug wird die Grünphase für Fußgänger unterbrochen. [124]

6.1.4 Daten- und Videoanalyse für operative Zwecke

Die in Kapitel 4.5 (Anwendungen der Kategorie ‚Daten- und Videoanalyse für operative Zwecke‘) dargestellten Potenziale lassen sich nur ausschöpfen, wenn auf die Erkenntnisse der durch Cloud-Computing gewonnen Anwendungen auch entsprechende Handlungen erfolgen. Die Anwendungen müssen den Verkehrsoperatoren oder anderen relevanten Akteuren zur Verfügung stehen. Die Empfehlungen der Anwendungen müssen durch die Anwender umgesetzt sein. Da die Anwendungen dieser Kategorie nicht steuernd in den Verkehr eingreifen können, ist ihre Wirksamkeit abhängig von der Maßnahmenimplementierung des zuständigen Anwenders.

6.2 Latenz in der Datenübertragung

Die Verzögerung bei der Übertragung von Datenpaketen zwischen Sender und Empfänger nennt man Latenz. Sie ist ein maßgebliches Kriterium für die Qualität einer Kommunikationsverbindung und insbesondere für Echtzeitanwendungen von großer Bedeutung. Da die Datenübertragung im Internet, wie in Abbildung 1 (Seite 24) dargestellt, eine zentrale Komponente des Cloud-Computing ist, stellen Latenzen eine Herausforderung dar.

Bei den in dieser Arbeit untersuchten Anwendungen ist die Latenz vor allem für die Kategorien ‚kooperativen intelligenten Verkehrssysteme‘, ‚proprietäre Datenanalyse und Warnung‘ sowie ‚community-getriebene Smartphone-Anwendungen‘ von Bedeutung. Erreicht eine Warnung den Fahrer aufgrund einer sehr hohen Latenz erst nach dem Eintreten der kritischen Situation, verliert die Information ihren Mehrwert. Sie kann im schlimmsten Fall ablenken und dadurch kritische Situationen hervorrufen. Die in Tabelle 9 zusammengefassten positiven Einflüsse auf die Straßenverkehrssicherheit dieser Anwendungen sind im Kontext einer großen Latenz in Frage zu stellen.

Tabelle 10: zurückgelegter Weg während Latenzzeit

Latenz [ms]	Geschwindigkeit [km/h]	zurückgelegter Weg während Latenzzeit [m]
1	200	0,06
	130	0,04
	90	0,03
	50	0,01
	30	0,01
30	200	1,67
	130	1,08
	90	0,75
	50	0,42
	30	0,25
250	200	13,89
	130	9,03
	90	6,25
	50	3,47
	30	2,08

Die Latenzzeiten sind abhängig von der Strecke, die die Nachricht zurücklegen muss, der Topographie der Erde in diesem Bereich sowie von der Verfügbarkeit und dem Ausstattungsgrad von Telekommunikationsnetzen in der jeweiligen Region. Die typischen Latenzzeiten in LTE-Netzen liegen in der Regel zwischen 15 – 30 Millisekunden. In 5G-Netzen fallen diese deutlich niedriger aus und sollen sich im einstelligen Millisekundenbereich bewegen- idealerweise liegen sie sogar nur bei einer Millisekunde oder darunter. [125] Die Latenzzeiten bei der

WLAN-Datenübertragung für vernetzte Fahrzeuge (IEEE 802.11p) liegen bei ungefähr einer Millisekunde. [126] Die Reaktionsgeschwindigkeit des Menschen liegt im Bereich von 200 bis 300 Millisekunden. [127] Tabelle 10 stellt die zurückgelegte Wegstrecke eines Fahrzeuges bei verschiedenen Latenzzeiten und Geschwindigkeiten dar.

Aus den Werten in Tabelle 10 lässt sich ableiten, dass ein Fahrzeug bei den regulären Datenübertragungslatenzzeiten in LTE-, 5G- und WLAN-Netzen bei 130 km/h (Richtgeschwindigkeit auf deutschen Autobahnen) maximal etwas mehr als einen Meter zurücklegt. Bei einer bidirektionalen Datenübertragung (Fahrzeug sendet Position und erhält basierend hierauf eine standortspezifische Information) muss dieser Wert ungefähr verdoppelt werden. Zudem muss er noch um eine Datenverarbeitungszeit, die abhängig von den jeweiligen Anwendungen ist, vergrößert werden.

Für die meisten in dieser Arbeit untersuchten Anwendungen, stellen Latenzen in den oben genannten Bereichen damit kein Problem dar. Sollten die Latenzen jedoch größer sein, kann der Mehrwert der übertragenen Nachrichten verloren gehen, weil der Empfänger die Nachricht zu spät erhält. Eine geringe Latenz ist in jedem Fall erstrebenswert. Je dynamischer und schneller sich die Informationen verändern, die bei der jeweiligen Anwendung übertragen werden, desto anfälliger wird sie für große Latenzzeiten. Beispielsweise verändern sich die verteilten Informationen bei der Warnung vor ungeschützten Verkehrsteilnehmern sehr dynamisch. Fußgänger und Radfahrer bewegen sich kontinuierlich. Eine Baustelle oder eine Nebelbank ist im Vergleich zu einem Fußgänger oder Radfahrer statischer. Nebelbänke verändern sich im Laufe der Zeit, während eine Baustelle ihren Ort im Laufe der Zeit nicht verändert. Sie ist vorhanden oder nicht vorhanden. Geringe Latenzzeiten sind demnach für die Warnung vor Fußgängern wichtiger als für die Warnung vor Baustellen. Für alle anderen in dieser Arbeit betrachteten Anwendungen gilt das ebenso.

Der Latenz entgegenwirken könnte man mit einer Systemarchitektur, dessen zentraler Anteil vorausschauend Warnungen versendet, die mit hoher Wahrscheinlichkeit in Kürze für das Fahrzeug wichtig werden könnten. Diese Informationen müssten im Fahrzeug/Nutzerendgerät zwischenspeichert werden. Das Fahrzeug, beziehungsweise das jeweilige Endgerät, müsste mit entsprechender Rechenleistung ausgestattet werden und hätte die Aufgabe, einen Positionsabgleich vorzunehmen, die Aktualität der Warnung zu prüfen und dem Fahrer zum richtigen Zeitpunkt anzuzeigen.

Die in dieser Arbeit untersuchten Anwendungen greifen nicht automatisiert in das Fahrgeschehen ein. Sie stellen lediglich zusätzliche Informationen zur Verfügung, die im Idealfall die Sicherheit verbessern können. Anders stellt sich die Sachlage bei automatisierten Fahrzeugen dar, die auf externe Informationen in Echtzeit angewiesen sind. Die Verkehrssicherheit betreffende Anwendungen mit Echtzeitanforderungen (Latenz nahezu 0) können heutzutage durch Cloud-Computing aufgrund der Übertragungswege nicht realisiert werden. Für diese Fälle ist das sogenannte ‚Edge-Computing‘ (dezentrale Datenverarbeitung am Rand des Netzwerkes) besser geeignet und sollte bevorzugt werden. Die Fahrzeuge können in solch einem System selbst als ‚Edge-Geräte‘, Feldkomponenten mit Rechenleistung, fungieren.

6.3 Cloud-Computing und das automatisierte Fahren

Cloud-Computing stellt für das automatisierten Fahren gemäß Stufe 4 und 5 der SAE J3016-Norm (Hoch- und Vollautomatisierung) Sicherheitspotenziale aber auch -gefahren dar. Durch die höhere Zuverlässigkeit von technischen Systemen sowie die schnellere Reaktionsfähigkeit im Vergleich zum Menschen können Informationen, welche Fahrzeugen von außen zukommen, effektiver verarbeitet werden. Dadurch werden die Sicherheitspotenziale der Anwendungen aus dem Feld der ‚kooperativen intelligenten Verkehrssysteme‘ sowie der ‚proprietären Datenanalyse und Warnung‘ zunehmen. Die ‚Austroads‘ Studie kam zu folgendem Ergebnis: Die Wirksamkeit der Knotenpunktkollisionswarnung könnte signifikant verbessert werden, wenn eine auf eine Warnung folgende Intervention automatisiert vom Fahrzeug durchgeführt würde und nicht einer menschlichen Ausführung bedürfe. [104] Sicherlich ließe sich ein derartiges Potenzial auch bei anderen Anwendungen ableiten.

Zu beachten ist hierbei allerdings auch, dass automatisierte Reaktionen qualitativ sehr hochwertige und genaue Informationen benötigen, da der Mensch als Kontrollorgan wegfällt. Die Integrität der Daten muss sichergestellt sein. Außerdem muss überprüfbar sein, woher die Informationen stammen, und ob sie von einer vertrauenswürdigen Quelle versendet wurden. Eine automatisierte Reaktion des Fahrzeugs stellt hohe Anforderungen an die IT-Sicherheit. Die Cyberrisiken für den Straßenverkehr steigen und, da die IT-Sicherheit und die Zuverlässigkeit der Systeme in einem direkten Zusammenhang mit der Verkehrssicherheit stehen, ergeben sich ebenfalls Risiken für die Verkehrssicherheit. [128] [129] Zu beachten ist zudem die Latenz bei der Datenübertragung. Dies wird in Kapitel 6.2 diskutiert.

Sind die Systeme nicht hinreichend geschützt, kann es durch Manipulation und Missbrauch zu unnötigen Eingriffen in den Verkehrsablauf kommen, die die Sicherheit gefährden. Beispielsweise kann es zu (Auffahr)- Unfällen aufgrund von abrupten Brems- oder Lenkvorgängen kommen. Gelingt es Hackern mit böswilligen Absichten in kooperative intelligente Verkehrssysteme einzudringen, könnten sie die Kontrolle über automatisierte Fahrzeuge übernehmen und hiermit massiven Schaden anrichten. [128]

Bereits heutzutage sind Fahrzeuge vernetzt und kommunizieren mit zentralen Recheninstanzen, beispielsweise zur Durchführung von Software-Updates, Weitergabe von Wartungsinformationen etc. Auch in diesem Zusammenhang muss für die IT-Sicherheit Sorge getragen werden. Im Zuge des voll automatisierten Fahrens steigen diese Anforderungen nochmals. [128] Die Brisanz des Themas spiegelt sich auch in der Anzahl der Forschungsprojekte wider. Um den Gefahren entgegenzuwirken, regulieren Gesetzgeber die Cybersicherheit im Kraftfahrzeug zunehmend. Beispielsweise wurde am 9. März 2021 im Amtsblatt ein vom ‚Weltforum für die Harmonisierung von Fahrzeugvorschriften der Vereinten Nationen (WP.29)‘ entwickelter Regulierungsentwurf für Cybersicherheit und Softwareupdates im Automobilsektor auf europäischer Ebene umgesetzt. [130]

6.4 Lokale Rechenzentren

Cloud-Computing unterscheidet sich von einem lokalen Rechenzentrum in erster Linie dadurch, dass die Rechenressourcen angemietet werden (Cloud-Computing) beziehungsweise sich im Besitz des Unternehmens/der Person, die die Anwendung verwendet, befinden (lokales Rechenzentrum). Die in dieser Arbeit untersuchten Anwendungen können daher theoretisch auch alle in lokalen Rechenzentren implementiert werden. Voraussetzung hierfür ist, dass das lokale Rechenzentrum an das Internet angebunden ist und mit den verschiedenen angeschlossenen Datenquellen und -empfängern kommunizieren kann.

Demnach können die in dieser Arbeit herausgearbeiteten Einflüsse auf die Straßenverkehrssicherheit nicht ganz so einfach dem Cloud-Computing zugeschrieben werden. Cloud-Computing bietet gegenüber dem Aufbau eines eigenen lokalen Rechenzentrums allerdings gewisse Vorteile, die die Entwicklung und Bereitstellung der in dieser Arbeit dargestellten Anwendungen vereinfacht bzw. zum Teil sogar erst ermöglicht. Detaillierte Informationen können zudem Kapitel 2.1.1 entnommen werden.

- keine Anfangsinvestition in Recheninfrastruktur

Ein lokales Rechenzentrum muss, bevor irgendeine Anwendung darauf installiert werden kann, eingekauft und eingerichtet werden. Dies bedarf einer Anfangsinvestition. Insbesondere rechenintensive Anwendungen, beispielsweise bildbearbeitende Anwendungen der Kategorie ‚Daten- und Videoanalyse für operative oder Planungszwecke‘, benötigen viel Rechenleistung.

- keine Wartungsarbeiten und Betriebskosten

Ein lokales Rechenzentrum muss gewartet werden. Die Server müssen nach einer gewissen Laufzeit ausgetauscht und die Infrastruktur in einem funktionsfähigen Zustand gehalten werden. Außerdem müssen Schutzkonzepte erstellt und Maßnahmen für Cybersicherheit durchgeführt werden. Ebenfalls fallen eine Raummiete und eventuell Klimatisierungskosten für den Standort des Rechenzentrums an.

- einfache Skalierbarkeit

Bei einem lokalen Rechenzentrum muss für den Fall, dass die Leistung nach oben gesteigert werden soll, entweder ungenutzte Rechenleistung vorgehalten werden oder neue Recheninfrastruktur geschaffen und eingerichtet werden. Ersteres kostet Geld und ist eine Verschwendung von Ressourcen. Letzteres benötigt Zeit und macht das System unflexibel. Im umgekehrten Fall - die Leistung einer Anwendung soll reduziert werden - entsteht ungenutzte Recheninfrastruktur. Der Dienst wird dadurch unwirtschaftlicher.

- bezahlen nach Verbrauch

Ein lokales Rechenzentrum kostet unabhängig von der tatsächlichen Verwendung einen fixen Betrag, welcher sich aus den Anfangsinvestitionen und laufenden Kosten zusammensetzt. Rechenressourcen in der Cloud werden nach tatsächlichem Verbrauch bezahlt.

Zusammenfassend erlaubt Cloud-Computing durch die aufgelisteten Vorteile einen einfachen, risikoarmen Zugang zu Recheninfrastruktur. Innovationen können hierdurch gefördert werden. Grundsätzlich erscheint es jedoch auch möglich, dass die Anwendungen in eine lokale Recheninfrastruktur implementiert werden.

6.5 Fahrerassistenzsysteme

Neben den Cloud-Anwendungen gibt es auch andere Systeme, die das Ziel haben, die Verkehrssicherheit zu verbessern. Die Frage ist, ob sich die verschiedenen Anwendungen ergänzen, koexistieren oder sich nur eine langfristig durchsetzen wird. Besonders betrifft dies die Anwendungen der Kategorien ‚kooperative intelligente Verkehrssysteme‘, ‚proprietäre Datenanalyse und Warnung‘ sowie ‚community-getriebene Smartphone-Anwendungen‘, dessen Anwendungsfelder insbesondere auch von Fahrerassistenzsystemen abgedeckt werden. Diese bauen auf Sensorik und Datenverarbeitung im Fahrzeug auf. Beispiele hierfür sind:

- Verkehrszeichenerkennung

Mithilfe einer in der Front des Fahrzeuges eingebauten Kamera werden Verkehrszeichen am Wegesrand automatisch identifiziert, ausgelesen und dem Fahrer im Cockpit des Fahrzeuges angezeigt. Die Erkennungsrate solcher Systeme ist bei vielen Herstellern schlecht. Insbesondere bei widrigen Witterungsbedingungen oder Verschmutzung von Schildern oder Kamera kommt es zu Problemen bei der Erkennung. [131] Neben der Kamera-Erfassung gibt es auch Systeme, die einen Abgleich mit Kartenmaterial vornehmen und damit die Genauigkeit erhöhen. Um die Qualität des Dienstes für den Fahrer zu erhöhen, erscheint die Ergänzung der Fahrzeugsysteme mit den Anwendungen ‚Schilder im Fahrzeug‘ und ‚LSA-Geschwindigkeitsempfehlung‘ sinnvoll.

- Fußgängererkennung

Eine im Fahrzeug eingesetzte Sensorik, zum Beispiel Kamera, Ultraschall-, oder Radarsensoren, detektiert Fußgänger in unmittelbarer Umgebung des Fahrzeuges und warnt den Fahrer bzw. leitet eine Bremsung ein. Die eingebauten Detektoren können nur detektieren, was für sie sichtbar ist. Wird ein Fußgänger durch ein anderes Fahrzeug, einen Busch oder Häuserecken verdeckt, wird er nicht detektiert. Die ergänzende Verwendung von Fahrzeugsensorik und Informationen einer zentralen Anwendung kann die Qualität des Dienstes insgesamt verbessern. Durch die zentralen Informationen kann das Fahrzeug auch auf Hindernisse reagieren, die außerhalb des eigenen

Detektionsumfeldes liegen.

- automatische Distanzregelung (engl: ‚Adaptive Cruise Control‘)

Die automatische Distanzregelung funktioniert mittels im Fahrzeug befindlicher Sensorik und stellt durch Fahrtgeschwindigkeitsregulierung sicher, dass ein genügend großer Abstand zum vorausfahrenden Fahrzeug eingehalten wird. Dies verhindert Auffahrunfälle und könnte die Anwendung ‚Verkehrssituationswarnung‘ ersetzen. Eine Warnung vor einem Stauende ist beispielsweise nicht mehr notwendig, wenn das Fahrzeug automatisch den Abstand reguliert. Allerdings gibt es im Straßenverkehr unübersichtliche Situationen, beispielsweise ein Stauende hinter einer scharfen Kurve, welche erst sehr spät von der Fahrzeugsensorik erfasst werden können. Durch die zentralen Informationen der ‚Verkehrssituationswarnung‘-Anwendung können Fahrzeuge bzw. Fahrer auf solche Situationen aufmerksam gemacht und kritische Situationen vermieden werden. Eine geringe Latenzzeit, siehe Kapitel 6.2, ist für diesen Anwendungsfall von kritischer Bedeutung.

Zusammenfassend: Cloud-Anwendungen und Intra-Fahrzeug-Anwendungen können sich ergänzen, um die Qualität der jeweiligen Dienste zu erhöhen. Zu diesem Ergebnis kommt auch eine Studie, die den Einfluss von verschiedenen Systemen auf die Straßenverkehrssicherheit mittels Simulation untersucht und wie folgt beschreibt: Die automatische Distanzregelung des Fahrzeuges in Kombination mit externen Informationen (Vehicle-to-Vehicle-Kommunikation) führt zu einer Steigerung der Verkehrssicherheit. [19]

Zu beachten ist, dass die Unfallursachen, welche von den Anwendungen fokussiert werden, dieselben sind. Die Sicherheitspotenziale von Fahrerassistenzsystemen und Cloud-Anwendungen können daher nicht einfach addiert werden. Durch die Informationsfusionierung verschiedener Quellen, steigt die Qualität der Dienste. Ergänzen sich fahrzeugsensorikbasierte Fahrerassistenzsysteme mit Anwendungen der Kategorien ‚kooperative intelligente Verkehrssysteme‘, ‚proprietäre Datenanalyse und Warnung‘ oder ‚community-getriebene Smartphone-Applikationen‘ ist zu erwarten, dass das Potenzial für die Verkehrssicherheit zwischen den einzelnen Potenzialen und der Summe dieser Potenziale liegt.

6.6 Weiterer Forschungsbedarf

Die in dieser Dissertation gewonnenen Erkenntnisse ließen sich durch nachfolgende weitere Untersuchungen ergänzen:

1. Quantifizierung des Zusammenhangs zwischen Beinahe-Unfällen und tatsächlichen Unfällen zur genaueren Bewertung des Potenzials der Anwendungen aus der Kategorie ‚Daten- und Videoanalyse für Planungszwecke‘
2. Untersuchung der tatsächlichen Verhaltensanpassungen von Menschen bei der Verwendung der in dieser Arbeit untersuchten Anwendungen

3. Untersuchung des Sicherheitspotenzials der Anwendungen der Kategorien, welche in dieser Arbeit nicht berücksichtigt wurden, siehe Abbildung 7 (Seite 42): ‚Online-Vermittlungsdienste zur Personenbeförderung‘, ‚Standort- und Kartierungsplattformen‘, ‚Digitale Plattformen für Fahrzeug-Dienste‘, ‚Flottenmanagement‘ und ‚Mautlösungen‘
4. Untersuchung des Einflusses von Cloud-Computing auf die Verkehrssicherheit anderer Verkehrsarten, wie beispielsweise dem Schienen- oder dem Luftverkehr
5. Erstellung von Konzepten zur Gewährleistung eines hohen Cybersicherheitsschutzes, insbesondere in Hinblick auf das automatisierte Fahren
6. Untersuchung des Potenzials von Cloud-Computing für die Straßenverkehrssicherheit in Entwicklungs- und Schwellenländern
7. Untersuchung des Sicherheitspotenzials der einzelnen Anwendungen im Rahmen von standardisierten Studien zum besseren Vergleich der Ergebnisse

7 Zusammenfassung

Im Rahmen dieser Dissertation wurde der Einfluss von Cloud-Computing auf die Straßenverkehrssicherheit untersucht. Bei der Literaturrecherche konnten keine Publikationen gefunden werden, die Cloud-Computing im Zusammenhang mit der Straßenverkehrssicherheit betrachten.

Es wurden vier Forschungsfragen formuliert und untersucht. Zur Beantwortung der ersten Forschungsfrage – ‚Wo wird Cloud-Computing im Straßenverkehr aktuell angewandt?‘ - trugen Recherchen, Gespräche mit Branchenexperten, Messebesuche sowie die eigene Berufserfahrung bei. Die ermittelten Anwendungen wurden in verschiedene Kategorien gruppiert und sind in Abbildung 7 (Seite 42) dargestellt. Anwendungen folgender Kategorien wurden im Rahmen dieser Arbeit weiter untersucht:

- Straßenverkehrsmanagement
- kooperative intelligente Verkehrssysteme
- proprietäre Datenanalyse und Warnung
- Daten- und Videoanalyse für Planungszwecke
- Daten- und Videoanalyse für operative Zwecke
- community-getriebene Smartphone-Anwendungen

Zur Beantwortung der zweiten Forschungsfrage – ‚Welche Cloud-Anwendungen haben Einfluss auf die Straßenverkehrssicherheit?‘ - wurden detaillierte Analysen der einzelnen Anwendungen vorgenommen: Die meisten in dieser Dissertation näher untersuchten Anwendungen haben einen direkten oder indirekten Einfluss auf die Straßenverkehrssicherheit. Anwendungen der Kategorie ‚Straßenverkehrsmanagement‘, welche klassische Verkehrsrechner und Verkehrsmanagementfunktionalitäten in die Cloud überführen, wurde durch die Nutzung von Cloud-Computing kein zusätzlicher positiver Einfluss auf die Straßenverkehrssicherheit zugesprochen.

Die dritte Forschungsfrage – ‚Welchen Einfluss hat Cloud-Computing auf die physische Sicherheit im Straßenverkehr?‘ - wurde durch Studienergebnisse, Herstellerangaben sowie eigene Kalkulationen untersucht. Der Einfluss wurde anhand von drei Kenngrößen identifiziert:

- ‚Auswirkung auf Anzahl getöteter Personen in Prozent‘,
- ‚Auswirkung auf Anzahl verletzter Personen in Prozent‘,
- ‚Anzahl Unfälle, die vermieden werden können, in Prozent‘

Die beiden Anwendungen ‚Knotenpunktkollisionswarnung‘ und ‚behördlich/kontextbezogene Geschwindigkeitsbeschränkungen‘ haben das größte Potenzial, die Straßenverkehrs-

sicherheit positiv zu beeinflussen. Da die ermittelten Zahlen von unterschiedlichen Quellen stammen und nicht unter denselben Rahmenbedingungen erhoben wurden, ist ein direkter Vergleich, um beispielsweise die Wirksamkeit verschiedener Maßnahmen zu beurteilen, nicht möglich. Zu beachten ist außerdem, dass alle Werte eine Felddurchdringungsrate von 100 % voraussetzen, die heute noch nicht erreicht ist. Mögliche Verhaltensanpassungen, beispielsweise eine verringerte Aufmerksamkeit der Fahrer sowie die Nutzerakzeptanz, können den positiven Effekten entgegenwirken. Der tatsächliche Systemnutzen der einzelnen Anwendungen kann erst nach einer ausreichenden Felddurchdringung aus den Veränderungen in den Unfallstatistiken abgelesen werden. Der Nutzen ist nicht klar abgrenzbar von anderen Anwendungen, die ebenfalls die Straßenverkehrssicherheit verbessern, aber nicht auf Cloud-Computing basieren, wie beispielsweise einige fahrzeugsensorikbasierte Fahrerassistenzsysteme.

Die vierte und letzte Forschungsfrage – ‚Welche Gefahr stellen Cyberangriffe und Netzausfälle bei Cloud-Anwendungen für die Straßenverkehrssicherheit dar?‘ - wurde durch die Betrachtung verschiedener Extremszenarien untersucht. Die zwei möglichen Folgen ‚Dienst ist nicht verfügbar‘ und ‚Integrität des Dienstes ist gestört‘ können einen indirekten, sicherheitskritischen Einfluss auf die Verkehrssicherheit haben. Die Auswirkungen einer Störung der Integrität eines Dienstes wird dabei als potenziell gefährlicher eingeschätzt, als wenn dieser Dienst nicht verfügbar wäre. Am kritischsten werden Cyberangriffe auf Cloud-Anwendungen und Netzausfälle im Bereich der ‚kooperativen intelligenten Verkehrssysteme‘ sowie der ‚proprietären Datenanalyse und Warnung‘ eingeschätzt, sofern diese eine direkte Schnittstelle zum Fahrzeug aufweisen und nicht auf einem separaten Endgerät verwendet werden. Cyberangriffe auf Cloud-Anwendungen und Netzausfälle im Bereich ‚Daten- und Videoanalyse für Planungszwecke‘ werden als unkritisch eingeschätzt. Wird Cloud-Computing für das automatisierte Fahren verwendet, erhöht sich das Risiko für Cyberangriffe. In Bezug auf einen möglichen Datenverlust, der aufgrund eines Cyberangriffs auftreten kann, lässt sich nicht von einem negativen Einfluss auf die Straßenverkehrssicherheit ausgehen. Die in dieser Arbeit untersuchten Anwendungen speichern wenige bis keine, zumeist unkritische, personenbezogene Daten. Eine Ausnahme stellt die Anwendung ‚Waze‘, der Kategorie ‚community-getriebene Smartphone-Anwendungen‘ dar.

Als Ergebnis dieser Dissertation lässt sich zusammenfassen: Cloud-Computing ermöglicht durch den einfachen, risikoarmen Zugang zu unlimitierten Rechenressourcen die Entwicklung und den Betrieb von Anwendungen, die Einfluss auf die Verkehrssicherheit nehmen. Es ist davon auszugehen, dass die Anwendungen bei einer weiter voranschreitenden Felddurchdringungsrate positiven Einfluss auf die Straßenverkehrssicherheit in Deutschland und anderen Industriestaaten nehmen und damit aktiv zur Reduzierung der Anzahl Verkehrstoter und -verletzter beitragen werden. Cloud-Computing wird somit ein indirekt positiver Einfluss auf die Straßenverkehrssicherheit zugeschrieben.

Literaturverzeichnis

- [1] WORLD HEALTH ORGANIZATION: *Global status report on road safety 2018*. Geneva, Switzerland : World Health Organization, 2018
- [2] 2010/40/EU. *RICHTLINIE 2010/40/EU DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 7. Juli 2010 zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern*
- [3] ARUTYUNOV, V. V.: *Cloud computing: Its history of development, modern state, and future considerations*. In: *Scientific and Technical Information Processing* 39 (2012), Nr. 3, S. 173–178
- [4] JAWORSKI, Pawel ; EDWARDS, Tim ; MOORE, Jonathan ; BURNHAM, Keith: *Cloud computing concept for Intelligent Transportation Systems*. In: AUTHOR, IEEE Staff Corporate (Hrsg.): *2011 14th International IEEE Conference on Intelligent Transportation Systems* : IEEE, 2011 - 2011, S. 391–936
- [5] YANG, Zhaosheng ; MEI, Duo ; YANG, Qingfang ; ZHOU, Huxing ; LI, Xiaowen: *Traffic Flow Prediction Model for Large-Scale Road Network Based on Cloud Computing*. In: *Mathematical Problems in Engineering* 2014 (2014), S. 1–8
- [6] YU, Xi ; SUN, Fuquan ; CHENG, Xu: *Intelligent Urban Traffic Management System Based on Cloud Computing and Internet of Things*. In: *2012 International Conference on Computer Science and Service System*. [Place of publication not identified] : IEEE, 2012, S. 2169–2172
- [7] TRIVEDI, Prashant ; DESHMUKH, Kavita ; SHRIVASTAVA, Manish: *Cloud computing for intelligent transportation system*. In: *International Journal of Soft Computing and Engineering (IJSCE)* 2 (2012), Nr. 3, S. 2231–2307
- [8] JAWORSKI, Pawel: *Cloud computing based adaptive traffic control and management*. Doktorarbeit : Coventry University in collaboration with MIRA Limited, 2013
- [9] JANKOVIC, Sladana ; MILOJKOVIC, Jelena ; MLADENOVIC, Snezana ; DESPOTOVIC-ZRAKIC, Marijana ; BOGDANOVIC, Zorica: *Cloud Computing Framework for B2B Integrations in the Traffic Safety Area*. In: *Metalurgia International* 17 (2012), Nr. 9, S. 166
- [10] SHENGDONG, Mu ; ZHENGXIAN, Xiong ; YIXIANG, Tian: *Intelligent Traffic Control System Based on Cloud Computing and Big Data Mining*. In: *IEEE Transactions on Industrial Informatics* 15 (2019), Nr. 12, S. 6583–6592
- [11] ZHANG, Yongnan ; ZHOU, Yonghua: *Distributed coordination control of traffic network flow using adaptive genetic algorithm based on cloud computing*. In: *Journal of Network and Computer Applications* 119 (2018), S. 110–120
- [12] LEE, Euisin ; LEE, Eun-Kyu ; GERLA, Mario ; OH, Soon: *Vehicular cloud networking: architecture and design principles*. In: *IEEE Communications Magazine* 52 (2014), Nr. 2, S. 148–155
- [13] GOUMIDI, Hadjer ; ALIOUAT, Zibouda ; HAROUS, Saad: *Vehicular Cloud Computing Security: A Survey*. In: *Arabian Journal for Science and Engineering* 45 (2020), Nr. 4, S. 2473–2499

- [14] SKONDRAS, Emmanouil ; MICHALAS, Angelos ; VERGADOS, Dimitrios D.: *Mobility management on 5G Vehicular Cloud Computing systems*. In: *Vehicular Communications* 16 (2019), S. 15–44
- [15] SHARMA, Manish Kumar ; KAUR, Arvinder: A survey on Vehicular Cloud Computing and its security. In: *2015 1st International Conference on Next Generation Computing Technologies (NGCT)* : IEEE, uuuu-uuuu, S. 67–71
- [16] TAHMASEBI, Masoud ; KHAYYAMBASHI, Mohammad Reza: *An efficient model for vehicular cloud computing with prioritizing computing resources*. In: *Peer-to-Peer Networking and Applications* 12 (2019), Nr. 5, S. 1466–1475
- [17] AHMAD, Iftikhar ; NOOR, Rafidah M. D. ; ALI, Ihsan ; QURESHI, Muhammad Ahsan: The Role of Vehicular Cloud Computing in Road Traffic Management: A Survey, Bd. 185. In: FERREIRA, Joaquim; ALAM, Muhammad (Hrsg.): *Future Intelligent Vehicular Technologies*. Cham : Springer International Publishing, 2017 (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering), S. 123–131
- [18] LOUWERSE, W.J.R. ; HOOGENDOORN, S. P.: ADAS safety impacts on rural and urban highways. In: *2004 IEEE intelligent vehicles symposium : Parma, Italy, June 14-17, 2004*. Piscataway NJ : IEEE, 2004, S. 887–890
- [19] VALIDI, Aso ; LUDWIG, Thomas ; HUSSEIN, Ahmed ; OLAVERRI-MONREAL, Cristina: *Examining the Impact on Road Safety of Different Penetration Rates of Vehicle-to-Vehicle Communication and Adaptive Cruise Control*. In: *IEEE Intelligent Transportation Systems Magazine* 10 (2018), Nr. 4, S. 24–34
- [20] VAA, T. ; PENTTINEN, M. ; SPYROPOULOU, I.: *Intelligent transport systems and effects on road traffic accidents: state of the art*. In: *IET Intelligent Transport Systems* 1 (2007), Nr. 2, S. 81
- [21] MAI, Marcus: *Fahrerverhaltensmodellierung für die prospektive, stochastische Wirksamkeitsbewertung von Fahrerassistenzsystemen der Aktiven Fahrzeugsicherheit*. Doktorarbeit. 1st ed. Göttingen : Cuvillier Verlag, 2017 (Schriftenreihe des Lehrstuhls Kraftfahrzeugtechnik v. 4)
- [22] MICHON, John A.: A Critical View of Driver Behavior Models: What Do We Know, What Should We Do? In: EVANS, Leonard; SCHWING, Richard C. (Hrsg.): *Human Behavior and Traffic Safety*. N. Boston : Springer US, 1986, S. 485–524
- [23] SILLA, Anne ; RÄMÄ, Pirkko ; LEDEN, Lars ; NOORT, Martijn ; KRUIJFF, Janiek ; BELL, Daniel ; MORRIS, Andrew ; HANCOX, Graham ; SCHOLLIERS, Johan: *Quantifying the effectiveness of ITS in improving safety of VRUs*. In: *IET Intelligent Transport Systems* 11 (2017), Nr. 3, S. 164–172
- [24] KULMALA, Risto: *Ex-ante assessment of the safety effects of intelligent transport systems*. In: *Accident Analysis and Prevention* 42 (2010), Nr. 4, S. 1359–1369
- [25] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *Cloud Computing Grundlagen*. URL https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Grundlagen/grundlagen_node.html – Überprüfungsdatum 2021-11-13
- [26] LUBER, Stefan: *Was ist Virtualisierung?* URL <https://www.cloudcomputing-insider.de/was-ist-virtualisierung-a-756279/>. – Aktualisierungsdatum: 2018-09-21 – Überprüfungsdatum 2022-09-26

- [27] MELL, Peter ; GRANCE, Timothy: *The NIST Definition of Cloud Computing : Recommendations of the National Institute of Standards and Technology*. NIST Special Publication 800-145
- [28] ELEKTRONIK-KOMPENDIUM.DE: *Cloud Computing*. URL <https://www.elektronik-kompodium.de/sites/com/1404051.htm> – Überprüfungsdatum 2021-11-14
- [29] BUNDESAMT FÜR SICHERHEIT IN DER KOMMUNIKATIONSTECHNIK: *IT-Grundschutz-Kompodium*
- [30] TÜV SÜD: *ISO/IEC 27001 - ISMS-Zertifizierung*. URL <https://www.tuvsud.com/de-de/dienstleistungen/auditierung-und-zertifizierung/cyber-security-zertifizierung/iso-27001> – Überprüfungsdatum 2022-01-08
- [31] ISO/IEC 27002:2013. 10-2013. *Information technology — Security techniques — Code of practice for information security controls*
- [32] TÜV SÜD: *ISO/IEC 27017 - ISMS-ZERTIFIZIERUNG*. URL <https://www.tuvsud.com/de-de/dienstleistungen/auditierung-und-zertifizierung/cyber-security-zertifizierung/cloud-zertifizierung-iso-27017> – Überprüfungsdatum 2022-01-08
- [33] TÜV SÜD: *ISO/IEC 27018 - ISMS-Zertifizierung*. URL <https://www.tuvsud.com/de-de/dienstleistungen/auditierung-und-zertifizierung/cyber-security-zertifizierung/cloud-zertifizierung-iso-27018> – Überprüfungsdatum 2022-01-08
- [34] Oktober 2020. *Cloud Computing Compliance Criteria Catalogue – C5:2020*
- [35] NAFEA, Roaa Al ; AMIN ALMAIAH, Mohammed: Cyber Security Threats in Cloud: Literature Review. In: *2021 International Conference on Information Technology (ICIT)* : IEEE, 2021, S. 779–786
- [36] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *Sichere Nutzung von Cloud Diensten : Schritt für Schritt von der Strategie bis zum Vertragsende*
- [37] SENATSVERWALTUNG FÜR UMWELT, VERKEHR UND KLIMASCHUTZ: *Berliner Mobilitätsgesetz (MobG)* (04/2021)
- [38] *RICHTLINIE 2008/96/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 19. November 2008 über ein Sicherheitsmanagement für die Straßenverkehrsinfrastruktur : Geändert durch: Richtlinie (EU) 2019/1936 des Europäischen Parlaments und des Rates vom 23. Oktober 2019*. In: *Amtsblatt der Europäischen Gemeinschaft* (2008), L 319, S. 59. URL <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L1936>
- [39] TIEFBAU- UND VERKEHRSAMT ERFURT, ABTEILUNG VERKEHR: *Technische Anforderungen an Lichtsignalanlagen des Tiefbau- und Verkehrsamtes Erfurt : Forderungen zur Planung und Errichtung von Lichtsignalanlagen, in Trägerschaft der Stadt Erfurt* (2014-01-29)
- [40] BUNDESMINISTERIUM FÜR DIGITALE UND VERKEHR: *Neue Fahrzeugsicherheitssysteme*. URL <https://www.bmvi.de/SharedDocs/DE/Artikel/StV/Strassenverkehr/neue-fahrzeugsicherheitssysteme.html>. – Aktualisierungsdatum: 2022-02-09 – Überprüfungsdatum 2022-05-07
- [41] VOLKSWAGEN FINANCIAL SERVICES: *Aktiv & passiv: Sicherheitssysteme im Auto | fortynine*. URL <https://www.vwfs.de/magazin/auto-und-mobilitaet/sicherheitssysteme-auto.html>. – Aktualisierungsdatum: 2021-12-31 – Überprüfungsdatum 2022-05-07
- [42] KRAMER, Florian: Die integrale Sicherheit. In: FRANZ, Ulrich; LORENZ, Bernd; REMFREY, James; SCHÖNEBURG, Rodolfo; KRAMER, Florian (Hrsg.): *Integrale Sicherheit von Kraftfahrzeugen*. Wiesbaden : Springer Fachmedien Wiesbaden, 2013, S. 1–9

- [43] STATISTISCHES BUNDESAMT: *Verkehrsunfälle : Kraftrad- und Fahrradunfälle im Straßenverkehr 2020*. – Aktualisierungsdatum: 2021-08-05
- [44] MINISTERIUM DES INNERN DES LANDES NORDRHEIN-WESTFALEN: *Unfallhäufungsstellen erkennen – mit EUSKa*. URL <https://polizei.nrw/artikel/unfallhaeuftungsstellen-erkennen-mit-euska>. – Aktualisierungsdatum: 2020-06-12 – Überprüfungsdatum 2022-10-21
- [45] UNFALLFORSCHER DER VERKEHRSSICHERER: *Verkehrssicherheits-Management : Unfallkommission*. URL <https://www.udv.de/udv/themen/unfallkommission-75644>. – Aktualisierungsdatum: 06.01.207 – Überprüfungsdatum 2022-09-15
- [46] WIKIPEDIA: *Datei:Unfalltypenkarte.png – Wikipedia*. URL <https://de.m.wikipedia.org/wiki/Datei:Unfalltypenkarte.png> – Überprüfungsdatum 2022-07-31
- [47] STATISTISCHES BUNDESAMT: *Verkehrsunfälle in Deutschland*. URL https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Verkehrsunfaelle/_inhalt.html;jsessionid=965FCF6EE39E438D2F119A57BA8BA1E3.live712#sprg475750. – Aktualisierungsdatum: 2019-08-22 – Überprüfungsdatum 2022-05-08
- [48] STATISTISCHES BUNDESAMT: *Unfallbilanz 2021: 150 Verkehrstote weniger als im Vorjahr*. URL https://www.destatis.de/DE/Presse/Pressemitteilungen/2022/02/PD22_076_46241.html;jsessionid=965FCF6EE39E438D2F119A57BA8BA1E3.live712. – Aktualisierungsdatum: 2022-02-25 – Überprüfungsdatum 2022-05-08
- [49] EUROPÄISCHES PARLAMENT: *Verkehrsunfallstatistiken in der EU (Infografik)*. URL <https://www.europarl.europa.eu/news/de/headlines/society/20190410STO36615/verkehrsunfallstatistiken-in-der-eu-infografik>. – Aktualisierungsdatum: 2021-10-06 – Überprüfungsdatum 2022-05-08
- [50] STATISTA: *Verkehrstote in Europa 2021 | Statista*. URL <https://de.statista.com/statistik/daten/studie/30164/umfrage/verkehrstote-in-europa/>. – Aktualisierungsdatum: 2022-08-19 – Überprüfungsdatum 2022-08-19
- [51] ISO 26262:2018. 12-2018. *Road vehicles — Functional safety*
- [52] MACHER, Georg ; SCHMITTNER, Christoph ; VELEDAR, Omar ; BRENNER, Eugen: ISO/SAE DIS 21434 Automotive Cybersecurity Standard - In a Nutshell, Bd. 12235. In: CASIMIRO, António; ORTMEIER, Frank; SCHOITSCH, Erwin; BITSCH, Friedemann; FERREIRA, Pedro (Hrsg.): *Computer Safety, Reliability, and Security. SAFECOMP 2020 Workshops*. Cham : Springer International Publishing, 2020 (Lecture Notes in Computer Science), S. 123–135
- [53] EUROPÄISCHE UNION: *UN-Regelung Nr. 155 — Einheitliche Bedingungen für die Genehmigung von Fahrzeugen hinsichtlich der Cybersicherheit und des Cybersicherheitsmanagementsystems [2021/387]* (in Kraft getr. am 22. 1. 2021) (2021-01-22)
- [54] VDE VERLAG: *DIN VDE V 0832-700 VDE V 0832-700:2019-03 : Straßenverkehrs-Signalanlagen. Teil 700: Branchenspezifischer Sicherheitsstandard (B3S) für Verkehrssteuerungs- und Leitsysteme im kommunalen Straßenverkehr*. URL <https://www.vde-verlag.de/normen/0800549/din-vde-v-0832-700-vde-v-0832-700-2019-03.html> – Überprüfungsdatum 2021-01-01
- [55] BUNDESANSTALT FÜR STRAßENWESEN: *Volkswirtschaftliche Kosten von Straßenverkehrsunfällen in Deutschland*. Bergisch Gladbach, November 2021

- [56] STATISTISCHES BUNDESAMT: *Verkehrsunfälle : Zeitreihen 2020*. Bergisch Gladbach, 07. Juli 2021
- [57] STATISTISCHES BUNDESAMT: *Verkehrsunfälle : Unfälle unter dem Einfluss von Alkohol oder anderen berauschenden Mitteln im Straßenverkehr 2020*. Bergisch Gladbach, 07.12.2021
- [58] FROMMEYER, Lena: *Tag der Verkehrssicherheit: Das sind die größten Risiken im Straßenverkehr*. In: *DER SPIEGEL* (2020-06-20)
- [59] BUBB, Heiner: *Menschliche Zuverlässigkeit - Ergonomische Anforderungen und Methoden der Bewertung : VDI 4006 Blatt 1 und 2*. Technische Universität München. Januar 2002
- [60] SWARCO: *Swarco MyCity : Urban Mobility Management*. URL <https://www.swarco.com/de/produkte/software/urbanes-verkehrsmanagement/swarco-mycity> – Überprüfungsdatum 2022-01-22
- [61] SWARCO: *OMNIA : Verkehrsmanagement-Plattform*. URL <https://www.swarco.com/de/produkte/software/urbanes-verkehrsmanagement/omnia>
- [62] YUNEX TRAFFIC: *Verkehrsmanagement der nächsten Generation - Sitraffic Symphony / Yunex Traffic*. URL <https://www.yunextraffic.com/global/de/portfolio/verkehrsmanagement/verkehrs-zentralen/next-generation-traffic-management>. – Aktualisierungsdatum: 2022-07-31 – Überprüfungsdatum 2022-07-31
- [63] PARSONS CORPORATION: *Smart Mobility Platform | iNET™* -. URL <https://www.parsons.com/products/inet/>. – Aktualisierungsdatum: 2022-07-27 – Überprüfungsdatum 2022-07-31
- [64] ECONOLITE: *Systems Software*. URL <https://www.econolite.com/solutions/systems/software/> – Überprüfungsdatum 2022-01-29
- [65] Q-FREE: *Product Sheet OPENTMS*
- [66] Q-FREE: *Kinetic Mobility*. URL <https://www.q-free.com/product/kinetic-mobility/> – Überprüfungsdatum 2022-01-30
- [67] CUBIC: *Transport Management Platform* – Überprüfungsdatum 2022-01-30
- [68] NOTRAFFIC: *Our Technology : How it works*. URL <https://notraffic.tech/how-it-works/> – Überprüfungsdatum 2022-04-24
- [69] FROST, Adam: *Q-Free to deploy its cloud-based ATMS platform in Iowa*. URL <https://www.traffictoday.com/news/traffic-management/q-free-to-deploy-its-cloud-based-atms-platform-in-iowa.html>. – Aktualisierungsdatum: 2019-05-24 – Überprüfungsdatum 2022-02-06
- [70] VIRGINIA DEPARTMENT OF TRANSPORTATION: *REQUEST FOR PROPOSAL 156859-RFP : Project Name: Artificial Intelligence-Based Decision Support System (AI-DSS) for Enhancing Transportation Incident Management*
- [71] CHATTANOOGA DEPARTMENT OF TRANSPORTATION: *Request for Qualifications : Software Development, Deployment, and Integration for TDOT PIN 114321.01 Federal Project No. CM-9202(118) State Project No. 33LPLM-F1-138 City Contract Number T-16-006 Chattanooga Advanced Transportation Management System*. December 2020

- [72] SCOTT COUNTY HIGHWAY DEPARTMENT: *Request for Proposal to Provide an Advanced Traffic Management System for Scott County*
- [73] WISSENSCHAFTSSTADT DARMSTADT, Mobilitätsamt: *DAnalytics Umweltsensitives Verkehrsmanagement - Komponente Ampelphasenassistent Referenznummer der Bekanntmachung: RITT-2021-0004*. URL [https://ausschreibungen-deutschland.de/852714_DAnalytics_Umweltsensitives_Verkehrsmanagement_-_Komponente_AmpelphasenassistentReferenznummer_2021_Darmstadt_-Aktualisierungsdatum: 2021-11-24 – Überprüfungsdatum 2022-02-13](https://ausschreibungen-deutschland.de/852714_DAnalytics_Umweltsensitives_Verkehrsmanagement_-_Komponente_AmpelphasenassistentReferenznummer_2021_Darmstadt_-Aktualisierungsdatum:2021-11-24-Überprüfungsdatum2022-02-13)
- [74] LANDESHAUPTSTADT STUTTGART, HAUPT- UND PERSONALAMT: *Verkehrsflussoptimierung Referenznummer der Bekanntmachung: 2020-054-App-O-EU*. URL [https://ausschreibungen-deutschland.de/652890_VerkehrsflussoptimierungReferenznummer_der_Bekanntmachung_2020-054-App-O-EU_2020_Stuttgart_-Aktualisierungsdatum: 2020-05-14 – Überprüfungsdatum 2022-02-13](https://ausschreibungen-deutschland.de/652890_VerkehrsflussoptimierungReferenznummer_der_Bekanntmachung_2020-054-App-O-EU_2020_Stuttgart_-Aktualisierungsdatum:2020-05-14-Überprüfungsdatum2022-02-13)
- [75] BUNDESANSTALT FÜR STRAßENWESEN: *Kooperative Intelligente Verkehrssysteme – C-ITS*. URL <https://www.bast.de/Forschungsplanung/DE/Mobilitaet/Beitr%C3%A4ge/C-ITS.html> – Überprüfungsdatum 2022-02-13
- [76] Technical Specification ETSI TR 102 638. 2009-06. *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions*
- [77] AUSTRIATECH: *The following Day 1-services are in the focus of the C-Roads platform*. URL <https://www.c-roads.eu/pilots/implemented-services.html> – Überprüfungsdatum 2022-03-13
- [78] ITS INTERNATIONAL: *SNCF uses ITS to make crossings safer*. URL [https://www.itsinternational.com/its2/its4/its5/its7/feature/sncf-uses-its-make-crossings-safer_-Aktualisierungsdatum: 2021-05-19 – Überprüfungsdatum 2022-05-24](https://www.itsinternational.com/its2/its4/its5/its7/feature/sncf-uses-its-make-crossings-safer_-Aktualisierungsdatum:2021-05-19-Überprüfungsdatum2022-05-24)
- [79] Technical Specification ETSI TS 102 940. 2021-07. *Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management; Release 2*
- [80] BÖHM, Martin ; FALCO, Francesco ; FICKEL, Frank ; KHESRAVI, Ariana: *Mehr Sicherheit auf Europas Straßen durch C-ITS : Pressemitteilung*. URL <https://its-mobility.de/mehr-sicherheit-auf-europas-strassen-durch-c-its/> – Überprüfungsdatum 2022-02-27
- [81] PARTNERSHIP TALKING TRAFFIC: *Talking Traffic : The partnership*. URL <https://www.talking-traffic.com/en/talking-traffic/the-partnership> – Überprüfungsdatum 2022-04-13
- [82] PARTNERSHIP TALKING TRAFFIC: *What if traffic regulates traffic? : How the Dutch government and business community join forces to enhance everyday traffic*. URL <https://www.talking-traffic.com/images/Documenten/TT-Brochure.pdf> – Überprüfungsdatum 2022-04-13
- [83] GOVERNMENT OF FLANDERS: *Mobilidata creates innovative traffic solutions that help make traffic flow more smoothly, more sustainably and more safely for every road user*. URL <https://mobilidata.be/en/about-mobilidata> – Überprüfungsdatum 2022-04-13
- [84] JACQUES, Anna Johansson: *About NordicWay*. URL <https://www.nordicway.net/previousprojects> – Überprüfungsdatum 2022-04-13
- [85] KULMALA, Risto: *Cloud-to-cloud vehicle connectivity improves road safety*

- [86] JACQUES, Anna Johansson: *NordicWay*. URL <https://www.nordicway.net/> – Überprüfungsdatum 2022-04-13
- [87] JACQUES, Anna Johansson: *Services*. URL <https://www.nordicway.net/services> – Überprüfungsdatum 2022-04-13
- [88] PARTNERS SAFETY RELATED TRAFFIC INFORMATION ECOSYSTEM: *Safety Related Traffic Information Ecosystem: Data for Road Safety*. In: *Partners Safety Related Traffic Information Ecosystem* (2018-03-06)
- [89] PARTNERS SAFETY RELATED TRAFFIC INFORMATION ECOSYSTEM: *Proof of Concept*. In: *Partners Safety Related Traffic Information Ecosystem* (2020-10-02)
- [90] PIONEER CORPORATION: *Pioneer builds a map-based accident prediction platform and Intelligent Pilot, an ADAS solution for on-the-road cars*. – Aktualisierungsdatum: 2016-11-25
- [91] NOTRAFFIC: *Future of Mobility : Digitizing Infrastructure*. URL <https://notraffic.tech/future-of-mobility/> – Überprüfungsdatum 2022-04-24
- [92] ROBERT BOSCH GMBH: *Cloudbasierte Falschfahrerwarnung*. URL <https://www.bosch-mobility-solutions.com/de/loesungen/assistentensysteme/cloud-basierte-falschfahrerwarnung/>. – Aktualisierungsdatum: 2022-05-20 – Überprüfungsdatum 2022-05-27
- [93] MICHELIN: *How Near Misses Can Help Prevent Car Crashes : A White Paper by Michelin DDi*. URL https://ccbghib.r.af.d.sendibt2.com/tr/cl/c4u0yH4stqm2e1b87oFxAJedp3CrErQNYbDRyIeILh22xXdoGzP6BnRkWZASsd4Opkl-Z1Tpj_eFkcwjDNfPiQcwU-KmOQRUZ-QlsYcXd6W9_WTvf-IBKRR5UveLBNh_UmjJwOsrilEtAWhx6dmU4U9SJYiIwmaIAquVki5Uh8yQpK9DZGC13aEcHr6I2Y03Y5GIMGOwhlQvsQbzjqXxCzq9iTBYGcML9BCKs9zfXw1z7EGRzHu_Kf2EGOv8o4GFcWxK9Y06i1Dqilxz5Ll42GMKV0oRwE_PBGyBoOsQIISIdOeh3JyzPggRBFPy99rU_NldG29weTLUOqvR6z0-7ACxN22DeKrdItQCdZY7qCJNfuBgDTn9SORvr8Do1FEmvcyauNLgGxFPXugnovusZ4Wa39TcMverwFr46gdgJO84HpWt0WYJIV4Pic2rDi86QRG2ewCt74Yixtbg – Überprüfungsdatum 2022-08-20
- [94] BUDNICK, Noah ; TOGETHER FOR SAFER ROADS ; LOEWENHERZ, Franz ; BELLEVUE (WA) TRANSPORTATION DEPARTMENT ; SHAH, Hardik ; AMERICAN STRUCTUREPOINT, INC. ; VICE-CHAIR OF ITE CONSULTANTS COUNCIL: *Making the Invisible Visible – Conflict Data Analytics for Vision Zero, A Thought Leadership Report by the Council Leadership Team 2021 Edition*. In: *Developing Trends Facing the Transportation Profession*, S. 12–13
- [95] *Microtraffic | Road Safety Video Analytics*. URL <https://www.microtraffic.com/>. – Aktualisierungsdatum: 2022-05-07 – Überprüfungsdatum 2022-05-07
- [96] REKOR SYSTEMS: *Roadway Monitoring and Response : Strengthen roadway monitoring and enable rapid incident response*. URL <https://www.rekor.ai/applications/roadway-monitoring-and-response> – Überprüfungsdatum 2022-04-24
- [97] STEINBERGS, Raitis: *Improving Traffic Safety with Waze User Reports – Official Site of the International Road Federation*. URL <https://www.irf.global/improving-traffic-safety-with-waze-user-reports-2/>. – Aktualisierungsdatum: 2021-07-09 – Überprüfungsdatum 2022-05-28

- [98] STEINBERGS, Raitis ; KLAGIS, Maris: *Improving Traffic Safety By Using Waze User Reports*. In: *IOP Conference Series: Materials Science and Engineering* 1202 (2021), Nr. 1, S. 12031
- [99] GOOGLE: *Using Google Cloud to Store and Analyze Waze for Cities Data - Waze Partners Help*. URL <https://support.google.com/waze/partners/answer/10715739?hl=en>. – Aktualisierungsdatum: 2022-05-28 – Überprüfungsdatum 2022-05-28
- [100] HAAS ALERT: *Waze and Safety Cloud® are Keeping Streets Safer, One Alert at a Time*. URL <https://www.haasalert.com/news/waze-alerts-keeping-streets-safe>. – Aktualisierungsdatum: 2022-03-08 – Überprüfungsdatum 2022-05-28
- [101] WAZE MAPS: *Waze macht die Straßen sicher*. URL <https://www.waze.com/de/wazeforcities/casestudies/keeping-streets-safer-one-alert-at-a-time> – Überprüfungsdatum 2022-05-29
- [102] TOMTOM: *AmiGO von TomTom*. URL https://www.tomtom.com/de_de/drive/amigo/. – Aktualisierungsdatum: 2021-04-07 – Überprüfungsdatum 2022-08-07
- [103] SWARCO: *Cloud Solutions : SLA SWARCO Cloud Services*. URL https://www.swarco.com/sites/default/files/public/2019-12/Swarco_SLA_Cloud_Solutions_V2.1_ENG.pdf
- [104] LOGAN, David B. ; YOUNG, Kristie ; ALLEN, Trevor ; HORBERRY, Tim: *Safety Benefits of Cooperative ITS and Automated Driving in Australia and New Zealand*
- [105] INNAMAA, Satu ; KOSKINEN, Sami ; KAUVO, Kimmo: *Evaluation Outcome Report Finland : NordicWay*. Version 1.0
- [106] MALONE, Kerry ; RECH, Joerg ; HOGEMA, Jeroen ; INNAMAA, Satu ; HAUSBERGER, Stefan ; DIPPOLD, Martin ; VAN NOORT, Martijn ; DE FEIJTER, Erica ; RÄMÄ, Pirkko ; AITTONIEMI, Elina ; BENZ, Thomas ; BURCKERT, Axel ; ENIGK, Holger ; GIOSAN, Ion ; GOTSCHOL, Catrin ; GUSTAFSSON, Dan ; HEINIG, Ines ; KATSAROS, Konstantinos ; NEEF, David ; OJEDA, Luciano ; SCHINDHELM, Roland ; SÜTTERLIN, Christin ; VISINTAINER, Filippo: *DRIVE C2X Deliverable D11.4 : Impact Assessment and User Perception of Cooperative Systems*
- [107] KULMALA, Risto ; LEVIÄKANGAS, Pekka ; SIHVOLA, Niina ; RÄMÄ, Pirkko ; FRANCIS, Jonathan ; HARDMAN, Ewan ; BALL, Simon ; SMITH, Bob ; MCCRAE, Ian ; BARLOW, Tim ; STEVENS, Alan: *Final study report : CODIA Deliverable 5*
- [108] MEYER, Helmuth: *Geisterfahrer: Tipps für den Ernstfall*. URL <https://www.adac.de/verkehr/verkehrssicherheit/gefahrensituation/geisterfahrer/>. – Aktualisierungsdatum: 2019-12-19 – Überprüfungsdatum 2022-05-25
- [109] DEUTSCHE BAHN AG: *Schranken schließen nicht ohne Grund! : Unfälle durch richtiges Verhalten vermeiden*. URL https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjXiLn63fr3AhUI_7sIHRdPBIAQFnoECDkQAQ&url=https%3A%2F%2Fwww.deutschebahn.com%2Fresource%2Fblob%2F1173482%2Fdcfd07a490ff6a1d2c8ea26b49278b8b%2Funfaelle_bahnueb-data.pdf&usg=AOvVaw29JGnm4d1Dru_oi-Odirmu – Überprüfungsdatum 2022-05-25
- [110] LENI SIREGAR, Martha ; AGAH, Heddy R. ; HIDAYATULLAH, Fauzi: *Near-miss accident analysis for traffic safety improvement at a 'channelized' junction with U-turn*. In: *International Journal of Safety and Security Engineering* 8 (2018), Nr. 1, S. 31–38. URL <https://www.witpress.com/elibrary/sse-volumes/8/1/2104>
- [111] REKOR SYSTEMS: *Transportation Departments - Rekor Systems*. URL <https://www.rekor.ai/industries/transportation>. – Aktualisierungsdatum: 2022-05-22 – Überprüfungsdatum 2022-05-22

- [112] WAZE MOBILE: *Einsatz von Crowdsourcing-Daten zum Verhindern von Unfällen und Verbessern der Reaktionszeiten*. URL <https://www.waze.com/de/wazeforcities/casestudies/using-data-to-prevent-crashes>. – Aktualisierungsdatum: 2022-05-29 – Überprüfungsdatum 2022-05-29
- [113] BAUER, Manuel: *Android Auto und AppleCar Play: Waze-App macht Probleme*. URL <https://www.computerbild.de/artikel/cb-News-Connected-Car-Android-Auto-Apple-CarPlay-Waze-App-Probleme-33292653.html>. – Aktualisierungsdatum: 2022-08-08 – Überprüfungsdatum 2022-09-25
- [114] PETERANDERL, Sonja: *Polizisten fühlen sich durch die Navi-App Waze bedroht*. URL <https://www.gq-magazin.de/auto-technik/article/die-navi-app-waze-kann-auch-als-polizei-tracker-genutzt-werden>. – Aktualisierungsdatum: 2015-01-28 – Überprüfungsdatum 2022-09-25
- [115] HOBERG, Fabian: *Blitzer-Warner: So illegal sind Apps und Störgeräte fürs Auto - WELT*. URL <https://www.welt.de/wirtschaft/webwelt/article225636317/Blitzer-Warner-So-illegal-sind-Apps-und-Stoergeraete-fuers-Auto.html>. – Aktualisierungsdatum: 2021-02-04 – Überprüfungsdatum 2022-09-25
- [116] CAREY, Christopher: *Transport for London and Waze team up on safety alert system - Cities Today*. URL <https://cities-today.com/transport-for-london-and-waze-team-up-on-safety-alert-system/>. – Aktualisierungsdatum: 2021-05-27 – Überprüfungsdatum 2022-05-29
- [117] NAUJOKS, Frederik ; TOTZKE, Ingo: *Verhaltensanpassungen bedingt durch vorausschauende Warnsysteme am Beispiel von Stauende-Warnungen*, 2013
- [118] THE ASSOCIATED PRESS: *West Virginia Parkways Authority hit by cyberattack*. In: *Associated Press* (2021-11-12)
- [119] KONDRUSS, Bert: *Cyberangriffe auf Verkehr, Transport und Logistik im 2. Halbjahr 2021: Statistik*. In: *KonBriefing.com* (2022-03-30)
- [120] DATA FOR ROAD SAFETY: *Privacy Statement- Data for Road Safety*. – Aktualisierungsdatum: 06.07.21 – Überprüfungsdatum 2022-06-05
- [121] EUROPÄISCHES PARLAMENT: *DELEGIERTE VERORDNUNG (EU) Nr. 886/2013 DER KOMMISSION zur Ergänzung der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates in Bezug auf Daten und Verfahren für die möglichst unentgeltliche Bereitstellung eines Mindestniveaus allgemeiner für die Straßenverkehrssicherheit relevanter Verkehrsdaten für die Nutzer* (in Kraft getr. am 15. 5. 2013) (2013-05-15). URL <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32013R0886>
- [122] WAZE MOBILE: *Privacy Policy of Waze, the GPS Navigation App*. URL <https://www.waze.com/de/legal/privacy>. – Aktualisierungsdatum: 2022-06-06 – Überprüfungsdatum 2022-06-06
- [123] CAR 2 CAR COMMUNICATION CONSORTIUM: *C-ITS FAQs*. URL <https://www.car-2-car.org/about-c-its/c-its-faqs/>. – Aktualisierungsdatum: 2022-05-27 – Überprüfungsdatum 2022-05-27
- [124] RACHAEL REVESZ, Gregor Honsel: *Ampeln in London: Grüne Welle für Fußgänger*. URL <https://www.heise.de/hintergrund/Ampeln-in-London-Grueene-Welle-fuer-Fussgaenger-7178305.html>. – Aktualisierungsdatum: 2022-07-14 – Überprüfungsdatum 2022-08-27

- [125] ENQT | INNOVATIVE MESSTECHNIK & KOMPETENTE BERATUNG: *LTE vs. 5G (Teil 2): Latenzzeiten – ENQT | Innovative Messtechnik & kompetente Beratung*. URL <https://enqt.de/2020/10/latenzzeiten5g/>. – Aktualisierungsdatum: 2022-08-13 – Überprüfungsdatum 2022-08-13
- [126] ELEKTRONIK-KOMPENDIUM.DE: *IEEE 802.11p / pWLAN / ITS-G5 (Car2Car)*. URL <https://www.elektronik-kompodium.de/sites/net/2407231.htm>. – Aktualisierungsdatum: 2022-08-13 – Überprüfungsdatum 2022-08-13
- [127] WESTPHAL, Ann-Christin: *#schongewusst: Davon ist die Reaktionszeit abhängig - Universum Bremen*. URL <https://universum-bremen.de/schongewusst-davon-ist-die-reaktionszeit-abhaengig/>. – Aktualisierungsdatum: 2022-05-13 – Überprüfungsdatum 2022-08-13
- [128] KESTNER, Peter: *Cyber-Security: Wenn Hacker Betriebssysteme von Autos knacken*. URL <https://klardenker.kpmg.de/cyber-security-wenn-hacker-betriebssysteme-von-autos-knacken/>. – Aktualisierungsdatum: 2020-09-17 – Überprüfungsdatum 2022-08-28
- [129] FISCHER, Hans-Peter ; DR. MINZLAFF, Moritz: Digitaler Wandel der Autobranche : Cybersicherheit als Erfolgsfaktor, Eine Sonderveröffentlichung von Euroforum Deutschland November 2019. In: *Handelsblatt Journal, Cyb3r\$EcUrity & Dat3n\$(huTz*, S. 22–23
- [130] WUHRMANN, Daniel ; DEEG, Thorsten ; HESSEL, Stefan: *Neue Cybersicherheits- und Softwareupdatestandards in der Automobilbranche*. URL <https://www.reuschlaw.de/news/neue-cybersicherheits-und-softwareupdatestandards-in-der-automobilbranche/>. – Aktualisierungsdatum: 2021 – Überprüfungsdatum 2022-08-28
- [131] UCKROW, Klaus: *Ist die verpflichtende Verkehrszeichenerkennung sinnvoll?* URL <https://www.autozeitung.de/verkehrszeichenerkennung-kommentar-201461.html>. – Aktualisierungsdatum: 2022-03-25 – Überprüfungsdatum 2022-08-14

Anhang

A Berechnungen

A.1 Austroads Studie

Gesamtsumme betrachteter Unfälle in Studie: 72

Formel: *Globale Unfallvermeidungswahrscheinlichkeit* = $\frac{\text{Relevante betrachtete Unfälle}}{\text{Gesamtsumme betrachteter Unfälle}} * \text{Unfallvermeidungswahrscheinlichkeit}$

Anwendung	Relevante betrachtete Unfälle	Unfallvermeidungswahrscheinlichkeit	Globale Unfallvermeidungswahrscheinlichkeit
Cooperative Forward Collision Warning (mit menschlicher Intervention)	15	34%	7%
Cooperative Forward Collision Warning (mit automatisierter Intervention)	15	56%	12%
Curve Speed Warning	20	24%	7%
Intersection Movement Assist (mit menschlicher Intervention)	10	42%	6%
Intersection Movement Assist (mit automatisierter Intervention)	10	71%	10%
Right Turn Assist (mit menschlicher Intervention)	13	34%	6%
Right Turn Assist (mit automatisierter Intervention)	13	69%	12%
Cooperative Forward Collision Warning (mit menschlicher Intervention)	15	34%	7%

A.2 NordicWay 1

Formel:

$$\bar{d} = \frac{\frac{c_{max}}{b_{max} * a_{max}} + \frac{c_{min}}{b_{min} * a_{min}}}{2}$$

Anwendung	In der Studie angenommene Warnungsabde- ckung Minimum (a_{min})	In der Studie angenommene Warnungsabde- ckung Maximum (a_{max})	In der Studie angenommene Fahrzeugaus- stattungsquote Minimum (b_{min})	In der Studie angenommene Fahrzeugaus- stattungsquote Maximum (b_{max})	Unfallreduzie- rung laut Studie Minimum (c_{min})	Unfallreduzie- rung laut Studie Maximum (c_{max})
Unfall	70%	90%	31%	65%	0,02%	0,08%
Tiere & Menschen	40%	70%	31%	65%	0,30%	1,68%
Hindernis	50%	80%	31%	65%	0,02%	0,09%
Baustelle	95%	100%	31%	65%	0,13%	0,58%
Glätte	30%	70%	31%	65%	0,29%	2,12%
Schlechte Sichtverhält- nisse	40%	80%	31%	65%	0,01%	0,05%
Außergewöhnliche Wetterverhältnisse	60%	90%	31%	65%	0,11%	0,58%

Anwendung	Zielwert War- nungsabdeckung	Zielwert Fahrzeug- ausstattungsquote	Unfallreduzierung unter Berücksichti- gung von Zielwer- ten Minimum (d_{min})	Unfallreduzierung unter Berücksichti- gung von Zielwer- ten Maximum (d_{max})	Unfallreduzierung unter Berücksichti- gung von Zielwer- ten Durchschnitt (\bar{d})
Unfall	100%	100%	0,09%	0,14%	0,11%
Tiere & Menschen	100%	100%	2,42%	3,69%	3,06%
Hindernis	100%	100%	0,13%	0,17%	0,15%
Baustelle	100%	100%	0,44%	0,89%	0,67%
Glätte	100%	100%	3,12%	4,66%	3,89%
Schlechte Sichtverhältnisse	100%	100%	0,08%	0,10%	0,09%
Außergewöhnliche Wetter- verhältnisse	100%	100%	0,59%	0,99%	0,79%